

COMUNE DI COMO

Misure organizzative per la Gestione delle Segnalazioni di Whistleblowing

(Adeguate al D.Lgs. 24/2023 e alle Linee Guida ANAC)

Approvate con D.G.C. n. 109 in data 5/6/2026

Modificate con D.G.C. n. 203 in data 21/9/2026

Art. 1 - Oggetto, Ambito di Applicazione e Definizioni

Il presente atto definisce le modalità operative per la ricezione, l'analisi e il trattamento delle segnalazioni di violazioni che ledono l'interesse pubblico o l'integrità del Comune di Como, in attuazione del D.Lgs. 24/2023.

Ambito soggettivo

Le disposizioni del presente atto si applicano, per quanto di rispettiva competenza:

- ai soggetti segnalanti, quali dipendenti, collaboratori, fornitori, consulenti, liberi professionisti, volontari, tirocinanti e tutti i soggetti indicati dall'art. 3 del D.Lgs. 24/2023;
- ai soggetti preposti alla gestione del canale: il Gestore (RPCT), il Sostituto del Gestore e il personale espressamente autorizzato e istruito per il supporto alle attività istruttorie. Per quest'ultimo, l'autorizzazione è limitata nel tempo e circoscritta esclusivamente ai dati e ai documenti strettamente necessari per lo svolgimento dell'incarico istruttorio puntuale conferito dal Gestore;
- ai soggetti coinvolti o menzionati nella segnalazione, quali autori presunti della violazione o persone a conoscenza dei fatti.

Ambito oggettivo

Sono oggetto di segnalazione:

- illeciti amministrativi, contabili, civili o penali;
- violazioni del diritto dell'Unione Europea;
- violazioni del Codice di comportamento;
- condotte che ledono l'imparzialità e il buon andamento dell'azione amministrativa.

Definizioni

Ai fini del presente atto si intende per:

- **Gestore delle Segnalazioni:** il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), individuato nel Segretario Generale. In caso di conflitto di interessi, assenza o impedimento del Titolare, le funzioni sono svolte dal Vice Segretario Generale vicario in qualità di Sostituto del Gestore;
- **Segnalazione:** comunicazione di informazioni sulle violazioni;
- **Segnalante:** la persona fisica che effettua la segnalazione;
- **Facilitatore:** la persona che assiste il segnalante nel processo di segnalazione;
- **Segnalato:** il soggetto a cui è attribuita la presunta violazione;
- **Persona coinvolta:** il soggetto che, pur non essendo l'autore diretto, potrebbe risultare partecipe o collegato ai fatti segnalati;
- **Persona menzionata:** il soggetto citato nella segnalazione per ragioni descrittive o quale possibile testimone;
- **Ritorsione:** qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, che provoca o può provocare un danno ingiusto al segnalante.

Obbligatorietà

Il rispetto delle disposizioni contenute nel presente atto è vincolante per tutti i soggetti sopra indicati, al fine di garantire:

- l'integrità del processo;
- la riservatezza delle informazioni;
- la protezione da ogni forma di ritorsione.

Art. 2 - Canali di Segnalazione

A) Interno

1. **Canale Prioritario (Piattaforma Informatica):** Il Comune di Como mette a disposizione dei soggetti legittimati un portale web dedicato, accessibile dal sito istituzionale. Oltre alla possibilità di effettuare segnalazioni in forma scritta, è possibile effettuare tramite la piattaforma segnalazioni in forma vocale o richiedere un incontro diretto con il Gestore, da fissarsi entro 15 giorni. In caso di incontro, la segnalazione viene comunque documentata e successivamente digitalizzata all'interno del portale, dotato delle

opportune misure di sicurezza, secondo le modalità previste dall'Art. 14 del D.Lgs. 24/2023.

2. Eventuali altri canali (sconsigliati): Il Comune di Como assicura la ricezione delle segnalazioni inoltrate anche tramite altri canali, quali, a titolo esemplificativo e non esaustivo, PEC, email, posta cartacea. Tuttavia, l'Ente informa che l'utilizzo di tali strumenti **non garantisce** di per sé gli standard di sicurezza e protezione dell'identità del segnalante, come invece assicura il portale dedicato descritto al precedente punto 1. Per la posta cartacea, l'Ente raccomanda l'utilizzo del **"Protocollo Tre Buste"** dettagliato al successivo Art. 4.

B) Canale di Segnalazione Esterna (ANAC): Il segnalante può ricorrere al canale esterno gestito dall'ANAC qualora il canale interno non sia momentaneamente attivo o vi sia fondato motivo di ritenere che la segnalazione non avrà seguito o possa determinare ritorsione oppure nel caso in cui in cui la segnalazione è già stata fatta e non ha avuto seguito. Il canale esterno deve essere utilizzato anche nei casi in cui il contenuto della segnalazione determini un conflitto di interessi nel Gestore e nel Sostituto del canale interno prioritario.

C) Divulgazione Pubblica: Il segnalante può ricorrere alla divulgazione pubblica (tramite stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone) esclusivamente qualora ricorra una delle seguenti condizioni previste dall'Art. 15 del D.Lgs. 24/2023, riportate sinteticamente di seguito:

- abbia già effettuato una segnalazione interna ed esterna senza ricevere riscontro nei termini;
- abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- abbia fondato motivo di ritenere che la segnalazione sul canale esterno possa comportare il rischio di ritorsioni o non possa avere efficace seguito per le circostanze specifiche del caso.

