Data Privacy Impact Assessment (DPIA)

Whistleblowing

CONSORZIO 1 TOSCANA NORD

01	01	22.10.2024	Prima Emissione	Certim srl	Titolare
Edizione	**Revisione**	**Data**	**Descrizione**	**Redatto**	**Approvato**

SOMMARIO

1. Premessa

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), la DPIA corrisponde alla valutazione d'impatto del trattamento del dato sulla protezione dei dati personali, qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ciò considerata la natura, il contesto e le finalità del trattamento.

Il GDPR introduce dunque una valutazione di stampo preliminare, che consente al Titolare del trattamento di prendere visione del rischio prima ancora di procedere al trattamento e di attivarsi perché tale rischio possa essere, se non annullato, quantomeno fortemente ridotto.

I principi fondamentali della DPIA risultano pertanto:

- i diritti e le libertà fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR;
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio.

Una DPIA poggia sui pilastri:

I. i principi e i diritti fondamentali, i quali sono "non negoziabili", stabiliti dalla legge e che devono essere rispettati e non possono essere soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi;

II. la gestione dei rischi per la privacy dei soggetti interessati, che determina i controlli tecnici e organizzativi opportuni a tutela dei dati personali.

La Metodologia di analisi dei rischi adottata nella conduzione delle attività di Data Privacy Impact Assessment è la metodologia di analisi CNIL del Garante Francese (o altra metodologia definita dal Titolare del trattamento).

2. Contesto

2.1. Abbreviazioni

- **RPD** Responsabile per la protezione dei dati personali
- **RTDP** Responsabile della tutela dei dati personali e della riservatezza dei dati aziendali

2.2. Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi del D.lgs. n. 24/2023.

La gestione delle segnalazioni viene effettuata attraverso canale esterno (piattaforma adottato dalla Società, di cui vengono riportate le principali caratteristiche.

Infrastruttura e Sicurezza del sistema per il Whistleblowing come dichiarato da WHISTLEBLOWINGIT	
Le principali caratteristiche del software per la segnalazione degli illeciti	Whistleblowing Solutions, in qualità di responsabile del trattamento, si occupa della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.
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 utilizzati 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.

2.3. Responsabilità connesse al trattamento

Ruoli	Nominativi
Titolare del trattamento	**CONSORZIO 1 TOSCANA NORD**
Responsabile Protezione Dati	**Certim srl**
Responsabile trattamento	**Whistleblowing Solutions** Il Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato: • ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019 • ISO 9001:2015 • CSA STAR Level 1 • ACN
Sub Responsabile	**Seeweb** Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS) **Transparency International Italia** Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing
Incaricati al trattamento	Gestore delle segnalazioni appositamente incaricato

2.4. Standard applicabili al trattamento

Al trattamento in materia di segnalazioni e normativa whistleblowing si applicano le seguenti normative e standard.

Riferimenti richiamati
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
Direttiva UE 1937/2019
D. Lgs. n. 24/2023
Parere su uno schema di decreto legislativo recante 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 (cd. direttiva whistleblowing) - 11 gennaio 2023 [9844945]
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. Procedure per la presentazione e gestione delle segnalazioni esterne. Approvate dall'Anac con Delibera n° 311 del 12 luglio 2023

2.5. Dati, processi e risorse di supporto

Di seguito si riportano le tipologie di dati personali che sono oggetto di trattamento a seguito di una segnalazione fatta ai sensi del D. Lgs. n. 24/2023

Categoria di dato personale	Categoria di interessati
Dati personali comuni e di contatto	➢ Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto ➢ Fornitori che effettuano una segnalazione o vengono segnalati
Dati personali particolari (es. dati relativi alla salute, dati relativi all'appartenenza sindacale)	➢ Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto ➢ Fornitori che effettuano una segnalazione o vengono segnalati
Dati giudiziari (es. condanne penali)	➢ Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto ➢ Fornitori che effettuano una segnalazione o vengono segnalati

Ciclo di vita del trattamento dei dati (descrizione funzionale)

1) Attivazione e configurazione della piattaforma
2) Utilizzo della piattaforma – invio delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei soggetti autorizzati

3) Dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.

