PROCEDURA DI VALUTAZIONE DI IMPATTO

Treviso, lì 13 maggio 2025

Nome del DPO/RPD
Giuseppe Croari, DPO di Opi Treviso

Parere del DPO/RPD

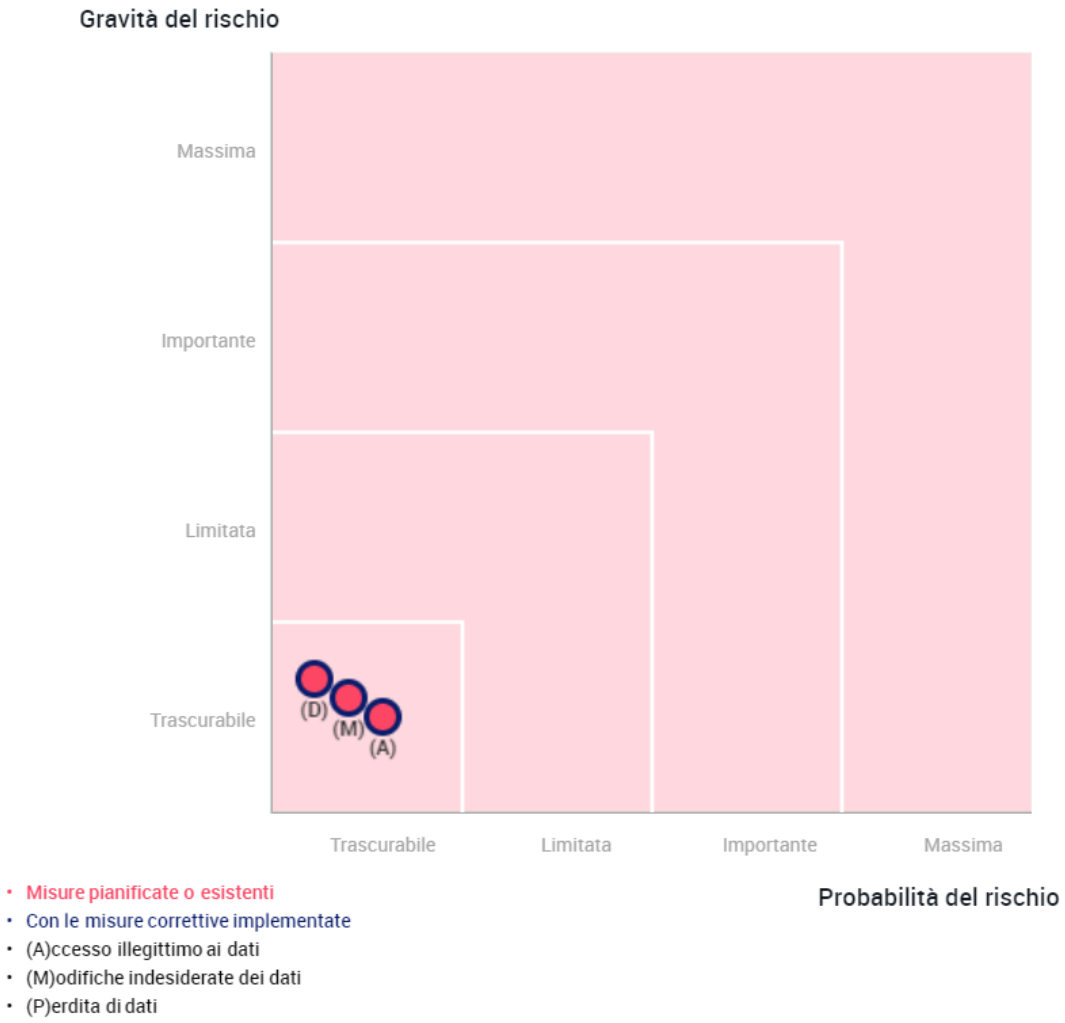
Le modalità e le misure pianificate per la gestione dei trattamenti nell'ambito delle procedure di whistleblowing previste dal d.lgs. 24/2023 appaiono allo stato idonee a garantire un livello di protezione adeguata dei dati e dei diritti degli interessati. Sarà necessario verificare la necessità di ripetere la DPIA in caso di future variazioni della procedura.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Stante la disciplina normativa che regola ed impone l'adozione della procedura in oggetto, non si è posta la necessità di richiedere pareri agli interessati.



