1. Finalità

Il sistema di segnalazione di CMSA consente ai dipendenti di riportare, anche in forma anonima, comportamenti o fatti che possano arrecare danno, anche solo reputazionale, all'Azienda. Questo strumento è conforme al D.Lgs. 24/2023, che tutela chi segnala violazioni di normative nazionali o dell'Unione Europea apprese in ambito lavorativo, pubblico o privato.

Attraverso la piattaforma informatica dedicata al Whistleblowing, il personale CMSA e soggetti terzi possono segnalare fatti, anche omissivi, già avvenuti o potenzialmente futuri, riferibili a colleghi o terzi, che possano danneggiare CMSA. Le segnalazioni possono riguardare:

- Violazioni del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001;
- Infrazioni al Codice Etico di CMSA;
- Illeciti o irregolarità in violazione di leggi, regolamenti o procedure interne.

2. Chi può segnalare

Possono presentare una segnalazione:

- Dipendenti CMSA, sia a tempo determinato che indeterminato, inclusi candidati in fase di selezione o in prova;
- Stagisti durante lo svolgimento delle loro attività;
- Collaboratori e consulenti esterni;
- Lavoratori di aziende fornitrici o subappaltatori operanti per CMSA;
- Ex collaboratori o dipendenti di fornitori, se le informazioni sono state acquisite durante il rapporto lavorativo.

CMSA garantisce la gestione riservata anche delle segnalazioni anonime, purché sufficientemente dettagliate e pertinenti. Il segnalatore anonimo può in qualsiasi momento decidere di rivelare la propria identità per accedere alle tutele previste contro eventuali ritorsioni.

3. Che cosa segnalare

Le segnalazioni devono riguardare fatti, anche omissivi, riferibili a persone interne o esterne a CMSA, che possano costituire:

- Violazioni del Modello 231, del Codice Etico o di normative interne;
- Reati previsti dal D.Lgs. 231/2001 o da atti dell'Unione Europea;
- Atti lesivi degli interessi finanziari dell'UE o del mercato interno;
- Comportamenti che compromettono gli obiettivi delle normative europee;
- Illeciti che rientrano nell'ambito di applicazione degli atti dell'unione europea o nazionali (riportati nell'allegato al D.lgs 24/23), con particolare riguardo a:
  - Appalti pubblici;
  - Prevenzione del riciclaggio e del finanziamento del terrorismo;
  - Sicurezza e conformità dei prodotti;

- Sicurezza dei trasporti;
- Tutela dell'ambiente;
- Tutela della vita privata e protezione dei dati personali;
- Sicurezza delle reti e dei sistemi informativi.

Le segnalazioni devono basarsi su fatti conosciuti direttamente e su motivi fondati per ritenere che le informazioni siano veritiere.

Non sono considerate segnalazioni valide:

- Reclami o controversie personali legate al proprio rapporto di lavoro;
- Conflitti interpersonali non connessi a violazioni del Modello 231;
- Eventi della sfera privata non rilevanti per l'attività lavorativa.

Le segnalazioni devono essere effettuate il prima possibile, in modo da consentire una verifica efficace dei fatti.

4. Canali di segnalazione interni

Le segnalazioni possono essere trasmesse attraverso i seguenti canali:

1. **Piattaforma informatica** accessibile dal sito web aziendale (canale preferenziale);
2. **Modalità cartacea**, secondo le Linee Guida ANAC (Delibera n. 311 del 12 luglio 2023);
3. **Incontro verbale** con il personale incaricato (Internal Auditing o Presidente del CdA).

La **piattaforma informatica** è lo strumento raccomandato, in quanto garantisce maggiore riservatezza dell'identità del segnalante e adeguate misure di sicurezza informatica.
Attraverso la piattaforma è possibile:

- Inviare una nuova segnalazione;
- Aggiornare o integrare una segnalazione già inviata;
- Verificare lo stato di avanzamento;
- Ricevere un riscontro sull'esito della segnalazione.

5. Segnalazioni esterne e divulgazione pubblica

Il D.Lgs. 24/2023 consente di effettuare segnalazioni esterne all'**Autorità Nazionale Anticorruzione (ANAC)** o di **divulgare pubblicamente** le violazioni, ma solo nei seguenti casi:

- Il canale interno non è attivo o non è conforme alla normativa;
- La segnalazione interna non ha ricevuto seguito;
- Il segnalante ha fondati motivi per ritenere che la segnalazione interna non sarebbe efficace o comporterebbe ritorsioni;
- La violazione rappresenta un pericolo imminente o evidente per l'interesse pubblico.

