Valutazione d’impatto sulla protezione dei dati ai sensi del regolamento UE 2016/679, in relazione al trattamento di dati effettuato per l’inoltro e la gestione della segnalazione di condotte illecite da parte del dipendente (decreto legislativo 24/2023)

Sommario

[**1. INFORMAZIONI SULLA DPIA** 5](#_Toc173568140)

[**1.1 Nome della valutazione d’impatto** 5](#_Toc173568141)

[**1.2 Nome autore** 5](#_Toc173568142)

[**1.3 Nome valutatore** 5](#_Toc173568143)

[**1.4 Nome validatore** 5](#_Toc173568144)

[**1.5 Data** 5](#_Toc173568145)

[**2. CONTESTO** 5](#_Toc173568146)

[**2.1 Qual è il trattamento in considerazione?** 5](#_Toc173568147)

[**2.2 Quali sono le responsabilità connesse al trattamento?** 6](#_Toc173568148)

[**2.3 Ci sono standard applicabili al trattamento?** 6](#_Toc173568149)

[**3. Dati, processi e risorse di supporto** 6](#_Toc173568150)

[**3.1 Quali sono i dati trattati?** 6](#_Toc173568151)

[**3.2 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?** 7](#_Toc173568152)

[**3.3 Quali sono gli strumenti utilizzati per il trattamento?** 7](#_Toc173568153)

[**4. Proporzionalità e necessità** 8](#_Toc173568154)

[**4.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?** 8](#_Toc173568155)

[**4.2 Quali sono le basi legali che rendono lecito il trattamento?** 8](#_Toc173568156)

[**4.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?** 8](#_Toc173568157)

[**4.4 I dati sono esatti e aggiornati?** 9](#_Toc173568158)

[**4.5 Qual è il periodo di conservazione dei dati?** 9](#_Toc173568159)

[**5. Misure a tutela dei diritti degli interessati** 9](#_Toc173568160)

[**5.1 Come sono informati del trattamento gli interessati?** 9](#_Toc173568161)

[**5.2 Ove applicabile: come si ottiene il consenso degli interessati?** 10](#_Toc173568162)

[**5.3 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?** 10](#_Toc173568163)

[**5.4 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?** 10](#_Toc173568164)

[**5.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?** 10](#_Toc173568165)

[**5.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?** 11](#_Toc173568166)

[**5.7 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?** 11](#_Toc173568167)

[**6. MISURE DI SICUREZZA** 11](#_Toc173568168)

[**7. RISCHI** 11](#_Toc173568169)

[**7.1 PERDITA DI DATI** 12](#_Toc173568170)

[**7.1.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio di PERDITA DI DATI dovesse concretizzarsi?** 12](#_Toc173568171)

[**7.1.2 Quali sono le fonti di rischio?** 12](#_Toc173568172)

[**7.1.3 Come stimereste la GRAVITÀ del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? (Livello: 1-5)** 13](#_Toc173568173)

[**7.1.4 Come stimereste la PROBABILITÀ del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? (Livello 1-3)** 13](#_Toc173568174)

[**7.1.5 RISCHIO (GxP)** 13](#_Toc173568175)

[**7.2 MODIFICHE INDESIDERATE DI DATI** 13](#_Toc173568176)

[**7.2.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio di MODIFICHE INDESIDERATE DI DATI dovesse concretizzarsi?** 13](#_Toc173568177)

[**7.2.2 Quali sono le fonti di rischio?** 14](#_Toc173568178)

[**7.2.3 Come stimereste la GRAVITÀ del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? (Livello: 1-5)** 14](#_Toc173568179)

[**7.2.4 Come stimereste la PROBABILITÀ del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? (Livello 1-3)** 14](#_Toc173568180)

[**7.2.5 RISCHIO (GxP)** 15](#_Toc173568181)

[**7.3 ACCESSO ILLEGITTIMO AI DATI** 15](#_Toc173568182)