CONTESTO

Questa sezione permette una visione complessiva del trattamento o dei trattamenti di dati personali in questione.

DATI, PROCESSI E RISORSE DI SUPPORTO

Questa sezione permette di definire e descrivere nei dettagli il trattamento in oggetto.

1. Quale è il trattamento in considerazione?

Il trattamento di dati personali è relativo all'attivazione del canale di segnalazione interno a Opi Treviso come previsto dal d.lgs 24/2023 recante la disciplina in materia di whistleblowing.

La finalità del canale è consentire ai soggetti legittimati dalla normativa – i segnalanti- di presentare segnalazioni scritte o orali concernenti violazioni appartenenti alle tipologie specificamente individuate dalla disciplina, apprese all'interno del contesto lavorativo.

Il canale interno in forma scritta può essere attivato presentando una segnalazione digitalmente; a tal proposito la società si avvale del software Globaleaks Whistleblowing fornita dalla società Whistleblowing Solutions I.S. S.r.l. al fine di gestire la procedura e l'oggetto della segnalazione stessa.

Per l'utilizzo della modalità orale, il segnalante può contattare il gestore del canale tramite una linea telefonica dedicata.

Inoltre, il segnalante può chiedere un incontro diretto ai soggetti deputati alla gestione della segnalazione, che verrà svolto entro un termine ragionevole in un luogo adatto a garantire la riservatezza del segnalante.

Dell'incontro, verrà stilato un verbale, che previa verifica del contenuto sarà sottoscritto anche dalla persona segnalante, oltre che dal soggetto che ha ricevuto la dichiarazione. Copia del verbale dovrà essere consegnata al segnalante.

I dati oggetto della segnalazione saranno trattati per gestire la segnalazione, per darvi seguito e per adottare le misure di protezione previste dalla normativa vigente. Il trattamento potrebbe riguardare informazioni di particolare delicatezza (es: dati particolari, giudiziari) e sarà effettuato dai soggetti deputati alla gestione del canale di segnalazione, anche eventualmente con la collaborazione di terzi. Infatti, il responsabile della gestione del canale di segnalazione, di cui oltre, al fine di espletare l'attività istruttoria volta all'accertamento delle violazioni potrebbe avere necessità di coinvolgere altre strutture aziendali, specialisti o professionisti esterni. In ogni caso saranno adottate adeguate misure per garantire la riservatezza del trattamento.

In ultima istanza i dati pervenuti attraverso il canale di segnalazione potranno essere trasmessi anche all'autorità giudiziaria, contabile o amministrativa, qualora dall'istruttoria emerga la fondatezza della segnalazione.

Il Titolare del trattamento è Opi Treviso.

Sono responsabili del trattamento la società Whistleblowing Solutions I.S. S.r.l.fornitrice del software Globaleaks Whistleblowing, nonché eventuali terzi coinvolti nella fase istruttoria al fine di gestire le segnalazioni.

Sono subreponsabili del trattamento Transparency International Italia In relazione all'accordo per il supporto alla gestione delle piattaforme di whistleblowing, nonché Seeweb S.r.l. per la fornitura dei prodotti Foundation Server PRO (fs20585, fs20687, Cloud Data Protection (cdp000132), Appliance VPN OPNsense (vm9619).
È autorizzato al trattamento il Responsabile per la prevenzione della corruzione e trasparenza in quanto soggetto deputato alla gestione delle segnalazioni.

