

COMUNE DI ORTACESUS

Procedura per la gestione delle segnalazioni interne whistleblowing

ai sensi del D.Lgs. 10 marzo 2023, n. 24

Campo	Valore
Ente	Comune di Ortacesus
Responsabile della prevenzione della corruzione e della trasparenza (RPCT) / Gestore	RPCT pro tempore del Comune di Ortacesus
Sostituto del gestore in caso di conflitto o assenza	Soggetto preventivamente individuato dall'atto organizzativo
RPD/DPO	RPD/DPO pro tempore; recapiti pubblicati nella sezione Privacy/Amministrazione trasparente del sito istituzionale
Atto di approvazione	Atto organizzativo di adozione del sistema whistleblowing
Versione	Luglio 2026

Approvata con deliberazione di Giunta comunale n. 32 del 30.07.2026

Indice

1. Premessa, fonti e finalità
2. Adozione della procedura, aggiornamento e coordinamento con PIAO e Codice di comportamento
3. Ambito soggettivo e soggetti protetti
4. Ambito oggettivo, esclusioni e segnalazioni anonime
5. Canali interni di segnalazione
6. Gestore del canale, struttura di supporto, conflitto di interessi e sostituzione
7. Ricezione e gestione della segnalazione
8. Riservatezza, tutele, divieto di ritorsione e procedimento disciplinare
9. Trattamento dei dati personali, sicurezza e conservazione
10. Canale esterno ANAC, divulgazione pubblica e denuncia
11. Pubblicità, formazione, monitoraggio e riesame

Allegati operativi A-H, contenuti in separato documento allegato alla presente procedura

1. Premessa, fonti e finalità

La presente procedura disciplina il canale interno di segnalazione del Comune di Ortacesus per la ricezione, la valutazione e la gestione delle segnalazioni di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione, secondo il decreto legislativo 10 marzo 2023, n. 24.

La procedura è costruita assumendo come base le indicazioni operative dell'Autorità Nazionale Anticorruzione e del Garante per la protezione dei dati personali, adattate alla struttura organizzativa comunale, al ruolo del RPCT, alla disciplina privacy, al PIAO, al Codice di comportamento e ai processi documentali e informatici dell'Ente.

Fonti principali

D.Lgs. 24/2023; Direttiva (UE) 2019/1937; L. 190/2012; D.P.R. 62/2013; D.Lgs. 165/2001; D.Lgs. 33/2013; L. 241/1990; GDPR; D.Lgs. 196/2003; Linee guida ANAC Delibera n. 311/2023, come modificate dalla Delibera n. 479/2025; Linee guida ANAC n. 1/2025 sui canali interni, Delibera n. 478/2025; provvedimento/parere del Garante per la protezione dei dati personali n. 581 del 9 ottobre 2025; principi organizzativi UNI ISO 37002:2021 come best practice non vincolante.

La procedura persegue finalità di prevenzione della corruzione, dell'illegalità e della cattiva amministrazione, tutela della persona segnalante e degli altri soggetti protetti, corretta gestione delle informazioni acquisite e rafforzamento dell'integrità organizzativa del Comune.

La conformità della presente procedura deve essere valutata non solo sul piano documentale, ma anche in relazione alla concreta effettività del canale, alla riservatezza assicurata nella pratica, alla formazione del personale, alla sicurezza della piattaforma e alla tracciabilità riservata delle attività del gestore.

2. Adozione, aggiornamento e coordinamento organizzativo

La procedura è adottata con atto organizzativo del Comune dopo il coinvolgimento preventivo delle rappresentanze o organizzazioni sindacali ai sensi dell'art. 4, comma 1, del D.Lgs. 24/2023. Il coinvolgimento ha carattere informativo e interlocutorio: prima dell'approvazione l'Ente trasmette il testo della procedura e le informazioni essenziali sul canale, assegna un termine congruo e non perentorio per eventuali osservazioni, che non hanno natura vincolante, e manifesta la disponibilità a un incontro. Nel fascicolo sono conservati la comunicazione, la prova di ricezione, le eventuali osservazioni o l'attestazione del decorso del termine e la relativa valutazione. Gli aggiornamenti sostanziali sono sottoposti al medesimo passaggio.

La procedura è coordinata con il PIAO, sottosezione "Rischi corruttivi e trasparenza", con il Codice di comportamento del Comune, con le misure di sicurezza informatica, con la gestione documentale, con le istruzioni privacy interne e con gli eventuali contratti o atti di nomina dei fornitori coinvolti.