[**7.3.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio di ACCESSO ILLEGITTIMO AI DATI dovesse concretizzarsi?** 15](#_Toc173568183)

[**7.3.2 Quali sono le fonti di rischio?** 15](#_Toc173568184)

[**7.3.3 Come stimereste la GRAVITÀ del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? (Livello: 1-5)** 17](#_Toc173568185)

[**7.3.4 Come stimereste la PROBABILITÀ del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? (Livello 1-3)** 17](#_Toc173568186)

[**7.3.5 (GxP)** 17](#_Toc173568187)

[**8. ESITO** 17](#_Toc173568188)

[**Parere del VALUTATORE** 18](#_Toc173568189)

[**Pareri degli interessati** 18](#_Toc173568190)

## **1. INFORMAZIONI SULLA DPIA**

### **1.1 Nome della valutazione d’impatto**

Valutazione d’impatto sulla protezione dei dati ai sensi del regolamento UE 2016/679, in relazione al trattamento di dati effettuato per l’inoltro e la gestione della segnalazione di condotte illecite da parte del dipendente (decreto legislativo 24/2023).

### **1.2 Nome autore**

Studio Avvocati D’Agostini Via Vittorio Veneto n.32 - 33100 UDINE Partita IVA: 02595350303

### **1.3 Nome valutatore**

D.P.O. dott. Mauro Annibali

### **1.4 Nome validatore**

D.P.O. dott. Mauro Annibali

### **1.5 Data**

Roma \_\_\_\_\_\_\_\_\_\_\_\_ 2024

## **2. CONTESTO**

### **2.1 Qual è il trattamento in considerazione?**

L’oggetto della presente DPIA è rappresentato dal trattamento dei dati personali forniti dal segnalante attraverso specifica applicazione messa a disposizione dal Titolare, per la segnalazione di fatti e condotte illecite (c.d. whistleblowing).

Le finalità del trattamento sono rappresentate dalla necessità:

* di consentire all’interessato di segnalare presunte condotte illecite di cui sia venuto a conoscenza in ragione del proprio rapporto di lavoro;
* di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l’adozione dei conseguenti provvedimenti.

Il trattamento, in particolare, deve svolgersi garantendo la riservatezza sull’identità del segnalante. Quest’ultima, in particolare, potrà essere rivelata dietro consenso espresso del segnalante, eventualmente prestato in sede di compilazione della specifica applicazione messa a disposizione del segnalante e al fine di rendere utilizzabile la segnalazione in sede di procedimento disciplinare nel caso in cui la contestazione dell’addebito disciplinare nei confronti del segnalato sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato.

### **2.2 Quali sono le responsabilità connesse al trattamento?**

Titolare: AUTOMOBILE CLUB UDINE, C.F./P.IVA 00160740304, con sede in Udine, Viale Tricesimo n°46

Contitolare: nessuno.

Responsabile: ISWEB SPA, con sede legale in Via Cadorna, n.31 - 67051 - Avezzano (AQ).

Sub-Responsabile: Seeweb srl, con sede legale in Corso Lazio 9/A – 03100 Frosinone.

### **2.3 Ci sono standard applicabili al trattamento?**

È applicabile lo standard ISO 37002:2021 - Whistleblowing management systems — Guidelines

## **3. Dati, processi e risorse di supporto**

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

Il trattamento ha ad oggetto i dati personali comuni identificativi del segnalante, e in particolare:

- Nome;

- Cognome;

- E-mail – Obbligatorietà che dipende dal tipo di segnalazione: potrebbe non essere obbligatorio nel caso il segnalante voglia segnalare in completo anonimato;

- Voce del segnalante;

- Tracciamento della prestazione del consenso alla rivelazione dell’identità all’interno del sistema di raccolta delle segnalazioni;

- Dichiarazione di aver letto l'informativa sulla protezione dei dati personali.