2. Quali sono le responsabilità connesse al trattamento?
Come detto, il titolare del trattamento è Opi Treviso. Quest'ultimo è responsabile della corretta gestione e conservazione dei dati personali raccolti a fronte dell'istituzione del canale interno, nonché della tutela della sicurezza e riservatezza dei dati del segnalante, della protezione del medesimo da trattamenti non autorizzati, illeciti, della perdita e della distruzione o del danno accidentale.
I responsabili del trattamento sono la società Whistleblowing Solutions I.S. S.r.l. fornitrice del software Globaleaks Whistleblowing, nonché eventuali terzi coinvolti nella fase istruttoria al fine di gestire le segnalazioni. I soggetti in questione vengono designati tenendo conto delle conoscenze specialistiche, affidabilità, risorse e per l'adozione di misure tecniche ed organizzative atte a garantire la protezione dei dati.
Sono subreponsabili del trattamento Transparency International Italia In relazione all'accordo per il supporto alla gestione delle piattaforme di whistleblowing, nonché Seeweb S.r.l. per la fornitura dei prodotti Foundation Server PRO (fs20585, fs20687, Cloud Data Protection (cdp000132), Appliance VPN OPNsense (vm9619).
Il gestore del canale di segnalazione interno è la Dott.ssa Danusca Gorza, Responsabile della prevenzione della corruzione e della trasparenza dell'Ente, che tratta i dati in qualità di soggetto autorizzato al trattamento e soltanto su espressa autorizzazione del Titolare ed ha ricevuto adeguata formazione in privacy.

3. Ci sono standard applicabili al trattamento?
Si applicano le previsioni di cui al d.lgs. 24/2023, con particolare riferimento all'art. 13 del decreto.
Il fornitore della piattaforma, Whistleblowing Solutions I.S., applica i seguenti standard:
- ISO/IEC 27001:2022
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- ISO 9001:2015
- CSA STAR Level 1
- ACN

Valutazione: Accettabile

Commento di valutazione: Il trattamento è eseguito in esecuzione e secondo la disciplina normativa di cui al d.lgs. 24/2023.

4. Quali sono i dati trattati?

Vengono trattate le seguenti tipologie di dati personali:

- dati comuni della persona segnalante, tra cui, nome, cognome, telefono, e-mail, inquadramento, ruolo, qualifica;
- dati della persona segnalante forniti per descrivere i fatti oggetto della segnalazione;
- dati della persona coinvolta o di soggetti terzi che la persona segnalante ha inteso fornire per rappresentare i fatti descritti nella segnalazione;
- dati di soggetti terzi a vario titolo coinvolti nella procedura di segnalazione e che beneficiano della tutela apprestata dalla normativa, quali, ad esempio, il facilitatore.

I dati personali raccolti potrebbero essere particolari o consistere in dati giudiziari.

I dati personali trattati sono conservati per un periodo di cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

I dati personali anzidetti saranno comunicati ai soggetti deputati alla gestione della segnalazione e agli eventuali ulteriori soggetti che saranno individuati al solo fine di gestire (es. fornitore di servizi informatici, consulente legale, etc.) e di dar seguito alla segnalazione (es. datore di lavoro, autorità giudiziaria, autorità amministrativa, etc.), in ogni caso nel rispetto delle previsioni del D. Lgs. 24/2023.

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

I dati personali vengono raccolti con le modalità indicate di seguito.

Per la modalità scritta, attraverso il software Globaleaks Whistleblowing secondo la procedura anzidetta.

Per la modalità orale, per via telefonica oppure mediante registrazione, previo consenso dell'utente, di messaggi vocali di segreteria oppure, in caso di incontro di persona o di mancanza del consenso alla registrazione, mediante redazione di un verbale del colloquio.

Successivamente, i dati personali così raccolti vengono conservati nei seguenti archivi: i dati della piattaforma Globaleaks Whistleblowing sono conservati su server localizzati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea. Non esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE. Gli eventuali documenti cartacei saranno conservati in un archivio chiuso a chiave con accesso riservato al solo gestore delle segnalazioni o al custode dell'identità del segnalante.

Soltanto i soggetti deputati alla gestione del canale interno hanno accesso a tali dati e potranno comunicarli al datore di lavoro o all'Autorità competente non appena l'attività istruttoria condotta, volta ad accertare gli illeciti eventualmente commessi dall'ente, sarà giunta a termine e faccia emergere la fondatezza della segnalazione.

