COMUNE DI AVIO

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

a norma dell'art. 35 Regolamento (UE) 2016/679

sull'attività di trattamento relativa a

ricevimento e gestione

delle segnalazioni di violazioni – whistleblowing

Dati del titolare e del Responsabile del Trattamento	
Titolare del trattamento	
Nome	**Comune di Avio**
Indirizzo	Piazza V. Emanuele III n. 1 – 38063 Avio (TN)
E-mail	segreteria@comune.avio.tn.it
PEC	segreteria@pec.comune.avio.tn.it
Responsabile del trattamento	
Nome	**Whistleblowing Solutions Impresa Sociale S.r.l.**
Indirizzo	Viale Abruzzi 13/A, 20131, Milano
E-mail	info@whistleblowingsolutions.it
PEC	info@pec.whistleblowingsolutions.it
Parte del trattamento gestita	Fornitura e gestione del sistema di whistleblowing
Subresponsabili del trattamento	
Nome	**Seeweb S.r.l.**
Parte del trattamento gestita	Gestione dell'infrastruttura (IaaS)
Nome	**Transparency International Italia**
Parte del trattamento gestita	Collaborazione con il Responsabile nella gestione del sistema di whistleblowing
DPO	Consorzio dei Comuni Trentini – dott.ssa Laura Marinelli
Sindaco	Ivano Fracchetti
Segretario comunale	dott. Luca Graiff
Responsabile Servizio Segreteria e Affari generali	dott. Luca Graiff
ADS – Amministratore di Sistema	Alto Garda Informatica

Data di completamento della Valutazione di impatto 09/06/2026

CRONOLOGIA DELLE REVISIONI

Versione	Data	Motivo

Sommario

Introduzione

L’articolo 35 del Regolamento UE 679/16 (Regolamento generale sulla protezione dei dati – GDPR), stabilisce che “*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*”.
La valutazione d’impatto (Data Protection Impact Assessment – DPIA) costituisce dunque una procedura volta a descrivere il trattamento, valutarne necessità e proporzionalità e a gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento, valutando detti rischi e determinando le misure per affrontarli, prevista dagli articoli 35 e seguenti GDPR.

Ai sensi del Regolamento UE 679/16, il titolare del trattamento deve attuare misure adeguate per garantire ed essere in grado di dimostrare il rispetto del Regolamento stesso, tenendo conto tra l’altro dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche (art. 24, par. 1, GDPR). L’obbligo per i titolari del trattamento di realizzare una valutazione d’impatto sulla protezione dei dati va inteso nel contesto dell’obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi presentati dal trattamento di dati personali.

La DPIA è uno strumento importante in termini di *accountability* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni.

Il GDPR prevede che, se necessario, il titolare del trattamento proceda a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

L’art. 35, par.3, GDPR fornisce alcuni esempi nei quali un trattamento può presentare rischi elevati. Tale elenco non è esaustivo, potendoci essere ulteriori trattamenti, non ricompresi nel predetto elenco, che possono comunque presentare rischi elevati per gli interessati.

Sull’argomento, un importante guida e supporto viene fornita dalle Linee Guida WP 248 rev. 01 del 04.04.2017 del WP 29 (Gruppo di Lavoro articolo 29 per la protezione dei dati), le quali forniscono una serie di criteri specifici per individuare i trattamenti che possono presentare rischi elevati per gli interessati.

Nel caso oggetto della presente valutazione l’obbligatorietà della stessa è prevista direttamente dal legislatore ed in particolare dall’art. 13 co. 6 del d.lgs. 10 marzo 2023, n. 24.

Normativa di riferimento

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- D.lgs n.196/2003 s.m.i. (c.d. Codice Privacy);
- Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 (WP 248) adottate il 04 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.
- Standard ISO.

A cosa serve la Valutazione di Impatto privacy

Le Linee Guida in materia di valutazione d'impatto sulla protezione dei dati adottate dal Gruppo di Lavoro dei Garanti Europei (WP 248 rev.01/2017) precisano che una valutazione d'impatto sulla protezione dei dati **è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.**

La valutazione d'impatto sulla protezione dei dati è uno **strumento** importante per la **responsabilizzazione** (c.d. Accountability tool) in quanto sostiene i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24).

In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

I Garanti Europei illustrano nel seguente modo il processo di una Valutazione di impatto privacy:

1. CONTESTO DEL TRATTAMENTO

1.1. Descrizione del trattamento

Il Regolamento Generale sulla protezione dei dati definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 7, e considerando 84 e 90):

- *"una descrizione dei trattamenti previsti e delle finalità del trattamento";*
- *"una valutazione della necessità e proporzionalità dei trattamenti";*
- *"una valutazione dei rischi per i diritti e le libertà degli interessati";*
- *"le misure previste per:*
    - *"affrontare i rischi";*
    - *"dimostrare la conformità al presente regolamento".*

Il trattamento oggetto di valutazione di impatto privacy (c.d. Data Protection Impact Assessment – DPIA) resa ai sensi dell'art. 35 Regolamento (UE) 2016/679 (GDPR) è ***la procedura di ricezione e gestione interna delle segnalazioni di illeciti - whistleblowing (di seguito "Procedura Whistleblowing")*** che il Comune ha definito con deliberazione della Giunta comunale n. 26 di data 19.02.2026 in attuazione del decreto legislativo 10 marzo 2023 n. 24 che ha recepito nel nostro ordinamento la 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.

Tenuto conto della propria realtà organizzativa e delle previsioni di legge, lette anche alla luce delle "*Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione* delle *segnalazioni esterne*" approvate dall'Autorità Nazionale Anticorruzione con delibera n. 311 del 12.07.2023 e le successive Linee guida sui Canali interni di segnalazione, adottate con delibera n. 478 del 26.11.2025, (di seguito "Linee Guida ANAC), il Comune ha ritenuto di adottare i seguenti canali interni di segnalazione:

- in forma scritta, attraverso l'utilizzo di una procedura informatica. L'accesso alla procedura informatica avviene tramite il link pubblicato nel portale dell'Ente, alla pagina dedicata in Amministrazione trasparente – sezione Altri contenuti - Prevenzione della corruzione: segnalazione scritta mediante piattaforma web-app WhistleblowingPA;
- in forma orale, attraverso la linea telefonica, contattando direttamente l'RPCT ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole;

di seguito al singolare "Segnalazione" e al plurale "Segnalazioni".

Il trattamento dati connesso ai canali di Segnalazione è espressamente soggetto a DPIA secondo quanto previsto dall'art. 13, comma 6, d.lgs. 24/2023.