2.6. Risorse a supporto dei dati

Piattaforma Web **WHISTLEBLOWINGIT**,
(www.whistleblowing.it)

3. Principi Fondamentali

Gli scopi del trattamento sono specifici, espliciti e legittimi?	Il trattamento è finalizzato esclusivamente alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing. Gestione delle segnalazioni previste nel decreto legislativo 10 marzo 2023, n. 24 (di seguito anche "Decreto"), pubblicato nella Gazzetta Ufficiale del 15 marzo 2023, è stata recepita nell'ordinamento italiano la direttiva UE 2019/1937 riguardante "*la protezione delle persone che segnalano violazioni del diritto dell'Unione*".
Quali sono le basi giuridiche che rendono lecito il trattamento?	Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui è tenuto il titolare (Art. 6.1. lett. c) GDPR). Ci possono essere trattamenti, con espresso consenso del segnalante (art. 6, par 1 lett. a)), nei seguenti casi: i. all'interno di un procedimento disciplinare, nel caso in cui siano necessari per lo svolgimento del procedimento; ii. per registrazione e/o trascrizione della segnalazione in presenza, telefonica o tramite messaggistica vocale; iii. rivelazione a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.
I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D.lgs. n. 24/2023. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (art. 5.1. lett. c) GDPR).
I dati sono esatti e aggiornati?	Il trattamento dei dati personali relativi alle segnalazioni sono costantemente aggiornati in quanto i soggetti incaricati di ricevere e gestire le segnalazioni ne verificano preliminarmente la corrispondenza a verità.

Qual è il periodo di conservazione dei dati?	Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e, se del caso, all'adozione dei provvedimenti disciplinari conseguenti e/o all'esaurirsi di eventuali contenziosi avviati a seguito della segnalazione. Il trattamento non si protrarrà oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione. I dati potranno essere successivamente anonimizzati per finalità statistiche o di storicizzazione

4.1 Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?	Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR. L'informativa viene resa disponibile secondo le seguenti modalità: - Processo comunicazione aziendale sull'esistenza del canale di segnalazione interno (canale informatico); - Pubblicazione sito internet – sezione dedicata al Whistleblowing
Ove applicabile: come si ottiene il consenso degli interessati?	Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (Art.6.1. lett. c) del GDPR). Nel caso invece ricorra l'ipotesi di comunicazione dei dati personali a soggetti diversi da quelli espressamente autorizzati dal Titolare, il segnalante dovrà prestare il suo consenso specifico alla segnalazione ai sensi degli, tramite piattaforma artt. 6.1. lett. a) e 7 del GDPR.
Come fanno gli interessati a esercitare i loro diritti previsti dagli artt. 15 ss. GDPR?	Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso l'indirizzo di posta elettronica dedicato nei limiti di cui all'articolo 2-undecies del Codice Privacy: - e-mail dedicata
Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del trattamento ai sensi dell'art. 28 GDPR, attraverso contratti o altri atti giuridici
In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?	Per questa tipologia di trattamento non è previsto un trasferimento di dati personali fuori dall'Unione Europea.

4. Misure esistenti

DESCRIZIONE DELLA PIATTAFORMA DI WHISTLEBLOWING

Whistleblowing Solutions, in qualità di responsabile del trattamento, si occupa della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.

DESCRIZIONE E ANALISI DEL CONTESTO

Responsabilità connesse al trattamento	**PA, Ente o Organizzazione** > Titolare del trattamento **Gestore delle segnalazioni** > Soggetto autorizzato dal Titolare del Trattamento a trattare i dati relativi alle segnalazioni **Whistleblowing Solutions** > Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing **Seeweb** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS) **Transparency International Italia** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing
Standard applicabili	Il contesto normativo di riferimento richiede conformità a: • D.Lgs. n. 24/2023 o altra normativa nazionale in caso di entità giuridiche con sede in altro Paese. • DIRETTIVA (UE) 2019/1937 (WHISTLEBLOWING) • GENERAL DATA PROTECTION REGULATION - 2016/679 (GDPR) Il servizio erogato adotta misure progettate in aderenza allo standard internazionale ISO37002:2021 in materia di gestione dei processi di whistleblowing. Il Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato: • ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019 • ISO 9001:2015 • CSA STAR Level 1 • ACN