Art. 3 - Garanzie Tecniche e Procedura di Adozione della Piattaforma

- **Presupposto di Conformità (DPIA)**: la piattaforma informatica, quale canale prioritario di segnalazione, è corredata di una specifica Valutazione di Impatto sulla Protezione dei Dati (DPIA), ai sensi dell'Art. 35 del GDPR. Tale documento definisce le misure tecniche necessarie a garantire la riservatezza del segnalante e l'integrità del trattamento.
- Il set di misure di sicurezza tecnologiche e organizzative implementate, esposte nella DPIA, è stato sottoposto all'esame del Responsabile della Protezione dei Dati (DPO) dell'Ente.

- Al fine di garantire il costante allineamento allo stato dell'arte tecnologico e alle linee guida ANAC/Garante, la DPIA e la configurazione del canale sono sottoposte a revisione e aggiornamento con cadenza almeno annuale.

Art. 4 - Protocolli di Sicurezza e Riservatezza Operativa

- 1. Principio di Accountability e Vincoli Contrattuali:** Il Comune di Como, in qualità di Titolare del Trattamento, impegna il Fornitore del servizio, nominato Responsabile Esterno ai sensi dell'Art. 28 del GDPR, all'adozione di misure tecniche e organizzative adeguate ai sensi dell'Art. 32 del medesimo Regolamento. Tali obblighi sono recepiti e dettagliati nell'apposito Atto di Nomina (Addendum Privacy), che costituisce parte integrante del rapporto contrattuale e definisce i livelli di sicurezza minimi che il Fornitore è tenuto a garantire per la protezione dei dati e dell'identità del segnalante.
- 2. Obbligo di Diligenza del Gestore:** Il Gestore e i collaboratori autorizzati sono tenuti ad operare con la massima diligenza per impedire l'accesso non autorizzato ai dati. Ciò include l'adozione di protocolli sicuri per l'accesso (quali SPID o credenziali complesse), la gestione protetta degli endpoint e la rimozione sicura dei dati dai dispositivi utilizzati in caso di download temporaneo di documenti o ascolto di file audio, in coerenza con le misure di sicurezza descritte nella DPIA dell'Ente.
- 3. Sicurezza dell'Identità (Metadati):** L'Ente adotta soluzioni atte a separare l'identità del segnalante dal contenuto della segnalazione. L'Ente invita il segnalante a verificare l'eventuale presenza di elementi (metadati) dai quali possa essere indirettamente desumibile la propria identità.
- 4. Policy No-Log:** Al fine di massimizzare la tutela, il Comune assicura sulle proprie reti misure tecniche e organizzative volte alla minimizzazione e, ove possibile, alla anonimizzazione dei log di accesso al portale, al fine di ridurre il rischio di identificazione indiretta del segnalante
- 5. Sicurezza delle segnalazioni analogiche (Protocollo Tre Buste):** Qualora il segnalante scelga il canale postale, deve adottare il protocollo di segregazione fisica dei dati così strutturato:
 - **Busta (A):** contenente i dati identificativi del segnalante;
 - **Busta (B):** contenente esclusivamente l'oggetto della segnalazione e i fatti esposti;
 - **Busta (C) Esterna:** contenente le prime due buste, chiusa e recante obbligatoriamente la dicitura **"RISERVATA PERSONALE GESTORE WHISTLEBLOWING"**.

Conflitto di interessi del Gestore: Se la segnalazione riguarda il Gestore titolare (RPCT), la busta esterna (C) deve essere indirizzata nominativamente al Sostituto del Gestore con la dicitura **"RISERVATA PERSONALE SOSTITUTO DEL GESTORE WHISTLEBLOWING"**.

Il personale addetto al protocollo o alla ricezione della corrispondenza ha l'**obbligo tassativo di non aprire la busta** e di consegnarla integra e chiusa direttamente al destinatario (Gestore o Sostituto), il quale provvederà alla registrazione in un registro riservato o alla digitalizzazione protetta in piattaforma.

Art. 5 - Designazione e Gerarchia di Gestione: Titolare e Sostituto

1. Il Gestore (RPCT): Il Responsabile della Prevenzione della Corruzione e della Trasparenza è il titolare unico della funzione di ricezione e gestione. Egli agisce come "Amministratore" della piattaforma e primo referente dell'istruttoria. Viene nominato con provvedimento formale del Sindaco, autorizzato e istruito ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del Codice Privacy. Il Gestore garantisce il rispetto dei principi di imparzialità, riservatezza e indipendenza nello svolgimento delle proprie funzioni.

2. La Catena di Sussidiarietà (Sostituti): Al fine di garantire la continuità del servizio e risolvere ogni potenziale stallo dovuto a conflitti di interesse, sono individuabili due figure di supporto e subentro, configurate come utenze distinte e segregate in piattaforma:

- **Il Sostituto Vicario:** Subentra nelle funzioni del Gestore in caso di assenza, impedimento temporaneo o conflitto di interessi del Titolare (RPCT).
- **Il Sostituto di Riserva (Eventuale):** Interviene qualora si verifichi una contemporanea situazione di conflitto di interessi, assenza o impedimento sia del Gestore Titolare che del Sostituto Vicario. Questa figura garantisce la funzionalità del canale anche nelle situazioni di "impasse" organizzativo.

3. Qualifica, Istruzioni e Granularità: I Sostituti (Vicario e di Riserva) sono designati quali "Soggetti Autorizzati" ai sensi del GDPR e ricevono istruzioni scritte vincolanti. Costoro agiscono in piena autonomia funzionale e indipendenza solo quando chiamati a gestire un fascicolo in sostituzione del Titolare.

4. Accountability e Sicurezza Informatica:

- **Incedibilità e Log: Le credenziali** (SPID o password) sono strettamente personali. La piattaforma traccia ogni accesso e operazione (Audit Log) riconducendola univocamente all'utente (Titolare o Sostituti). È fatto divieto assoluto di condivisione delle credenziali.