Si precisa che non vi sono codici di condotta ai sensi dell'art. 40 GDPR nè meccanismi di certificazione ai sensi dell'art. 42 GDPR applicabili.

Per quanto riguarda la segnalazione mediante piattaforma, la stessa si basa sul software open source di Globaleaks, il quale presenta 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- ACN;
- Certificazione CSA Star.

1.2. Finalità del trattamento

Il trattamento di dati connessi alla Procedura Whistleblowing è finalizzato all'esclusiva gestione ed istruttoria delle Segnalazioni di whistleblowing tramite i canali interni istituiti dal Comune di Avio in adempimento degli obblighi di legge.

La base giuridica del trattamento, a seconda della tipologia di dati trattati, è costituita da:

i. per i dati "comuni", dall'adempimento degli obblighi di legge gravanti sul titolare e dall'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lettera c) ed e) GDPR – d.lgs. 24/2023);

ii. per i dati particolari ex art. 9 GDPR, dalla necessità di assolvere gli obblighi ed esercitare i diritti del titolare o dell'interessato in materia di diritto del lavoro e da motivi di interesse pubblico rilevante (art. 9, par. 2 lettera b) e g) GDPR – art. 2 sexies del d.lgs. 196/2003);

iii. per i dati relativi a condanne ex art. 10 GDPR, per adempiere un obbligo di legge gravante sul titolare (art. 10 GDPR – 2 octies d.lgs. 196/2003).

1.3. Soggetti e ruoli del trattamento

Il titolare del trattamento è il Comune di Avio, in persona del Sindaco, con sede in Piazza V. Emanuele III n. 1, Avio (di seguito anche solo il "Comune" o il "Titolare del trattamento").

Il Comune di Avio, anche alla luce delle Linee Guida ANAC, ha affidato la gestione delle Segnalazioni al proprio Responsabile della Prevenzione della Corruzione e della Trasparenza (di seguito "RPCT").

Per quanto riguarda la segnalazione mediante piattaforma, Whistleblowing Solutions I.S. s.r.l. è il responsabile del trattamento per la fornitura e gestione del sistema. Seeweb s.r.l. è sub responsabile del trattamento nominato da Whistleblowing Solutions per la gestione dell'infrastruttura (attività di trattamento demandate: archiviazione, hosting, cloud, iass). Transparency International Italia è sub responsabile del trattamento nominato da Whistleblowing Solutions per la collaborazione nella gestione del sistema (attività di trattamento demandate: supporto utenti, amministratore di Sistema).

1.4. Tipologia di dati trattati

I dati oggetto di trattamento possono essere costituiti da:

- dati personali diversi da particolari categorie di dati (c.d. dati comuni). La tipologia di dati trattati, a titolo meramente esemplificativo, comprende le informazioni identificative come nome, cognome, matricola o altro numero di identificazione, codice fiscale, dati anagrafici e relativi all'ubicazione, dati sullo svolgimento della prestazione lavorativa nonché altri dati ai sensi dell'art. 4 par. 1 n. 1 del Regolamento;
- dati personali appartenenti a particolari categorie di dati (c.d. dati sensibili). La tipologia di dati trattati, a titolo meramente esemplificativo, comprende quelli che possano rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la vita sessuale l'orientamento sessuale, ed altri dati ai sensi dell'art. 9 par. 1 e 2 del Regolamento;
- dati personali relativi a condanne penali e reati (c.d. dati giudiziari). La tipologia di dati trattati, a titolo meramente esemplificativo, comprende quelli concernenti i precedenti penali, l'esercizio dell'azione penale, il

rinvio a giudizio, le sentenze di condanna e assimilabili, le archiviazioni di procedimenti penali, l'applicazione delle misure di sicurezza e delle misure cautelari ed altri dati ai sensi dell'art. 10 del Regolamento;

- dati relativi allo stato di salute, genetici, biometrici (c.d. dati supersensibili). La tipologia di dati trattati, a titolo meramente esemplificativo, comprende i dati attinenti alla salute fisica o mentale, compresa la prestazione di servizi di assistenza sanitaria che rivelano informazioni relative allo stato di salute ed altri dati ai sensi dell'art. 4 nn. 13, 14 e 15 del Regolamento,

del segnalante, del segnalato e/o di altri soggetti menzionati all'interno della segnalazione.

1.5. Categoria di interessati al trattamento

I soggetti interessati al trattamento possono essere i seguenti:

- **Segnalante:** persona fisica che effettua la segnalazione nell'ambito del contesto lavorativo con il Comune. Alla luce della normativa vigente, possono assumere il ruolo di Segnalante i seguenti soggetti:
  - dipendenti dell'Ente anche se in servizio presso altre Pubbliche Amministrazioni in posizione di comando, distacco (o situazioni analoghe);
  - lavoratori autonomi, collaboratori, liberi professionisti, tirocinanti, volontari che svolgono o prestano attività presso l'Ente;
  - i dipendenti delle società in house, degli organismi di diritto pubblico o dei concessionari di pubblico servizio, nonché i dipendenti di società ed enti di diritto privato sottoposto a controllo pubblico da parte dell'Ente, limitatamente a violazioni che coinvolgono l'Ente;
  - lavoratori o collaboratori che svolgono la propria attività lavorativa presso soggetti del settore pubblico che forniscono beni o servizi o che realizzano opere in favore di terzi;
  - persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza presso l'Ente o di altri soggetti del settore pubblico, limitatamente a violazioni che coinvolgono l'Ente;
- **persona coinvolta nella Segnalazione**: persona a cui viene attribuita la violazione/illecito nella Segnalazione o che è comunque implicata nella violazione segnalata;
- **facilitatore**: persona fisica che assiste una persona segnalante nel processo di segnalazione operante all'interno del medesimo contesto lavorativo;
- **persone diverse dal Segnalato ma comunque menzionate nella Segnalazione** (ad esempio persone indicate come testimoni).

1.6. Ciclo di vita del trattamento

La procedura si compone delle seguenti fasi:

1 - Avvio della Procedura: la Segnalazione

A) Segnalazione mediante piattaforma *WhistleblowingPA*

Invio di una Segnalazione mediante la Piattaforma, inserendo i dati e le informazioni richieste dai vari campi. Alcuni dati sono facoltativi di default, altri campi sono obbligatori.

La Piattaforma permette anche la presentazione di segnalazioni anonime, integrabili eventualmente con i dati personali in un secondo momento.

B) Segnalazione orale mediante linea telefonica

Segnalazione effettuata telefonicamente, contattando direttamente l'RPCT.

C) Segnalazione orale mediante incontro diretto

Incontro diretto con il RPCT su richiesta del Segnalante.