3. Ambito soggettivo e soggetti protetti

3.1 Persone che possono effettuare segnalazioni

Possono utilizzare il canale interno del Comune le persone che abbiano acquisito informazioni sulle violazioni nell'ambito del proprio contesto lavorativo o professionale con l'Ente, anche quando il rapporto non sia ancora iniziato o sia cessato.

- dipendenti del Comune, a tempo indeterminato o determinato, anche in comando, distacco, assegnazione temporanea o altre forme di utilizzo;
- Segretario comunale, responsabili di servizio/area, titolari di incarichi di Elevata Qualificazione e personale comunque operante presso il Comune;
- lavoratori autonomi, collaboratori, consulenti, liberi professionisti e altri soggetti che prestano attività presso o in favore del Comune;

- lavoratori e collaboratori degli operatori economici che forniscono beni, servizi o lavori in favore del Comune;
- volontari e tirocinanti, retribuiti e non retribuiti;
- persone coinvolte in procedure selettive, precontrattuali o di affidamento, se le informazioni sono state acquisite in tale fase;
- persone il cui rapporto con il Comune sia cessato, se le informazioni sono state acquisite nel corso del rapporto;
- persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza presso il Comune, nei limiti in cui rientrano nell'ambito soggettivo del D.Lgs. 24/2023.

3.2 Soggetti protetti diversi dalla persona segnalante

Le misure di protezione si applicano, ricorrendone i presupposti di legge, anche ai facilitatori, alle persone del medesimo contesto lavorativo legate alla persona segnalante da stabile legame affettivo o parentela entro il quarto grado, ai colleghi con rapporto abituale e corrente, agli enti di proprietà della persona segnalante o per i quali essa lavora e agli enti che operano nel medesimo contesto lavorativo.

4. Ambito oggettivo, esclusioni e segnalazioni anonime

4.1 Violazioni segnalabili

Possono essere oggetto di segnalazione informazioni, compresi fondati sospetti, riguardanti violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità del Comune, conosciute nel contesto lavorativo o professionale.

Rientrano nel perimetro, nei limiti dell'art. 2 del D.Lgs. 24/2023 e con riferimento al settore pubblico: gli illeciti amministrativi, contabili, civili o penali; gli illeciti che rientrano nell'ambito degli atti dell'Unione europea o nazionali indicati dal decreto, tra cui contratti pubblici, servizi e mercati finanziari, prevenzione del riciclaggio, sicurezza e conformità dei prodotti, trasporti, ambiente, radioprotezione e sicurezza nucleare, alimenti e mangimi, salute e benessere animale, salute pubblica, protezione dei consumatori, tutela della vita privata, protezione dei dati personali e sicurezza delle reti e dei sistemi informativi; gli atti od omissioni che ledono gli interessi finanziari dell'Unione, il mercato interno o che vanificano oggetto e finalità delle disposizioni richiamate, sempreché le informazioni siano acquisite nel contesto lavorativo e la violazione leda l'interesse pubblico o l'integrità dell'Ente. I riferimenti alle condotte e ai modelli di cui al D.Lgs. 231/2001 non sono pertinenti al Comune e non integrano autonomamente l'ambito oggettivo del canale comunale.

4.2 Esclusioni

Non rientrano nella presente procedura le contestazioni, rivendicazioni o richieste aventi carattere esclusivamente personale e attinenti al rapporto individuale di lavoro o di impiego pubblico, né le doglianze relative ai rapporti con superiori gerarchici o colleghi prive di collegamento con l'interesse pubblico o con l'integrità dell'amministrazione.

Sono escluse o restano regolate dalle rispettive discipline speciali: le contestazioni esclusivamente personali relative al rapporto individuale di lavoro prive di rilievo per l'interesse pubblico; le segnalazioni in materia di sicurezza nazionale e gli appalti relativi ad aspetti di difesa o sicurezza nazionale, salvo quanto coperto dal diritto dell'Unione; le informazioni classificate; il segreto professionale forense e medico; la segretezza delle deliberazioni degli organi giurisdizionali; le norme di procedura penale e l'autonomia della magistratura; i reclami privacy, le istanze di esercizio dei diritti, le richieste di accesso e i reclami sindacali o lavoristici quando non contengano una violazione rilevante ai sensi del D.Lgs. 24/2023. Il gestore, senza pregiudicare la riservatezza, può indirizzare l'interessato verso il canale competente.