- **Segregazione del Fascicolo:** In caso di conflitto di interessi segnalato, l'utenza del soggetto in conflitto è tecnicamente inibita dall'accesso a quel determinato fascicolo, che resterà visibile solo al Sostituto competente.
- **Permanenza del Vincolo:** L'impegno di segretezza assunto dal Gestore e dal Sostituto permane anche dopo la cessazione del rapporto di lavoro o dell'incarico.

Art. 6 - Obblighi di Trasparenza e Monitoraggio degli Accessi

1. Il **Gestore** e i soggetti autorizzati operano esclusivamente tramite sistemi che garantiscono la separazione logica tra identità del segnalante e segnalazione.
2. **Obbligo di Motivazione:** Ogni accesso ai dati identificativi del segnalante deve essere preceduto da una motivazione analitica che ne giustifichi la necessità istruttoria.
3. **Diritto di Controllo del Segnalante:** L'Ente garantisce al segnalante che utilizza la piattaforma informatica il diritto di monitorare, tramite accesso alla propria segnalazione, ogni operazione di decifratura della propria identità, inclusi nominativo dell'autore, data, ora e motivazione.

Art. 7 - Procedura di Gestione e Tempistiche

1. Ammissibilità delle segnalazioni anonime. Le segnalazioni da cui non è possibile ricavare l'identità del segnalante sono prese in considerazione dal Gestore a condizione che risultino adeguatamente circostanziate e rese con un grado di dettaglio tale da consentire l'analisi della loro fondatezza. In caso contrario, il Gestore procede all'archiviazione per carenza di elementi.

2. Ricevuta Tecnica di Trasmissione. Al momento dell'invio della segnalazione, la piattaforma rilascia una ricevuta tecnica di corretta trasmissione. Tale atto non costituisce l'avviso di ricevimento ex lege.

3. Avviso di Ricevimento e Presa in Carico. Il Gestore provvede all'apertura e alla presa in carico della segnalazione entro 7 giorni dalla ricezione. Tale atto costituisce il formale avviso di ricevimento. Dalla data della presa in carico decorre il termine di tre mesi per il riscontro finale. L'avviso di ricevimento, a seconda della modalità utilizzata, sarà comunicato mediante la piattaforma informatica o, in caso di mancato utilizzo della piattaforma, sarà inoltrato al recapito indicato dalla persona segnalante nella segnalazione o, in assenza di quest'ultima indicazione, a quello utilizzato dalla persona segnalante per inoltrare la segnalazione. In caso di segnalazione che non consenta di comunicare al segnalante l'avviso di ricevimento, il termine di tre mesi decorre dal giorno successivo al 7° giorno dalla presentazione della segnalazione.

4. Esame preliminare della segnalazione ricevuta. Preliminarmente il gestore verifica che la segnalazione sia stata presentata da una delle persone legittimate ai sensi del d.lgs. n. 24/2023

e che l'oggetto della stessa rientri nell'ambito di applicazione del medesimo decreto (cd. presupposti soggettivi e oggettivi).

Nel caso in cui manchino i suddetti requisiti e, dunque, la segnalazione non sia qualificabile come di *whistleblowing*, il gestore potrà trasmetterla al competente soggetto/ufficio interno all'ente che la tratterà, laddove previsto, come una segnalazione ordinaria, dandone contestualmente comunicazione alla persona segnalante. Gli enti potranno comunque valutare, per una maggiore tutela della persona segnalante, di mantenerne riservata l'identità anche se la segnalazione non è qualificabile come di *whistleblowing*.

Il gestore valuta altresì che la segnalazione:

- si basi su fatti sufficientemente precisi;
- contenga una descrizione dei fatti oggetto della segnalazione e, ove presenti, anche le modalità attraverso cui la persona segnalante è venuto a conoscenza dei fatti;
- contenga le generalità della persona coinvolta (se conosciute) o altri elementi che consentano di identificare la persona coinvolta nella segnalazione.

Resta ferma la possibilità per il gestore di richiedere alla persona segnalante ulteriori chiarimenti, documenti e informazioni a supporto della segnalazione.

Laddove non siano state fornite le integrazioni e le delucidazioni richieste, il gestore potrà archiviare la segnalazione, fornendo in ogni caso alla persona segnalante la motivazione della decisione

5. Analisi e valutazione della fondatezza. Istruttoria e accertamento della segnalazione.

Verificata l'ammissibilità della segnalazione il gestore può procedere con l'istruttoria vera e propria, che consiste nell'effettuare tutte le opportune verifiche, analisi e valutazioni circa la fondatezza o meno dei fatti segnalati.

Tali attività di accertamento possono essere svolte, ad esempio:

- direttamente, acquisendo dalla persona segnalante gli elementi informativi necessari;
- mediante il coinvolgimento di altre strutture interne all'ente o anche di soggetti specializzati esterni, ove ritenuto necessario, in considerazione delle specifiche competenze tecniche e professionali utili per il caso di specie (ad esempio tramite audizioni). Nel caso in cui il Gestore debba coinvolgere soggetti terzi (interni o esterni all'amministrazione) per le verifiche sui fatti segnalati avrà cura di non trasmettere la segnalazione a tali soggetti, ma solo gli esiti delle verifiche eventualmente condotte e, se del caso, estratti accuratamente anonimizzati della segnalazione, prestando sempre la massima attenzione per evitare che dalle informazioni e dai fatti descritti si possa risalire all'identità della persona segnalante.

Una volta completata l'attività di accertamento, il Gestore della segnalazione può:

- archiviare la segnalazione, motivandone le ragioni;
- rivolgersi, previa valutazione del *fumus* di fondatezza della segnalazione, agli organi/funzioni interne ed esterni competenti per i relativi seguiti.

