

# Consiglio Notarile di Padova

Padova, Via Giovanni Berchet 17  
C.F. 80033340284

## VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

### WHISTLEBLOWING

#### Sommario

|  |    |
|--|----|
| 1. Informazioni sulla DPIA.....  | 2  |
| 2. Contesto.....   | 2  |
| 2.1 Panoramica del trattamento.....  | 2  |
| 2.1.1 Oggetto del trattamento.....   | 2  |
| 2.1.2 Responsabilità connesse al trattamento.....                                | 2  |
| 2.1.3 Standard applicabili al Trattamento.....                                   | 3  |
| 2.2 Dati, processi e risorse di supporto .....                                   | 3  |
| 2.2.1 Quali sono i dati trattati? .....  | 3  |
| 2.2.2 Qual è il ciclo di vita del trattamento dei dati?.....                     | 3  |
| 2.2.3 Quali sono le risorse di supporto ai dati? .....                           | 3  |
| 3. Principi fondamentali.....  | 4  |
| 3.2 Misure a tutela dei diritti degli interessati.....                           | 4  |
| 4. Misure esistenti .....  | 6  |
| 5. Rischi.....   | 8  |
| 5.1 Metodologia .....  | 8  |
| 5.1.1 Anali dei rischi.....  | 10 |
| 6. Piano d'azione.....   | 12 |
| 6.1 Misure e procedure adottate o programmate per la mitigazione dei rischi..... | 12 |
| 7. Parere delle parti interessate.....   | 12 |
| 8. Parere del DPO.....   | 12 |
| 9. Conclusioni .....   | 12 |

## 1. Informazioni sulla DPIA

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 su due pilastri:

1. 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;
2. la gestione dei rischi per la privacy dei soggetti interessati, che determina i controlli tecnici e organizzativi opportuni a tutela dei dati personali.

È espressamente prevista dall'art. 13, co. 6 D.Lgs. 24/2023.

## 2. Contesto

### 2.1 Panoramica del trattamento

#### 2.1.1 Oggetto del trattamento

In relazione al D.Lgs. 24/2023 " *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 e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*", il Consiglio Notarile di Padova ha aderito alla piattaforma "WHISTLEBLOWINGPA" che permette al RPCT di ricevere segnalazioni di illeciti da parte dei soggetti previsti dalla normativa.

#### 2.1.2 Responsabilità connesse al trattamento

| <b>Ruolo</b>                     | <b>Nominativo</b>  |
|----------------------------------|--|
| Titolare del Trattamento         | Consiglio Notarile di Padova   |
| Responsabile del Trattamento     |  |
| Sub Responsabile del Trattamento |  |
| Incarichi al trattamento         | Responsabile della prevenzione della corruzione e della trasparenza (RPCT)<br>Organismo di Vigilanza aziendale |

### *2.1.3 Standard applicabili al Trattamento*

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

## **2.2 Dati, processi e risorse di supporto**

### *2.2.1 Quali sono i dati trattati?*

I dati personali raccolti e trattati nell'ambito della segnalazione possono includere dati personali "comuni", del "segnalante", del "segnalato" e del facilitatore.

### *2.2.2 Qual è il ciclo di vita del trattamento dei dati?*

1. Attivazione della piattaforma
2. Configurazione della piattaforma
3. Utilizzo della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi
4. Dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge con conseguente cancellazione sicura dei dati da parte del fornitore.

### *2.2.3 Quali sono le risorse di supporto ai dati?*

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.  |
| 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). Alcuni trattamenti specifici si basano sul consenso del segnalante, ai sensi dell'art. 6 par. 1 lett. a) GDPR.  |
| 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, 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. 14/2023. |

#### 3.1 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: <ul style="list-style-type: none"><li>- Processo comunicazione aziendale sull'esistenza del canale di segnalazione interno (canale informatico);</li><li>- Pubblicazione sito internet, sezione dedicata al Whistleblowing</li></ul> |
| Ove applicabile: come si ottiene il consenso degli interessati? | Per quanto riguarda l'eventuale registrazione su dispositivo idoneo alla conservazione e all'ascolto o trascrizione integrale delle Segnalazioni effettuate mediante linea telefonica registrata, la base giuridica del trattamento è il consenso dell'interessato ai sensi dell'art. 6 par. 1 lett. a) del Regolamento UE 679/2016. Identica base giuridica  |