4.3 Contenuto minimo della segnalazione

La segnalazione deve essere il più possibile circostanziata. È utile che indichi la descrizione dei fatti, le circostanze di tempo e luogo, i soggetti coinvolti o altri elementi identificativi, eventuali persone informate sui fatti, documenti o riscontri disponibili e ogni ulteriore informazione utile alla valutazione.

La mancanza di uno o più elementi non determina automaticamente l'esclusione dal perimetro. Quando la comunicazione consente una verifica preliminare, il gestore richiede, ove possibile, integrazioni attraverso il canale riservato. L'archiviazione per genericità o insufficiente circostanziazione è adottata solo dopo avere valutato la possibilità di integrazione, oppure quando gli elementi risultino oggettivamente inadatti a consentire verifiche, con motivazione riservata e tracciata.

4.4 Segnalazioni anonime

Le segnalazioni dalle quali non sia possibile ricavare l'identità della persona segnalante sono considerate anonime. Se circostanziate, sono esaminate come segnalazioni ordinarie riservate e sono registrate e conservate con modalità idonee a consentirne il successivo reperimento. La registrazione riporta un codice, la data, il canale, l'oggetto sintetico, lo stato e l'esito, senza introdurre dati identificativi non disponibili.

Qualora l'autore della segnalazione anonima sia successivamente identificato e comunichi di avere subito ritorsioni in ragione della segnalazione, la segnalazione e la relativa documentazione devono poter essere ricondotte al caso originario, ai fini dell'applicazione delle tutele previste dal D.Lgs. 24/2023. A tal fine la documentazione anonima è conservata nel rispetto del termine massimo applicabile e delle cautele di riservatezza.

4.5 Condizioni per beneficiare delle tutele

Le misure di protezione si applicano quando, al momento della segnalazione, denuncia o divulgazione pubblica, la persona aveva fondato motivo di ritenere che le informazioni fossero vere e rientrassero nell'ambito del D.Lgs. 24/2023 e abbia utilizzato uno dei canali o delle modalità previsti dalla legge. I motivi personali della segnalazione sono irrilevanti. Le tutele non coprono informazioni manifestamente false, mere supposizioni prive di elementi o acquisizioni illecite non scriminate dalla legge.

5. Canali interni di segnalazione

5.1 Canale scritto principale: piattaforma informatica dedicata

Il canale scritto principale del Comune è costituito dalla piattaforma WhistleblowingPA, servizio SaaS gratuito basato sul software open source GlobalLeaks, raggiungibile dalla sezione "Whistleblowing" del sito istituzionale all'indirizzo <https://comunediorlacesus.whistleblowing.it>. Il canale assicura la riservatezza dell'identità della persona segnalante, della persona coinvolta, degli altri soggetti menzionati, del contenuto della segnalazione e della documentazione allegata.

La piattaforma deve prevedere misure coerenti con il rischio, tra cui cifratura dei dati in transito e a riposo, segregazione degli accessi, autenticazione del gestore, tracciamento degli accessi autorizzati, non tracciabilità della persona segnalante nella fase di accesso al canale, disponibilità del servizio, backup, continuità e gestione sicura degli allegati. La non tracciabilità deve essere verificata anche rispetto ai sistemi sotto il controllo dell'Ente - sito, cookie e strumenti analytics, DNS, proxy, firewall, apparati di rete, sistemi di sicurezza, SIEM e log applicativi - evitando la raccolta o correlazione di IP, user agent e metadati non necessari.

La piattaforma consente alla persona segnalante di compilare un percorso guidato, allegare eventuale documentazione, ricevere un codice identificativo univoco e mantenere, ove previsto dalla configurazione del servizio, un'interlocazione riservata con il RPCT/gestore del canale.

Il codice identificativo deve essere conservato con cura dalla persona segnalante, poiché consente di accedere alla segnalazione, monitorarne lo stato, rispondere a eventuali richieste di chiarimenti e integrare la documentazione. In caso di smarrimento del codice, il Comune potrebbe non essere in grado di ripristinare l'accesso alla segnalazione attraverso il medesimo canale, in ragione delle misure tecniche poste a tutela della riservatezza.

