Data Privacy Impact Assessment (DPIA)

Whistleblowing - Francigena srl

01	01	18.07.2023	Prima Emissione	RPD	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

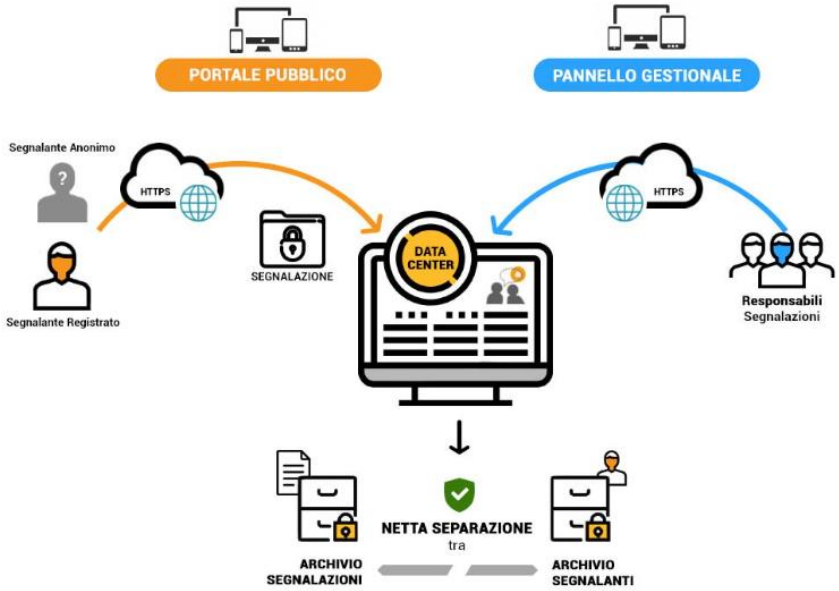
- **RPD** Responsabile per la protezione dei dati personali
- **RTDP** Responsabile della tutela dei dati personali e della riservatezza dei dati aziendali

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 DigitalPA	
Le principali caratteristiche del software per la segnalazione degli illeciti	• Accesso regolamentato a norma privacy (complessità password e cambio password trimestrale) • **Netta separazione del processo di iscrizione dal processo di segnalazione**, per una corretta separazione dei dati a tutela dell'anonimato del segnalante • **Segnalazioni scritte e vocali** • Possibilità di **gestire le segnalazioni di utenti registrati e non registrati** (a discrezione del committente) • Erogazione del servizio in S.a.a.S, **con accesso all'area riservata via web** o tramite rete interna • **Multilingua** • **Multicanale**: piattaforma web e **App mobile Legality Whistleblowing** • Gestione dedicata per **RPCT, ODV e Collaboratori** • Assegnazione automatica delle segnalazioni ai responsabili **in base alla tipologia** • Possibilità di interazione con **soggetti terzi** rispetto al segnalante e al responsabile • Complete **stastistiche** e **log di sistema** che tracciano tutte le operazioni effettuate sulla piattaforma • **SLA di massimo livello** con garanzia di massima raggiungibilità del servizio, in linea con quanto previsto dall'art. 50-bis del Codice dell'Amministrazione Digitale (continuità operativa)
Infrastruttura e sicurezza applicativa	• **Server dedicati DigitalPA** – Massima protezione dei dati e dei livelli di sicurezza, garantiti sia dalla certificazione DigitalPA ISO IEC 27001/2017 che dalla infrastruttura della *server farm* certificata ISO 27001/2017; • **OWASP tested** *(Open Web Application Security Project)* **–** adozione e test attraverso *best practice* di settore in tema di vulnerabilità e sicurezza; • **Firewall hardware e Software integrato –** Ogni piattaforma dispone di un firewall integrato con strettissime regole, che limitano gli accessi e le azioni agli esclusivi compiti dedicati al software, i firewall si integrano e potenziano ulteriormente la sicurezza; • **Blocco IP** – Accesso limitato ad una *access list* di indirizzi IP del committente, accessibile quindi dalla rete internet o esclusivamente dalla intranet; • **Certificato SSL –** Il software Segnalazioni.net Whistleblowing è accessibile esclusivamente tramite accesso HTTPS (Secure Sockets Layer); • **IP e Certificato SSL dedicati –** per ciascun Cliente; • **Validazioni input utente –** la piattaforma è basata su un approccio di validazione input dell'utente. Attraverso regole estremamente rigide l'utente viene **verificato** sia a livello client che a livello server; • **Prevenzione CSRF**: tutte le richieste gestite dalla piattaforma sono protette da *token CSRF* (*Cross-site request forgery*); • **Adempiente agli standard ISO 37301 e ISO 37001** dedicati ai sistemi di gestione della compliance e dell'anticorruzione.