VALUTAZIONI IN MERITO AI TRATTAMENTI
PRINCIPI FONDAMENTALI

Adeguatezza, pertinenza e limitazione a quanto è necessario in relazione alle finalità per le quali i dati sono trattati (minimizzazione)	Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI). Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia. 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. 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. Al fine di consentire la possibilità di segnalazioni orali e al contempo tutelare l'anonimato e la confidenzialità, il sistema applica avanzate tecniche di "vocoding" (atte a evitare di raccogliere il timbro vocale) e "pitch shifting" (atte a variare il tono della voce in modo casuale) capaci di offrire elevate caratteristiche di anonimizzazione al passo con la ricerca specifica nello specifico contesto d'uso. Tali tecniche permettono ai riceventi di ascoltare anche collegialmente la registrazione senza essere in condizione di identificare la voce direttamente e rendendo altamente inefficaci le moderne tecniche di de-anonimizzazione.
Esattezza e aggiornamento dei dati	L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.
Periodo di conservazione dei dati	Policy di data retention di default delle segnalazioni di 12 mesi, con cancellazione automatica sicura delle segnalazioni che raggiungono la data di scadenza. Il gestore può anticipare la scadenza delle segnalazioni fino a 3 mesi dalla data dell'operazione e può prorogare la scadenza delle segnalazioni per il tempo ritenuto congruo al trattamento dei dati. Anticipazioni e proroghe delle scadenze possono essere fatte dal gestore più volte. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.

Definizione degli obblighi dei responsabili del trattamento e formalizzazione dei contratti	Gli accordi contrattuali sono definiti con le seguenti società: • Whistleblowing Solutions in qualità di Responsabile del trattamento • Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions • Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions
Protezione in caso di trasferimento di dati al di fuori dell'Unione europea:	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.

MISURE DI SICUREZZA

CRITTOGRAFIA

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.

Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.

Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni.

Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento

Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.

Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

CONTROLLO DEGLI ACCESSI LOGICI

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.

Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.

Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

TRACCIABILITÀ

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.

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.

ARCHIVIAZIONE

L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM.

Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

GESTIONE DELLE VULNERABILITÀ TECNICHE

L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review.

A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente.

Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html

BACKUP

I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo dunque una RPO di 8 ore.

MANUTENZIONE

E' prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza.

MISURE ADDIZIONALI

A queste si aggiunge un crescente insieme altre misure al passo con la ricerca e la tecnica in ambito di sicurezza informatica reperibile alle seguenti pagine web:

- THREAT MODEL
- APPLICATION SECURITY

5. Rischi

5.1. Metodologia

In riferimento alla procedura "Valutazione del Rischio Trattamenti ad Alto rischio"

Come indicato dal considerando 76, l'azienda si è dotata di un sistema di calcolo del rischio basato su **parametri oggettivi**, al fine di stabilire se esiste un rischio o un rischio elevato per il trattamento specifico. L'Oggettivazione del rischio pertanto passa attraverso un modello di creazione della probabilità e della Gravità in grado di rispecchiare il contesto in cui l'organizzazione opera. Sono state identificate griglie oggettive di calcolo delle Probabilità e Gravità con riguardo ai diritti e libertà dell'interessato.

Matrice Ri = P x G					
	Probabilità	1 - Trascurabile	2 – Limitata	3 – Importante	4 – Massima
Gravità	1 - Trascurabile	1	2	3	4
	2 – Limitata	2	4	6	8
	3 – Importante	3	6	9	12
	4 – Massima	4	8	12	16

Gravità	Significato	Descrizione generica degli impatti (diretti e indiretti)
4	Massima	I soggetti interessati possono incontrare conseguenze irreversibili.
3	Importante	I soggetti interessati possono incontrare conseguenze significative, e difficoltà nella loro risoluzione, ma comunque superabili.
2	Limitata	I soggetti interessati possono incontrare inconvenienti superabili.
1	Trascurabile	Gli interessati non saranno coinvolti o potrebbero incontrare alcuni lievi inconvenienti senz'altro superabili.