Qualora la piattaforma utilizzata consenta modalità di accesso rafforzate o strumenti ulteriori di tutela della riservatezza, anche rispetto all'indirizzo IP o ad altri metadati tecnici, il Comune ne dà informazione nella pagina dedicata, fermo restando che tali strumenti non sostituiscono gli obblighi del Comune in materia di protezione dei dati personali, sicurezza del canale, DPIA, nomina del fornitore quale responsabile del trattamento e verifica delle misure tecniche e organizzative.

La PEC del protocollo generale, le caselle e-mail ordinarie del Comune e le caselle personali non costituiscono canali ordinari di segnalazione. Tali strumenti possono compromettere la riservatezza dell'identità della persona segnalante e degli altri soggetti coinvolti.

Il Comune utilizza la piattaforma WhistleblowingIT, fornita in modalità SaaS da Whistleblowing Solutions Impresa Sociale S.r.l., Viale Abruzzi 13/A, 20131 Milano, C.F./P.IVA 09495830961, accessibile all'indirizzo <https://comunedioracesus.whistleblowing.it>. Il servizio impiega GlobaLeaks e la filiera documentata comprende Seeweb S.r.l. per l'infrastruttura IaaS e Transparency International Italia per il supporto alla gestione. Il Comune conserva contratto, nomina ex art. 28 GDPR, accordi di sub-responsabilità e documentazione tecnica aggiornata.

5.2 Canale orale e incontro diretto

Il Comune assicura la modalità orale mediante incontro diretto con il RPCT/gestore, su richiesta della persona segnalante. La richiesta può essere presentata tramite la piattaforma <https://comunedioracesus.whistleblowing.it>, inserendo esclusivamente la richiesta di colloquio e un recapito sicuro, oppure mediante plico chiuso riservato al RPCT. L'incontro è fissato entro un termine ragionevole e si svolge in un ambiente idoneo a garantire riservatezza. La segnalazione è documentata mediante registrazione, previo consenso, oppure mediante verbale sottoposto a verifica, rettifica e sottoscrizione della persona segnalante. La versione gratuita WhistleblowingPA non include la messaggistica vocale né la funzione nativa di richiesta di contatto diretto; tali funzionalità non sono pertanto dichiarate come attive.

Della segnalazione orale è redatto verbale, sottoposto alla persona segnalante per verifica, rettifica e conferma. Se il canale prevede registrazione, questa è effettuata solo nei limiti consentiti dalla legge, previa informazione e consenso della persona segnalante ove richiesto.

Il verbale della segnalazione orale è conservato con le medesime cautele previste per le segnalazioni scritte e non è inserito nel protocollo generale o in fascicoli ordinari accessibili a soggetti non autorizzati. La persona segnalante riceve indicazioni sulle modalità con cui potrà ricevere l'avviso di ricevimento, fornire integrazioni e ottenere il riscontro nei termini previsti dalla legge.

5.3 Modalità cartacea residuale

In via residuale, la segnalazione può essere presentata mediante plico cartaceo riservato indirizzato al RPCT/gestore. Il plico deve riportare all'esterno la dicitura "Riservata personale - segnalazione whistleblowing - non aprire al protocollo generale".

La persona segnalante può inserire in una prima busta separata i propri dati identificativi e, solo quando strettamente necessario per verificarne l'identità e senza automatismi, un documento o altro elemento idoneo; in una seconda busta inserisce la segnalazione e l'eventuale documentazione. Le due buste sono collocate in una terza busta chiusa indirizzata al RPCT/gestore. La mancata produzione della copia del documento non comporta di per sé l'inammissibilità e resta sempre possibile la segnalazione anonima circostanziata. Il protocollo registra esclusivamente l'involucro esterno, senza aprire le buste interne, e lo trasmette immediatamente al gestore per la registrazione riservata.

Qualora il plico sia erroneamente aperto da personale non competente, il soggetto che ne prende conoscenza deve interrompere ogni ulteriore trattamento, non effettuare copie, non diffondere il contenuto e trasmettere immediatamente la documentazione al RPCT/gestore, dando evidenza riservata dell'accaduto. L'episodio è valutato dal Comune anche ai fini dell'eventuale gestione come incidente di riservatezza o violazione di dati personali.

5.4 Segnalazioni ricevute da soggetti non competenti

Qualora una segnalazione sia presentata a un soggetto diverso dal RPCT/gestore e la persona segnalante dichiara espressamente di voler beneficiare delle tutele whistleblowing, o tale volontà sia desumibile dal contenuto della comunicazione, dall'oggetto, dalla modulistica o dal richiamo alla normativa, il destinatario la trasmette senza ritardo e comunque entro sette giorni al RPCT/gestore, dando contestuale notizia della trasmissione alla persona segnalante, ove possibile.