6. Riscontro Finale. Entro il termine di cui all'art. 5, comma 1, lett. d) D.Lgs. 24/2023, come sopra esplicitato, il Gestore, ove possibile, fornisce riscontro al segnalante comunicando l'esito o lo stato di avanzamento della pratica. Poiché il termine non è perentorio¹, può infatti verificarsi che alcuni accertamenti e analisi richiedano tempi maggiori. Resta, tuttavia, ferma la necessità di comunicare l'esito dell'istruttoria della segnalazione.

Art. 8 - Riservatezza nelle Interlocuzioni Istruttorie

1. **Principio di Anonimizzazione del Quesito:** Qualora il Gestore necessiti di acquisire atti presso uffici interni o esterni, le richieste devono essere formulate come ordinaria attività di controllo, evitando riferimenti all'esistenza di una segnalazione Whistleblowing.
2. **Divieto di Rivelazione:** È vietato comunicare l'identità del segnalante ai soggetti interpellati durante l'istruttoria.
3. **Vincolo di Segretezza per l'Interpellato:** Se è indispensabile rivelare la natura della verifica, il soggetto interpellato deve essere preventivamente ammonito circa l'obbligo di segretezza, con avvertimento delle responsabilità disciplinari e penali.
4. **Segregazione dei Riscontri:** Le informazioni acquisite non devono transitare nei flussi documentali ordinari (protocollo generale), ma devono essere conservate esclusivamente nella piattaforma Whistleblowing.

Art. 9 - Rapporti con l'Ufficio Procedimenti Disciplinari (UPD)

1. Qualora l'istruttoria confermi la sussistenza di profili disciplinari, il Gestore trasmette i soli fatti accertati all'UPD per l'opportuna verifica degli estremi sanzionatori.
2. Resta ferma la disciplina di cui all'art. 12, comma 5, del Decreto Legislativo 24/2023.

Art. 10 - Rapporti con le Autorità Esterne (ANAC, Corte dei Conti, Autorità Giudiziaria e altre Autorità competenti)

1. **Valutazione e Obbligo di Denuncia:** Qualora gli elementi esaminati facciano emergere fatti che possano integrare ipotesi di reato, responsabilità erariale o violazioni di competenza ANAC o di altre Autorità competenti, il Gestore provvede alla trasmissione delle risultanze alle Autorità competenti

¹ Cfr. LLGG di cui alla delibera ANAC n. 311/2023 come modificata dalla delibera ANAC n. 479 del 26/11/2025.

(ex Art. 331 c.p.p.). La trasmissione avviene senza indebito ritardo, secondo le scadenze di legge.

2. **Dichiarazione di Origine e Etichettatura:** In ogni atto di trasmissione, il Gestore dichiara esplicitamente che la documentazione trae origine da una segnalazione di Whistleblowing (D.Lgs. 24/2023). Tutti i documenti e le comunicazioni devono recare la dicitura: **"Segnalazione protetta ai sensi del D.Lgs. 24/2023 - Identità riservata"**, al fine di attivare il regime di tutela rafforzata presso l'ente ricevente.
3. **Trasmissione dell'Identità del Segnalante:** L'identità del segnalante non è trasmessa automaticamente in allegato alla notizia di reato o di danno erariale, a meno che non sia richiesta dalla natura stessa dell'atto. Il Gestore la comunicherà qualora l'Autorità procedente ne dichiari la necessità ai fini dell'attività investigativa o della prosecuzione del procedimento, garantendo che il dato transiti attraverso canali che ne preservino la massima riservatezza (es. busta chiusa sigillata o canali digitali protetti).
4. **Vincolo di Riservatezza per l'Autorità Ricevente:** Il Gestore richiama formalmente l'Autorità ricevente all'obbligo di segretezza dell'identità (ex Art. 12 del D.Lgs. 24/2023), specificando che tale garanzia deve permanere in tutte le fasi del procedimento di competenza dell'Autorità esterna, nei limiti previsti dai rispettivi codici di procedura.

Art. 11 - Continuità Operativa e Gestione del Conflitto di Interessi

1. Canale Preferenziale per Conflitto del Gestore. Qualora la segnalazione riguardi il Gestore (RPCT), il segnalante è invitato a utilizzare il canale esterno ANAC. Qualora scelga il canale interno, la gestione è affidata in via sussidiaria al Sostituto Vicario.

2. Ricezione Accidentale e Obbligo di Astensione. Nel caso in cui una segnalazione coinvolgente il Gestore pervenga sul canale interno, questi ha l'obbligo tassativo di astenersi non appena rilevata la sussistenza del conflitto, senza accedere ai dati identificativi del segnalante né compiere atti istruttori.

3. Protocollo Tecnico di Inversione dei Ruoli. In presenza di conflitto del Gestore titolare, questi attiva la funzione di Inversione dei Ruoli sull'intera piattaforma. Tale operazione comporta il declassamento tecnico del Gestore titolare al profilo di "Collaboratore" e l'elevazione del Sostituto Vicario al profilo di "Responsabile".

- Il nuovo Responsabile (ex Sostituto) acquisisce la visione integrale delle sole segnalazioni inibite al Gestore titolare;

- Il Gestore titolare (ora Collaboratore) resta tecnicamente inibito dalla visione del fascicolo in conflitto;
- Per garantire la continuità sulle altre pratiche, il nuovo Responsabile provvederà ad assegnare i relativi fascicoli al Collaboratore (ex Gestore), affinché quest'ultimo possa proseguire l'attività ordinaria sotto la supervisione del nuovo Responsabile.