|   |  |
|---|--|
|   | <p>opera per quanto riguarda l'eventuale registrazione su dispositivo idoneo alla conservazione e all'ascolto o trascrizione integrale delle Segnalazioni effettuate oralmente nel corso di un incontro con il personale addetto. Inoltre, soltanto con lo specifico ed espresso consenso dell'interessato si potrà procedere alla rivelazione della sua identità ai sensi dell'art. 12 c. 2 o ai sensi dell'art. 12 c. 5 del Decreto. Il conferimento dei dati da parte del segnalante è necessario per poter dare seguito alla Segnalazione e per fornire il dovuto riscontro al segnalante. Il consenso è raccolto presso l'interessato previa informazione mediante relativa informativa privacy messa a disposizione sia sul sito sia su richiesta.</p> |
| <p>Come fanno gli interessati a esercitare i loro diritti previsti dagli artt. 15 ss. GDPR?</p>                       | <p>Gli interessati possono esercitare i diritti previsti degli artt. 15 ss. Del GDPR attraverso l'indirizzo di posta elettronica dedicato <a href="mailto:consigliopadova@notariato.it">consigliopadova@notariato.it</a> nel limite di cui l'articolo 2-undecies del Codice Privacy</p>  |
| <p>Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?</p>      | <p>Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del Trattamento ai sensi dell'art. 28 GDPR.</p>  |
| <p>In caso di trasferimento di dati al di fuori dell'Unione Europea, i dati godono di una protezione equivalente?</p> | <p>Per questa tipologia di trattamento non è previsto un trasferimento di dati al di fuori dell'Unione Europea</p>   |

## 4. Misure esistenti

|  |  |
|--|--|
| <b>Crittografia</b>                          | Ogni informazione viene protetta in transito da protocollo TLS 1.2 con cifrature AES128/SHA256   |
| <b>Controllo degli accessi logici</b>        | 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.  |
| <b>Tracciabilità</b>                         | 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.   |
| <b>Archiviazione</b>                         | 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.   |
| <b>Gestione delle vulnerabilità tecniche</b> | 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.  |
| <b>Backup</b>                                | <p>Il server virtuale è ulteriormente garantito da una soluzione di Backup CDP (Continuous Data Protection) basata su R1Soft CDP. Il sistema di backup CDP effettua snapshot incrementali delle macchine virtuali con una cadenza oraria, assicurando una protezione aggiornata dei dati nel tempo senza causare interruzioni del servizio.</p> <p>Gli snapshot incrementali vengono salvati su Storage server esterni, che sono fisicamente separati dal server che ospita le macchine virtuali su network zone distinte all'interno dello stesso datacenter. Questo approccio assicura un'adeguata sicurezza e protezione dei dati, garantendo che le copie di backup siano conservate in un ambiente separato e affidabile.</p> |
| <b>Manutenzione</b>                          | L'amministratore di sistema incaricato effettua interventi almeno trimestrali (in assenza di criticità elevate) per allineare le versioni del software in uso (sia di sistema, che applicativo) con le ultime patch migliorative stabili pubblicate dai rispettivi fornitori; provvede inoltre ai passaggi di versione, laddove sopraggiungano le scadenze del supporto ufficiale dei suddetti software.   |
| <b>Sicurezza dei canali informatici</b>      | Tutte le connessioni sono protette tramite protocollo TLS 1.2. Le connessioni amministrative privilegiate avvengono con protocollo SSH.  |
| <b>Sicurezza dell'hardware</b>               | <p>I server sono ospitati in un datacenter, situato sul territorio italiano, fisicamente isolato dove sono in essere le seguenti misure di sicurezza:</p> <ul style="list-style-type: none"> <li>- Sistema di rilevamento anti-intrusione;</li> <li>- Presidio con agenti di vigilanza 24 ore su 24, per sette giorni su sette;</li> <li>- Telecamere a circuito chiuso e archiviazione digitale delle riprese;</li> <li>- Sistemi di rilevamento anti-fumo, anti-incendio e anti-</li> </ul>  |

|   |   |
|---|---|
|   | <p>allagamento;</p> <ul style="list-style-type: none"> <li>- Alimentazioni multiple e indipendenti con percorsi diversificati;</li> <li>- Sistema di raffreddamento a doppio circuito di alimentazione;</li> <li>- Gruppi elettrogeni in ambienti separati;</li> <li>- Connettività verso internet 100Gbps multi operatore;</li> </ul> <p>provider è inoltre certificato ISO 27001:2013, ISO 14001:2015, ISO 27017:2015, ISO 27018:2019 e ha ricevuto la Certificazione dell'Agenzia per la Cybersicurezza Nazionale.</p> |
| <p><b>Gestire gli incidenti di sicurezza e le violazioni dei dati personali</b></p> <p><b>Lotta contro il malware</b></p> | <p>Il prodotto è conforme con le normative GDPR in materia.</p> <p>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.</p>   |
| <p><b>Politica di tutela della privacy</b></p>  | <p>La società adotta un Modello Organizzativo sulla protezione dei dati personali.</p>  |
| <p><b>Gestione dei rischi</b></p>   | <p>L'analisi dei rischi viene condotta secondo metodologia CNIL (o altra metodologia definita dal Titolare).</p>  |
| <p><b>Gestire gli incidenti di sicurezza e le violazioni dei dati personali</b></p>                                       | <p>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.</p>  |
| <p><b>Vigilanza sulla protezione dei dati</b></p>   | <p>Vigilanza svolta da DPO/Comitato Privacy/funzioni incaricate dal Titolare del trattamento (a seconda di quanto definito nell'organigramma privacy aziendale).</p>  |