2 - Analisi e verifica dell'ammissibilità della Segnalazione – istruttoria

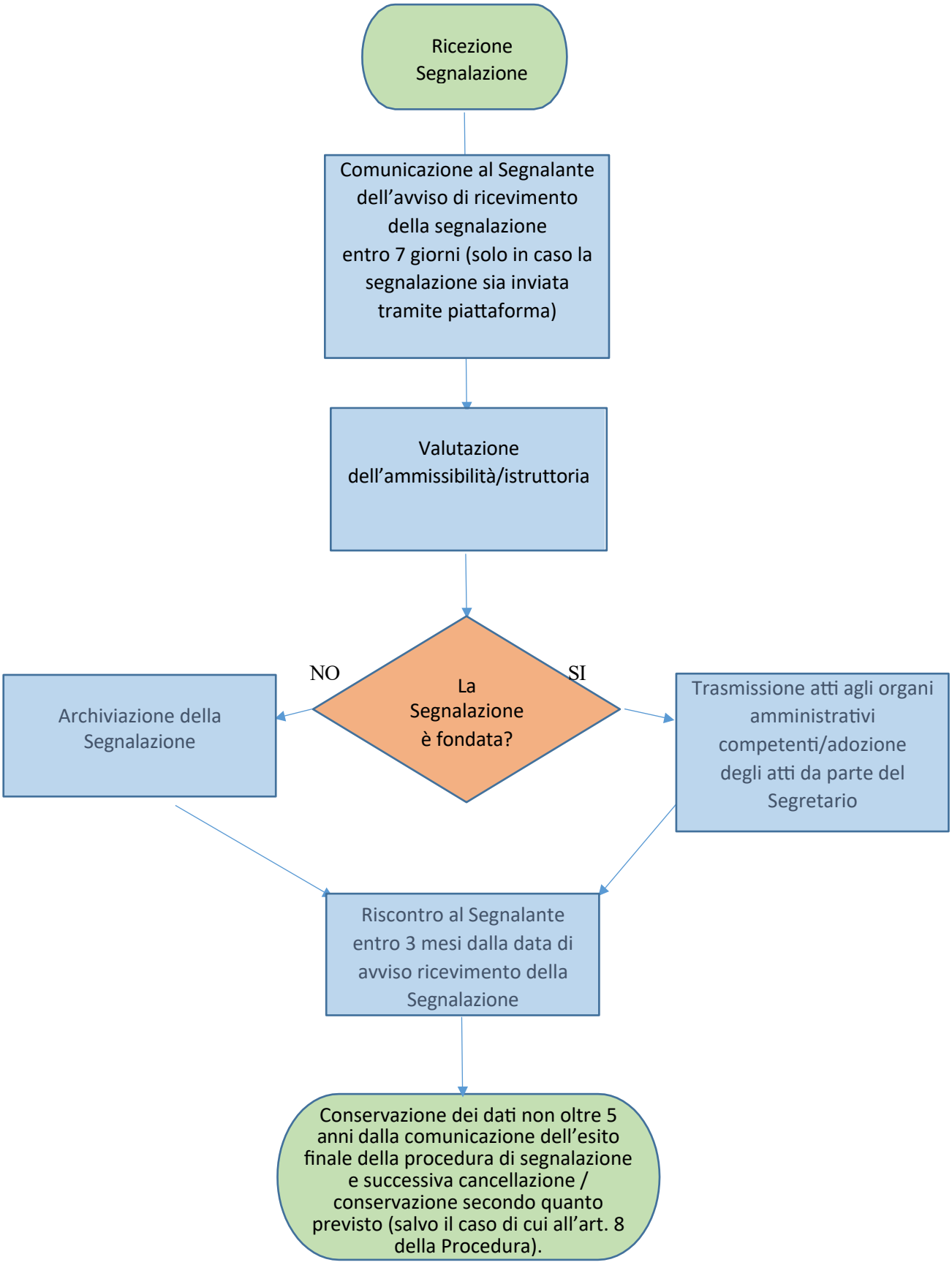
L'RPCT procede all'esame degli elementi essenziali della Segnalazione, al fine di vagliarne l'ammissibilità ed accordare le tutele previste dalla legge. Qualora la Segnalazione sia inammissibile, l'RPCT provvede all'archiviazione della Segnalazione. In caso contrario si avvia l'istruttoria interna.

3 - Valutazione conclusiva

L'RPCT, una volta ultimata l'attività di accertamento, potrà archiviare la Segnalazione oppure considerarla fondata e trasmetterla agli organi amministrativi competenti o adottando direttamente gli atti di propria competenza, dandone riscontro in ogni caso al Segnalante tramite la Piattaforma oppure tramite comunicazione diretta con il Segnalante, in caso di segnalazione orale.

4 - Cancellazione dati

Decorso il termine di legge i dati verranno cancellati o conservati secondo quanto previsto dal Manuale di gestione documentale del Comune di Avio, approvato con deliberazione della Giunta comunale n. 60 di data 26.06.2025.



FLUSSO DEI DATI PERSONALI

1.7. Periodo di conservazione dei dati

Le Segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque fino al tempo massimo di 5 (cinque) anni dalla data della comunicazione dell'esito finale della segnalazione, nel rispetto di quanto previsto dall'art.14, comma 1, d.lgs. 24/2023. Per quanto riguarda la segnalazione mediante piattaforma, la stessa prevede una data retention di default di 12 mesi, prorogabile più volte dal Gestore.
Resta fermo che laddove la segnalazione dia avvio ad un procedimento disciplinare, i relativi atti (tra cui la segnalazione, secondo quanto previsto dall'art. 8 della Procedura di segnalazione) sono conservati permanentemente secondo quanto previsto Manuale di gestione documentale del Comune di Avio, approvato con deliberazione della Giunta comunale n. 60 di data 26.06.2025.

1.8. Risorse di supporto dei dati

La procedura di gestione delle segnalazioni si avvale dei seguenti supporti, a seconda del tipo di canale scelto dal Segnalante:

1) soluzione applicativa WhistleblowingPA basata sul software open source Globaleaks;

- ARCHITETTURA DI SISTEMA: l'architettura di sistema è principalmente composta da:
  - un cluster di due firewall perimetrali;
  - un cluster di due server fisici dedicati;
  - una Storage Area Network pienamente ridondata
- ARCHITETTURA DI RETE: firewall perimetrale
- PC in uso al Gestore delle segnalazioni per l'accesso via web alla Piattaforma;

Per quanto riguarda la segnalazione mediante piattaforma, si rinvia al documento allegato di supporto elaborato da Whistleblowing Solutions (allegato alla presente e comunque reperibile, unitamente ad altra documentazione utile, al seguente link: WBIT documentazione tecnica).

