CONSORZIO INTERCOMUNALE DEI SERVIZI SOCIALI
C.I.S.S. OSSOLA

Valutazione d'impatto (DPIA) del sistema di ricevimento e gestione delle segnalazioni interne WHISTLEBLOWING

Ai sensi dell'art. 35 REGOLAMENTO (UE) 2016/679

Titolare del trattamento	CONSORZIO INTERCOMUNALE DEI SERVIZI SOCIALI - C.I.S.S. OSSOLA		
Responsabile della Protezione dei Dati personali (DPO/RPD):	Ing. Danilo Roggi c/o ERREGI SERVICE S.R.L. Via E. Montale, 26 – 28021 Borgomanero (NO)		
Data di emissione	21/12/2023	**Versione**	1.0

Sommario

1. Premessa

La valutazione d'impatto (o, altrimenti detta, DPIA – *Data Protection Impact Assessment*) è una procedura prevista dall'articolo 35 del Regolamento (UE) 2016/679 (GDPR) che il titolare deve svolgere allorquando intraprenda un'attività di trattamento particolarmente delicata. Lo scopo è quello di verificare l'impatto del trattamento sui diritti e le libertà degli interessati, valutandone, da una parte, la necessità e la proporzionalità rispetto al fine da perseguire, dall'altra, l'idoneità delle misure di sicurezza approntate per annullare o almeno limitare i rischi di incidenti.

I soggetti sono tenuti a norma del D.lgs. 24/2023 ad adottare un modello di ricevimento e gestione delle segnalazioni interne di whistleblowing che comporta il trattamento di informazioni su illeciti (dati giudiziari) commessi all'interno dell'ente rivelati da segnalanti la cui identità deve rimanere riservata e conoscibile solo dalle persone autorizzate.
Tali segnalazioni comportano un trattamento di dati personali che può rappresentare un rischio elevato per i diritti e le libertà del segnalante. Pertanto, risulta obbligatoria la redazione del presente documento ai sensi dell'art. 35 GDPR anche alla luce dell'espressa previsione contenuta nell'art. 13, comma 6, del D.lgs. 24/2023.

La valutazione deve contenere almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

2. Contesto

2.1. Panoramica del trattamento

Il trattamento dei dati riguarda le persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica, di cui siano venute a conoscenza nel contesto lavorativo ai sensi della L. 179/2017 e del D.lgs. 24/2023. Inoltre, il trattamento dei dati riguarda anche i soggetti a cui è attribuito l'illecito e gli eventuali altri soggetti coinvolti come i facilitatori, persone del medesimo contesto lavorativo legate al segnalante da uno stabile legame affettivo o di parentela entro il quarto grado e i colleghi di lavoro del segnalante che hanno con detta persona un rapporto abituale e corrente.

Chi segnala fornisce informazioni che possono portare all'indagine, all'accertamento e al perseguimento dei casi di violazione delle norme, rafforzando in tal modo i principi di trasparenza e responsabilità delle istituzioni democratiche.

Garantire la protezione dei soggetti che si espongono con segnalazioni, denunce o con l'istituto della divulgazione pubblica, contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per la stessa amministrazione e, di riflesso, per l'interesse pubblico collettivo.

2.2. Responsabilità connesse al trattamento

Il C.I.S.S. OSSOLA è Titolare del trattamento, che gestisce le segnalazioni pervenute attraverso il canale di segnalazione interna.

Il C.I.S.S. OSSOLA si avvarrà di un soggetto esterno che fornisce la piattaforma di segnalazione e gestione degli illeciti. In particolare, tale soggetto, Whistleblowing Solutions Impresa Sociale S.r.l., sarà Responsabile del trattamento in quanto si occuperà 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.

Il Responsabile del trattamento, Whistleblowing Solutions, si avvale di altri soggetti esterni per l'erogazione del servizio che ha nominato come Sub-Responsabili; tali soggetti sono Seeweb quale Sub-Responsabile del trattamento per la gestione dell'infrastruttura (IaaS) e Transparency International Italia quale Sub-Responsabile del trattamento per la collaborazione nella gestione del sistema di whistleblowing.