Sono inoltre oggetto del trattamento altre informazioni contenute nella segnalazione, che descrivendo specifiche circostanze possono riportare dati personali (di tipo comune, particolare, giudiziario e/o sanitario) di soggetti terzi:

- Oggetto;

- Tipologia segnalante;

- Tipologia illecito;

- Soggetto/i coinvolto/i che ha/hanno commesso il fatto;

- Eventuali persone informate sui fatti;

- Unità organizzativa delle persone coinvolte;

- Luogo fisico in cui si è verificato il fatto;

- Periodo e/o data in cui si è verificato il fatto;

- Testo della segnalazione;

- Possibilità di allegare file a supporto della segnalazione.

### **3.2 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?**

**Raccolta dei Dati**: i dati personali vengono acquisiti tramite l'applicazione dedicata alla segnalazione. Questi possono includere identificativi del segnalante (salvo opzione di anonimato), dettagli sulle condotte illecite riferite e altre informazioni pertinenti. La raccolta avviene nel rispetto dei principi di minimizzazione e limitazione della finalità dei dati.

**Trasmissione e Archiviazione**: i dati sono trasmessi e memorizzati sulla piattaforma cloud. È imperativo assicurare la sicurezza dei dati durante la trasmissione (per esempio, mediante crittografia) e mantenere integrità e confidenzialità una volta depositati nel cloud.

**Accesso ed Elaborazione**: i dati vengono quindi elaborati dal Gestore delle Segnalazioni. Tale elaborazione include l'analisi dei dati, la raccolta di ulteriori informazioni e, ove il segnalante non sia anonimo, comunicazioni con lo stesso. L'accesso ai dati è rigidamente controllato e limitato al personale autorizzato.

**Decisione e Azione**: sulla base delle indagini, si prendono decisioni relative alle azioni da intraprendere. Queste possono includere ulteriori indagini interne, azioni disciplinari, o modifiche ai processi aziendali. In alcuni casi, può essere necessario il coinvolgimento di soggetti esterni.

**Conservazione dei Dati**: I dati legati alla segnalazione sono conservati per un periodo determinato, in accordo con la normativa vigente.

**Cancellazione**: al termine del periodo di conservazione, i dati personali sono cancellati

### **3.3 Quali sono gli strumenti utilizzati per il trattamento?**

Piattaforma Cloud Whistleblowing basato sul software Open Source Globaleaks e manutenuto da ISWEB S.p.a.: questa piattaforma rappresenta lo strumento centrale per il trattamento dei dati nell'ambito del sistema di segnalazione. È un'applicazione cloud-based, configurata per facilitare la segnalazione di condotte illecite.

Questa piattaforma cloud è selezionata e configurata tenendo in considerazione la necessità di assicurare l'integrità, la riservatezza e la disponibilità dei dati trattati, in linea con i requisiti di protezione dei dati personali e le normative vigenti.

## **4.** **Proporzionalità e necessità**

### **4.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?**

Lo scopo del trattamento è specificamente finalizzato alla gestione, tramite specifica piattaforma informatica o tramite colloqui diretti, dell’istituto del whistleblowing.

Tale istituto prevede esplicitamente che i soggetti che hanno rapporti e/o prestano attività lavorativa direttamente o indirettamente per il Titolare possano segnalare allo stesso eventuali condotte illecite, attraverso gli strumenti messi a disposizione.

Lo scopo del trattamento è, inoltre, legittimo perché sancito dal decreto legislativo 24/2023, pubblicato sulla Gazzetta Ufficiale del 15 marzo 2023 in vigore dal 15 luglio 2023.

### **4.2 Quali sono le basi legali che rendono lecito il trattamento?**

La condizione di liceità (base legale) del trattamento è l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, par. 1, lett. c) RGPD.

Vengono in rilievo, in particolare:

1) il decreto legislativo 24/2023, pubblicato sulla Gazzetta Ufficiale del 15 marzo 2023 in vigore dal 15 luglio 2023;

2) i provvedimenti adottati dall’ANAC (ex multis la Delibera n. 311 del 12 luglio 2023 recante le “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”).