2) verbale cartaceo in caso di segnalazione orale mediante incontro diretto / telefonico.

In entrambi i casi la segnalazione è poi protocollata tramite Pitre dal RPCT in via riservata, in modo da garantirne la massima riservatezza. Si evidenzia come l'RPCT sia l'unico soggetto abilitato ad accedere a tali documenti una volta acquisiti in Pitre, in quanto gli stessi sono protocollati dal solo RPCT che li marca come "privati", precludendo dunque la visibilità a qualunque altro ruolo.

2. PRINCIPI FONDAMENTALI

2.1 Proporzionalità e necessità

VALUTAZIONE DELLE FINALITA' DEL TRATTAMENTO

Il trattamento è necessario per gli adempimenti degli obblighi di legge che gravano sul titolare del trattamento ai sensi del d.lgs. 24/2023.

Valutazione: accettabile, il trattamento è finalizzato all'adempimento degli obblighi di legge.

BASE GIURIDICA DEL TRATTAMENTO

La base giuridica del trattamento, a seconda della tipologia di dati trattati, è costituita da:

- per i dati "comuni", dall'adempimento degli obblighi di legge gravanti sul titolare e dall'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lettera c) ed e) GDPR – d.lgs. 24/2023);
- per i dati particolari ex art. 9 GDPR, dalla necessità di assolvere gli obblighi ed esercitare i diritti del titolare o dell'interessato in materia di diritto del lavoro e da motivi di interesse pubblico rilevante (art. 9, par. 2 lettera b) e g) GDPR – art. 2 sexies del d.lgs. 196/2003);
- per i dati relativi a condanne ex art. 10 GDPR, per adempiere un obbligo di legge gravante sul titolare (art. 10 GDPR – 2 octies d.lgs. 196/2003).

Non è quindi previsto il consenso degli interessati ad eccezione dei seguenti casi:

- nella segnalazione orale mediante incontro diretto, il Gestore può verbalizzare l'incontro, la relativa sottoscrizione da parte del Segnalante potrà avvenire solo col consenso dello stesso, che sarà documentato in modo adeguato;
- nel caso in cui sia avviato un procedimento disciplinare nei confronti del Segnalato, la contestazione si basi in tutto o in parte sulla segnalazione e la conoscenza dell'identità del Segnalante sia necessaria per la difesa dell'incolpato. In questo caso verrà data comunicazione scritta al Segnalante e gli verrà chiesto di prestare o meno il suo consenso espresso e in forma scritta alla rivelazione della propria identità.

Valutazione: accettabile, le basi giuridiche corrispondono a quanto indicato dal Garante per la protezione dei dati nel parere sulle Linee Guida ANAC del 6 luglio 2023.

VALUTAZIONE DEL RISPETTO DEL PRINCIPIO DI MINIMIZZAZIONE DEI DATI

La procedura prevede, nel rispetto della legge e per entrambe le modalità di segnalazione, il trattamento dei soli dati strettamente necessari alla valutazione e gestione delle Segnalazioni. La Piattaforma è configurata chiedendo, attraverso la compilazione dei form, la comunicazione dei soli dati necessari. In caso di forma orale sarà l'RPCT a verbalizzare i soli dati necessari.

Valutazione: accettabile

VALUTAZIONE DEL RISPETTO DEL PRINCIPIO DI ESATTEZZA DEI DATI

Il Segnalante, qualsiasi modalità di segnalazione scelga, può sempre integrare/rettificare una propria segnalazione. La Piattaforma raccoglie esattamente i dati comunicati dal Segnalante.

Valutazione: accettabile

VALUTAZIONE DEL RISPETTO DEL PRINCIPIO DI CONSERVAZIONE DEI DATI

I dati vengono conservati per il tempo necessario per la gestione della Segnalazione e comunque per il tempo massimo previsto dalla legge.

Qualora la segnalazione comporti l'instaurazione di un contenzioso o un procedimento disciplinare nei confronti del Segnalato o del Segnalante, i dati saranno conservati in via permanente secondo quanto previsto dal Manuale di gestione documentale del Comune di Avio, approvato con deliberazione della Giunta comunale n. 60 di data 26.06.2025 e dall'art. 8 della Procedura di Segnalazione.

Valutazione: accettabile, il periodo di conservazione corrisponde alle tempistiche previste dalla legge e, nel caso di contenzioso o di procedimento disciplinare, a quanto necessario alla tutela dell'Ente.

2.2 Proporzionalità e necessità

INFORMAZIONI PER GLI INTERESSATI

Il Comune, nel rispetto degli articoli 13 e 14 GDPR, informerà gli interessati mediante specifica informativa sul trattamento dati pubblicata sul sito internet istituzionale (alla stessa pagina che riporta al link della Piattaforma). Per inviare la segnalazione mediante piattaforma è necessario dichiarare di aver preso visione della privacy policy tramite l'apposito flag. In caso di segnalazione orale sarà onere del RPCT informare il segnalante sull'esistenza e sulla reperibilità dell'informativa. In casi estremi l'RPCT procederà a dare lettura dell'informativa.

Valutazione: accettabile, le modalità di informativa sono conformi alle prescrizioni di legge.

ESERCIZIO DEL DIRITTO DI ACCESSO E DI PORTABILITÀ DEI DATI

Diritto di accesso

Il segnalante, come dettagliatamente indicato nell'informativa sul trattamento dei dati personali, può sempre esercitare il diritto di accesso ai propri dati personali. I diritti che il segnalato o altri soggetti terzi menzionati nella segnalazione possono esercitare sono i medesimi accordati al segnalante. La facoltà di esercitare tali diritti può tuttavia subire delle limitazioni. Ai sensi dell'art. 2 – undecies del Codice Privacy, così come modificato dal D. Lgs. 24/2023, i diritti sopra menzionati non possono essere esercitati, né facendo richiesta al titolare del trattamento, né proponendo un reclamo all'Autorità Garante per la protezione dei dati personali, se dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona segnalante. In tali casi, questi diritti possono essere esercitati tramite il Garante per la protezione dei dati personali con le modalità dell'art. 160 del D. Lgs. 196/2003.

Diritto di portabilità

Il diritto di portabilità non è in concreto esercitabile, stante la tipologia di trattamento, il quale non rientra nei casi di cui all'art. 20 GDPR.

Valutazione: Accettabile. I limiti indicati sono necessari – e previsti direttamente dalla legge – per tutelare l'identità del segnalante.