Standard di sicurezza informatica	• **Server dedicati DigitalPA:** Massima protezione dei dati e dei livelli di sicurezza, garantiti dalla certificazione DigitalPA Iso 27001/2014 che dalla infrastruttura della server farm certificata ISO 27001/2014 • **OWASP tested:** adozione e test attraverso "best practice di settore" in tema di vulnerabilità e sicurezza • **Firewall hardware e Software integrato:** Ogni piattaforma dispone di un firewall integrato con strettissime regole, che limitano gli accessi e le azioni agli esclusivi compiti dedicati al software, i firewall si integrano e potenziano ulteriormente la sicurezza • **Blocco IP**: Accesso limitato ad una access listi di ip del committente, accessibile quindi dalla rete internet o esclusivamente dalla intranet • **Certificato SSL**: Il software di whistleblowing è accessibile esclusivamente tramite accesso HTTPS (Secure Sockets Layer) • **IP e Certificato SSL:** dedicati per ciascun cliente • **Validazioni input utente:** la piattaforma è basata su un approccio di validazione input dell'utente. Attraverso regole estremamente rigide l'utente viene verificato sia a livello client che a livello server • **Prevenzione CSRF**: tutte le richieste gestite dalla piattaforma sono protette da token CSRF  **GARANZIA DI RISERVATEZZA DEL SEGNALANTE**

Sicurezza del Segnalante e delle segnalazioni	• **Crittografica Asimmetrica** sui contenuti testuali e allegati "files". La crittografia non richiede azioni specifiche da parte del responsabile anticorruzione o segnalante o interventi da parte degli amministratori di sistema; Il sistema crittografico, garantisce che il messaggi e relativi allegati possano essere letti esclusivamente dal mittente e destinatario attraverso l'abbinamento della "chiave crittografica pubblica e privata" • Invio, al segnalatore, tramite e-mail o Pec dell'impronta digitale dei messaggi, a garanzia dell'immutabilità delle segnalazioni • Possibilità di accesso tramite smart card • Accesso regolamentato a norma privacy (complessità password e cambio password trimestrale) • L'applicativo è totalmente adempiente agli standard ISO 37301 (ex 19600) e ISO 37001, dedicati rispettivamente alle linee guida per il Compliance Management System e l'Anti-bribery Management System, e si configura quindi conforme all'ottenimento delle certificazioni da parte dell'azienda o ente che lo adotta
SaaS - Software as a Service	• Attraverso l'erogazione in SaaS è garantita la massima sicurezza dei sistemi, degli aggiornamenti di sicurezza del software e dell'efficienza dell'Help Desk dedicato.

2.3. Responsabilità connesse al trattamento

Ruoli	Nominativi
Titolare del trattamento	**Francigena srl**
Responsabile Protezione Dati	Dr. Ennio Fiocchi
Responsabile trattamento	DigitalPA
Sub Responsabile	Oracle Italia
Incaricati al trattamento	RPCT e ODV

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 collaborator 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 collaborator 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 **DigitalPA**,
(https://www.digitalpa.it/suite-software/whistleblowing/caratteristiche.html)

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: - privacy@certim.it
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