### **4.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?**

Il principio di minimizzazione è stato rispettato attraverso la raccolta e l’analisi dei dati strettamente necessari al perseguimento delle finalità, in ossequio al principio della “privacy by default”.

La raccolta di informazioni del segnalante è stata espressamente studiata per minimizzare i dati trattati dello stesso; i dati relativi alla segnalazione verranno successivamente sottoposti ad analisi finalizzata alla verifica delle circostanze nel rispetto della minimizzazione dei dati trattati.

### **4.4 I dati sono esatti e aggiornati?**

I dati forniti dal segnalante, in sede di inoltro della segnalazione, una volta inseriti nell’applicazione informativa non possono essere oggetto di modifica da parte del titolare.

Il segnalante può integrare le informazioni relative alla propria segnalazione; il sistema mantiene tutte le informazioni fornite durante tutte le fasi della segnalazione fino a chiusura della stessa.

Il segnalante può seguire lo stato di lavorazione della segnalazione e rispondere ad eventuali richieste del Responsabile attraverso l’area messaggi integrata.

La piattaforma verrà utilizzata anche per registrare e gestire le segnalazioni in forma orale mediante richiesta di incontro diretto con RPCT/Gestore delle segnalazioni.

### **4.5 Qual è il periodo di conservazione dei dati?**

Il periodo di conservazione dei dati personali è parametrato alla gestione della segnalazione presentata e agli adempimenti normativamente richiesti in materia di whistleblowing.

Le segnalazioni saranno conservate per 5 (cinque) anni dalla data della comunicazione dell'esito (cfr. art. 14 d.lgs. 24/23), salvo interruzioni / sospensioni dettate dall’insorgere di contenziosi dinanzi all’Autorità Giudiziaria e/o alle Autorità di Controllo.

## **5. Misure a tutela dei diritti degli interessati**

### **5.1 Come sono informati del trattamento gli interessati?**

**INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI**

Prima di utilizzare la piattaforma di whistleblowing, il segnalante riceve un'informativa dettagliata che spiega la natura e le finalità del trattamento dei dati. L'informativa è formulata in un linguaggio chiaro e accessibile, per garantire una completa comprensione.

**SESSIONI DI FORMAZIONE SUL WHISTLEBLOWING**

Vengono organizzate sessioni di formazione specifiche per i lavoratori, dove vengono spiegati il funzionamento della piattaforma di whistleblowing, l'importanza della protezione dei dati e le procedure da seguire in caso di segnalazione. Durante queste sessioni, i lavoratori hanno l'opportunità di porre domande e chiarire dubbi riguardo al trattamento dei loro dati nel contesto delle segnalazioni.

**MATERIALI DI SUPPORTO PER IL WHISTLEBLOWING**

Ai lavoratori vengono forniti materiali di supporto come brochure, manuali e FAQ (Domande Frequenti) specifiche per la piattaforma di whistleblowing, per aiutarli a comprendere meglio il sistema e le pratiche di trattamento dei dati.

### **5.2 Ove applicabile: come si ottiene il consenso degli interessati?**

Non applicabile (si veda quanto indicato nel paragrafo 4.2).

### **5.3 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?**

L’interessato potrà esercitare il diritto di accesso previsto dall’art. 15 del RGPD nei limiti previsti dall’art. 2-undecies lettera f del D. Lgs. 196/2003.

Il diritto alla portabilità dei dati non è esercitabile.

### **5.4 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?**

Nella specifica informativa che verrà predisposta sono indicate le modalità per l’esercizio dei diritti.

### **5.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?**

Nella specifica informativa che verrà predisposta sono indicate le modalità per l’esercizio dei diritti.

### **5.6 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?**

È stato siglato uno specifico Data Processing Agreement ai sensi dell’art. 28 del GDPR.

### **5.7 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?**

I dati non sono oggetto di trasferimenti.