ESERCIZIO DEL DIRITTO DI RETTIFICA E DI CANCELLAZIONE (DIRITTO ALL'OBLIO)

Il Segnalante, come indicato nell'informativa sul trattamento dei dati personali, può sempre in autonomia modificare o ritirare una segnalazione accedendo direttamente alla Piattaforma / richiedendolo al RPCT in caso di segnalazione orale. Ai sensi di quanto previsto dall'art. 2 - undecies d.lgs. 196/2003, la persona coinvolta o la persona menzionata nella Segnalazione, con riferimento ai propri dati personali trattati nell'ambito della Segnalazione, divulgazione pubblica o denuncia, non può esercitare il diritto né facendo richiesta al titolare del trattamento, né proponendo un reclamo all'Autorità Garante per la protezione dei dati personali, se dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona segnalante. In tali casi, questi diritti possono essere esercitati tramite il Garante per la protezione dei dati personali con le modalità dell'art. 160 del D. Lgs. 196/2003.

Valutazione: Accettabile. I limiti indicati sono necessari – e previsti direttamente dalla legge – per tutelare l'identità del segnalante.

ESERCIZIO DEL DIRITTO DI LIMITAZIONE E DI OPPOSIZIONE

Ai sensi di quanto previsto dall'art. 2 - undecies d.lgs. 196/2003, la persona coinvolta o la persona menzionata nella Segnalazione, con riferimento ai propri dati personali trattati nell'ambito della Segnalazione, divulgazione pubblica o denuncia, non può esercitare il diritto né facendo richiesta al titolare del trattamento, né proponendo un reclamo all'Autorità Garante per la protezione dei dati personali, se dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona segnalante. In tali casi, questi diritti possono essere esercitati tramite il Garante per la protezione dei dati personali con le modalità dell'art. 160 del D. Lgs. 196/2003.

Valutazione: Accettabile. I limiti indicati sono necessari – e previsti direttamente dalla legge – per tutelare l'identità del segnalante.

RESPONSABILI DEL TRATTAMENTO: VERIFICHE SUI CONTRATTI DI NOMINA A RESPONSABILE DEL TRATTAMENTO

Per quanto riguarda la segnalazione mediante piattaforma, è stata sottoscritta la nomina a responsabile del trattamento con WHISTLEBLOWING SOLUTIONS I.S. s.r.l., la quale comprende l'autorizzazione alla nomina a sub responsabili del trattamento di Seeweb s.r.l. e Transparency International Italia, per i trattamenti di competenza.

Nel caso di segnalazione orale direttamente al RPCT non sono presenti responsabili esterni del trattamento.

Valutazione: accettabile

TRASFERIMENTI VERSO PAESI EXTRA UE: RISPETTO DELLE PRESCRIZIONI DI LEGITTIMITA'

I dati personali oggetto di trattamento non sono trasferiti verso Paesi Extra Ue.

Valutazione: accettabile

3. RISCHI – VALUTAZIONE DELE MISURE ESITENTI E PIANIFICATE (con riferimento ad entrambe le modalità di segnalazione)

Misure esistenti o pianificate	Descrizione	Valutazione	Riferimento a piattaforma (P), forma orale (O), comune ad entrambe (C)	Commento di valutazione	Piano d'azione
Crittografia	Con riferimento al canale di segnalazione interno in forma scritta mediante la piattaforma, 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	Accettabile	P		

	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/stable/security/EncryptionProtocol.html				
Controllo degli accessi logici	L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. L'RPCT è l'unico soggetto in possesso della password per accedere alla piattaforma. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione eventuale a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.	Accettabile	P		Adottare entro il 2026 apposito disciplinare sulle misure di sicurezza informatiche ed organizzative
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	Accettabile	P		

	confidenzialità richiesta dal processo di whistleblowing. Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse. 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 nella piattaforma	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.	Accettabile	P		
Archiviazione della segnalazione	La segnalazione (sia acquisita tramite piattaforma, sia il verbale in caso di segnalazione orale) sarà protocollata	Accettabile	C		

	esclusivamente dal RPCT, che sarà anche l'unico soggetto abilitato ad avere accesso al documento nel programma di protocollo informatico.				
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/stable/security/PenetrationTests.html	Accettabile	P		
Back up	I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo	Accettabile	P		

	dunque una RPO di 8 ore.				
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.	Accettabile	P		
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.	Accettabile	P		
Sicurezza dell'hardware	I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di	Accettabile	P		

	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.				
Gestione incidenti degli incidenti di sicurezza e delle violazioni dei dati personali	Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.	Accettabile	P		
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.	Accettabile	P		
Misure addizionali	Whistleblowing Solutions con la documentazione presente sul proprio sito, 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	Accettabile	P		

	- WHISTLEBLOWINGIT				
Contratto con il responsabile del trattamento	E' stata sottoscritta la nomina con Whistleblowing Solutions	Accettabile	P		
Sicurezza della conservazione dei documenti cartacei	In caso di incontro in presenza, il verbale cartaceo e ogni altra documentazione cartacea verrà conservata in un armadio/cassetto chiuso a chiave e accessibile solo al RPCT. Come già indicato, inoltre, i documenti sono protocollati esclusivamente dal RPCT marcandoli come "privati" e dunque accessibili solo allo stesso.	Accettabile	O		
Riservatezza colloquio orale	L'eventuale colloquio orale (in presenza o telefonicamente) con il segnalante si svolgerà in un locale chiuso, alla presenza del solo RPCT e con l'adozione di tutte le misure necessarie (es. porta chiusa e tono di voce adeguato) affinché nessun altro possa sentire quanto riferito.	Accettabile	O		
Politica di tutela della privacy	Il Comune ha designato il DPO il quale è stato coinvolto nell'impostazione del sistema di gestione delle segnalazioni	Accettabile	C		

Gestione delle politiche di tutela della privacy	Il Comune gestisce tutti gli aspetti privacy con il supporto del DPO, il quale svolge periodici audit documentati	Accettabile	C		
Gestione dei rischi	Il Comune ha censito tutti i trattamenti svolti e ha adottato il registro delle attività di trattamento ai sensi dell'art. 30 GDPR.	Accettabile	C		
Integrare la protezione della privacy nei progetti	La procedura per la gestione delle segnalazioni è stata impostata con particolare attenzione alla protezione dei dati, tenendo in considerazione la normativa, le linee guida vigenti e le indicazioni del Garante per la protezione dei dati personali, scegliendo una piattaforma qualificata CAN.	Accettabile	C		
Gestire gli incidenti di sicurezza e le violazioni di dati personali	Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali. Anche il Comune ha adottato un proprio protocollo (Procedura per la gestione della violazione dei dati personali – Data Breach)	Accettabile	C		
Gestione del personale	Il RPCT, gestore delle segnalazioni, è	Accettabile	C		

	stato autorizzato al trattamento ai sensi dell'art. 2 quarter decies d.lgs. 196/2003- art. 29 GDPR				
Gestione dei terzi che accedono ai dati	La Procedura prevede espressamente che in caso di coinvolgimento di terzi nell'istruttoria siano oscurati/espunti tutti i dati personali relativi alle persone tutelate dalla legge. Si vedano poi le misure di tutela previste dalla normativa. Il personale eventualmente coinvolto è in ogni caso nominato e formato.	Accettabile	C		
Vigilanza sulla protezione dei dati	Il Comune provvederà nel tempo a valutare il livello di protezione dei dati correlato alla procedura di gestione delle segnalazioni mediante audit del DPO, adottando se nel caso le misure necessarie.	Accettabile	C		