6. Tutela del whistleblower

Le tutele previste dal D.Lgs. 24/2023 si applicano non solo al segnalante, ma anche a:

- Chi assiste il segnalante (facilitatore) nello stesso contesto lavorativo;
- Familiari e conviventi fino al quarto grado;
- Colleghi con un rapporto lavorativo attuale e regolare con il segnalante;
- Entità giuridiche collegate al segnalante (es. aziende di proprietà o presso cui lavora);

per **ritorsione** si intende qualsiasi atto, comportamento o omissione – anche solo minacciato – che, a seguito della segnalazione, possa causare un danno ingiusto, diretto o indiretto, al segnalante o a soggetti collegati.

Esempi di comportamenti ritorsivi

Sono considerati atti ritorsivi, tra gli altri:

- Licenziamento, sospensione o misure equivalenti;
- Declassamento o mancata promozione;
- Modifica delle mansioni, trasferimento, riduzione dello stipendio o variazione dell'orario di lavoro;
- Limitazione o esclusione da percorsi formativi;
- Valutazioni negative o referenze sfavorevoli;
- Sanzioni disciplinari o pecuniarie;
- Intimidazioni, molestie, isolamento o coercizione;
- Trattamenti discriminatori o comunque sfavorevoli;
- Mancata stabilizzazione del contratto a tempo determinato, in presenza di legittime aspettative;
- Mancato rinnovo o risoluzione anticipata del contratto;
- Danni alla reputazione, anche tramite social media, o perdite economiche e professionali;
- Inserimento in elenchi informali che ostacolano future opportunità lavorative;
- Risoluzione anticipata di contratti di fornitura;
- Revoca di licenze o permessi.

7. Gestione delle segnalazioni

Le segnalazioni vengono ricevute dai Responsabili Whistleblowing e sottoposte a valutazione congiunta con l'Ufficio Legale. La gestione delle stesse è affidata a un team dedicato, la cui composizione viene definita di volta in volta, in funzione della natura del reato oggetto della segnalazione.

- **Riscontro al segnalante**: entro 7 giorni dalla ricezione della segnalazione (art. 5, comma a, D.Lgs. 24/2023).

- **Conclusione dell'istruttoria**: entro 3 mesi dalla conferma di ricezione o, in assenza di conferma, entro 3 mesi dalla scadenza dei 7 giorni dalla presentazione (art. 5, comma d, D.Lgs. 24/2023).

8. Conservazione dei dati

Tutte le segnalazioni sono conservate per un periodo di **5 anni**, in modo sicuro e conforme al **Regolamento Generale sulla Protezione dei Dati (GDPR)**.

9. Formazione e sensibilizzazione

CMSA promuove la **formazione continua** del personale sulle modalità di segnalazione e sui **diritti e tutele del segnalante**, al fine di favorire una cultura aziendale improntata alla trasparenza e alla legalità.

CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA

1. Purpose

The CMSA reporting system allows employees to report, also anonymously, behaviours or facts that may damage the Company, even just from a reputational standpoint. This tool is compliant with Legislative Decree 24/2003, which protects whoever reports breaches of national / European Union laws learned in professional settings, both public and private.

Through the IT platform dedicated to whistleblowing, the CMSA personnel and third parties can report facts (including omissions) that have already happened or are likely to happen, and that are attributable to colleagues or third parties or may damage CMSA. The report may involve:

• Breaches of the Organization, Management and Control Model, pursuant to Legislative Decree 231/2001.

• Violations of CMSA Code of Conduct.

• Illegitimate actions or misconduct in breach of internal laws, regulations or procedures.

2. Who can report

A report may be submitted by:

• Both fixed-term and permanent CMSA employees, including candidates in the recruitment stage or in probation period.

• Trainees, while performing their activities.

• External coworkers and consultants.

• Workers from suppliers or subcontractors working for CMSA.

• Former coworkers or employees of suppliers, if the relevant information has been acquired during the professional relationship.

CMSA ensures the confidential management of anonymous reports, as long as the latter are detailed and relevant enough. The anonymous whistleblower may, at any time, decide to reveal his/her identity to access the protections in place against any retaliation.

3. What can be reported

The reports should involve facts (including omissions) that are attributable to CMSA external or internal people and may constitute:

• Breaches of Model 231, the Code of Conduct or internal laws.

• Offenses under Legislative Decree 231/2001 or European Union acts.

• Acts prejudicial to the EU financial interests or the internal market.

