Modello di Organizzazione e Gestione per la prevenzione dei reati ai sensi del D. Lgs. 231/2001

PM 8 Segnalazioni all'Organismo di Vigilanza

("Whistleblowing")

Revisione: 00	Redazione Coopolis Spa	Verifica Presidente	Approvazione Consiglio di Amm.ne
Data	27/10/2023	20/11/2023	27/11/2023
Firma			

Descrizione degli aggiornamenti

Data	Rev.	Argomento	Descrizione
27/11/2023	00	Prima emissione	Adozione Edizione 1
	01		
	02		
	03		
	04		
	05		
	06		
	07		
	08		
	09		

INDICE

1. SCOPO DELLA PROCEDURA

C.E.A.R. Società Cooperativa (di seguito anche "CEAR" o "Società" o "Ente") ha predisposto una procedura per la gestione delle segnalazioni, c.d. *procedura whistleblowing*, che costituisce parte integrante del Modello di Organizzazione Gestione e controllo ex D.Lgs. 231/2001 (di seguito anche "MOG231") adottato dalla Cooperativa.

La procedura ai sensi del D.Lgs. n.24/2023 ha lo scopo di disciplinare il processo di ricezione, analisi e trattamento delle segnalazioni di condotte che potrebbero integrare la commissione di uno o più reati rilevanti ai sensi del D.Lgs. n. 231/01 o costituire una violazione del MOG231 e/o del Codice Etico adottati da CEAR.

La procedura è predisposta ai sensi del D.Lgs. n.24/2023, nel rispetto delle previsioni di cui all'art. 6 comma 2 bis del D.Lgs. n. 231/2001 che impone di implementare all'interno dei modelli organizzativi l'attivazione di un canale interno di segnalazione, il divieto di ritorsione e l'applicazione di un sistema disciplinare.

La procedura disciplina anche le modalità di verifica di validità e fondatezza delle segnalazioni e le misure da intraprendere nel caso di segnalazioni al solo scopo di calunnia o diffamazione.

2. CAMPO DI APPLICAZIONE

La presente procedura considera come rilevanti le segnalazioni che riguardino condotte illecite, irregolarità o reati – consumati o tentati – di cui il segnalatore abbia avuto conoscenza diretta nell'esercizio delle proprie mansioni o funzioni, che possono consistere in azioni od omissioni:

- rilevanti ai sensi delle fattispecie di reato presupposto di cui al D.Lgs. 231/2001 ed ai fini dell'istituto della responsabilità amministrativa degli enti;
- atte a determinare violazioni di norme di condotta e/o principi di comportamento individuati nel MOG231 e nel Codice Etico adottati da CEAR.

In sintesi, la segnalazione potrà riguardare:

- violazioni del MOG231 adottato da CEAR;
- violazioni del Codice Etico di CEAR;
- la commissione, in specifico, di reati previsti dal D.Lgs. n. 231/01.

La segnalazione non può riguardare, ai sensi dell'art.1 comma 2 del D.Lgs. 24/2023,e contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate;

Per le segnalazioni riguardanti rimostranze di carattere personale del segnalante o rivendicazioni/istanze che rientrano nella disciplina del rapporto di lavoro occorre fare riferimento al Direttore, che condividerà tali segnalazioni con il Consiglio di Amministrazione anche per le questioni riguardanti il personale della Cooperativa.

3. SOGGETTI COINVOLTI

Sono tenuti all'applicazione della procedura i soggetti come indicati all'art. 3 commi 2 e 3 del D.Lgs. n. 24/2023 ed in specifico:

- i lavoratori subordinati di CEAR, ivi compresi i lavoratori il cui rapporto di lavoro è disciplinato dal D.Lgs. n. 81/2015, o dall'articolo 54-bis del D.L. n. 50/2017, convertito, con modificazioni, dalla L. n. 96/2017;
- lavoratori autonomi, ivi compresi quelli indicati al capo I della L. n. 81/2017, nonché i titolari di un rapporto di collaborazione di cui all'articolo 409 del c.p.c. e all'articolo 2 del D.Lgs. n. 81/2015, che svolgono la propria attività lavorativa presso CEAR;
- lavoratori o i collaboratori, che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato che forniscono beni o servizi o che realizzano opere in favore di CEAR;
- i liberi professionisti e i consulenti che prestano la propria attività a CEAR;
- i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività a CEAR;
- i soci di CEAR e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza di CEAR, anche qualora tali funzioni siano esercitate in via di mero fatto.

4. OGGETTO E CONTENUTO DELLA SEGNALAZIONE

Le segnalazioni devono essere circostanziate e fondate su elementi precisi e concordanti, avere ad oggetto fatti conosciuti e riscontrati direttamente dal segnalante e non riferiti da terzi, a meno del caso in cui la segnalazione è comunicata ad un soggetto diverso dal canale di segnalazione individuato nel qual caso valgono le misure individuate di seguito nella procedura stessa per la gestione della comunicazione della segnalazione.

La segnalazione inoltre deve possibilmente contenere tutte le informazioni necessarie per individuare con certezza e inequivocabilmente l'autore della condotta oggetto di segnalazione.
Le segnalazioni rese in forma anonima saranno prese in considerazione solo se circostanziate. Esse saranno equiparate alle segnalazioni ordinarie e trattate secondo la presente procedura. Il segnalante anonimo, se successivamente identificato, beneficerà delle tutele che il D.Lgs. n.24/2023 garantisce a fronte di misure ritorsive[1].

Per garantire la riservatezza del segnalante prevista dal D.Lgs. n.24/2023, CEAR adotta una piattaforma informatica per la gestione delle segnalazioni e delle comunicazioni tra soggetto segnalante e canale di segnalazione.

In particolare, la segnalazione (di seguito anche "segnalazione whistleblowing") deve contenere i seguenti elementi:

- le generalità di chi effettua la segnalazione;
- la chiara e completa esposizione dei fatti oggetto di segnalazione e delle modalità con le quali se ne è avuta diretta conoscenza;
- se conosciute, le circostanze di tempo e di luogo in cui si è verificato il fatto;
- se conosciute, le generalità o altri elementi che consentano di identificare il soggetto che ha determinato i fatti segnalati;
- l'indicazione di eventuali altri soggetti che possano dare informazioni rispetto ai fatti oggetto di segnalazione;

[1] Art. 16 c. 4 del D.Lgs. n.24/2023

- l'indicazione di eventuali documenti a conferma della fondatezza dei fatti riportati;
- ogni altra INFORMAZIONE UTILE AD UN RISCONTRO CIRCA LA SUSSISTENZA DEI FATTI SEGNALATI.