Crittografia	Ogni informazione viene protetta con **Crittografica Asimmetrica** dei contenuti testuali e allegati "files
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.
Tracciabilità	Viene utilizzato un meccanismo di audit minimale che memorizza un identificativo dell'operatore autorizzato e la data/ora di modifica/creazione delle informazioni presenti nel database. Le operazioni effettuate dai segnalanti hanno un identificativo completamente anonimizzato (autogenerato) e legato al singolo ticket (ovvero episodio circoscritto) e non alla persona del segnalante.
Archiviazione	L'applicativo ha completo ed esclusivo controllo della base dati ed implementa al suo interno le logiche di data retention e cancellazione sicura previste dalle policy normative.
Gestione delle vulnerabilità tecniche	L'amministratore di sistema incaricato riceve bollettini di sicurezza riguardanti i moduli software in uso dall'infrastruttura ed è in grado di intervenire tempestivamente, per poter mitigare eventuali vulnerabilità critiche di recente scoperta.
Backup	Il back up viene gestito su Server dedicati **DigitalPA** con massima protezione dei dati e dei livelli di sicurezza, garantiti sia dalla certificazione DigitalPA ISO IEC 27001/2017 che dalla infrastruttura della *server farm* certificata ISO 27001/2017;
Manutenzione	Garanzia certificate da DigitalPA ISO IEC 27001/2017 e dalla infrastruttura della *server farm* certificata ISO 27001/2017
Sicurezza dei canali informatici	**OWASP tested** *(Open Web Application Security Project)* **–** adozione e test attraverso *best practice* di settore in tema di vulnerabilità e sicurezza;
Sicurezza dell'hardware	• **Firewall hardware e Software integrato –** Ogni piattaforma dispone di un firewall integrato con strettissime regole, che limitano gli accessi e le azioni agli esclusivi compiti dedicati al software, i firewall si integrano e potenziano ulteriormente la sicurezza;

	• **Blocco IP** – Accesso limitato ad una *access list* di indirizzi IP del committente, accessibile quindi dalla rete internet o esclusivamente dalla intranet; • **Certificato SSL** – Il software Segnalazioni.net Whistleblowing è accessibile esclusivamente tramite accesso HTTPS (Secure Sockets Layer); • **IP e Certificato SSL dedicati –** per ciascun Cliente. • **Blocco IP**: Accesso limitato ad una access listi di ip del committente, accessibile quindi dalla rete internet o esclusivamente dalla intranet • **Certificato SSL**: Il software di whistleblowing è accessibile esclusivamente tramite accesso HTTPS (Secure Sockets Layer)
Gestire gli incidenti di sicurezza e le violazioni dei dati personali **Lotta contro il malware**	Il prodotto è conforme con le normative GDPR in materia. Gli amministratori e gli sviluppatori del prodotto operano in contesti di sicurezza conformi alle linee guida in materia, con firewall e antivirus aziendali al passo con le minacce informatiche di oggi.
Politica di tutela della privacy	La società adotta un Modello Organizzativo sulla protezione dei dati personali.
Gestione dei rischi	L'analisi dei rischi viene condotta secondo metodologia CNIL (o altra metodologia definita dal Titolare).
Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Gli incidenti di sicurezza e le violazioni dei dati personali vengono gestiti secondo la "Procedura Data Breach" adottata dalla Società in conformità a quanto prescritto dagli artt. 33-34 del GDPR.
Vigilanza sulla protezione dei dati	Vigilanza svolta da DPO/ODV/RPTC incaricati dal Titolare del trattamento (a secondo di quanto definito nell'organigramma privacy aziendale).

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:

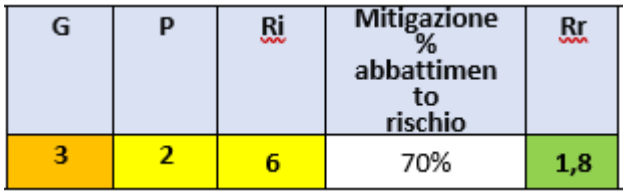
a. **Ri** è il Rischio Inerente valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione
b. **Rr** è il Rischio Residuo calcolato al netto delle misure di mitigazione del rischio (determinate in via percentuale - % abbattimento)
c. L'azienda valuta come Rischio Accettabile (**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	<table><tr><th>G</th><th>P</th><th>Ri</th><th>Mitigazione % abbattimento rischio</th><th>Rr</th></tr><tr><td>3</td><td>2</td><td>6</td><td>70%</td><td>1,8</td></tr></table>

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	

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	<table><tr><th>G</th><th>P</th><th>Ri</th><th>Mitigazione % abbattimento rischio</th><th>Rr</th></tr><tr><td>3</td><td>2</td><td>6</td><td>70%</td><td>1,8</td></tr></table>

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.