2.3. Standard applicabili al trattamento

Whistleblowing Solutions, quale Responsabile del trattamento dei dati, ha acquisito le seguenti certificazioni:

- 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.

3. Dati, processi e risorse di supporto

3.1 Dati trattati

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 interessato**
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

3.2 Destinatari dei dati

Sono destinatari dei dati raccolti a seguito della segnalazione, se del caso, l'Autorità Giudiziaria, la Corte dei conti e l'ANAC. Inoltre, fra i destinatari vi rientra anche Whistleblowing Solutions quale fornitore del servizio di erogazione e gestione operativa della piattaforma tecnologica di digital whistleblowing in qualità di Responsabile del trattamento ai sensi dell'art. 28 GDPR.

3.3 Ciclo di vita del trattamento dei dati (descrizione funzionale)

Le segnalazioni possono pervenire, ed essere quindi raccolte, tramite la piattaforma digitale messa a disposizione dei segnalanti.

Il ciclo di vita del trattamento è il seguente:

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. Analisi della segnalazione e gestione attraverso indagini interne o richieste con adozione di provvedimenti da parte del Titolare del trattamento;
5. Chiusura di una segnalazione e conservazione fino al termine di 5 anni dalla comunicazione di chiusura;
6. 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.

3.4 Risorse di supporto ai dati

Sono risorse di supporto ai dati:

1. Software di whistleblowing professionale GlobaLeaks;
2. Infrastruttura IaaS e SaaS privata basata su tecnologie:

   - VMWARE (virtualizzazione)
   - Debian Linux LTS (sistema operativo)
   - VEEAM (backup)
   - OPNSENSE (firewall)
   - OPENVPN (vpn)

4. Principi Fondamentali

4.1 Proporzionalità e necessità

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.
Quali sono le basi legali 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).

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	Il software di whistleblowing raccoglie segnalazioni secondo i questionari predisposti in ambito di whistleblowing in collaborazione con 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.
I dati sono esatti e aggiornati?	L'aggiornamento dei dati attraverso la piattaforma digitale messa a disposizione 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. In ogni caso il gestore dà seguito ad una richiesta di rettifica o integrazione dei dati personali da parte del segnalante o degli altri soggetti secondo la procedura di gestione delle richieste di esercizio dei diritti privacy.
Qual è il periodo di conservazione dei dati?	Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario alla gestione delle stesse e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione (art. 14 D.lgs. 24/2023). Inoltre, la piattaforma digitale ha una policy di data retention di default delle segnalazioni, prorogabili sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute.

4.2 Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?	Il C.I.S.S. OSSOLA mette a disposizione dei soggetti interessati (segnalante, segnalato, altri soggetti coinvolti) apposita informativa privacy resa ai sensi dell'art. 13 GDPR nella sezione dedicata alle segnalazioni di whistleblowing sul proprio sito internet istituzionale. In tale sezione verranno, inoltre, resi disponibili la procedura adottata dall'ente, il link di collegamento alla piattaforma digitale per l'invio delle segnalazioni e le ulteriori indicazioni sulla gestione delle segnalazioni di whistleblowing.
Ove applicabile: come si ottiene il consenso degli interessati?	Per il trattamento dei dati relativi alla procedura di whistleblowing non è necessario raccogliere un consenso dell'interessato in quanto il trattamento ha quale base giuridica l'adempimento di un obbligo di legge a cui è soggetto il Titolare del trattamento. Il D.lgs. 24/2023 disciplina però due ipotesi in cui è necessario raccogliere il consenso del segnalante quale soggetto interessato: 1. La prima ipotesi ricorre laddove nell'ambito di un procedimento disciplinare avviato nei confronti del presunto autore della condotta segnalata, l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare. In tal caso, oltre al previo consenso del segnalante da raccogliere per iscritto è necessario anche comunicare, sempre previamente, in forma scritta a quest'ultimo le motivazioni che conducono al disvelamento della sua identità. 2. La seconda ipotesi ricorre, invece, nel caso in cui nelle procedure di segnalazione interna ed esterna la rivelazione dell'identità del segnalante sia indispensabile anche ai fini della difesa della persona coinvolta. Anche in questo caso per disvelare l'identità del segnalante è necessario acquisire previamente sia il consenso espresso dello stesso che notificare allo stesso in forma scritta motivazioni alla base della necessità di disvelare la sua identità.
Come fanno gli interessati a esercitare i loro diritti previsti dall'art 15 del GDPR ?	Il C.I.S.S. OSSOLA ha adottato una procedura di gestione delle richieste di esercizio dei diritti in materia di privacy.
Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	Gli accordi contrattuali saranno 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. Ogni accordo disciplinerà in maniera puntale i rispettivi obblighi in materia di protezione dei dati personali.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?	I Dati Personali saranno trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea. Non esiste alcun trasferimento di dati personali verso paesi extra UE.