4. Ipotesi di Conflitto Congiunto (Gestore + Sostituto Vicario). Qualora la segnalazione coinvolga contemporaneamente il Gestore titolare e il Sostituto Vicario (entrambi presenti), il canale interno è considerato inidoneo, il Gestore informa il segnalante dell'impossibilità di garantire l'imparzialità e lo invita al canale esterno ANAC, procedendo all'archiviazione tecnica motivata. L'intervento del Sostituto di Riserva non è previsto in questa fattispecie.

5. Attivazione del Sostituto di Riserva (Impedimento Incrociato). La figura del Sostituto di Riserva interviene esclusivamente per sanare situazioni di stallo logistico o funzionale nelle seguenti combinazioni:

- Caso A: Il Sostituto Vicario è assente/impedito e il Gestore Titolare non può trattare la segnalazione (per assenza o conflitto di interessi);
- Caso B: Il Gestore Titolare è assente e il Sostituto Vicario è a sua volta assente o si trova in situazione di conflitto rispetto a una segnalazione pervenuta durante la sua reggenza.

6. Ripristino dei Ruoli e Tracciabilità (Log e Registro). Una volta conclusa l'istruttoria sul fascicolo in conflitto o terminata la causa di impedimento, i ruoli originari vengono ripristinati. La trasparenza delle operazioni è garantita da un doppio livello di controllo:

- Log di Audit: Registrazione inalterabile di ogni singola operazione compiuta;
- Registro dei Responsabili: Il Responsabile può consultare un registro dedicato che riporta analiticamente i periodi in cui ciascun utente ha rivestito il ruolo di "Responsabile", costituendo prova documentale della corretta segregazione dei dati.

7. Impedimento all'Inversione e Assistenza Tecnica. Qualora il soggetto che riveste il ruolo di Gestore sia tecnicamente impedito ad attivare autonomamente la procedura di inversione dei ruoli (es. per cessazione improvvisa del rapporto di lavoro senza preventivo passaggio di consegne), il Comune richiede l'intervento del fornitore del servizio per il ripristino dell'operatività e la creazione di una nuova utenza a seguito di nuovo provvedimento di nomina.

8. Obbligo di Verbale nei Passaggi Definitivi. Il verbale di passaggio di consegne (analogico) è richiesto solo per trasferimenti definitivi della funzione (es. pensionamento). Il verbale attesta lo stato delle pendenze e l'impegno del subentrante alla segretezza.

9. Sequenza Tecnica del Passaggio di Consegne (Gestione della *Vacatio*). Al fine di garantire la continuità del canale durante il periodo di *vacatio* tra il Gestore uscente e il subentrante, la procedura tecnica si articola in due fasi distinte e obbligatorie:

- **Fase 1: Passaggio dal Gestore uscente al Sostituto (Ponte):** Prima della cessazione del rapporto, il Gestore uscente assicura l'accesso al Sostituto Vicario elevandolo, se non già presente con tale profilo, al ruolo di **"Responsabile"**. Una volta verificata la piena operatività del Sostituto, quest'ultimo ha l'obbligo di **eliminare definitivamente l'utenza del Gestore uscente**. In questa fase, il Sostituto assume la piena custodia legale e tecnica delle segnalazioni pendenti.
- **Fase 2: Passaggio dal Sostituto al Gestore subentrante (Nomina):** All'atto dell'insediamento del nuovo Gestore titolare (nuovo RPCT), il Sostituto (che opera come Responsabile pro-tempore) provvede a inserire l'utenza del subentrante con il profilo di **"Collaboratore"** e a elevarlo immediatamente al ruolo di **"Responsabile"**.

Art. 12 - Gestione delle segnalazioni sui Canali diversi dal Canale prioritario (e istruzioni specifiche per il Servizio Protocollo).

1. Trasmissione a soggetti diversi dal Gestore: Qualunque soggetto diverso dal Gestore che riceva una segnalazione deve contattare tempestivamente il Gestore per ricevere dallo stesso le opportune istruzioni, senza effettuarne copia o protocollazione o altra attività di trattamento ed è vincolato all'obbligo di assoluta segretezza. Laddove il segnalante dichiara espressamente di voler beneficiare delle tutele in materia di whistleblowing o tale volontà sia desumibile dalla segnalazione, la segnalazione è considerata "segnalazione whistleblowing" e dovrà essere trasmessa, entro sette giorni dal suo ricevimento, al soggetto interno competente, dandone contestuale notizia alla persona segnalante. Diversamente, se il segnalante non dichiara espressamente di voler beneficiare delle tutele, o detta volontà non sia desumibile dalla segnalazione, quest'ultima sarà considerata segnalazione ordinaria.

2. Divieto Assoluto di Protocollazione Ordinaria: È fatto divieto assoluto di inserire le segnalazioni di Whistleblowing nel sistema di protocollo informatico generale dell'Ente. La segnalazione non deve essere scansionata, indicizzata né dotata di segnature di protocollo visibile.

2.1. Protocollo di Interruzione della Lettura: L'addetto al Protocollo che ravvisa elementi riconducibili a una segnalazione di Whistleblowing deve interrompere immediatamente la lettura, astenersi da ogni registrazione e procedere alla blindatura immediata.

2.2. Blindatura della Segnalazione Cartacea: L'operatore inserisce il plico aperto per errore in una nuova busta anonima sigillata con la dicitura **"RISERVATA PERSONALE - WHISTLEBLOWING"** e la consegna a mani del Gestore (o dei Sostituti secondo la gerarchia dell'Art. 10) entro 24 ore.