## **6. MISURE DI SICUREZZA**

Per quanto concerne la descrizione dettagliata e l’elencazione delle misure di sicurezza adottate, si ritiene opportuno rimandare ai documenti (allegati alla presente DPIA), che contengono informazioni esaustive e aggiornate in merito. In particolare, si fa riferimento ai seguenti documenti:

1. **Dichiarazione sulle misure di sicurezza applicate. Servizi ambito Whistleblowing**: Questo documento offre una panoramica completa delle misure di sicurezza implementate per garantire la protezione dei dati personali nel contesto dei servizi di whistleblowing. Include informazioni sulle procedure tecniche e organizzative adottate per prevenire accessi non autorizzati, trattamenti illeciti e perdite accidentali di dati.
2. **Certificazione di Compliance. Whistleblowing/PAWhistleblowing**: il documento è una autocertificazione delle misure di sicurezza applicate nello sviluppo del servizio Whistleblowing basato sul software Open Source Globaleaks e manutenuto da ISWEB S.p.a. ed ha lo scopo di certificarne il livello di adeguamento rispetto alle nuove misure di protezione introdotte dal regolamento UE 2016/679.

I suddetti documenti allegati rappresentano una componente essenziale dell’approccio alla sicurezza dei dati e sono parte integrante della nostra strategia complessiva di gestione del rischio. Essi forniscono un quadro chiaro e dettagliato delle misure adottate, dimostrando il nostro impegno continuo nel garantire la massima protezione dei dati personali trattati.

## **7. RISCHI**

## **7.1 PERDITA DI DATI**

### **7.1.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio di PERDITA DI DATI dovesse concretizzarsi?**

**Perdita di evidenze:**

Interessati: Segnalante; Persone indicate nella segnalazione.

La perdita di dati potrebbe significare che prove cruciali o dettagli rilevanti vengono persi, rendendo difficile o impossibile seguire la segnalazione.

**Mancata azione sulla segnalazione a causa della perdita di informazioni:**

Interessati: Segnalante; Persone indicate nella segnalazione.

La perdita di dati potrebbe significare che l'organizzazione non è in grado di agire sulla segnalazione o di condurre ulteriori indagini.

**Perdita di fiducia nella piattaforma di segnalazione:**

Interessati: Segnalante.

Se un segnalante percepisce che i suoi dati possono essere persi sulla piattaforma cloud, potrebbe esitare a utilizzarla per segnalazioni future.

### **7.1.2 Quali sono le fonti di rischio?**

**Guasti hardware o software:**

Malfunzionamenti dei server o della piattaforma potrebbero portare alla perdita di dati.

**Cancellazione accidentale:**

Un operatore e/o un software potrebbero erroneamente cancellare dati importanti.

**Mancanza di backup o backup corrotti:**

In assenza di backup regolari o a causa di backup difettosi, i dati potrebbero andare persi e non essere recuperabili.

**Attacchi informatici mirati:**

Alcuni attacchi, come quelli di tipo ransomware, potrebbero cifrare o cancellare dati, rendendoli inaccessibili.

**Disastri naturali:**

Anche le infrastrutture cloud possono essere vulnerabili a eventi come incendi o inondazioni se i data center non sono adeguatamente protetti.

**Interruzioni del servizio del provider cloud:**

Il provider di servizi cloud potrebbe avere interruzioni o malfunzionamenti che portano alla perdita di dati.

**Errore Umano:**

Il gestore della segnalazione potrebbe commettere errori che causano la perdita di informazioni.

### **7.1.3 Come stimereste la GRAVITÀ del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? (Livello: 1-5)**

La gravità del rischio è MEDIA (3)

### **7.1.4 Come stimereste la PROBABILITÀ del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? (Livello 1-3)**

La Probabilità è BASSA (1)

### **7.1.5 RISCHIO (GxP)**

Livello di rischio 3 su 15.