I dati non necessari ai fini dell'accertamento di una specifica segnalazione verranno immediatamente cancellati.
Se dallo svolgimento dell'attività istruttoria emerge l'infondatezza della segnalazione i dati del segnalante dovranno essere archiviati immediatamente.
Trascorsi 5 anni a decorrere dalla data di comunicazione dell'esito finale della procedura di segnalazione i dati verranno cancellati.

6. Quali sono le risorse di supporto ai dati?

- Per le segnalazioni scritte: software Globaleaks Whistleblowing;
- Per le segnalazioni orali: linea telefonica dedicata;
- Per le segnalazioni tramite colloquio orale: strumenti di lavoro per la verbalizzazione degli incontri, archivi cartacei
- Server aziendali
- Le risorse su cui si basano i trattamenti dei dati personali. Nota: possono comprendere hardware, software, reti, persone, supporti cartacei o documentazione

Valutazione: Accettabile
Commento di valutazione: misure rispettose della disciplina normativa vigente e adeguate a garantire il rispetto dei principi di riservatezza e di minimizzazione dei dati e dei trattamenti.

PRINCIPI FONDAMENTALI

Questa sezione permette di generare lo schema di adeguamento secondo i principi di protezione dei dati personali.

PROPORZIONALITÀ E NECESSITÀ

Questa sezione permette di dimostrare l'implementazione degli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

7. Gli scopi del trattamento sono specifici, espliciti e legittimi?

Sì: l'Ente raccoglie e tratta i dati personali degli interessati soltanto laddove necessari per adempiere a quanto imposto dal d.lgs 24/2023. Gli scopi, quindi, sono quelli previsti ex lege e di seguito riepilogati:

- consentire ai dipendenti e agli altri soggetti legittimati di presentare una segnalazione di violazioni di norme di legge,
- gestire e dare seguito alla segnalazione espletando le relative indagini e verifiche,
- applicare al segnalante e agli altri beneficiari le misure di protezione,
- procedere con gli eventuali provvedimenti verso il segnalato.

Valutazione: Accettabile

Commento di valutazione: le finalità coincidono con quelle previste dalla vigente normativa in materia (d. lgs. 24/2023)

8. Quali sono le basi legali che rendono lecito il trattamento?

Le basi giuridiche che legittimano il trattamento dei dati sono:

- l'adempimento di un obbligo legale a cui è soggetto il Titolare del trattamento: art. 6, co. 1, lett. c, e art. 9, co. 1, lett. b, GDPR.
- l'interesse legittimo del titolare prevalente: art. 6, co. 1, lett. f, e art. 9, co. 1, lett. f, GDPR fermo restando che l'interesse legittimo quale base giuridica è lecito nei casi in cui il trattamento sia necessario per la tutela, anche in sede stragiudiziale (es. procedure disciplinari), di diritti del titolare.

Valutazione: Accettabile

Commento di valutazione: fermo restando che l'interesse legittimo quale base giuridica è lecito nei casi in cui il trattamento sia necessario per la tutela, anche in sede stragiudiziali (es. procedure disciplinari), di diritti del titolare.

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

Sì: tutti i dati manifestatamente non utili alla trattazione di una specifica segnalazione devono essere immediatamente cancellati, così come i dati raccolti accidentalmente se non necessari. In aggiunta, nell'eventualità che i soggetti di cui sopra procedano a trasferire i dati a soggetti terzi sempre ai fini dell'accertamento della violazione di norme di legge o europee, i dati non necessari a tal fine saranno oscurati.

Valutazione: Accettabile
Commento di valutazione: la minimizzazione dei dati è parte delle istruzioni fondamentali per il trattamento dei dati

10. I dati sono esatti e aggiornati?
I dati trattati saranno esatti ed aggiornati in quanto forniti direttamente dalla persona del segnalante. Inoltre, il Titolare provvederà a condurre un'istruttoria per accertare i fatti oggetto della segnalazione e provvederà immediatamente a rettificare qualsiasi inesattezza o incompletezza riguardante i dati personali.