5. DESTINATARI DELLA SEGNALAZIONE E MODALITÀ DI TRASMISSIONE

La gestione del canale di segnalazione interno è affidata da CEAR ad un canale interno gestore delle segnalazioni (di seguito anche "Gestore") identificato nel componente monocratico dell'Organismo di Vigilanza (di seguito anche "ODV"). Il Gestore è destinatario delle segnalazioni whistleblowing secondo le modalità previste dalla piattaforma informatica dedicata, implementata dalla Società nelle pagine del proprio sito aziendale **https://cear-CEAR.whistletech.online**.

La piattaforma informatica implementata da CEAR per la gestione delle segnalazioni whistleblowing garantisce i requisiti di riservatezza previsti dalla normativa, dando la possibilità sia di segnalazioni scritte che orali. Inoltre, la piattaforma informatica consente la segnalazione, su richiesta della persona segnalante, mediante incontro diretto con il Gestore delle segnalazioni di CEAR.

Nel caso di segnalazione comunicata ad un soggetto diverso da quello sopra indicato, questa deve essere trasmessa al suddetto soggetto competente entro 7 giorni da suo ricevimento, dando contestuale notizia della trasmissione alla persona segnalante.

Per ogni riferimento alle modalità di trasmissione delle segnalazioni CEAR, oltre quanto indicato nella presente procedura, si rimanda per completezza alla piattaforma informatica implementata ed al relativo Manuale di regolamentazione e funzionamento della stessa (Manuale Whistletech) allegato della presente procedura.

6. CANALE DI SEGNALAZIONE INTERNO: VERIFICA, ACCERTAMENTO ED ESITI DELLE SEGNALAZIONI

Il Gestore delle segnalazioni, quale canale di segnalazione interno individuato da CEAR, riceve le segnalazioni a mezzo piattaforma informatica e gestisce le stesse secondo i seguenti criteri:

- rilascio alla persona segnalante di un avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione mediante la messa in lavorazione della stessa;
- formulazione di un primo giudizio di ricevibilità, escludendo le segnalazioni che non rientrino nell'oggetto della presente procedura (ad es. reclami generici, lamentele);
- mantenimento delle interlocuzioni con la persona segnalante con possibilità di richiedere a quest'ultima, se necessario, integrazioni;
- gestione diligente delle segnalazioni ricevute procedendo:
    - alla trasmissione della segnalazione, dopo averla resa completamente anonima e/o riprodotta per renderla non riconoscibile e/o altrimenti riconducibile all'autore, ad altri soggetti al fine di acquisire ulteriori informazioni ed osservazioni. Tali soggetti dovranno formulare le valutazioni e fornire i richiesti riscontri entro e non oltre quindici giorni dalla ricezione della richiesta;
    - all'archiviazione della segnalazione, con supporto di adeguata motivazione, nel caso in cui dalle prime verifiche effettuate essa risulti infondata o non sufficientemente circostanziata od ancora non pertinente;
    - nel caso di non archiviazione, alla comunicazione dell'esito della propria valutazione e/o verifica al Direttore per le opportune valutazioni ai fini disciplinari e

sanzionatori, ovvero per gli opportuni interventi sul MOG231 che lo stesso valuterà anche in condivisione con il Consiglio di Amministrazione della Società;
  - al riscontro delle valutazioni disciplinari e sanzionatorie attivate dal Consiglio di Amministrazione e delle eventuali valutazioni di interventi sul MOG231;
- tempistica di riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione;
- messa a disposizione di informative chiare sul canale, sulle procedure, sulla piattaforma informatica utilizzata e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne. In tal senso le suddette informazioni sono esposte e rese facilmente visibili nei luoghi di lavoro, nonché accessibili alle persone che pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico in una delle forme di cui all'art. 3, c. 3 – 4 del D.lgs. 24/2023.

7. TUTELA DEL SEGNALANTE

- OBBLIGO DI RISERVATEZZA SULL'IDENTITÀ DEL SEGNALANTE

Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante; tale tutela vale anche nei confronti degli organi di vertice di CEAR, che non possono disporre indagini o chiedere informazioni al fine di risalire all'identità del segnalante.

L'obbligo di mantenere la massima riservatezza sull'identità del segnalante e di non svolgere indagini o chiedere informazioni riguarda tutti coloro che, a qualunque titolo, vengano a conoscenza della stessa o siano coinvolti nel procedimento di accertamento della segnalazione.

Nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia invece fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.

Con riferimento alle ipotesi suddette, alla persona segnalante viene data informazione delle ragioni della rivelazione dei dati riservati mediante comunicazione scritta. Tale informativa è prevista nell'ambito delle attività di segnalazione interna ed esterna di cui alla presente procedura quando la rivelazione della identità della persona segnalante e delle informazioni è indispensabile anche ai fini della difesa della persona coinvolta.

La violazione della tutela della riservatezza del segnalante, fatti salvi i casi in cui sia ammessa la rivelazione dell'identità come sopra evidenziato, comporta l'avvio di un procedimento disciplinare conformemente a quanto previsto dalla normativa di riferimento e dal CCNL applicato vigente per i soggetti a cui esso è applicabile.

Non è dovuta alcuna tutela nel caso in cui il segnalante incorra, con propria denuncia, in responsabilità penale a titolo di calunnia (art. 368 c.p.) o diffamazione (art. 595 c.p.).

Nell'ambito delle attività di segnalazione interna ed esterna di cui alla presente procedura, la persona coinvolta può essere sentita, ovvero, su sua richiesta, è sentita, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

- DIVIETO DI DISCRIMINAZIONE NEI CONFRONTI DEL SEGNALANTE

I soggetti a cui si applica la presente procedura e che effettuano una segnalazione nel rispetto della stessa e delle previsioni normative di cui al D.Lgs. n. 24/2023 non possono subire alcuna ritorsione per le segnalazioni effettuate. In tal senso costituisce ritorsione, secondo la definizione di cui all'art. 2, comma 1, lettera m), del citato Decreto, qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.

