VALUTAZIONE DI IMPATTO

SULLA PROTEZIONE DEI DATI

WHISTLEBLOWIN

1. Premessa

La Valutazione d'Impatto sulla Protezione dei Dati (di seguito "DPIA) è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del titolare nei confronti dei trattamenti dallo stesso effettuati.

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.

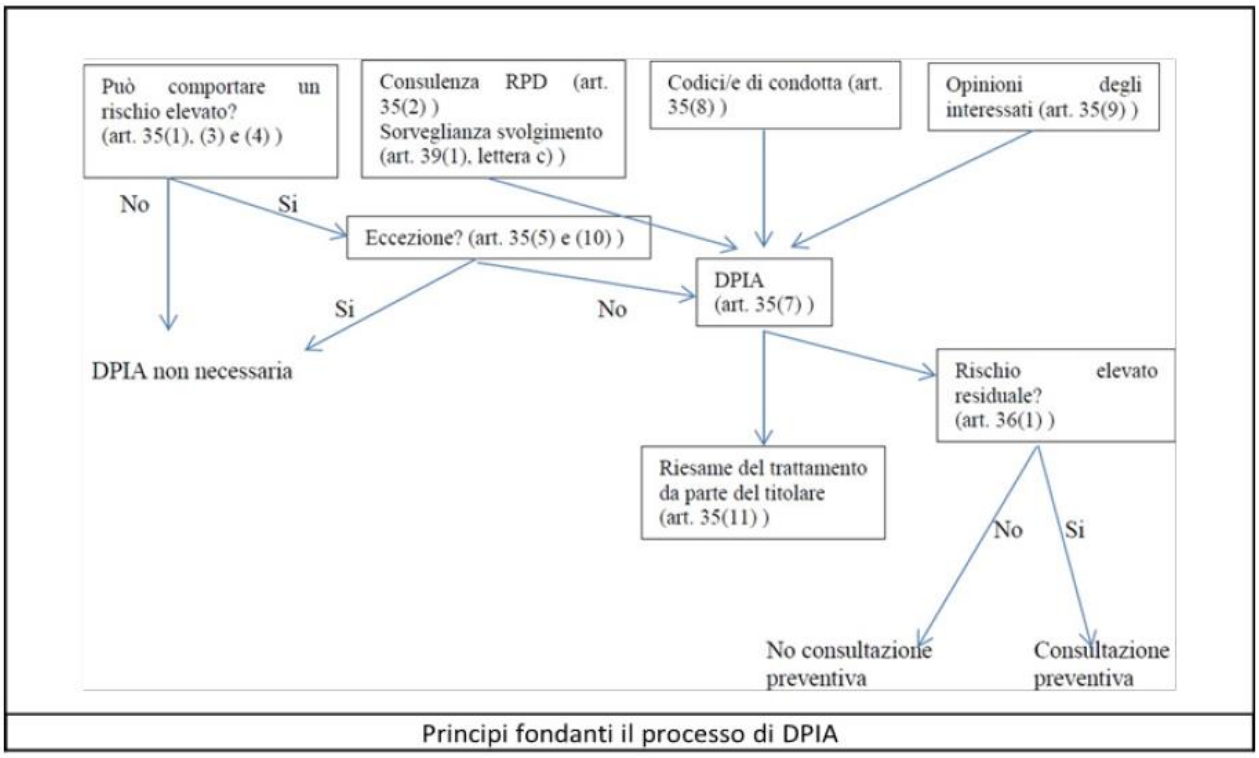
Il Titolare del trattamento, infatti, è tenuto non solo a garantire l'osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

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 su due pilastri:

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



Principi fondanti il processo di DPIA

2. Contesto

In questa prima fase deve essere definito il contesto in cui la valutazione deve essere condotta. Deve essere descritta la tipologia di dati personali trattati, come si sviluppa il trattamento, definendo i tempi di conservazione dei dati e quali sono gli strumenti utilizzati per effettuare il trattamento.

In questa fase il titolare deve stabilire, in sostanza, se, in base al trattamento da svolgere e alle sue caratteristiche, ricorra o meno la necessità stessa di effettuare una valutazione di impatto.

2.1 Panoramica del trattamento

Il trattamento ha per 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 interno, piattaforma adottata dall'Ente, di cui vengono riportate le principali caratteristiche:

Architettura di sistema	L'architettura di sistema è composta principalmente 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 GlobaLeafis. Vengono primariamente utilizzati le tecnologie open source: ▪ Debian/Linux (principale sistema operativo utilizzato); ▪ Postfix (mail server); ▪ Bind9 (dns server); ▪ OPNSense (firewall); ▪ OpenVPN (vpn). Le componenti software di natura proprietaria impiegate necessarie per finalità di gestione infrastrutturale e backup professionale, 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.