Se la comunicazione è inviata contemporaneamente a più soggetti interni, ciascun destinatario non competente applica la medesima regola di trasmissione riservata al gestore entro sette giorni e cancella le copie non necessarie. Se la comunicazione è stata inviata anche a un numero elevato di destinatari esterni, il gestore chiede chiarimenti, ove possibile, e valuta se ricorrano le condizioni della divulgazione pubblica ai sensi dell'art. 15 del D.Lgs. 24/2023, senza presumere automaticamente la perdita delle tutele.

Il destinatario non competente non deve svolgere valutazioni sul merito, non deve trattenere copie, non deve protocollare il contenuto in modalità ordinaria, non deve diffondere la comunicazione e deve mantenere la massima riservatezza sull'identità della persona segnalante e sugli altri soggetti coinvolti.

6. Gestore del canale, supporto, conflitto di interessi

6.1 Gestore del canale interno

La gestione del canale interno è affidata al Responsabile della prevenzione della corruzione e della trasparenza del Comune (RPCT), quale gestore delle segnalazioni. Il gestore opera con autonomia, imparzialità e indipendenza, senza interferenze dell'organo di indirizzo nella gestione delle singole segnalazioni.

Il gestore deve possedere competenze adeguate in materia di prevenzione della corruzione, procedimento amministrativo, riservatezza, protezione dei dati personali, sicurezza delle informazioni e gestione delle segnalazioni.

6.2 Struttura di supporto

Il Comune può individuare, con atto organizzativo, una struttura di supporto al RPCT/gestore. L'atto deve indicare nominativamente o per posizione organizzativa ciascun componente, le attività attribuite, i limiti di accesso e le responsabilità; i componenti devono possedere autonomia rispetto ai casi trattati, competenza e formazione specifica, essere autorizzati al trattamento ai sensi degli artt. 29 e 32, par. 4, GDPR e dell'art. 2-quaterdecies del Codice Privacy e accedere esclusivamente alle informazioni necessarie. Non è ammessa una generica abilitazione dell'intero ufficio.

6.3 RPD/DPO

Il Responsabile della protezione dei dati personali non è individuato quale gestore ordinario del canale interno. Il RPD/DPO è coinvolto, secondo il proprio ruolo consultivo e di sorveglianza, per gli aspetti inerenti alla DPIA, alle misure tecniche e organizzative, all'informativa, alle autorizzazioni interne, alla nomina dei responsabili del trattamento e al monitoraggio della conformità privacy.

6.4 Conflitto di interessi e assenza del gestore

In caso di conflitto di interessi del RPCT/gestore, anche potenziale o apparente, ovvero quando la segnalazione riguardi direttamente il gestore, la gestione è attribuita al sostituto individuato preventivamente nell'atto organizzativo. Il sostituto possiede requisiti di autonomia, imparzialità, indipendenza, competenza e formazione analoghi, è autorizzato al trattamento e accede al sistema esclusivamente durante la sostituzione. In caso di assenza superiore a sette giorni si applica la medesima regola.

In caso di assenza prolungata del gestore, ordinariamente superiore a sette giorni, di impedimento o di altra temporanea impossibilità di gestione, le funzioni sono esercitate dal sostituto. L'accesso del sostituto al canale e alla documentazione è consentito esclusivamente nei casi di effettiva sostituzione, mediante credenziali personali e nel rispetto dei principi di necessità, minimizzazione e tracciabilità riservata. Qualora anche il sostituto versi in conflitto di interessi o non sia possibile assicurare una gestione interna indipendente, la persona segnalante è informata della possibilità di ricorrere al canale esterno ANAC nei casi previsti dalla legge.

7. Ricezione e gestione della segnalazione

7.1 Fasi operative

Fase	Presidio operativo
1. Ricezione	Acquisizione tramite canale dedicato, attribuzione del codice identificativo univoco ove previsto dalla piattaforma, segregazione documentale, verifica del canale di provenienza e prima tutela della riservatezza.
2. Avviso	Avviso di ricevimento entro sette giorni dalla ricezione.
3. Valutazione preliminare	Verifica preliminare di ambito soggettivo, oggettivo, circostanziazione, competenza e conflitti.
4. Istruttoria	Richiesta di integrazioni tramite il canale riservato, acquisizione selettiva di elementi, eventuale coinvolgimento di uffici/autorità solo per quanto strettamente necessario e, ove possibile, mediante informazioni anonimizzate o minimizzate.
5. Esito	Archiviazione motivata, misure organizzative, trasmissione agli organi competenti o alle autorità.
6. Riscontro	Riscontro alla persona segnalante entro tre mesi, nei limiti della riservatezza.
7. Conservazione	Conservazione riservata non oltre cinque anni dalla comunicazione dell'esito finale.