Valutazione: Accettabile
Commento di valutazione: le procedure permettono di garantire l'aggiornamento dei dati

11. Qual è il periodo di conservazione dei dati?
I dati trattati saranno conservati per il tempo necessario al raggiungimento delle finalità anzidette e, comunque, non oltre 5 anni dalla comunicazione dell'esito finale della procedura, così come previsto dall'art. 14 del d.lgs 24/2023.

Valutazione: Accettabile
Commento di valutazione: periodo di conservazione previsto ex lege

12. Come sono informati del trattamento gli interessati?
Informativa ai sensi dell'art. 13 del GDPR messa a disposizione tramite il sito web dell'organizzazione, sulla piattaforma online per la segnalazione e mediante affissione all'interno delle bacheche aziendali.

Valutazione: Accettabile
Commento di valutazione: misure adeguate secondo la vigente normativa.

13. Ove applicabile: come si ottiene il consenso degli interessati?
Il trattamento dati in questione non necessita di alcun preventivo consenso dell'interessato poiché si fonda sulle basi giuridiche di cui agli artt: 6, co. 1, lett. c e lett. f; 9, co. 1, lett. b e lett. f, GDPR

Valutazione: Accettabile
Commento di valutazione: N/A

14. Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?
L'esercizio dei diritti viene garantito tramite il DPO e/o tramite il gestore delle segnalazioni. Al fine di tutelare il soggetto segnalante, alla persona coinvolta o menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, è limitato l'esercizio – per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata - dei diritti previsti dal GDPR.

Valutazione: Accettabile
Commento di valutazione: misure adeguate per garantire la corretta applicazione sia della normativa in materia di protezione dei dati personali che in materia di whistleblowing

15. Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?
L'esercizio dei diritti viene garantito tramite il DPO e/o tramite il gestore delle segnalazioni. Al fine di tutelare il soggetto segnalante, alla persona coinvolta o menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, è limitato l'esercizio – per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata - dei diritti previsti dal GDPR.

Valutazione: Accettabile
Commento di valutazione: vedi commento precedente

16. Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?
L'esercizio dei diritti viene garantito tramite il DPO e/o tramite il gestore delle segnalazioni. Al fine di tutelare il soggetto segnalante, alla persona coinvolta o menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, è limitato l'esercizio – per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata - dei diritti previsti dal GDPR.

Valutazione: Accettabile
Commento di valutazione: vedi commento precedente

17. Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?
Il Titolare Opi Treviso ha provveduto a stipulare un apposito contratto di nomina a responsabile del trattamento con la società Whistleblowing Solutions I.S. S.r.l. che mette a disposizione il software Globaleaks Whistleblowing . Nello specifico attraverso tale contratto sono esplicitati le tipologie di

dati personali che possono essere trattati al fine di erogare i servizi concordati con il titolare, le tipologie di operazioni che quest'ultimo può compiere su tali dati personali, gli obblighi che deve assumersi, le misure di sicurezza che deve predisporre per garantire la sicurezza, l'integrità e la riservatezza e la completezza dei dati personali.

Valutazione: Accettabile
Commento di valutazione: vedi commento precedente

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

Non sono previsti trasferimenti extra UE.

Valutazione: Accettabile
Commento di valutazione: vedi commento precedente

RISCHI

Questa sezione permette di valutare i rischi per la riservatezza, alla luce delle misure esistenti o pianificate.