4. VALUTAZIONE DEI RISCHI

Si riporta di seguito la valutazione dei rischi, in termini di Gravità dell'impatto sugli interessati, tenuto conto delle misure esistenti o programmate, e Probabilità che si verifichi il rischio, in termini di livello di vulnerabilità dei supporti e sistemi, sempre alla luce delle misure esistenti o programmate.

La **Gravità** dell'impatto viene valutata secondo la seguente scala.

TRASCURABILE	gli interessati potrebbero non subire alcuna conseguenza o potrebbero andare incontro ad alcuni inconvenienti, che saranno in grado comunque di superare senza problemi
LIMITATA	gli interessati potrebbero subire inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà
SIGNIFICATIVA	gli interessati potrebbero subire significative conseguenze che saranno in grado di superare con serie e reali difficoltà
MASSIMA	gli interessati potrebbero subire significativi, o anche irreversibili conseguenze, che potrebbero non essere in grado di superare

La **Probabilità** delle minacce viene valutata secondo la seguente scala:

TRASCURABILE	non sembra possibile, per la fonte di rischio valutata, di generare la minaccia sfruttando le proprietà dei supporti esistenti
LIMITATA	sembra difficile, per la fonte di rischio valutata, di generare la minaccia sfruttando le proprietà dei supporti esistenti
SIGNIFICATIVA	sembra possibile, per la fonte di rischio valutata, di generare la minaccia sfruttando le proprietà dei supporti esistenti
MASSIMA	sembra estremamente semplice, per la fonte di rischio valutata, di generare la minaccia sfruttando le proprietà dei supporti esistenti

Vengono presi in considerazione i rischi di:

- accesso illegittimo ai dati;
- modifiche indesiderate dei dati;
- perdita dei dati.

ACCESSO ILLEGITTIMO AI DATI

Impatti principali sugli interessati qualora il rischio dovesse concretizzarsi

In caso di accesso illegittimo ai dati ed in particolare alle generalità del Segnalante/Segnalato lo stesso potrebbe subire degli impatti significativi in quanto verrebbe meno la tutela della riservatezza garantita dalla legge. Per quanto riguarda il Segnalante, lo stesso potrebbe provare uno stato di preoccupazione ed ansia derivante dal timore di subire ritorsioni di varia natura da parte del Comune per il fatto della segnalazione, fermo restando che la legge, proprio al fine di tutelare il Segnalante, prevede delle forme di protezione dalle eventuali ritorsioni che il Segnalante dovesse subire, anche in forma tentata, incluse anche sanzioni pecuniarie nei confronti del responsabile delle ritorsioni.

Il Segnalato potrebbe parimenti subire uno stato di ansia e preoccupazione derivante da una possibile compromissione della propria reputazione aziendale o timore di subire ritorsioni, forme di mobbing da parte di colleghi, ecc.

Gli stessi timori potrebbero essere provati dagli altri soggetti contemplati nella Segnalazione o a cui la normativa estende il regime di protezione.

Principali minacce che potrebbero concretizzare il rischio

Avvenuta conoscenza delle credenziali di autenticazione per l'accesso alla Piattaforma da parte di terzi non autorizzati e conseguente accesso.
Ascolto dell'incontro in presenza o della segnalazione telefonica da parte di terzi non autorizzati.
Entrare in contatto con l'eventuale copia cartacea del verbale / con eventuali stampe.
Virus informatici

Fonti di rischio

Fonti umane interne ed esterne (RPCT, collaboratori, dipendenti, consulenti IT negligenti o malevoli, terzi non autorizzati che accedano in modo malevolo, hacker).
Fonti non umane esterne: virus informatici in generale

Misure che contribuiscono a mitigare il rischio

Nel caso di segnalazione mediante piattaforma: crittografia, controllo degli accessi logici, tracciabilità, minimizzazione dei dati, archiviazione, contratto con il responsabile del trattamento, vulnerabilità, lotta contro il malware, gestione postazioni, sicurezza dei siti web, manutenzione, sicurezza dei canali informatici, controllo degli accessi fisici, sicurezza dell'hardware, prevenzione delle fonti di rischio, protezione contro fonti di rischio non umane, politica di tutela della privacy, integrare la protezione della privacy nei progetti, gestire gli incidenti di sicurezza e le violazioni dei dati personali, gestione del personale, gestione dei terzi che accedono ai dati; vigilanza sulla protezione dei dati; attenzione ad eventuali stampe.

Nel caso di segnalazione in forma orale: minimizzazione dei dati, archiviazione, sicurezza dei documenti cartacei, vulnerabilità, lotta contro il malware, gestione postazioni, manutenzione, sicurezza dei canali informatici, controllo degli accessi fisici, sicurezza dell'hardware, prevenzione delle fonti di rischio, protezione contro fonti di rischio non umane, politica di tutela della privacy, integrare la protezione della privacy nei progetti, gestire gli incidenti di sicurezza e le violazioni dei dati personali, gestione del personale, gestione dei terzi che accedono ai dati, vigilanza sulla protezione dei dati, adozione di tutte le misure necessarie alla riservatezza del colloquio orale (colloquio in un locale chiuso, alla presenza del solo RPCT e con l'adozione di tutte le misure necessarie es. porta chiusa e tono di voce adeguato affinché nessun altro possa sentire quanto riferito) e alla custodia dei documenti cartacei (da conservarsi sotto chiave accessibili solo al RPCT).

Stima gravità del rischio, alla luce degli impatti potenziali delle misure pianificate
Gravità **LIMITATA** alla luce delle misure di protezione in essere, tenuto conto anche dei rimedi e garanzie di protezione previste dalla normativa vigente.