7.2 Avviso di ricevimento

Il gestore rilascia alla persona segnalante avviso di ricevimento entro sette giorni dalla ricezione della segnalazione. L'avviso ha natura meramente informativa e non implica alcuna valutazione sulla fondatezza, ammissibilità o rilevanza della segnalazione.

7.3 Verifica preliminare e istruttoria

Il gestore svolge una verifica preliminare sulla sussistenza dei presupposti soggettivi e oggettivi, sulla sufficiente circostanziazione dei fatti e sull'eventuale presenza di conflitti di interessi. Se necessario, mantiene le interlocuzioni con la persona segnalante e richiede integrazioni attraverso il canale prescelto.

Quando la segnalazione è presentata tramite piattaforma informatica, le interlocuzioni successive avvengono, di regola, attraverso l'area riservata associata al codice identificativo della segnalazione, evitando l'utilizzo di canali ordinari non progettati per garantire la riservatezza.

Il gestore può acquisire informazioni, documenti e chiarimenti dagli uffici comunali o da soggetti esterni, limitando la circolazione delle informazioni a quanto strettamente necessario e utilizzando, ove possibile, estratti anonimizzati o privi di elementi identificativi della persona segnalante.

L'accesso all'identità della persona segnalante è consentito solo quando strettamente necessario per la gestione del caso o nei casi previsti dalla legge. Ogni accesso o rivelazione deve essere motivato, limitato ai soggetti legittimati e registrato in un log o verbale riservato che indichi data, soggetto, presupposto e finalità, senza rendere tali informazioni accessibili a utenti non autorizzati.

7.4 Esiti possibili

All'esito dell'istruttoria, il gestore può archiviare la segnalazione con motivazione riservata; trasmettere gli elementi pertinenti all'ufficio o organo interno competente per misure organizzative, correttive o disciplinari; trasmettere gli atti all'autorità giudiziaria, contabile, amministrativa o ad altra autorità competente, ove ne ricorrano i presupposti.

Al gestore non compete l'accertamento definitivo di responsabilità individuali né l'adozione di provvedimenti disciplinari, gestionali, contabili o giudiziari, rimessi agli organi e agli uffici competenti. Il gestore non deve essere utilizzato come centro decisionale sostitutivo degli uffici competenti, né l'organo di indirizzo può interferire nella valutazione delle singole segnalazioni.

7.5 Riscontro entro tre mesi

Il gestore fornisce riscontro alla persona segnalante entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione. Il riscontro può consistere nella comunicazione dell'archiviazione, della trasmissione agli organi o enti competenti, dell'avvio o prosecuzione di attività istruttorie o delle misure che si intendono adottare, nei limiti compatibili con la riservatezza, la protezione dei dati personali e il corretto svolgimento dei procedimenti conseguenti.

8. Riservatezza, tutele, divieto di ritorsione e procedimento disciplinare

8.1 Riservatezza dell'identità

L'identità della persona segnalante e qualsiasi informazione da cui essa possa essere desunta, direttamente o indirettamente, non possono essere rivelate senza il consenso espresso della stessa, salvo i casi previsti dalla legge. Sono tutelati anche l'identità della persona coinvolta, delle persone menzionate nella segnalazione e degli altri soggetti protetti.

Quando la rivelazione dell'identità o di informazioni riservate sia necessaria nei casi previsti dal D.Lgs. 24/2023, il gestore dà avviso scritto alla persona segnalante delle ragioni della rivelazione, nei limiti consentiti dalla legge.

8.2 Procedimento disciplinare

Nell'ambito del procedimento disciplinare, qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa della persona incolpata, la segnalazione è utilizzabile solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.

La persona coinvolta può essere sentita ovvero, su sua richiesta, è sentita anche mediante procedimento cartolare, attraverso l'acquisizione di osservazioni scritte e documenti, nei limiti compatibili con la riservatezza della persona segnalante e con le esigenze istruttorie.