Di seguito sono indicate le fattispecie che possono costituire ritorsione:

a) il licenziamento, la sospensione o misure equivalenti;
b) la retrocessione di grado o la mancata promozione;
c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
e) le note di merito negative o le referenze negative;
f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
g) la coercizione, l'intimidazione, le molestie o l'ostracismo;
h) la discriminazione o comunque il trattamento sfavorevole;
i) la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
j) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
k) i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
l) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
m) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
n) l'annullamento di una licenza o di un permesso;
o) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

A tutela del segnalante, secondo quanto previsto dall'art. 17, commi 2 e 3, del suddetto Decreto (Divieto di ritorsione), nell'ambito di procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati nei confronti delle persone segnalanti, si presume che gli stessi siano stati posti in essere a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione, alla divulgazione pubblica o alla denuncia è a carico di colui che li ha posti in essere.
Inoltre, in caso di domanda risarcitoria presentata all'autorità giudiziaria dalle persone segnalanti, se tali persone dimostrano di aver effettuato, ai sensi del suddetto Decreto, una segnalazione, una divulgazione pubblica o una denuncia all'autorità giudiziaria o contabile e di aver subito un danno,

si presume, salvo prova contraria, che il danno sia conseguenza di tale segnalazione, divulgazione pubblica o denuncia all'autorità giudiziaria o contabile.
Le suddette tutele per le persone segnalanti non si applicano nel caso in cui non ricorrono le seguenti condizioni:

a) al momento della segnalazione o della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica, la persona segnalante o denunciante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate, divulgate pubblicamente o denunciate fossero vere e rientrassero nell'ambito oggettivo di cui al suddetto Decreto;
b) la segnalazione o divulgazione pubblica è stata effettuata sulla base di quanto previsto dalla normativa in materia e secondo la presente procedura.

Inoltre, è condizione per la protezione della persona segnalante, il fatto che i motivi che hanno indotto la persona a segnalare o denunciare o divulgare pubblicamente sono irrilevanti ai fini della sua protezione.

Nel caso in cui è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele previste normativamente per la persona segnalante non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare.

Le condizioni per l'applicazione delle tutele della persona segnalante e le misure disciplinari che si applicano nel caso di responsabilità penale di quest'ultima per come suddette, si applicano anche nei casi di segnalazione o denuncia all'autorità giudiziaria o contabile o divulgazione pubblica anonime, se la persona segnalante è stata successivamente identificata e ha subito ritorsioni, nonché nei casi di segnalazione presentata alle istituzioni, agli organi e agli organismi competenti dell'Unione europea, in conformità alle condizioni di cui all'art. 6 del D.Lgs. n. 24/2023.

La persona segnalante può comunicare all'ANAC le ritorsioni che ritiene di avere subito. In caso di ritorsioni commesse nel contesto lavorativo l'ANAC informa l'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza.

In tal senso, ai sensi dell'art. 19 del D.Lgs. n.24/2023 e al fine di acquisire elementi istruttori indispensabili all'accertamento delle ritorsioni, l'ANAC può avvalersi, per quanto di rispettiva competenza, della collaborazione dell'Ispettorato Nazionale del Lavoro, ferma restando l'esclusiva competenza dell'ANAC in ordine alla valutazione degli elementi acquisiti e all'eventuale applicazione delle sanzioni amministrative.
Gli atti assunti in violazione del divieto di ritorsione sono nulli.

Le persone segnalanti che siano state licenziate a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile hanno diritto a essere reintegrate nel posto di lavoro, ai sensi dell'art. 18 della L. 300/1970 (c.d. Statuto dei Lavoratori), o dell'art. 2 del D.Lgs. n. 23/2015, in ragione della specifica disciplina applicabile al lavoratore.

L'autorità giudiziaria adita adotta tutte le misure, anche provvisorie, necessarie ad assicurare la tutela alla situazione giuridica soggettiva azionata, ivi compresi il risarcimento del danno, la reintegrazione nel posto di lavoro, l'ordine di cessazione della condotta posta in essere in violazione

del sopra citato art. 17 e la dichiarazione di nullità degli atti adottati in violazione del medesimo articolo.

Infine quale limitazione della responsabilità della persona segnalante, ai sensi dell'art. 20 del D.Lgs. n. 24/2023, non è punibile il soggetto segnalante che riveli o diffonda informazioni sulle violazioni coperte dall'obbligo di segreto, diverso da quello di cui all'art. 1, c. 3, del suddetto decreto protette da segretezza, o relative alla tutela del diritto d'autore o alla protezione dei dati personali ovvero riveli o diffonda informazioni sulle violazioni che offendono la reputazione della persona coinvolta o denunciata, quando, al momento della rivelazione o diffusione, vi fossero fondati motivi per ritenere che la rivelazione o diffusione delle stesse informazioni fosse necessaria per svelare la violazione e la segnalazione, la divulgazione pubblica o la denuncia all'autorità giudiziaria o contabile è stata effettuata ai sensi dell'art. 16 del citato Decreto.

Fermo restando le tutele suddette garantite dalla normativa di riferimento, l'individuo che ritenga di aver subìto una discriminazione per il fatto di aver effettuato una segnalazione di illecito ne deve dare notizia immediata e circostanziata al soggetto Gestore delle segnalazioni.

Quest'ultimo, valutato quanto accaduto, ne dovrà riferire al Direttore di CEAR, per l'adozione di tutte le iniziative necessarie ed opportune in condivisione con il Consiglio di Amministrazione della Società.

- TRATTAMENTO DEI DATI PERSONALI

Ogni trattamento dei dati personali deve essere effettuato a norma del regolamento (UE) 2016/679 e del D.Lgs. n. 196/2003 (c.d. Codice Privacy). La comunicazione di dati personali da parte delle istituzioni, degli organi o degli organismi dell'Unione europea è effettuata in conformità del regolamento (UE) 2018/1725.

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

I trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni sono effettuati da CEAR, in qualità di titolare del trattamento, nel rispetto dei principi di cui agli articoli 5 e 25 del regolamento (UE) 2016/679, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.
CEAR definisce il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679.

- CONSERVAZIONE DELLA DOCUMENTAZIONE INERENTE ALLE SEGNALAZIONI

Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza e del trattamento dei dati personali sopra citati.

Se per la segnalazione si utilizza una linea telefonica registrata o un altro sistema di messaggistica vocale registrato, la segnalazione, previo consenso della persona segnalante, è documentata a cura del soggetto destinatario, di cui al canale di segnalazione interno, mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante trascrizione integrale. In caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Se per la segnalazione si utilizza una linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato la segnalazione è documentata per iscritto mediante resoconto dettagliato della conversazione a cura del soggetto destinatario, di cui al canale di segnalazione interno. La persona segnalante può verificare, rettificare e confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il soggetto Gestore del canale di segnalazione interno, essa, previo consenso della persona segnalante, è documentata a cura del suddetto soggetto Gestore delle segnalazioni mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

8. MODIFICHE DELLE MISURE DI PREVENZIONE DEI RISCHI

Qualora, a seguito delle segnalazioni e delle comunicazioni nei confronti degli organi di CEAR emergano elementi oggettivi idonei a rivelare carenze dei sistemi di controllo interno, il Consiglio di Amministrazione di CEAR dovrà tempestivamente provvedere al loro adeguamento o dare mandato al Direttore per le azioni correttive da porre in essere per l'adeguamento del sistema di controllo interno.