19. MISURE ESISTENTI O PIANIFICATE

Questa sezione permette di indicare le misure (esistenti o pianificate) che contribuiscono alla sicurezza dei dati:

a) **Crittografia**: L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington. Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.
   Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni.
   Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.
   Valutazione: Accettabile

b) **Anonimizzazione**: 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

c) **Controllo degli accessi logici:**
   L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.
   Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.
   Valutazione: Accettabile

d) **Tracciabilità**: L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.
   Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse. I log delle attività del segnalante sono privi delle informazioni identificative dei

segnalanti quali indirizzi IP e User Agent. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.
Valutazione: Accettabile

e) **Archiviazione**: L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.
Valutazione: Accettabile

f) **Sicurezza dei documenti cartacei**: documenti conservati in un archivio chiuso a chiave con accesso riservato al solo gestore delle segnalazioni o al custode dell'identità del segnalante.
Valutazione: Accettabile

g) **Minimizzazione dei dati**: è prevista l'eliminazione o l'oscuramento dei dati non necessari.
Valutazione: Accettabile

h) **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 che vengono forniti al progetto privatamente.
Audit di sicurezza:https://docs.globaleaks.org/en/stable/security/PenetrationTests.html#security-audits
Valutazione: Accettabile

i) **Lotta contro il malware:** Tutti i computer del personale del fornitore del software individuato e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware.
Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

Valutazione: Accettabile

j) **Gestione postazioni**: accesso consentito solo ai soggetti deputati alla gestione delle segnalazioni.
Valutazione: Accettabile

k) **Backup**: Il back-up avviene almeno con frequenza di 8 ore ed è eseguito da remoto. Le copie di back up vengono conservate per 7 giorni necessari per finalità di disaster recovery garantendo un RPO di 8 ore.
Valutazione: Accettabile

l) **Manutenzione:** È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza.
Valutazione: Accettabile

m) **Contratto con il responsabile del trattamento**: è stato sottoscritto idoneo contratto di nomina a responsabile del trattamento con il fornitore della piattaforma Globaleaks. Il coinvolgimento di eventuali soggetti terzi avverrà previa nomina ai sensi dell'art. 28 GDPR.
Valutazione: Accettabile

n) **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

o) **Controllo degli accessi fisici:** gli accessi fisici avvengono con modalità tali da garantire un adeguato livello di sicurezza conformemente agli standard applicati.
Valutazione: Accettabile

p) **Politica di tutela della privacy**: adozione dei principi di privacy by design e by default nell'organizzazione di ogni attività correlata alla procedura.
Valutazione: Accettabile

q) **Gestione delle politiche di tutela della privacy**: istruzioni fornire dal titolare e condivise con il responsabile, soggette a periodica verifica di adeguatezza.
Valutazione: Accettabile

r) **Integrare la protezione della privacy nei progetti:** eventuali variazioni nella procedura saranno previamente valutate ai fini del rispetto della normativa in materia di protezione dei dati personali.
Valutazione: Accettabile

s) **Gestire gli incidenti di sicurezza e le violazioni dei dati personali:** I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24.
I datacenter del fornitore IaaS sono certificati ISO27001.
Valutazione: Accettabile

t) **Vigilanza sulla protezione dei dati:** la riservatezza dei dati e l'adeguatezza delle misure di protezione saranno valutate periodicamente.
Valutazione: Accettabile

ACCESSO ILLEGITTIMO AI DATI

Analizzare le cause e le conseguenze di accesso illegittimo ai dati, stimandone la gravità e la probabilità,

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

Identificazione del segnalante, della persona coinvolta e degli altri soggetti di cui viene garantita la riservatezza, ritorsioni da parte del datore di lavoro e/o colleghi, interferenza con l'istruttoria, trasmissione di particolari categorie di dati personali a soggetti non autorizzati,

21. Quali sono le principali minacce che potrebbero concretizzare il rischio?
Accesso illecito ai dati, perdita di dati.

22. Quali sono le fonti di rischio?
Soggetti terzi malintenzionati che accedano illecitamente ai dati, incendio o allagamenti che determinino la distruzione dei documenti.

23. Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Il Titolare adotta le seguenti misure di sicurezza volte a limitare il rischio di accesso illegittimo ai dati: crittografia, anonimizzazione, controllo degli accessi logici, tracciabilità, archiviazione, sicurezza dei documenti cartacei, minimizzazione dei dati, vulnerabilità, lotta contro il malware, gestione postazioni, sicurezza dei canali informatici, controllo degli accessi fisici, politica di tutela della privacy, gestione delle politiche di tutela della privacy, integrazione della protezione della privacy nei progetti, vigilanza sulla protezione dei dati.

24. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Trascurabile, i rischi ipotizzabili riguardano ipotesi di accessi illeciti intenzionali e molto limitate.

25. Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Trascurabile, la probabilità che si verifichino i rischi ipotizzabili risultano molto basse, anche in relazione alle misure organizzative e di sicurezza adottate.

Valutazione: Accettabile.
Commento di valutazione: il concretizzarsi dei rischi e di eventuali danni per gli interessati risulta di minima probabilità.

MODIFICHE INDESIDERATE DEI DATI
Analizzare le cause e le conseguenze di modifiche indesiderate dei dati, e stimare la gravità e la probabilità dell'evento.

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

Interferenza con l'istruttoria, rischi di ripercussioni per i segnalanti, utilizzo improprio di dati personali che possono portare alla falsificazione della segnalazione o a fare in modo che l'accertamento non venga svolto correttamente.

27. Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?
Accesso illecito ai dati, perdita di dati, distruzione dei dati, alterazione o falsificazione dei dati.

28. Quali sono le fonti di rischio?
Fonti umane esterne, soggetti terzi malintenzionati che accedano illecitamente ai dati.

29. Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Il Titolare adotta le seguenti misure di sicurezza volte a limitare il rischio di modifiche indesiderate dei dati: crittografia, controllo degli accessi logici, tracciabilità, archiviazione, sicurezza dei documenti cartacei, vulnerabilità, lotta contro il malware, gestione postazioni, backup, manutenzione, sicurezza dei canali informatici, controllo degli accessi fisici, politica di tutela della privacy, integrazione della protezione della privacy nei progetti, gestione degli incidenti di sicurezza e le violazioni dei dati personali, vigilanza sulla protezione dei dati.

30. Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Trascurabile, l'impatto sugli interessanti potrebbe essere elevato, ma in considerazione delle misure e del contesto di riferimento il rischio è valutabile come trascurabile.

31. Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?
Trascurabile, le minacce alla riservatezza e all'integrità dei dati sono difficilmente concretizzabili e non appaiono rilevanti.

Valutazione: Accettabile.
Commento di valutazione: le misure adottate appaiono adeguate a contenere i rischi ipotizzabili.

PERDITA DI DATI
Analizzare le cause e le conseguenze di una perdita di dati stimandone la gravità e la probabilità.

32. Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Necessità di fornire nuovamente i dati, inutilizzabilità della segnalazione effettuata.

33. Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Distruzione dei dati, sottrazione dei dati, perdita di dati.

34. Quali sono le fonti di rischio?
Fonti umane esterne, soggetti terzi malintenzionati che accedano illecitamente ai dati, incendio o allagamenti che determinino la distruzione dei documenti.

35. Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Il Titolare adotta le seguenti misure di sicurezza volte a limitare il rischio di perdita dei dati: crittografia, anonimizzazione, controllo degli accessi logici, tracciabilità, archiviazione, sicurezza dei documenti cartacei, minimizzazione dei dati, vulnerabilità, lotta contro il malware, gestione postazioni, backup, manutenzione, contratto con il responsabile del trattamento, sicurezza dei canali informatici, controllo degli accessi fisici, politica di tutela della privacy, gestione delle politiche di tutela della privacy, integrazione della protezione della privacy nei progetti, gestione degli incidenti di sicurezza e le violazioni dei dati personali, vigilanza sulla protezione dei dati.

36. Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Trascurabile. Il rischio, anche ove concretizzato, sarebbe limitato, perché vi sarebbe per lo più la possibilità di recuperare – ricostruire i dati persi direttamente tramite il segnalante.

37. Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?
Trascurabile, la probabilità del rischio, come nei precedenti casi, si ritiene estremamente ridotta.

Valutazione: Accettabile.
Commento di valutazione: le misure adottate appaiono idonee a contenere e prevenire i rischi ipotizzabili e ragionevolmente prevedibili.