8.3 Divieto di ritorsione

È vietato qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, denuncia o divulgazione pubblica e che provochi o possa provocare alla persona segnalante o agli altri soggetti protetti un danno ingiusto, diretto o indiretto.

Le comunicazioni di ritorsioni devono essere trasmesse ad ANAC, quale autorità competente. Il Comune pubblica nella sezione dedicata del sito istituzionale le informazioni sul canale ANAC e sulle modalità di comunicazione delle ritorsioni.

8.4 Responsabilità della persona segnalante

Le tutele non sono garantite quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o calunnia, oppure la responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave. In tali ipotesi alla persona segnalante o denunciante è inoltre irrogata una sanzione disciplinare, quando applicabile, secondo l'art. 16, comma 3, del D.Lgs. 24/2023 e le garanzie del relativo procedimento.

9. Trattamento dei dati personali, sicurezza e conservazione

9.1 Ruoli privacy e basi giuridiche

Il Comune di Ortacesus è titolare del trattamento dei dati personali connessi alla ricezione e gestione delle segnalazioni interne. I dati sono trattati esclusivamente per le finalità previste dal D.Lgs. 24/2023 e nei limiti necessari alla gestione della segnalazione, alla tutela della persona segnalante e degli altri soggetti protetti, nonché all'eventuale adozione degli atti conseguenti da parte degli uffici o autorità competenti.

Il trattamento può riguardare dati personali comuni, categorie particolari di dati e dati relativi a condanne penali e reati, nei limiti di pertinenza e necessità rispetto alla segnalazione. I dati manifestamente non utili alla trattazione della segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati senza ritardo.

9.2 DPIA, registro trattamenti e informativa

Prima dell'attivazione o dell'aggiornamento sostanziale del canale, conformemente all'art. 13 co. 6 del D.Lgs. 24/2023, il Comune effettua o aggiorna la valutazione d'impatto sulla protezione dei dati personali ai sensi dell'art. 35 GDPR, aggiorna il registro delle attività di trattamento e rende apposita informativa agli interessati. La DPIA deve considerare almeno: natura dei dati trattati, rischi di identificazione o ritorsione, accessi autorizzati, canali utilizzati, piattaforma, conservazione, eventuali trasferimenti, subfornitori, misure di sicurezza, gestione dei log, metadati tecnici, indirizzi IP, eventuali strumenti di tracciamento, modalità di autenticazione, cancellazione, backup, continuità del servizio e incident response.

9.3 Fornitore della piattaforma e art. 28 GDPR

Whistleblowing Solutions Impresa Sociale S.r.l. è designata responsabile del trattamento ai sensi dell'art. 28 GDPR per la fornitura e gestione della piattaforma WhistleblowingIT. La filiera comprende Seeweb S.r.l. e Transparency International Italia quali sub-responsabili nei limiti degli accordi conservati nel fascicolo. Le variazioni della filiera sono registrate e valutate dal Comune.

Il servizio è erogato in modalità SaaS. Il Comune conserva la documentazione aggiornata del fornitore sulle misure tecniche, sulle certificazioni e qualificazioni dichiarate, sulla localizzazione dei dati, sulla continuità, sui backup e sugli incidenti. Tali evidenze integrano, senza sostituirle, la DPIA, la nomina ex art. 28 GDPR e le verifiche locali di non tracciabilità.

9.4 Autorizzazioni interne e riservatezza

Il personale eventualmente coinvolto a supporto del gestore è previamente autorizzato al trattamento ai sensi dell'art. 29 GDPR e dell'art. 2-quaterdecies del D.Lgs. 196/2003, riceve istruzioni specifiche e documentate, è formato e accede solo alle informazioni strettamente necessarie. Gli accessi sono limitati, profilati e verificabili.

9.5 Conservazione e cancellazione

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario alla trattazione e comunque non oltre cinque anni dalla comunicazione dell'esito finale. La piattaforma applica una scadenza tecnica predefinita di dodici mesi, che il gestore riesamina almeno trimestralmente, può anticipare sino a tre mesi o prorogare motivatamente entro il limite legale. Decorso il termine, originali e copie sono cancellati o distrutti in modo sicuro e l'operazione è annotata nel registro riservato. Gli atti autonomi di eventuali procedimenti conseguenti seguono le rispettive discipline senza incorporare, salvo stretta necessità, identità e segnalazione integrale.