2.3. Blindatura Digitale e Prelievo Protetto (Azione del Gestore): Al fine di evitare la "proliferazione di tracce digitali" (log di sistema, copie nella posta inviata, backup dei server), il trasferimento della segnalazione dalla casella PEC/Email al canale sicuro avviene prioritariamente tramite **Accesso Diretto**:

- **Notifica per le vie brevi:** L'addetto al Protocollo contatta immediatamente il Gestore (o il Sostituto) via telefono o di persona, informandolo della presenza di una segnalazione nella casella di posta, senza effettuarne l'inoltro elettronico.
- **Accesso alla Fonte:** Il Gestore accede direttamente alla casella di posta elettronica certificata istituzionale e procede al **prelievo protetto** della segnalazione, caricandola direttamente nella piattaforma sicura.
- **Divieto di Inoltro (Forward):** È vietato l'uso della funzione "Inoltra" verso caselle di posta ordinaria, in quanto tale operazione lascerebbe traccia del contenuto e dell'identità del segnalante nella cartella "Posta Inviata" e nei log di transito dei server dell'Ente.

3. Bonifica e Cancellazione (Sanitizzazione): Subito dopo il caricamento in piattaforma della segnalazione ricevuta con il diverso canale, il Gestore (o l'operatore sotto la sua supervisione) provvede alla **cancellazione definitiva** del messaggio originale dalla casella di posta elettronica certificata istituzionale e allo svuotamento del cestino. Questa operazione di "bonifica" è essenziale per garantire che nessuna traccia della segnalazione rimanga nei sistemi di posta elettronica non protetti da crittografia end-to-end. Nel caso di segnalazione pervenuta in forma cartacea il Gestore, a seguito delle risultanze dell'istruttoria può disporre la distruzione definitiva della fonte originale ovvero mantenerla per l'eventuale successiva trasmissione all'Autorità competente (distruzione fisica della carta tramite trituradocumenti).

4. Responsabilità e Formazione: Il personale addetto al Protocollo riceve specifica istruzione operativa. La violazione del divieto di protocollazione o la mancata blindatura del dato può costituire illecito atto e illecito sanzionabile dall'ANAC (*cf. artt. 12 "Obbligo di riservatezza" e 21, comma 1, "Sanzioni" D.Lgs. 24/2023*).

Art. 13 Gestione delle Divulgazioni Pubbliche tramite Segnalazione a cura del Gestore.

1. Acquisizione e Monitoraggio: Qualora il Gestore (RPCT), nell'ambito dell'attività di monitoraggio dei mezzi di diffusione di massa (stampa, web, social media), ravvisi una divulgazione pubblica riguardante condotte illecite o irregolarità interne all'Ente che presentino i requisiti di cui all'Art. 2, lettera C) del presente atto, può procedere alla creazione di una segnalazione all'interno della piattaforma informatica.

2. Finalità della Registrazione. L'inserimento in piattaforma a cura del Gestore risponde alla duplice esigenza di:

- **Conservazione e Tutela:** Garantire la tracciabilità della notizia al fine di assicurare tempestivamente le tutele di legge al segnalante qualora questi dovesse essere identificato e subire ritorsioni;
- **Valutazione Istruttoria:** Permettere al Gestore di esaminare i fatti esposti nella divulgazione pubblica per valutarne la gravità e l'impatto sull'integrità dell'Ente.

3. Potere Discrezionale del Gestore. Analizzato il contenuto della divulgazione pubblica, il Gestore ha la piena facoltà di:

- Archiviazione agli Atti. Qualora la notizia risulti generica, palesemente infondata o priva di elementi minimi di riscontro, limitandosi alla conservazione del dato per finalità di futura tutela del soggetto;
- Avvio di Istruttoria d'Ufficio. Qualora la notizia appaia circostanziata, verosimile e riguardi fatti gravi. In tal caso, il Gestore attiva i medesimi poteri istruttori previsti per le segnalazioni interne (Art. 7), dando atto delle risultanze nel fascicolo digitale della segnalazione indiretta.

4. Esiti e Trasparenza. Se l'istruttoria conferma la fondatezza della segnalazione, il Gestore procede alla trasmissione degli atti agli organi competenti (Autorità Giudiziaria, Corte dei Conti, ANAC e altre Autorità) secondo le modalità previste dall'Art. 10 del presente atto.

Art. 14 - Tutele, Diritti e Responsabilità del Segnalante

1. Divieto Assoluto di Ritorsione (Art. 17 D.Lgs. 24/2023): Il Comune di Como garantisce che nessun segnalante possa subire alcuna forma di ritorsione in ragione della segnalazione effettuata. Per ritorsione si intende qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione e che provoca o può provocare, direttamente o indirettamente, un danno ingiusto. A titolo esemplificativo e non esaustivo, il divieto comprende:

- **Per i dipendenti e collaboratori interni:** il licenziamento, la sospensione o misure equivalenti, il demansionamento, il trasferimento, o qualsiasi altra misura organizzativa con effetti negativi sulle condizioni di lavoro;
- **Per i soggetti esterni (fornitori, consulenti, liberi professionisti):** la risoluzione anticipata o il mancato rinnovo di contratti di fornitura o di incarichi professionali, la revoca di abilitazioni, o qualsiasi altra misura che pregiudichi i rapporti commerciali o professionali in essere con l'Ente.

2. Estensione delle Tutele (Soggetti Protetti – Art. 6 D.Lgs. 24/2023): Il regime di protezione dalle ritorsioni si applica altresì:

- Ai facilitatori (persone che assistono il segnalante nel processo di segnalazione²);
- Alle persone del medesimo contesto lavorativo legate al segnalante da uno stabile legame affettivo o di parentela entro il quarto grado;
- Ai colleghi di lavoro con cui il segnalante ha un rapporto abituale e corrente;
- Agli enti di proprietà del segnalante o per i quali lavora.

² N.B. Per conoscere facoltà e limiti della figura del facilitatore, cfr. Linee Guida Anac n. 311/2023 come modificate dalla Delibera ANAC 479/2025 citate in nota n. 54 alla Delibera Anac n. 478/2025 relativa ai Canali interni di segnalazione.