Probabilità	Significato	Criterio di scelta
4	Massima	Il verificarsi del danno dipende da condizioni direttamente connesse alla situazione; Il verificarsi del danno non provocherebbe alcuna reazione di stupore; Eventi simili sono già accaduti in azienda o in aziende dello stesso tipo
3	Importante	Il verificarsi del danno dipende da condizioni non direttamente connesse alla situazione ma possibili; Il verificarsi del danno provocherebbe reazioni di moderato stupore; Eventi simili sono stati già riscontrati
2	Limitata	Il verificarsi del danno dipende da condizioni impreviste; Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili si sono verificati molto raramente
1	Trascurabile	Il verificarsi del danno è subordinato a un concatenamento di eventi indipendenti tra loro; Il Verificarsi del danno è creduto impossibile dagli addetti; Non è mai accaduto nulla di simile

Valutazione % delle Misure Esistenti

Rating	Descrizione
1-25%	Non adeguate
26-50%	Minime
51-75%	Adeguate

Rating rischio residuo (Rr)

Rischio Alto	6,1-16
Rischio Medio	3,1-6
Rischio Basso	1-3

Elementi per la valutazione:

a. **Ri** è il Rischio Inerente valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione
b. **Rr** è il Rischio Residuo calcolato al netto delle misure di mitigazione del rischio (determinate in via percentuale - % abbattimento)
c. L'azienda valuta come Rischio Accettabile (**Ra**) = **3**
d. Se il rischio inerente **Ri** a seguito delle valutazioni oggettive, dovesse risultare superiore ad **Ra,**
   l'azienda interverrà con mitigazioni opportune tali che ad **Rr < Ra**

5.2. Analisi dei rischi

Accesso illegittimo –Perdita della riservatezza

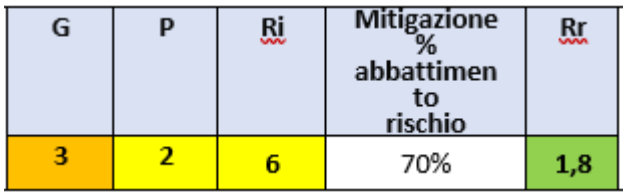
GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: disagio, diffusione indesiderata dei propri dati, consultazione dei propri da parte di personale non autorizzato, Ricatto economico, problematiche di natura giuslavoristica e contrattuale, mobbing, Discriminazioni lavorative, ritorsioni.
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili si sono verificati molto raramente
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)

MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento
CALCOLO DEL RISCHIO RESIDUO	G: 3 · P: 2 · Ri: 6 · Mitigazione % abbattimento rischio: 70% · Rr: 1,8

Modifiche indesiderate – Perdita dell'integrità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti. Eventi simili si sono verificati molto raramente.
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici.
MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento.
CALCOLO DEL RISCHIO RESIDUO	G: 3 · P: 2 · Ri: 6 · Mitigazione % abbattimento rischio: 70% · Rr: 1,8

Perdita del dato – Perdita della disponibilità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.
PROBABILITÀ (P)	Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti. Eventi simili si sono verificati molto raramente.
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici.
MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento.
CALCOLO DEL RISCHIO RESIDUO	

6. Parere delle parti interessate

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge. Ai fini dell'attivazione del canale di segnalazione interna, gli enti devono sentire le rappresentanze o le organizzazioni sindacali.

7. Parere DPO

DPO esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo.

8. Conclusioni

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono "rischi inerenti (Ri)" con impatto sui diritti e libertà degli interessati con stima a valore Medio. Nell'ottica di mitigazione di tali rischi, si evince che, con l'implementazione delle misure tecnico/organizzative pianificate ad integrazione di quelle già messe in atto, il valore di rischio residuo rientra nei parametri accettabili uguali o minori rispetto al Rischio accettato (Ra) dall'organizzazione aventi stima a *VALORE BASSO*, valore ritenuto accettabile dall'organizzazione in relazione dai parametri oggettivi considerati.

Si ritiene pertanto che il trattamento in oggetto presenta un grado di rischio sui diritti e libertà dell'interessato rientrante nei parametri accettabili e di conseguenza:

non è richiesta una consultazione preventiva all'Autorità Garante.