9.6 Accesso documentale, civico e diritti privacy

La segnalazione e la documentazione che consente di identificare la persona segnalante sono sottratte all'accesso documentale di cui agli artt. 22 e ss. della L. 241/1990 e all'accesso civico semplice e generalizzato di cui al D.Lgs. 33/2013, nei limiti previsti dall'art. 12, comma 8, D.Lgs. 24/2023.

Nei casi previsti dall'art. 2-undecies del D.Lgs. 196/2003, i diritti di cui agli artt. 15-22 GDPR non possono essere esercitati mediante richiesta al Titolare né mediante reclamo ai sensi dell'art. 77 GDPR qualora dal loro esercizio possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona segnalante. I diritti possono essere esercitati tramite il Garante secondo l'art. 160 del Codice Privacy. Ogni restrizione è applicata nella misura e per il tempo strettamente necessari, con valutazione documentata e senza estensioni automatiche a finalità diverse da quelle previste dalla legge.

10. Canale esterno ANAC, divulgazione pubblica e denuncia

La persona segnalante può ricorrere al canale esterno ANAC nei casi previsti dal D.Lgs. 24/2023, tra cui: assenza o non conformità del canale interno, mancato seguito alla segnalazione interna, fondato motivo di ritenere che la segnalazione interna non avrebbe efficacia seguito o potrebbe determinare ritorsioni, fondato motivo di ritenere che la violazione possa costituire pericolo imminente o palese per il pubblico interesse.

Restano ferme le condizioni previste dalla legge per la divulgazione pubblica e per la denuncia all'autorità giudiziaria o contabile. La presente procedura non limita in alcun modo la facoltà della persona segnalante di rivolgersi alle autorità competenti nei casi previsti dall'ordinamento.

Per i pubblici ufficiali e gli incaricati di pubblico servizio restano fermi gli obblighi di denuncia all'Autorità giudiziaria previsti dall'ordinamento, quando ne ricorrono i presupposti. L'utilizzo del canale whistleblowing non sostituisce tali obblighi e la trasmissione all'Autorità avviene con cautele idonee a preservare la riservatezza dell'identità del segnalante nei limiti di legge.

11. Pubblicità, formazione, monitoraggio e riesame

Nella sezione "Whistleblowing" del sito istituzionale sono pubblicati la procedura destinata alla pubblicazione, l'informativa privacy, le istruzioni per l'utilizzo del canale, il collegamento alla piattaforma e le informazioni sul canale esterno ANAC.

Nella sezione dedicata sono rese disponibili, in linguaggio chiaro, le istruzioni pratiche per l'utilizzo della piattaforma, la conservazione del codice identificativo, la presentazione di eventuali integrazioni, la richiesta di incontro diretto, l'utilizzo del plico cartaceo riservato e le modalità per evitare l'invio improprio di segnalazioni tramite PEC, protocollo generale o caselle e-mail ordinarie.

Il Comune assicura iniziative periodiche di informazione e formazione rivolte al personale, ai responsabili di servizio/area, al RPCT/gestore, al sostituto, alla struttura di supporto, al protocollo e ai soggetti che potrebbero ricevere erroneamente segnalazioni whistleblowing.

Il RPCT monitora annualmente l'effettività della procedura, anche ai fini del PIAO, verificando tempi di gestione, funzionamento del canale, formazione svolta, eventuali criticità organizzative, necessità di aggiornamento della DPIA, incidenti di riservatezza, richieste di accesso, reclami o comunicazioni ANAC/Garante. Il monitoraggio non deve contenere dati idonei a identificare persone segnalanti o coinvolte, salvo stretta necessità e in forma riservata.

Il monitoraggio utilizza indicatori aggregati e non identificativi: numero di segnalazioni per canale, rispetto dei termini, richieste di integrazione, esiti generali, incidenti, formazione, test tecnici, cancellazioni eseguite e azioni correttive. Ogni anomalia rilevante è associata a responsabile, termine di chiusura e verifica dell'efficacia.

Il Comune verifica la coerenza del Codice di comportamento e, ove necessario, lo aggiorna per richiamare il dovere di riservatezza, il divieto di ritorsione, il divieto di ostacolare o tentare di ostacolare la segnalazione, il dovere di trasmissione al gestore delle segnalazioni ricevute da soggetti non competenti e le conseguenze disciplinari nei casi previsti dalla legge.