Stima probabilità del rischio, con riguardo alle minacce, alle fonti di rischio e alle misure pianificate
Probabilità **TRASCURABILE** alla luce delle misure di protezione in essere, in particolare della crittografia dei dati e dell'autenticazione a due fattori (per la segnalazione tramite piattaforma) e delle modalità concrete di trattamento da parte del solo RPCT (per la segnalazione orale).

Valutazione: accettabile
Commento di valutazione: il rischio complessivo derivante da un accesso illegittimo ai dati è **limitato**, tenuto conto delle misure di sicurezza adottate.

MODIFICHE INDESIDERATE DEI DATI

Impatti principali sugli interessati qualora il rischio dovesse concretizzarsi
In caso di modifica dei dati del Segnalante, il Segnalante potrebbe subire un disagio limitato quale ad esempio l'impossibilità o difficoltà per il Gestore di contattarlo per eventuali chiarimenti, difficoltà superabile dal fatto che il Segnalante potrà in ogni momento chiedere un riscontro o un aggiornamento, comunicando i dati corretti, in modo agevole e senza particolari perdite di tempo, e rettificare in autonomia il contenuto della segnalazione o i dati, accedendo alla Piattaforma o comunicandolo al RPCT.

Ancora, in caso di modifiche dei dati di altri soggetti inseriti nella Segnalazione, l'RPCT potrebbe avere delle difficoltà nell'esecuzione dell'istruttoria, e il Segnalante potrebbe provare un disagio psicologico derivante dal fatto che l'RPCT non potrebbe dare adeguato seguito alla Segnalazione stessa. Anche in questo caso il disagio correlato alla necessità di dover conferire nuovamente i dati modificati è molto limitato.

Principali minacce che potrebbero concretizzare il rischio
Per entrambe le modalità: modifica accidentale dei dati da parte dei soggetti autorizzati o da soggetti non autorizzati; virus informatici in generale.

Fonti di rischio
Fonti umane interne ed esterne (RPCT, collaboratori, dipendenti, consulenti IT negligenti o malevoli, terzi non autorizzati che accedano in modo malevolo, hacker).
Fonti non umane esterne: virus informatici in generale

Misure che contribuiscono a mitigare il rischio
Nel caso di segnalazione mediante piattaforma: controllo degli accessi logici, tracciabilità, archiviazione, sicurezza dei documenti cartacei, vulnerabilità, lotta contro il malware, gestione postazioni, sicurezza dei siti web, backup, manutenzione, sicurezza dei canali informatici, manutenzione, sicurezza dell'hardware, controllo degli accessi fisici, prevenzione delle fonti di rischio, protezione contro fonti di rischio non umane, politica di tutela della privacy, integrare la protezione della privacy nei progetti, gestire gli incidenti di sicurezza e le violazioni dei dati, gestione del personale, vigilanza sulla protezione dei dati, sicurezza dei canali informatici, contratto con il responsabile del trattamento, gestione delle politiche di tutela della privacy, gestione dei rischi, politica di tutela della privacy; adozione specifica procedura di *data breach*.

Nel caso di segnalazione in forma orale: archiviazione, sicurezza dei documenti cartacei, vulnerabilità, lotta contro il malware, gestione postazioni, sicurezza dei siti web, backup, manutenzione, sicurezza dei canali informatici, manutenzione, sicurezza dell'hardware, controllo degli accessi fisici, prevenzione delle fonti di rischio, protezione contro fonti di rischio non umane, politica di tutela della privacy, integrare la protezione della privacy nei progetti, gestire gli incidenti di sicurezza e le violazioni dei dati, gestione del personale, vigilanza sulla protezione dei dati, sicurezza dei canali informatici, contratto con il responsabile del trattamento, gestione delle politiche di tutela della privacy, gestione dei rischi, politica di tutela della privacy, custodia sotto chiave accessibile al RPCT dei documenti cartacei; adozione specifica procedura di *data breach*.

Stima gravità del rischio, alla luce degli impatti potenziali delle misure pianificate
Gravità **TRASCURABILE**, considerate le misure di sicurezza adottate e tenuto conto che sono dati che il Segnalante può nuovamente conferire senza particolari disagi.

Stima probabilità del rischio, con riguardo alle minacce, alle fonti di rischio e alle misure pianificate
Probabilità **TRASCURABILE**, considerate le misure di sicurezza adottate.

Valutazione: accettabile

Commento di valutazione: il rischio complessivo di modifica dei dati è **trascurabile**, tenuto conto delle misure di sicurezza in essere

PERDITA DEI DATI

Impatti principali sugli interessati qualora il rischio dovesse concretizzarsi
In caso di perdita dei dati, il Segnalante potrebbe subire un disagio limitato derivante dal fatto che l'RPCT potrebbe avere difficoltà oppure l'impossibilità di gestire la Segnalazione, disagio comunque superabile per il fatto che il Segnalante può sempre integrare la propria segnalazione, fornendo nuovamente i dati al RPCT, o effettuarne una nuova, con un disagio limitato.

Principali minacce che potrebbero concretizzare il rischio
Per entrambe le modalità: attacco informatico, cancellazione accidentale dei dati, danneggiamenti del data center, perdita del verbale cartaceo non ancora protocollato.

Fonti di rischio.
Fonti umane interne ed esterne (RPCT, collaboratori, dipendenti, consulenti IT negligenti o malevoli, terzi non autorizzati che accedano in modo malevolo, hacker).
Fonti non umane esterne (es. virus informatico, incendio, fulmine od altri eventi)

Misure che contribuiscono a mitigare il rischio
Nel caso di segnalazione mediante piattaforma: controllo degli accessi logici, tracciabilità, vulnerabilità, archiviazione, back up, manutenzione, contratto con il responsabile del trattamento, sicurezza dei canali informatici, sicurezza dell'hardware, gestire gli incidenti di sicurezza e le violazioni dei dati, lotta contro il malware, sicurezza dei siti web, controllo degli accessi fisici, protezione contro fonti di rischio non umane, integrare la protezione della privacy nei progetti, gestione del personale, prevenzione delle fonti di rischio, politica di tutela della privacy, sicurezza dei documenti cartacei, gestione postazioni, gestione dei rischi, vigilanza sulla protezione dei dati, adozione specifica procedura di *data breach*.

Nel caso di segnalazione orale: controllo degli accessi logici, tracciabilità, vulnerabilità, archiviazione, back up, manutenzione, contratto con il responsabile del trattamento, sicurezza dei canali informatici, sicurezza dell'hardware, gestire gli incidenti di sicurezza e le violazioni dei dati, lotta contro il malware, sicurezza dei siti web, controllo degli accessi fisici, protezione contro fonti di rischio non umane, integrare la protezione della privacy nei progetti, gestione del personale, prevenzione delle fonti di rischio, politica di tutela della privacy, sicurezza dei documenti cartacei, gestione postazioni, gestione dei rischi, vigilanza sulla protezione dei dati, adozione specifica procedura di *data breach*.