3. Condizioni per la Protezione: Per la disciplina relativa alle condizioni per la protezione del segnalante e ai limiti della stessa, si rinvia alle previsioni dell'art. 16 D.Lgs. 24/2023.

4. Limitazione della Responsabilità: Per la disciplina relativa alle limitazioni della responsabilità vedasi l'art. 20 D.Lgs 24/2023 e le ulteriori norme dallo stesso richiamate.

5. Misure di Sostegno e Rapporti con il Terzo Settore: Il segnalante (e i soggetti di cui al punto 2) può avvalersi delle misure di sostegno previste dall'Art. 18 del D.Lgs. 24/2023 al quale si rinvia. A tal fine:

- L'ANAC istituisce e aggiorna l'elenco degli Enti del Terzo Settore (ETS) accreditati che forniscono assistenza e consulenza gratuita a titolo informativo, legale e psicologico. Tale elenco è raggiungibile dalla [pagina informativa](#) del portale istituzionale del Comune relativa alla possibilità di presentare la segnalazione tramite ANAC..

6. Diritto alla Riservatezza ed Eccezioni Legali: L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni senza il consenso espresso del segnalante stesso, fatti salvi i casi e gli obblighi previsti dalla normativa vigente (D.Lgs. 24/2023) e dalle Autorità competenti.

Art. 15 - Garanzie e Tutela della Persona Segnalata, Coinvolta o Menzionata

1. Le tutele di riservatezza e le garanzie previste dal presente articolo si applicano alla Persona Segnalata, alla Persona Coinvolta e alla Persona Menzionata, come definiti all'Articolo 1 del presente atto.

2. Riservatezza dell'Identità (Ex Art. 12 D.Lgs. 24/2023): L'identità di tali soggetti è protetta in ogni fase della gestione della segnalazione, fino alla chiusura dell'istruttoria. L'obbligo di segretezza grava sul Gestore (RPCT) e su chiunque venga a conoscenza dei fatti, con divieto assoluto di rivelare nomi o dettagli che consentano l'identificazione di tali persone a soggetti non autorizzati.

3. Limitazione dei Diritti dell'Interessato (Ex Art. 2-undecies Codice Privacy): In conformità ai pronunciamenti del Garante per la Protezione dei Dati Personali e all'Art. 23 del Reg. UE 2016/679, l'esercizio dei diritti da parte del Segnalato o delle Persone Coinvolte (accesso, rettifica, cancellazione, opposizione) è **limitato o escluso** qualora possa derivarne un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante o all'integrità dell'istruttoria.

4. Informativa e diritto di difesa. In coerenza con le Linee Guida ANAC e il D.Lgs. 24/2023:

- **Differimento dell'informativa:** L'esercizio del diritto di informazione nei confronti della Persona Segnalata può essere ritardato o limitato qualora ciò sia strettamente necessario per garantire la riservatezza dell'identità del segnalante o per evitare un pregiudizio effettivo e concreto all'integrità dell'attività di verifica degli elementi segnalati.

- **Sede del contraddittorio:** Il diritto di difesa e il contraddittorio sono garantiti esclusivamente nelle sedi procedurali successive (disciplinari, civili, penali) che dovessero scaturire dalle risultanze trasmesse dal Gestore.
- **Riservatezza dell'identità:** L'identità della persona segnalata è protetta fino alla conclusione del procedimento da parte del Gestore.

Art. 16 - Formazione, Sensibilizzazione e Aggiornamento

1. **Obbligo Formativo:** Il Comune di Como riconosce la formazione come misura fondamentale per la prevenzione di violazioni della riservatezza e per l'efficacia del sistema di Whistleblowing. La formazione è obbligatoria e differenziata in base ai ruoli e alle responsabilità. Le attività formative sono inserite annualmente nella sezione 'Rischi corruttivi e trasparenza' del **PIAO (Piano Integrato di Attività e Organizzazione)** dell'Ente.
2. **Formazione Specialistica (Gestore, Sostituto e Collaboratori):** I soggetti incaricati della gestione delle segnalazioni devono ricevere una formazione specifica e periodica riguardante:
 - Il quadro normativo nazionale (D.Lgs. 24/2023) e le Linee Guida ANAC;
 - L'utilizzo tecnico avanzato della piattaforma informatica;
 - Le misure di sicurezza operativa (cifatura dischi, uso cuffie, gestione file audio);
 - La gestione dei profili privacy (GDPR) e le tecniche di istruttoria.
3. **Istruzioni Operative per il Personale di "Primo Contatto"** (Protocollo): Il personale addetto all'Ufficio Protocollo e alla Segreteria deve essere specificamente istruito sulle modalità di:
 - Riconoscimento tempestivo di una segnalazione whistleblowing;
 - Applicazione del protocollo di "Interruzione della Lettura";
 - Procedure di blindatura e trasferimento protetto (cifatura file o busta chiusa) al Gestore.
4. **Sensibilizzazione del Personale Dipendente (Generalità dei Lavoratori):** L'Ente promuove azioni di sensibilizzazione rivolte a tutto il personale per illustrare:
 - L'esistenza e il funzionamento dei canali di segnalazione;
 - Il regime delle tutele contro le ritorsioni;
 - Le garanzie tecnologiche adottate (Policy No-Log e crittografia) a tutela del segnalante;
 - L'affissione di informative sintetiche (poster o estratti del presente atto) presso le bacheche fisiche dei vari settori e nelle aree comuni, garantendo la massima visibilità dei canali di segnalazione anche al personale che non dispone di postazione informatica fissa.
5. **Periodicità e Tracciabilità:** Le attività formative devono essere aggiornate con cadenza almeno annuale o in occasione di rilevanti modifiche normative o tecnologiche della

piattaforma. La partecipazione ai corsi deve essere formalmente documentata e i relativi attestati conservati agli atti dell'ufficio per finalità di Audit e Accountability.