2.2 Responsabilità connesse al trattamento

Titolare del trattamento	Comune di Issime
Responsabile del trattamento (per la fornitura e la gestione del sistema di whistleblowing)	Whistleblowing Solutions Impresa sociale
Sub Responsabile (per la gestione dell'infrastruttura – IaaS) nominato da Whistleblowing Solutions	Seeweb
Sub Responsabile (per la collaborazione nella gestione del sistema whistleblowing) nominato da Whistleblowing Solutions	Transparency International Italia
Incaricati al trattamento	R.P.C.T.

2.3 Dati, processi e risorse di supporto

Operazioni di trattamento: Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti.

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 di registrazione	Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (Responsabile Anticorruzione).
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) – Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.	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). Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.	Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto Fornitori che effettuano una segnalazione o vengono segnalati

<u>Ciclo di vita del trattamento dei dati (descrizione funzionale):</u>

1. Attivazione e configurazione della piattaforma
2. Utilizzo della piattaforma: caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei soggetti riceventi autorizzati
3. Dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.

<u>Risorse a supporto dei dati:</u>

Software di whistleblowing professionale GlobaLeaks

Infrastruttura IaaS e SaaS privata basata su tecnologie:

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

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*.
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).
I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati).	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.
I dati sono esatti e aggiornati	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	Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 24/2023: Policy di data retention di default delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.

3.1 Tutela degli interessati

Informazione del trattamento agli 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 interna sull'esistenza del canale di segnalazione interno (canale informatico); ▪ Pubblicazione sito internet: sezione dedicata al Whistleblowing
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 artt. 6.1. lett. a) e 7 del GDPR, tramite piattaforma
Esercizio dei 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 (mail RPCT pa.longis@cm-walser.vda.it), nei limiti di cui all'articolo 2-undecies del Codice Privacy.
Definizione degli obblighi dei responsabili del trattamento	Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del trattamento ai sensi dell'art. 28 GDPR, attraverso Accordo di responsabilità.
Protezione in caso di trasferimento di dati al di fuori dell'Unione europea.	Per questa tipologia di trattamento non è previsto un trasferimento di dati personali fuori dall'Unione Europea.

4. Misure esistenti

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. 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 giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.
Manutenzione	E' 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 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 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 7:24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7:24. I datacenter del fornitore IaaS sono certificati ISO27001.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali	*Whistleblowing Solutions* ha definito una procedura per la gestione delle violazioni dei dati personali.
Lotta contro il malware	Tutti i computer 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. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.
Politiche di tutela della privacy	L'Ente ha adotta un Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali in attuazione del Regolamento UE 2016/679.
Gestione dei rischi	L'analisi dei rischi viene condotta secondo metodologia CNIL.
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 dall'Ente in conformità a quanto prescritto dagli artt. 33-34 del GDPR.
Vigilanza sulla protezione dei dati	Vigilanza svolta da DPO/funzioni incaricate dal Titolare del trattamento (a seconda di quanto definito nell'organigramma privacy dell'Ente).

4.1 Misure addizionali

Il presente documento sintetizza una serie di metodologie standard conformi con la normativa vigente in ambito nazionale ed internazionale in materia di trattamento sicuro dell'informazione, privacy e whistleblowing.

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. Gestione dei Rischi

5.1 Metodologia

Come indicato dal considerando 76, l'ente adotta 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.

Gravità	Significato	Descrizione generica degli impatti (diretti ed indiretti)
4	Massima	I soggetti interessati possono incontrare conseguenze irreversibili
3	Importante	I soggetti interessati possono incontrare conseguenze significative, difficoltà nella loro soluzione, ma comunque superabili
2	Limitata	I soggetti interessati possono incontrare inconvenienti insuperabili
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 nell'Ente o in Enti dello stesso tipo
3	Importante	I soggetti interessati possono incontrare conseguenze significative, difficoltà nella loro soluzione, ma comunque superabili
2	Limitata	I soggetti interessati possono incontrare inconvenienti insuperabili
1	Trascurabile	Gli interessati non saranno coinvolti o potrebbero incontrare alcuni lievi inconvenienti senz'altro superabili

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''Ente 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

5.2.1 Accesso illegittimo – Perdita della riservatezza

GRAVITA' (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 dati da parte di personale non autorizzato, ricatto economico, problematiche di natura giuslavoristica e contrattuale, Mobbing, discriminazioni lavorative, ritorsioni.
PROBABILITA' (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 4del 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>

5.2.2 Modifiche indesiderate – Perdita dell'integrità

GRAVITA' (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 dati da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.
PROBABILITA' (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 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>

5.2.3 Perdita del dato – Perdita della disponibilità

GRAVITA' (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 dati da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.
PROBABILITA' (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 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. Pareri 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

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.

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.

9. Fonti normative

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

- ✓ 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

SOMMARIO