## **7.2 MODIFICHE INDESIDERATE DI DATI**

### **7.2.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio di MODIFICHE INDESIDERATE DI DATI dovesse concretizzarsi?**

**Modifica delle informazioni del segnalante:**

Interessati: Segnalante.

Se le informazioni digitali del segnalante vengono modificate, ciò potrebbe portare a una mancata identificazione o a confusione sulla sorgente della segnalazione.

**Alterazione delle informazioni digitali sulle persone indicate nella segnalazione:**

Interessati: Persone indicate nella segnalazione.

Se le informazioni riguardanti le persone indicate vengono alterate, ciò potrebbe portare a indagini errate, accuse infondate o inesatte, o a una mancata responsabilità per comportamenti effettivamente scorretti.

### **7.2.2 Quali sono le fonti di rischio?**

**Vulnerabilità software della piattaforma:**

Se il software ha vulnerabilità, potrebbe essere sfruttato per modificare le segnalazioni.

**Mancanza di procedure di verifica e controllo:**

L'assenza di log di modifica o di meccanismi di controllo può permettere modifiche non autorizzate senza che vengano rilevate.

**Accesso interno non regolamentato:**

Se troppi dipendenti hanno accesso alla piattaforma senza adeguate restrizioni, potrebbe aumentare il rischio di modifiche indesiderate.

**Mancanza di backup e protocolli di recupero:**

Se non ci sono backup regolari e protocolli di recupero, una modifica indesiderata potrebbe non essere facilmente annullabile, compromettendo l'integrità delle segnalazioni.

**Vulnerabilità nella connessione cloud:**

Se la connessione tra l'utente e la piattaforma cloud non è sicura, potrebbero verificarsi intercettazioni e modifiche dei dati durante la trasmissione.

**Errore Umano:**

Il gestore della segnalazione potrebbe commettere errori che causano l’alterazione di informazioni.

### **7.2.3 Come stimereste la GRAVITÀ del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? (Livello: 1-5)**

La gravità del rischio è ALTA (4)

### **7.2.4 Come stimereste la PROBABILITÀ del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? (Livello 1-3)**

La Probabilità è BASSA (1)

### **7.2.5 RISCHIO (GxP)**

Livello di rischio 4 su 15.

## **7.3 ACCESSO ILLEGITTIMO AI DATI**

### **7.3.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio di ACCESSO ILLEGITTIMO AI DATI dovesse concretizzarsi?**

**Esposizione digitale dell'identità del segnalante:**

Interessati: Segnalante.

Se l'accesso illegittimo avviene sulla piattaforma cloud, l'identità e le informazioni personali del segnalante potrebbero essere esposte a un pubblico più ampio, aumentando il rischio di ritorsioni, discriminazioni o attacchi informatici mirati.

**Diffusione digitale delle informazioni sulle persone indicate nella segnalazione:**

Interessati: Persone indicate nella segnalazione.

Le informazioni delle persone menzionate potrebbero essere divulgate, compromettendo la loro privacy e reputazione su una scala potenzialmente globale.

**Perdita di fiducia nella piattaforma digitale di segnalazione:**

Interessati: Segnalante.

Se un segnalante percepisce che la piattaforma cloud non è sicura, potrebbe esitare a utilizzarla per segnalazioni future, limitando la trasparenza e l'efficacia del sistema di segnalazione.

### **7.3.2 Quali sono le fonti di rischio?**

**Vulnerabilità software della piattaforma:**

La piattaforma potrebbe avere debolezze o vulnerabilità che permettono accessi non autorizzati.

**Attacchi di phishing o ingegneria sociale:**

Gli aggressori potrebbero tentare di ottenere credenziali di accesso ingannando gli utenti o il personale responsabile.

**Accesso interno non regolamentato:**

L'accesso non regolato o eccessivo da parte dei dipendenti all'infrastruttura cloud potrebbe permettere intrusioni non autorizzate.