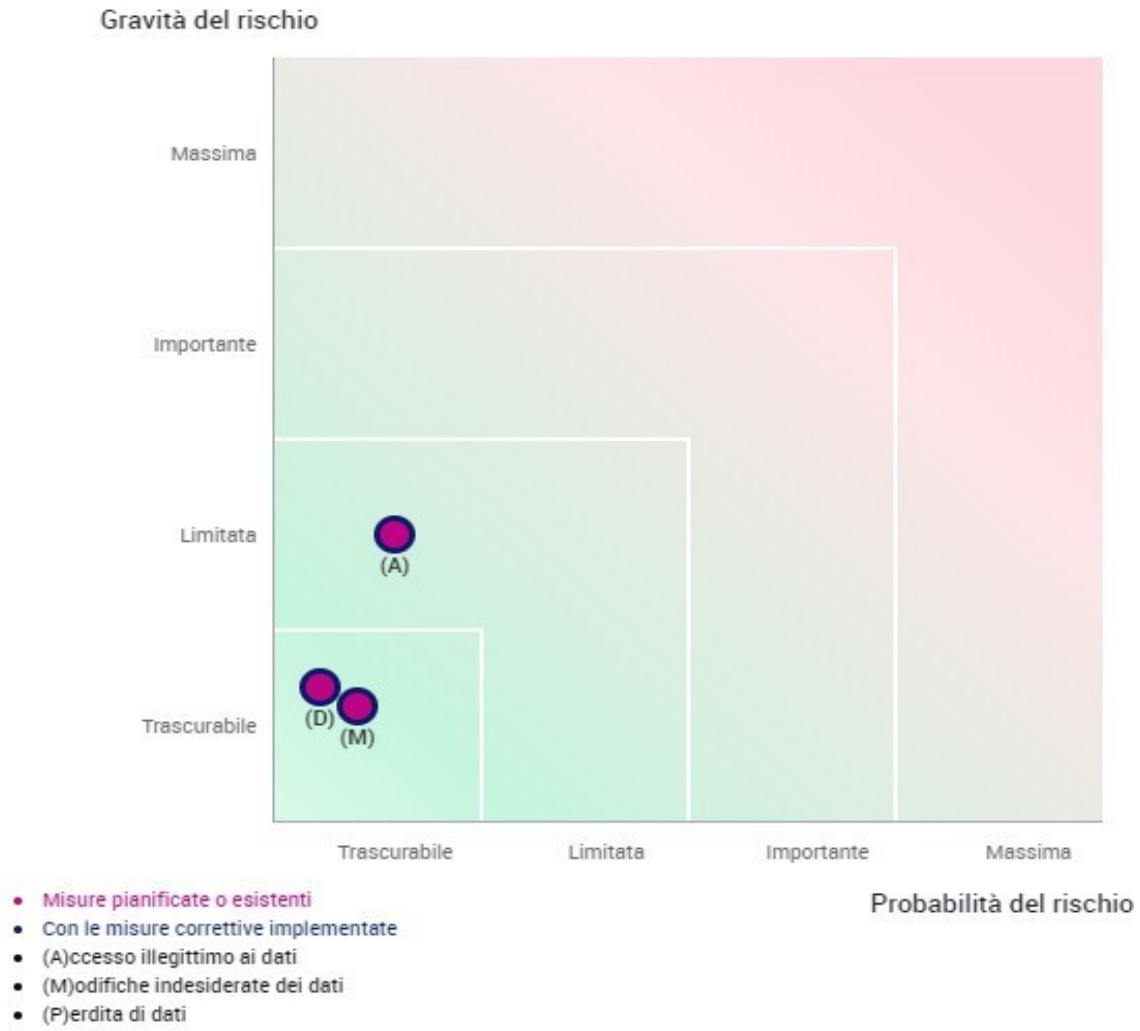
Stima gravità del rischio, alla luce degli impatti potenziali delle misure pianificate
Gravità **TRASCURABILE** in quanto le misure di protezione sono adeguate.

Stima probabilità del rischio, con riguardo alle minacce, alle fonti di rischio e alle misure pianificate
Probabilità **TRASCURABILE** in quanto le misure di protezione sono adeguate, tenuto conto delle misure di sicurezza relative al data center

Valutazione: accettabile

Commento di valutazione: il rischio complessivo derivante dalla perdita dei dati è ritenuto **trascurabile**, tenuto conto delle misure di sicurezza adottate.

MAPPATURA DEI RISCHI



****

5. PIANO D'AZIONE

Il presente documento sarà tempestivamente aggiornato in caso di necessità o di variazioni.

Entro l'anno 2026 sarà adottato, quale ulteriore misura di mitigazione del rischio, apposito disciplinare sulle misure di sicurezza informatiche ed organizzative.

6. PARERE DEL DPO

Il DPO, dott.ssa Laura Marinelli, esprime parere favorevole alla valutazione d'impatto sulla protezione dei dati effettuata in riferimento ai trattamenti dati relativi alla gestione delle segnalazioni di illeciti - whistleblowing in quanto conformi alle previsioni di legge.

7. RICHIESTA DEL PARERE DEGLI INTERESSATI

Per quanto riguarda la richiesta di parere degli interessati si evidenzia che, secondo quanto previsto dall'art. 4 co. 1 del d.lgs. 24/2023, dell'intenzione di adottare la procedura di segnalazione è stata data informativa preventiva alle OO.SS. maggiormente rappresentative a livello provinciale.
In risposta non sono pervenute osservazioni.

8. CONCLUSIONI e VALIDAZIONE DPIA

Il Comune, in persona del Segretario comunale, valida la presente DPIA.
Il trattamento è finalizzato all'adempimento degli obblighi di legge che gravano sul Comune.
La procedura è stata impostata nel rispetto delle prescrizioni di legge e delle indicazioni di cui alle Linee Guida ANAC.
La configurazione del sistema, le misure di sicurezza applicate, rendono il trattamento conforme ai diritti e principi fondamentali in materia di protezione dei dati personali. I rischi per i diritti e le libertà degli interessati, a seguito delle misure di sicurezza adottate, possono essere qualificati come accettabili in relazione alle finalità perseguite dal trattamento.
Di conseguenza, non essendoci un rischio elevato, non è necessario procedere alla consultazione del Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR.

FRACCHETTI
IVANO
09.06.2026
13:58:45
GMT+02:00

Il Sindaco
Ivano Fracchetti
(documento firmato digitalmente)

***