9. DOCUMENTI DI RIFERIMENTO

- Decreto Legislativo 231, 8 giugno 2001: "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della Legge 29 settembre 2000 n. 300" e successive modifiche ed integrazioni."
- Decreto Legislativo 24, 10 marzo 2023: "Attuazione della direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali."
- Modello di organizzazione, gestione e controllo adottato da CEAR.
- Codice Etico adottato da CEAR.
- Regolamentazione piattaforma informatica per applicazione procedura whistleblowing.

10. ALLEGATI ALLA PROCEDURA

-Regolamento piattaforma informatica – Piattaforma Whistletech

WHISTLETECH

Manuale operativo

Service	WHISTLETECH
Revision	1
Classification	Public
Software version	4.13.11

Sommario

Introduzione

WhistleTech è una piattaforma progettata per consentire la gestione sicura e anonima delle segnalazioni di whistleblowing. Questo strumento è fondamentale per le aziende che desiderano offrire un canale sicuro e affidabile per i propri dipendenti, collaboratori o fornitori che vogliano segnalare comportamenti illeciti o poco etici.

Questo manuale guiderà gli utenti attraverso il processo di utilizzo di WhistleTech per inviare e gestire segnalazioni in modo sicuro ed efficace.

Nei paragrafi dedicati, verrà trattata nel dettaglio l'operatività delle diverse figure coinvolte nel processo:

- **Segnalante (Whistleblower):** la persona che inserisce una segnalazione sulla piattaforma
- **Ricevente:** la persona che è abilitata a leggere, verificare e analizzare le segnalazioni dei whistleblower. I destinatari possono anche comunicare con i whistleblower tramite la piattaforma per richiedere ulteriori informazioni e prove, scambiando messaggi, anche in modo anonimo.
- **Custode:** la persona che può concedere o meno, al ricevente che ne fa richiesta, l'accesso all'identità del segnalante.

Autenticazione a due fattori e chiave di recupero account

A garanzia della sicurezza di accesso al sistema, le utenze con profilo di **Ricevente** e **Custode** sono protette mediante l'autenticazione a due fattori e la chiave di recupero account.

Autenticazione a due fattori

Le segnalazioni di whistleblowing spesso contengono informazioni sensibili e riservate.
L'autenticazione a due fattori contribuisce a garantire che solo gli utenti autorizzati possano accedere al sistema e visualizzare queste informazioni, riducendo il rischio di accessi non autorizzati.
Perciò, su ogni utenza è attiva l'autenticazione a due fattori tramite app authenticator standard.
Prima di procedere alla registrazione sulla piattaforma, l'utente dovrà scaricare sul suo smartphone personale una app di autenticazione. Solitamente consigliamo *Google Authenticator* o *Microsoft Authenticator* (o simili, purché compatibili con lo standard RFC 6238: TOTP).
Una volta ricevuta l'e-mail di registrazione, al primo login su WhistleTech, dopo aver impostato una password che il sistema rilevi come *Robusta*[1], ***verrà richiesto di sincronizzare la app con il QR code mostrato a video***, in modo che l'Authenticator rilasci poi dinamicamente un codice OTP di 6 cifre necessario al completamento dell'accesso.

Chiave di recupero dell'account

Per consentire agli utenti di recuperare l'accesso al proprio account in caso di perdita della password, il sistema implementa un meccanismo di recupero delle chiavi e mette a disposizione di ogni utente una chiave di recupero dell'account.
Questa misura garantisce che gli utenti in possesso della propria chiave di recupero dell'account possano sempre ripristinare l'accesso al proprio account e ai dati in esso contenuti.

Al primo accesso sulla piattaforma ***l'utente deve copiare la Recovery Key personale***, disponibile all'interno

[1] Una password robusta dovrebbe essere formata da lettere maiuscole, lettere minuscole, numeri e simboli, essere lunga almeno 12 caratteri e includere una varietà di almeno 10 input diversi.

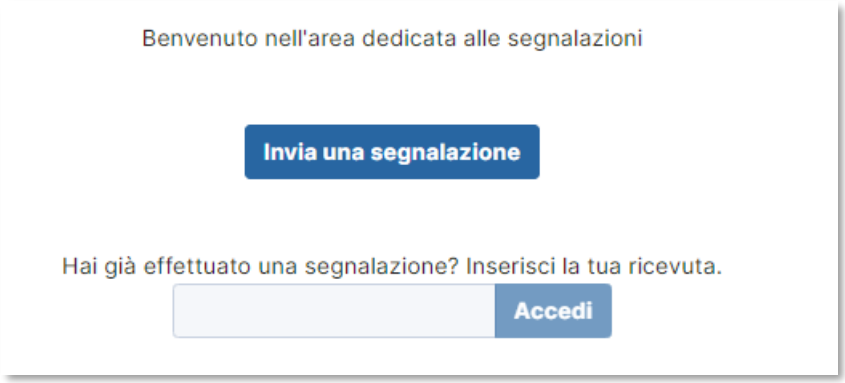
della sezione in *Preferenze --> Chiave di recupero account* e conservarla in modo sicuro. Senza questo codice, infatti, non sarà per lui possibile né completare un reset password, in caso di smarrimento della stessa, né accedere alla piattaforma e alle relative segnalazioni, in caso di perdita delle credenziali di accesso.

L'utenza sarebbe in questo caso da considerarsi 'perduta' e, con essa, le relative segnalazioni a cui ha accesso, dal momento che non abbiamo la possibilità di agire sulla password utente, nemmeno per rigenerarne una temporanea.

Segnalante: come effettuare e consultare una segnalazione

Compilazione ed invio della segnalazione

Il segnalate/whistleblower che vuole fare una segnalazione (di seguito: WB) accede alla piattaforma tramite web-browser all'URL della home page concordata. Non deve essere in possesso di un account, ma semplicemente cliccare sul tasto *Invia una segnalazione*



Se sulla piattaforma è stato configurato più di un canale, il WB deve selezionare quello di proprio interesse; diversamente, viene direttamente reindirizzato al questionario a step da compilare.