5. Rischi

5.1 Misure esistenti o pianificate

Crittografia	La piattaforma digitale utilizzata dal C.I.S.S. OSSOLA e fornita da Whistleblowing Solutions ha alla base l'applicativo GlobaLeaks che 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 all'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. 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. Le segnalazioni eventualmente ricevute in modalità cartacea sono conservate in archivio non accessibile a persone non autorizzate.
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/main/security/PenetrationTests.html.
Backup	I sistemi sono soggetti a backup effettuato dal fornitore della piattaforma.
Manutenzione	È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua 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 attraverso cui 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 svolgere le modifiche al sistema e installare gli aggiornamenti previsti.
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.
Sicurezza dell'hardware	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.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Il C.I.S.S. OSSOLA ha adottato una procedura di gestione dei data breach. Inoltre, anche il Responsabile del trattamento Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.
Lotta contro il malware	Tutti i computer del C.I.S.S. OSSOLA e del personale di Whistleblowing 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.
Contratto con il responsabile del trattamento	Il C.I.S.S. OSSOLA sottoscriverà apposito atto con il Responsabile del trattamento dei dati Whistleblowing Solutions al fine di disciplinare i rispettivi obblighi in materia di trattamento dei dati personali.
Politica di tutela della privacy	Il C.I.S.S. OSSOLA ha nominato un DPO esterno ai sensi dell'art. 37 GDPR che svolge i compiti stabiliti dall'art. 39 GDPR sulla base di un contratto di servizi. Inoltre, il personale dipendente del C.I.S.S. OSSOLA svolge periodicamente una formazione in materia di protezione dei dati personali comprensiva anche dei rischi informatici ed è stato istruito rispetto al coretto trattamento dei dati.

5.2 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

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**

5.3 Analisi dei rischi

Accesso illegittimo ai dati (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 5.1 del presente documento
CALCOLO DEL RISCHIO RESIDUO	

G	P	Ri	Mitigazione % abbattimento rischio	Rr
3	2	6	70%	1,8

Modifiche indesiderate dei dati (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, 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 5.1 del presente documento
CALCOLO DEL RISCHIO RESIDUO	

G	P	Ri	Mitigazione % abbattimento rischio	Rr
3	2	6	70%	1,8

Perdita di dati (perdita della disponibilità)

<table>
<tr><td>GRAVITÀ (G)</td><td>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.</td></tr>
<tr><td>PROBABILITÀ (P)</td><td>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.</td></tr>
<tr><td>FONTI DI RISCHIO</td><td>- 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)</td></tr>
<tr><td>MISURE</td><td>Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 5.1 del presente documento</td></tr>
<tr><td>CALCOLO DEL RISCHIO RESIDUO</td><td>
<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>
</td></tr>
</table>

6. Parere delle parti interessati

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge.

7. Parere del DPO

Il 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. La valutazione d'impatto risulta essere stata eseguita correttamente ed il rischio risulta essere accettabile.

8. Conclusioni

Dopo aver valutato nel dettaglio quanto richiesto dal par. 7 dell'art. 35 GDPR, il Comune può concludere che il trattamento dei dati relativo alla ricezione e gestione delle segnalazioni di whistleblowing analizzato risulta:

1) **Proporzionato** alla finalità previste da normativa: le misure poste a protezione dei dati personali dei soggetti coinvolti nel procedimento di whistleblowing consente di ritenere il trattamento proporzionato rispetto ai diritti e alle libertà dei soggetti interessati.

2) È **necessario**, in quanto tale finalità è prevista da legge nel rispetto di adeguate misure di sicurezza poste a protezione dei dati personali degli interessati.