Art. 17 - Conservazione e Tracciabilità

Tutta la documentazione, inclusi allegati multimediali (foto, video, audio), è conservata, anche in caso di segnalazione anonima, per il tempo necessario al trattamento e comunque non oltre **5 anni** dalla comunicazione dell'esito finale, nel rispetto delle misure di sicurezza previste dalla DPIA dell'Ente.

Art. 18 - Trasparenza, Accessibilità e Informativa

1. Collocazione del Link Istituzionale. Al fine di garantire la massima accessibilità, il Comune assicura la presenza di un link diretto alla piattaforma "Whistleblowing Intelligente" in [Homepage](#) e nella sezione "[Amministrazione Trasparente](#)".

2. Pagina Informativa sul Sito Istituzionale. Il link indirizza l'utente ad una prima pagina di atterraggio interna al sito del Comune di Como, volta a fornire un inquadramento generale. Tale pagina deve contenere:

- **Finalità del Canale:** Descrizione dei soggetti tutelati e delle violazioni segnalabili;
- **Informativa sui Canali Esterni:** Indicazione delle condizioni per ricorrere ad ANAC o alla divulgazione pubblica;
- **Link di Accesso al Portale:** Pulsante per accedere all'ambiente protetto di segnalazione.

3. Pagina Pubblica sul Portale di Segnalazione. All'interno del portale sicuro, prima di procedere all'invio, l'utente accede a una pagina che fornisce le istruzioni tecniche e la documentazione legale obbligatoria, tra cui:

- **Guida Tecnica:** Istruzioni sull'invio e sulla conservazione del codice univoco;
- **Garanzie Tecnologiche:** Esplicitazione del sistema di crittografia Zero-Knowledge;
- **Documentazione Obbligatoria:** Sono resi permanentemente disponibili per il download il presente Regolamento (Atto Organizzativo) e l'Informativa Privacy specifica per il trattamento whistleblowing (ex Art. 13 e 14 GDPR), al fine di garantire la piena trasparenza e la validità del trattamento dei dati.

4. Aggiornamento e Manutenzione. Il Gestore (RPCT), tramite la Segreteria Generale, assicura che i documenti obbligatori sul portale di segnalazione siano costantemente aggiornati e accessibili.

Art. 19 - Sistema Sanzionatorio

1. **Sanzioni a tutela del Segnalante:** Il compimento di atti ritorsivi, l'intralcio alla presentazione delle segnalazioni o la violazione degli obblighi di riservatezza dell'identità costituiscono illeciti disciplinari. Il Comune di Como applica le sanzioni previste dalla legge e dal CCNL, ferma restando la competenza dell'ANAC per l'irrogazione delle sanzioni amministrative pecuniarie (da € 10.000 a € 50.000).
2. **Sanzioni a carico del Segnalante (Responsabilità e Malafede):** Fuori dai casi previsti dall'art. 20 D.Lgs.24/2023, qualora venga accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione, ovvero la sua responsabilità civile per dolo o colpa grave (segnalazioni manifestamente false o strumentali), l'Ente applica le previsioni dell'art. 16, comma 3, D.Lgs. 24/2023 e segnala l'accaduto all'**ANAC**.
3. **Aggiornamento del Codice di Comportamento:** Il Comune di Como si impegna a recepire le disposizioni del presente atto organizzativo e quelle previste dalla Linee Guida ANAC approvate con Deliberazione n. 478/2025 all'interno del proprio **Codice di Comportamento**, inserendo espliciti riferimenti, tra gli altri, all'obbligo di riservatezza, al divieto di ritorsione, al divieto di uso strumentale o ostruzionistico dei canali di segnalazione e alle specifiche responsabilità disciplinari derivanti dalla violazione delle tutele previste per il segnalante, al fine di garantire la massima coerenza e deterrenza del sistema sanzionatorio complessivo.

Art. 20 - Monitoraggio, Statistica e Relazione Annuale

1. **Obbligo di Rendicontazione:** Il Gestore (RPCT) provvede annualmente alla redazione di una relazione sull'efficacia del sistema di Whistleblowing del Comune di Como da inserire nell'ambito delle azioni di monitoraggio contenute nel PIAO.
2. **Contenuto dei Dati (Forma Aggregata):** Per garantire l'assoluta riservatezza e l'impossibilità di rintracciare l'identità dei segnalanti, la relazione contiene esclusivamente dati statistici e aggregati, riguardanti:
 - Numero di segnalazioni ricevute nell'anno solare di riferimento;
 - Canali di ricezione utilizzati da parte del segnalante;
 - Tipologia delle violazioni segnalate (es. corruzione, appalti, gestione del personale, violazioni del Codice di Comportamento, ecc.);
 - Dati relativi all'osservanza dei termini procedurali, con specifica indicazione del rispetto dei 7 giorni per l'avviso di ricevimento e dei 90 giorni per il riscontro finale;
 - Stato di avanzamento e/o esiti finali delle istruttorie (numero di archiviazioni, trasmissioni all'UPD, trasmissioni all'Autorità Giudiziaria o contabile e altre Autorità);
3. **Finalità di Revisione:** L'analisi dei dati contenuti nel report annuale costituisce la base per l'eventuale aggiornamento del presente atto organizzativo, della Valutazione di

Impatto sulla Protezione dei Dati (DPIA) e delle misure di prevenzione dei rischi corruttivi inserite nel **PIAO (Piano Integrato di Attività e Organizzazione)**.