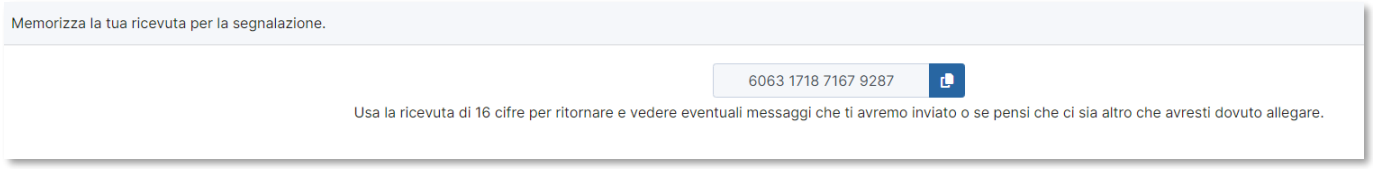
L'utente è guidato attraverso un modulo interattivo in cui potrà inserire le informazioni relative alla violazione o all'abuso che desidera segnalare.

Il modello in questione può includere risposte aperte o chiuse, e prevede l'obbligatorietà di risposta per alcune domande.

Se necessario e a seconda del questionario impostato, è possibile allegare documenti, immagini o altri file pertinenti alla segnalazione, oltre a registrare messaggi vocali.

Una volta completato il modulo, il WB può inviare la segnalazione, pigiando il tasto *Invia.*

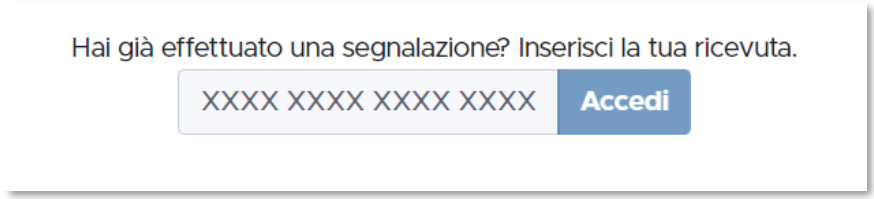
Al termine della procedura di segnalazione, il software restituirà come ricevuta un codice di 16 cifre.



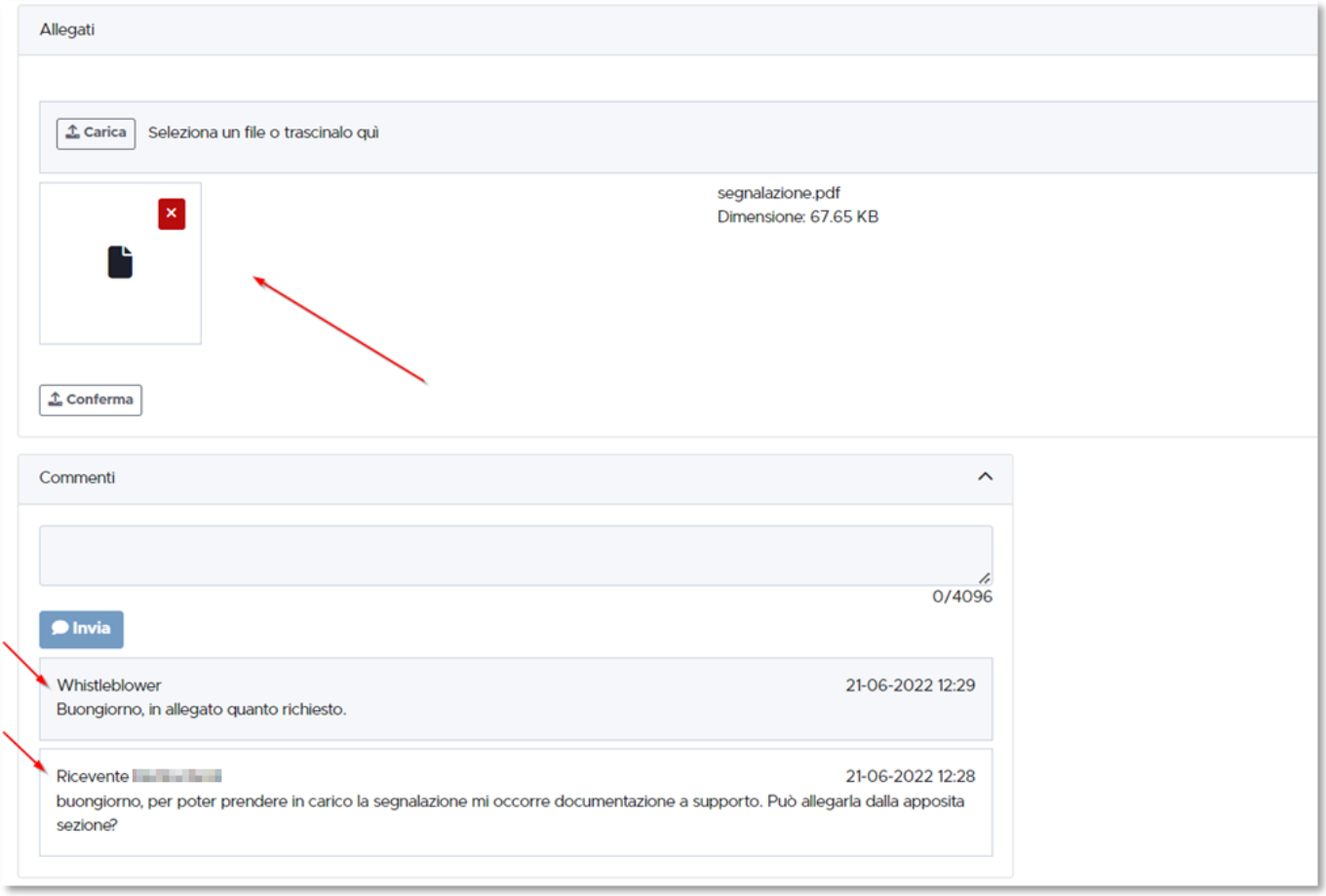
È molto importante ricordare che questo codice numerico deve essere copiato e custodito con cura, poiché costituisce l'unica possibilità, per il WB, di controllarne lo stato di presa in carico della segnalazione ed interagire con il gestore del canale. Se viene smarrito, non è in alcun modo possibile recuperarlo.