**Intercettazioni durante la trasmissione dei dati:**

Se la connessione tra l'utente e la piattaforma cloud non è cifrata o protetta adeguatamente, potrebbero verificarsi intercettazioni dei dati.

**Attacchi informatici mirati (es. DDoS, man-in-the-middle):**

Gli attacchi potrebbero essere rivolti alla piattaforma per compromettere la sua integrità o per accedere alle informazioni.

**Interferenze nel traffico di rete:**

L'invio di segnalazioni attraverso la rete potrebbe essere intercettato o manipolato da terzi, se non protetto adeguatamente.

**Vulnerabilità del software:**

La piattaforma potrebbe avere vulnerabilità sconosciute o non patchate che potrebbero essere sfruttate da hacker.

**Dipendenza dal fornitore cloud:**

Se il fornitore cloud subisce una violazione, anche le informazioni sulla piattaforma di segnalazione potrebbero essere compromesse.

**Mancata cifratura:**

Se i dati non sono cifrati, sia in transito che in riposo, sono maggiormente esposti a potenziali compromissioni.

**Gestione degli accessi:**

La mancata implementazione di un sistema robusto di gestione degli accessi può permettere a personale non autorizzato di accedere alle segnalazioni.

**Problemi di autenticazione:**

Senza meccanismi di autenticazione a due fattori o simili, gli account degli utenti e degli amministratori possono essere più facilmente compromessi.

**Malware e ransomware:**

La piattaforma potrebbe essere bersaglio di malware, inclusi ransomware che potrebbero criptare o bloccare l'accesso alle segnalazioni.

**Errore Umano:**

Il gestore della segnalazione potrebbe commettere errori che causano l’accesso illegittimo alle informazioni.

### **7.3.3 Come stimereste la GRAVITÀ del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? (Livello: 1-5)**

La gravità del rischio è ELEVATA (5)

### **7.3.4 Come stimereste la PROBABILITÀ del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? (Livello 1-3)**

La Probabilità è BASSA (1)

### **7.3.5 (GxP)**

Livello di rischio 5 su 15.

## **8. ESITO**

|  |  |
| --- | --- |
| [ ] RISCHIO RESIDUO ELEVATO | Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non sono ritenute sufficienti. Il rischio residuale per i diritti e le libertà degli interessati resta elevato. |
| [x] **RISCHIO RESIDUO NON ELEVATO** | **Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento sono ritenute sufficienti.** |

### **Parere del VALUTATORE**

Il DPO

- letta la suestesa valutazione d'impatto sulla protezione dei dati inerente all'applicazione informatica messa a disposizione dal Titolare, per la segnalazione di fatti e condotte illecite (c.d. Whistleblowing);

- esaminata la documentazione a supporto della medesima valutazione e, in particolare, quella inviata dal fornitore della soluzione tecnologica;

- esaminato il d.lgs. 10 marzo 2023, n.24;

- lette le Linee guida in materia di whistleblowing approvate dall'ANAC;

- in ottemperanza a quanto previsto dall'art. 39 par. 1 lett. c) del Regolamento (UE) 2016/679;

1) rileva che, in ossequio all'art. 25 del GDPR (“privacy by design” e “privacy by default” ivi stabiliti) il Titolare nel corso della valutazione d'impatto ha attuato in modo efficace i principi di protezione dei dati, in particolare quello di minimizzazione, avendo limitato i dati trattati a quanto necessario rispetto alle finalità del trattamento;

2) prende atto delle misure di sicurezza adottate a tutela dei dati personali, con particolare riferimento alla riservatezza dell'identità del segnalante;

3) ritiene condivisibili le valutazioni effettuate dal Titolare del trattamento e, pertanto, esprime parere favorevole;

4) raccomanda di programmare audit c/o il Responsabile del Trattamento.

### **Pareri degli interessati**

Non è stato chiesto il parere degli interessati in quanto non necessario, poiché la base legale del trattamento è costituita dall'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, par. 1, lett. c) GDPR.