## 5. Rischi

### 5.1 Metodologia

#### In riferimento alla procedura "Valutazione del Rischio\_Trattamenti ad Alto rischio"

Come indicato dal considerando 76, l'ente 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 |
| G<br>r<br>a<br>v<br>i<br>t<br>à | 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;<br>Il verificarsi del danno non provocherebbe alcuna reazione di stupore;                |
| 3           | Importante   | Il verificarsi del danno dipende da condizioni non direttamente connesse alla situazione ma possibili;<br>Il verificarsi del danno provocherebbe reazioni di moderato stupore; |
| 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   |

### 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:

- Ri** è il Rischio Inerente valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione
- Rr** è il Rischio Residuo calcolato al netto delle misure di mitigazione del rischio (determinate in via percentuale - % abbattimento)
- L'azienda valuta come Rischio Accettabile (**Ra**) = **3**
- 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**

### 5.1.1 Anali 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:<br>disagio<br>Diffusione indesiderata dei propri dati,<br>Consultazione dei propri dati 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<br>Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti;<br>Eventi simili si sono verificati molto raramente  |    |                               |     |                               |    |   |   |   |     |     |
| Fonti di rischio    | Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale)<br>Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker)<br>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 | <table border="1"> <thead> <tr> <th>G</th> <th>P</th> <th>Ri</th> <th>Mitigazione %<br/>abbattimento</th> <th>Rr</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>2</td> <td>6</td> <td>70%</td> <td>1,8</td> </tr> </tbody> </table>   | G  | P                             | Ri  | Mitigazione %<br>abbattimento | Rr | 3 | 2 | 6 | 70% | 1,8 |
| G                   | P  | Ri | Mitigazione %<br>abbattimento | Rr  |                               |    |   |   |   |     |     |
| 3                   | 2  | 6  | 70%                           | 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:<br>disagio<br>Diffusione indesiderata dei propri dati,<br>Consultazione dei propri dati 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<br>Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti;<br>Eventi simili si sono verificati molto raramente  |

| Fonti di rischio    | <p>Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale)</p> <p>Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker)</p> <p>Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)</p> |    |                               |     |                               |    |   |   |   |     |     |
|---------------------|---|----|-------------------------------|-----|-------------------------------|----|---|---|---|-----|-----|
| Misure              | Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento  |    |                               |     |                               |    |   |   |   |     |     |
| Calcolo del rischio | <table border="1"> <thead> <tr> <th>G</th> <th>P</th> <th>Ri</th> <th>Mitigazione %<br/>abbattimento</th> <th>Rr</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>2</td> <td>6</td> <td>70%</td> <td>1,8</td> </tr> </tbody> </table>  | G  | P                             | Ri  | Mitigazione %<br>abbattimento | Rr | 3 | 2 | 6 | 70% | 1,8 |
| G                   | P   | Ri | Mitigazione %<br>abbattimento | Rr  |                               |    |   |   |   |     |     |
| 3                   | 2   | 6  | 70%                           | 1,8 |                               |    |   |   |   |     |     |

#### Modifiche indesiderate – Perdita della disponibilità

| Gravità (G)         | <p>I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: disagio</p> <p>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.</p> |    |                               |     |                               |    |   |   |   |     |     |
|---------------------|---|----|-------------------------------|-----|-------------------------------|----|---|---|---|-----|-----|
| Probabilità (P)     | <p>Il verificarsi del danno dipende da condizioni impreviste</p> <p>Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti;</p> <p>Eventi simili si sono verificati molto raramente</p>  |    |                               |     |                               |    |   |   |   |     |     |
| Fonti di rischio    | <p>Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale)</p> <p>Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker)</p> <p>Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)</p>   |    |                               |     |                               |    |   |   |   |     |     |
| Misure              | Le misure che contribuiscono a mitigare il rischio sono quelle descritte al paragrafo 4 del presente documento  |    |                               |     |                               |    |   |   |   |     |     |
| Calcolo del rischio | <table border="1"> <thead> <tr> <th>G</th> <th>P</th> <th>Ri</th> <th>Mitigazione %<br/>abbattimento</th> <th>Rr</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>2</td> <td>6</td> <td>70%</td> <td>1,8</td> </tr> </tbody> </table>  | G  | P                             | Ri  | Mitigazione %<br>abbattimento | Rr | 3 | 2 | 6 | 70% | 1,8 |
| G                   | P   | Ri | Mitigazione %<br>abbattimento | Rr  |                               |    |   |   |   |     |     |
| 3                   | 2   | 6  | 70%                           | 1,8 |                               |    |   |   |   |     |     |

## 6. Piano d'azione

### 6.1 Misure e procedure adottate o programmate per la mitigazione dei rischi

Individuazione di strumenti di protezione dei locali e degli armadi contenenti la documentazione cartacea e degli strumenti elettronici.

## 7. 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.

## 8. Parere del 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.

## 9. 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.

---

### Allegati

- Procedura di gestione delle segnalazioni
- Trattamento dati relativi alle segnalazioni di condotte illecite
- Informativa privacy