Accesso alla segnalazione ed interazione col Ricevente

Per accedere all'area riservata e visualizzare la segnalazione trasmessa è sufficiente premere il tasto *Vedi la tua segnalazione* oppure collegarsi alla homepage, inserendo il codice e premendo il tasto *Accedi*



Da questa sezione può inviare messaggi che saranno letti dal funzionario che segue la pratica, ed allegare anche documentazione a supporto, qualora fosse necessario o venisse richiesto



Ricevente: monitoraggio e gestione della segnalazione

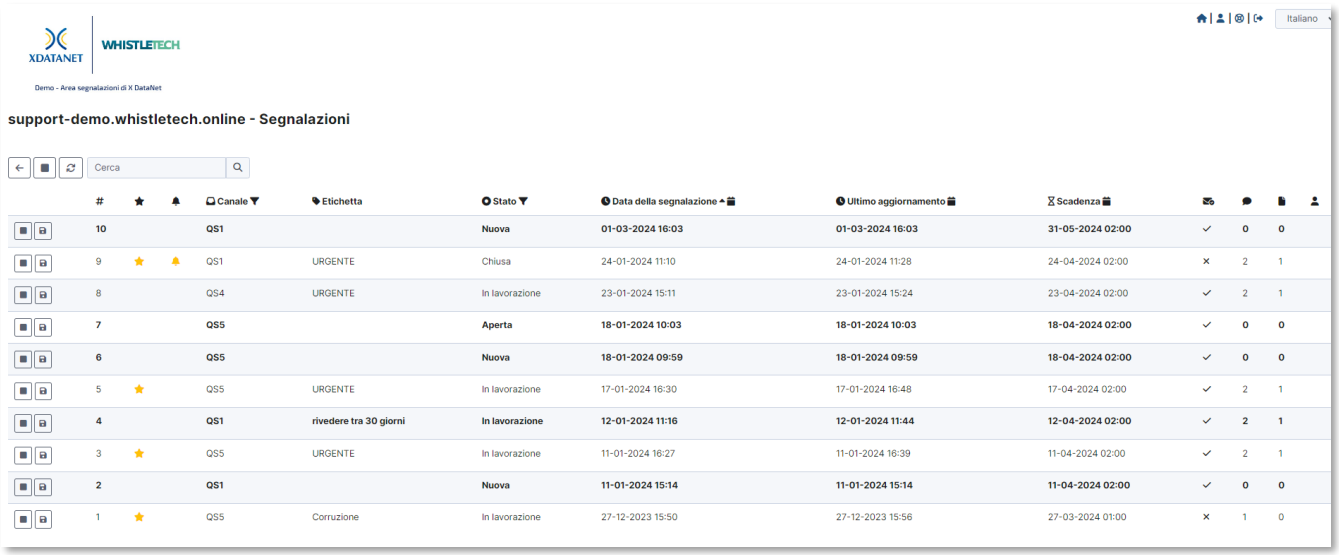
Accesso alla segnalazione ed interazione col Whistleblower

Per accedere alla piattaforma WhistleTech come Ricevente, è necessario avere le credenziali di accesso fornite dall'amministratore del sistema. Una volta ottenute le credenziali, è possibile accedere al sistema attraverso un browser web utilizzando l'URL relativo.

All'inserimento di una segnalazione da parte di un WB, al Ricevente sarà recapitata una e-mail, corredata dal link di accesso diretto.

A seconda dei canali a cui un Ricevente è abilitato, potrà vedere le segnalazioni di propria competenza.

La home page contiene, nella sezione *Segnalazioni*, l'elenco di tutte le pratiche a lui assegnate, a cui potrà accedere semplicemente cliccandoci sopra.



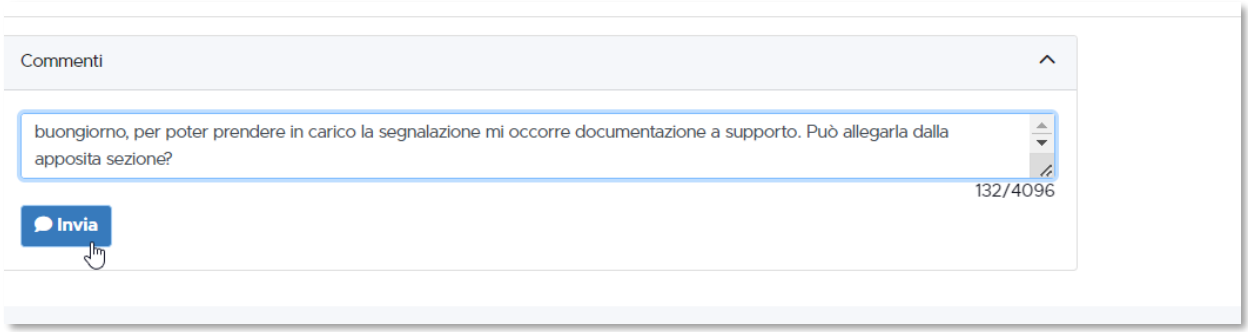
#	Canale	Etichetta	Stato	Data della segnalazione	Ultimo aggiornamento	Scadenza			
10	QS1		Nuova	01-03-2024 16:03	01-03-2024 16:03	31-05-2024 02:00	✓	0	0
9	QS1	URGENTE	Chiusa	24-01-2024 11:10	24-01-2024 11:28	24-04-2024 02:00	✗	2	1
8	QS4	URGENTE	In lavorazione	23-01-2024 15:11	23-01-2024 15:24	23-04-2024 02:00	✓	2	1
7	QS5		Aperta	18-01-2024 10:03	18-01-2024 10:03	18-04-2024 02:00	✓	0	0
6	QS5		Nuova	18-01-2024 09:59	18-01-2024 09:59	18-04-2024 02:00	✓	0	0
5	QS5	URGENTE	In lavorazione	17-01-2024 16:30	17-01-2024 16:48	17-04-2024 02:00	✓	2	1
4	QS1	rivedere tra 30 giorni	In lavorazione	12-01-2024 11:16	12-01-2024 11:44	12-04-2024 02:00	✓	2	1
3	QS5	URGENTE	In lavorazione	11-01-2024 16:27	11-01-2024 16:39	11-04-2024 02:00	✓	2	1
2	QS1		Nuova	11-01-2024 15:14	11-01-2024 15:14	11-04-2024 02:00	✓	0	0
1	QS5	Corruzione	In lavorazione	27-12-2023 15:50	27-12-2023 15:56	27-03-2024 01:00	✗	1	0

Cliccando sulla segnalazione desiderata, si aprirà così il dettaglio e sarà possibile per lui comunicare con il WB qualora dovesse avere richieste specifiche da sottoporgli.
Dalla schermata della segnalazione è anche possibile allegare files, video o immagini.

Nella sezione in basso, all'interno della pagina della segnalazione, vi sono tre aree differenti, contrassegnate con le etichette: *Pubblico, Interno, Personale*

- **Pubblico**: visibile al WB ed agli altri eventuali Riceventi attivi sul canale
- **Interno**: visibile, oltre a sé stesso, agli altri Riceventi di quel canale e a quelli eventualmente a cui è stato fornito l'accesso in un secondo momento
- **Personale**: visibile solo al Ricevente, in cui può inserire annotazioni private ed allegare documenti

Se il Ricevente vuole comunicare solo con il WB, dovrà quindi utilizzare la chat presente nel tab *Pubblico*

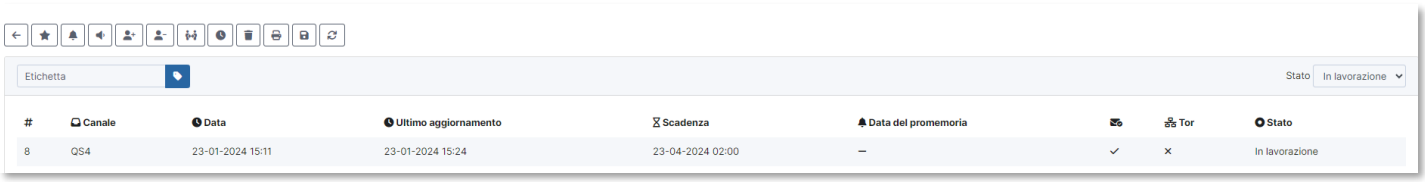


Inoltre, se vuole che il suo nome utente non sia visibile al WB, deve avere l'accortezza di impostare un *Nome Pubblico*, all'interno della sezione Preferenze della propria area personale.

Quando il WB manda un messaggio al Ricevente che sta interagendo con lui, quest'ultimo verrà sempre notificato via e-mail del fatto che vi è stato un aggiornamento della segnalazione.

Gestione della segnalazione e funzionalità applicative

Nella parte alta della schermata della segnalazione, compaiono tutte le funzionalità a disposizione del Ricevente.



È importante notare che alcune di esse (contrassegnate di seguito da un asterisco *) dipendono dalla configurazione dell'utenza Ricevente, decisa dalla propria organizzazione.

- **Segna come importante:**
  per contrassegnare come importante una segnalazione (la stella sarà visibile nella schermata delle *Segnalazioni*)
- **Imposta un promemoria:**
  per impostare un promemoria e-mail con una scadenza personalizzati
- **Disabilita e-mail di notifica:**
  Per disabilitare la ricezione delle e-mail di notifica relative alla segnalazione (sconsigliato)
- *** Consenti accesso:**
  per concedere l'accesso alla singola segnalazione ad altro/i Ricevente/i, così che possano gestire la segnalazione. Questo accesso include la visibilità anche dei commenti inseriti sia dal Ricevente che ha concesso l'accesso, che dal WB. La concessione è sempre reversibile per chi la effettua.

- *** Revoca accesso:** 

  per revocare l'accesso concesso con la modalità di cui sopra

- *** Trasferisci accesso:** 

  per trasferire l'accesso alla singola segnalazione ad altro Ricevente, così che possa gestire la segnalazione. Questo accesso include la visibilità anche dei commenti inseriti sia dal Ricevente che ha concesso l'accesso, che dal WB.

  Il trasferimento dell'accesso alla segnalazione non è reversibile ed il Ricevente che lo effettua poi non vedrà più la segnalazione in questione.

- *** Posticipa la data di scadenza:** 

  permette al Ricevente di modificare la data di scadenza della segnalazione (*report retention policy*), definita sul singolo canale.

  Alla scadenza del periodo impostato, infatti, la segnalazione viene automaticamente cancellata dalla piattaforma. **Il Ricevente può modificare la data di scadenza della segnalazione, eventualmente posponendola secondo le necessità del caso.**

  Inoltre, all'approssimarsi della scadenza impostata, una e-mail di promemoria con cadenza quotidiana informa il Ricevente che ha una o più segnalazioni in scadenza[2].

- *** Cancella:** 

  consente al Ricevente di anticipare la distruzione di una segnalazione, rispetto alla eventuale report retention policy impostata.

- **Stampa:** 

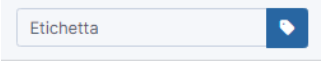
  permette al Ricevente di effettuare una stampa della pagina web.

- **Esporta:** 

  consente al Ricevente di esportare la segnalazione sottoforma di cartella zip con il contenuto testuale della pratica ed i files eventualmente allegati ad essa (foto, documenti, audio e video).

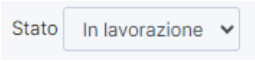
- **Aggiorna:** 

  consente di aggiornare la pagina

- **Etichetta:** 

[2] L'e-mail in questione viene spedita a partire da 3 giorni prima della scadenza della segnalazione stessa in caso di retention policy settata a 90 giorni, o da 21 giorni prima in caso di retention impostata da 180 giorni in su.

permette di inserire una etichetta sulla segnalazione, in modo da poterla categorizzare al meglio all'interno della vista Segnalazioni

- **Stato:** 

  Consente di cambiare stato alla segnalazione, scegliendo quello adatto dalle opzioni presenti nel menu a tendina

Richiesta al Custode per l'accesso all'identità del WB

Il Custode è una specifica utenza - o più di una - che non ha accesso alle segnalazioni: il suo ruolo fa sì che possa concedere o meno, al ricevente che ne fa esplicita e motivata richiesta, l'accesso all'identità del segnalante.

L'identità del segnalante non è nota al Custode: egli non è coinvolto nel trattamento dei dati personali presenti nella segnalazione. Tale ruolo può anche coincidere con quello di RPCT (Responsabile Prevenzione della Corruzione e Trasparenza).

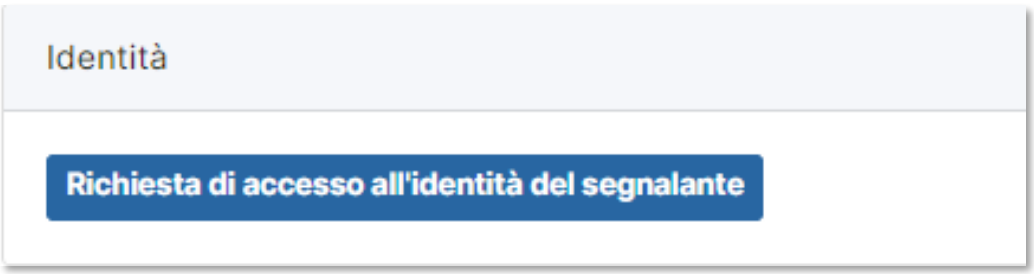
Questa funzionalità è utilizzabile mediante un modello di domanda predefinito che si attiva sul questionario, e fa sì che al ricevente i dati identificativi del whistleblower non siano visibili senza una specifica autorizzazione.

Se non si attiva il ruolo e non si utilizza questo modello di domanda, i dati relativi all'identità del whistleblower, se inseriti, saranno automaticamente visibili al ricevente.

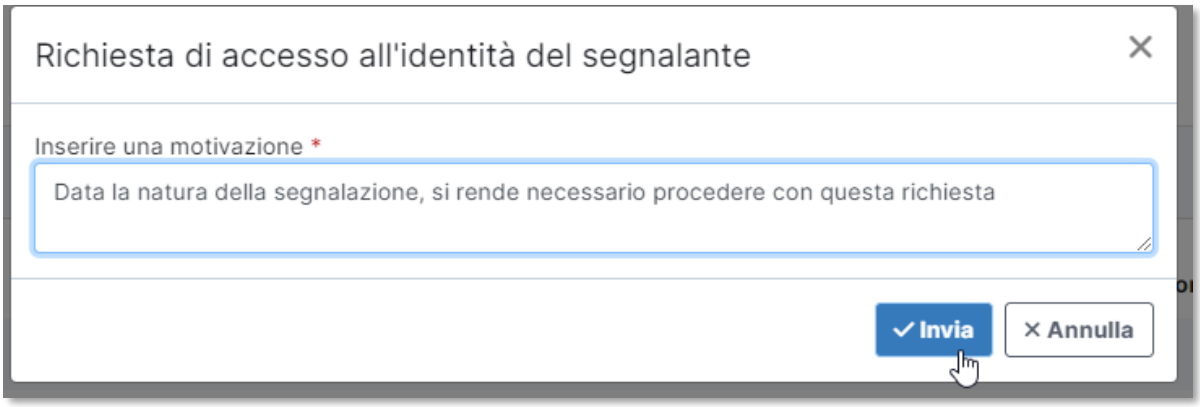
Si tratta di un ruolo specifico che va attivato qualora la vostra gestione del canale per il Whistleblowing lo richiedesse.

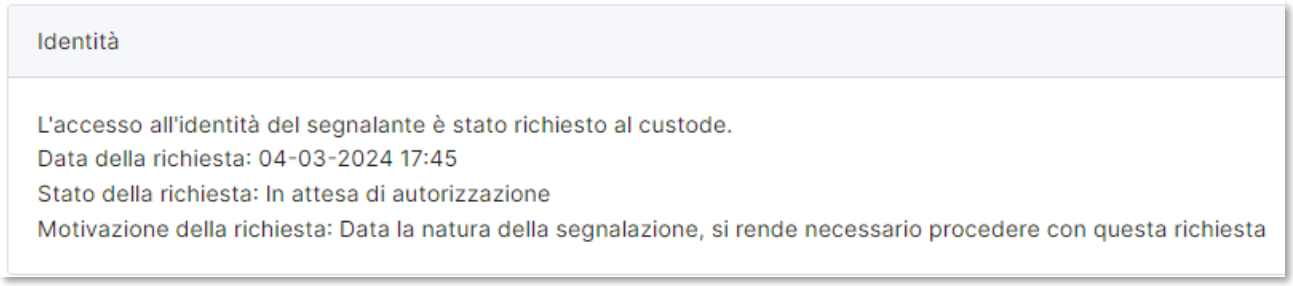
A seconda della configurazione del modello di questionario scelto, l'identità del WB potrebbe quindi essere nascosta al Ricevente.

In questo caso, egli avrà la possibilità di chiedere al Custode di rendergli visibile l'identità del WB: tale richiesta si attiva cliccando sull'apposito pulsante



Verrà richiesto inoltre di inserire una motivazione nella casella di testo, e si potrà procedere all'invio





La richiesta sarà in attesa fino all'intervento del Custode.

Ogni operazione da lui compiuta verrà notificata tramite e-mail al Ricevente.

Il Custode può anche negare il consenso, ed il Ricevente potrà opporsi e fare nuova richiesta cliccando sul pulsante.

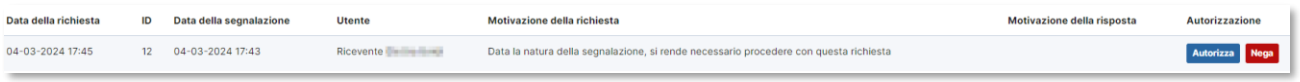
È importante ricordare che, una volta che i dati del WB sono stati resi accessibili al Ricevente che ne ha fatto richiesta, questi saranno visibili anche ad altri Riceventi eventualmente abilitati alla gestione della stessa segnalazione; lo stesso vale per quelli a cui viene fornito l'accesso alla pratica in un secondo momento.

Custode: come gestire una richiesta di accesso all'identità del WB

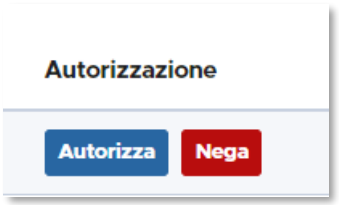
Per accedere alla piattaforma WhistleTech come Custode, è necessario avere le credenziali di accesso fornite dall'amministratore del sistema. Una volta ottenute le credenziali, è possibile accedere al sistema attraverso un browser web utilizzando l'URL relativo.

Se un Ricevente manda una richiesta di accesso all'identità di un WB, il Custode riceverà una e-mail, corredata dal link di accesso diretto.

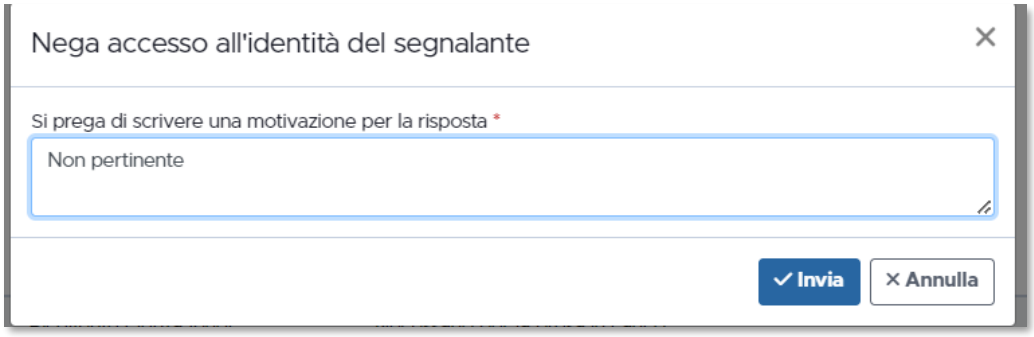
La home page contiene, nella sezione *Richieste*, l'elenco di tutte le pratiche pervenute.



Per autorizzare o negare dovrà premere sul pulsante corrispondente



Se sceglierà di negare l'accesso, dovrà inserire una motivazione



Il Ricevente verrà notificato e potrà comunque effettuare una nuova richiesta, motivandola.