• Behaviours that may compromise the goals of European laws.

• Illegitimate actions falling within the scope of European Union or national acts (reported in the annex to Legislative Decree 24/23), with specific focus on:

- Public contracts.

- Prevention of recycling and funding of terrorism.

- Product safety and compliance.

- Transport safety.

- Protection of the environment.

- Protection of private life and personal data.

- Safety of networks and information systems.

The reports should be based on facts personally known and reasonable grounds to think that the information is truthful.

The following shouldn't be regarded as valid reports:

• Complaints or personal disputes related to one's own professional relationship.

• Interpersonal conflicts which aren't related to breaches of Model 231.

• Private events which aren't relevant for one's own professional activity.

The reports should be submitted as soon as possible, to allow an effective assessment of facts.

4. Internal reporting channels

The reports can be submitted through the following channels:

1. IT platform accessible from the company website (preferential channel);

2. Paper format, according to the ANAC guidelines (Deliberation no. 311, of 12 July 2023);

3. Verbal meeting with the designated staff (Internal Auditing or President of the Board of Directors).

The IT platform is the recommended tool, since it ensures more confidentiality as regards the whistleblower's identity and adequate IT safety measures.

The platform allows to:

• Send a new report.

• Update or integrate a report that had already been sent.

• Assess the progress status.

• Receive feedback on the outcome of the report.

5. External reporting and public disclosure

Legislative Decree 24/2023 allows to submit external reports to the Italian National Anti-Corruption Authority (ANAC) or to publicly disclose breaches, but only in the following cases:

• The internal channel isn't active or compliant to the law.

• The internal report did not lead to further action.

• The whistleblower has reasonable grounds to think that the internal report isn't effective or may lead to retaliation.

• The breach constitutes an impending or clear danger for public interest.

6. Protection of whistleblowers

The protections provided for by Legislative Decree 24/2023 do not just apply to the whistleblower, but also to:

• Whoever assists the whistleblower (facilitator) in the same professional setting.

• Family members and cohabiting persons, up to the fourth degree of kinship.

• Colleagues with a current and regular professional relationship with the whistleblower.

• Legal entities related to the whistleblower (e.g., companies owned by the whistleblower or where the latter works).

with the term retaliation, we refer to any acts, behaviours or omissions – even just threatened – which, following the report, may lead to wrongful (direct or indirect) damage to the whistleblower or any related subjects.

Examples of retaliatory behaviours

The following are regarded as retaliatory acts, among others:

• Dismissal, suspension or equivalent measures.

• Downgrading or non-promotion.

• Change of duties, relocation, reduction in salary or change of working hours.

• Limitation or exclusion from educational pathways.

• Negative assessments or unfavorable references.

• Disciplinary or financial penalties.

• Intimidation, harassment, isolation or coercion.

• Discriminatory or unfavorable treatments.

• Failure to convert a fixed-term contract into a permanent one, in presence of legitimate expectations.

• Failure to renew or terminate the contract early.

• Reputational damage, also through social media, or economic and professional losses.

• Insertion into informal lists that may impair future professional opportunities.

• Early termination of supply contracts.

• Revocation of licenses or permits.

7. Management of reports

Reports are received by Whistleblowing Managers and assessed jointly with the Legal Department. Their management is entrusted to a dedicated team, whose structure is defined periodically, in function of the crime to be reported.

• Feedback to the whistleblower: within 7 days of receipt of report (article 5, paragraph a, Legislative Decree 24/2023).

• Conclusion of the investigation: within 3 months of receipt of report or, in the absence of confirmation, within 3 months of the deadline of 7 days from the date of submission (article 5, paragraph d, Legislative Decree 24/2023).

8. Data retention

All reports are retained for 5 years, in a safe manner and compliant to the General Data Protection Regulation (GDPR).

9. Training and awareness

CMSA promotes the continuous training of staff members on reporting methods and rights and protections of the whistleblower, aimed at promoting a company culture focused on transparency and lawfulness.

CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA

SEGN.IO.01

ISTRUZIONE DEL SISTEMA DI GESTIONE INTEGRATO

CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CSA CMSA CMSA CMSA

Manuale Piattaforma Whistleblowing

SOMMARIO

1 SCOPO 2
2 CAMPO DI APPLICAZIONE 2
3 PROCEDURA 2
3.1 Accesso 2
3.2 Modalità con fornitura dati da parte del segnalatore 3
3.3 Modalità accesso anonimo 6
3.4 InBox Sicura 6
4 CONCLUSIONI 9
5 NOTE 11

CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CSA CMSA CMSA CMSA

LISTA REVISIONI

Revisione	Data	Descrizione	Redazione	Verifica	Approvazione
00	05/06/2023	Emissione	Bruno Di Biase	Daniela Iacomelli	Emanuele Natalini

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione

1 SCOPO

Lo scopo di questo documento è quello illustrare agli utenti interni aziendali, ma anche a chiunque voglia usufruirne, la procedura che l'azienda ha messo a disposizione per l'inserimento di segnalazioni con riferimento alla normativa cosiddetta "Whistleblowing".

Si fa notare, comunque, che le segnalazioni (ai sensi dell'art. 4 comma 3 D.lgs. 24/2023) possono essere effettuate (in alternativa al portale descritto in questo documento) anche:

- in forma scritta

- forma orale

- su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole.

Inoltre, all'interno del portale stesso, nella sezione "Informativa sulla Privacy" è riportata un'informativa relativa al trattamento dei dati personali inseriti.

2 CAMPO DI APPLICAZIONE

La procedura si applica in tutti quei casi in cui si desidera utilizzare la piattaforma di Whistleblowing fornita dalla società EQS a CMSA Società Cooperativa.

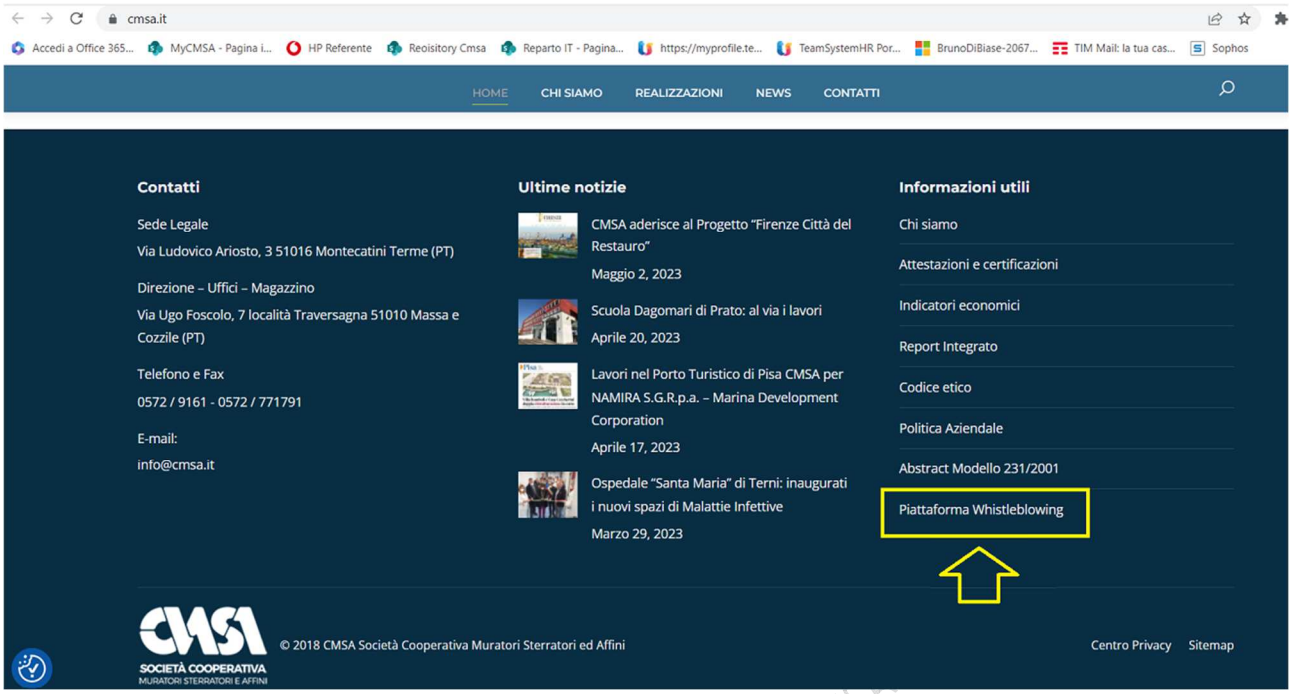
3 PROCEDURA

Di seguito il dettaglio delle modalità operative

3.1 *Accesso*

L'accesso alla piattaforma può avvenire sia attraverso l'apposito link pubbicato nell'area "contatti" del sito www.cmsa.it :

CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA



Oppure digitando , in qulasiasi browswer , il seguente indirizzo :

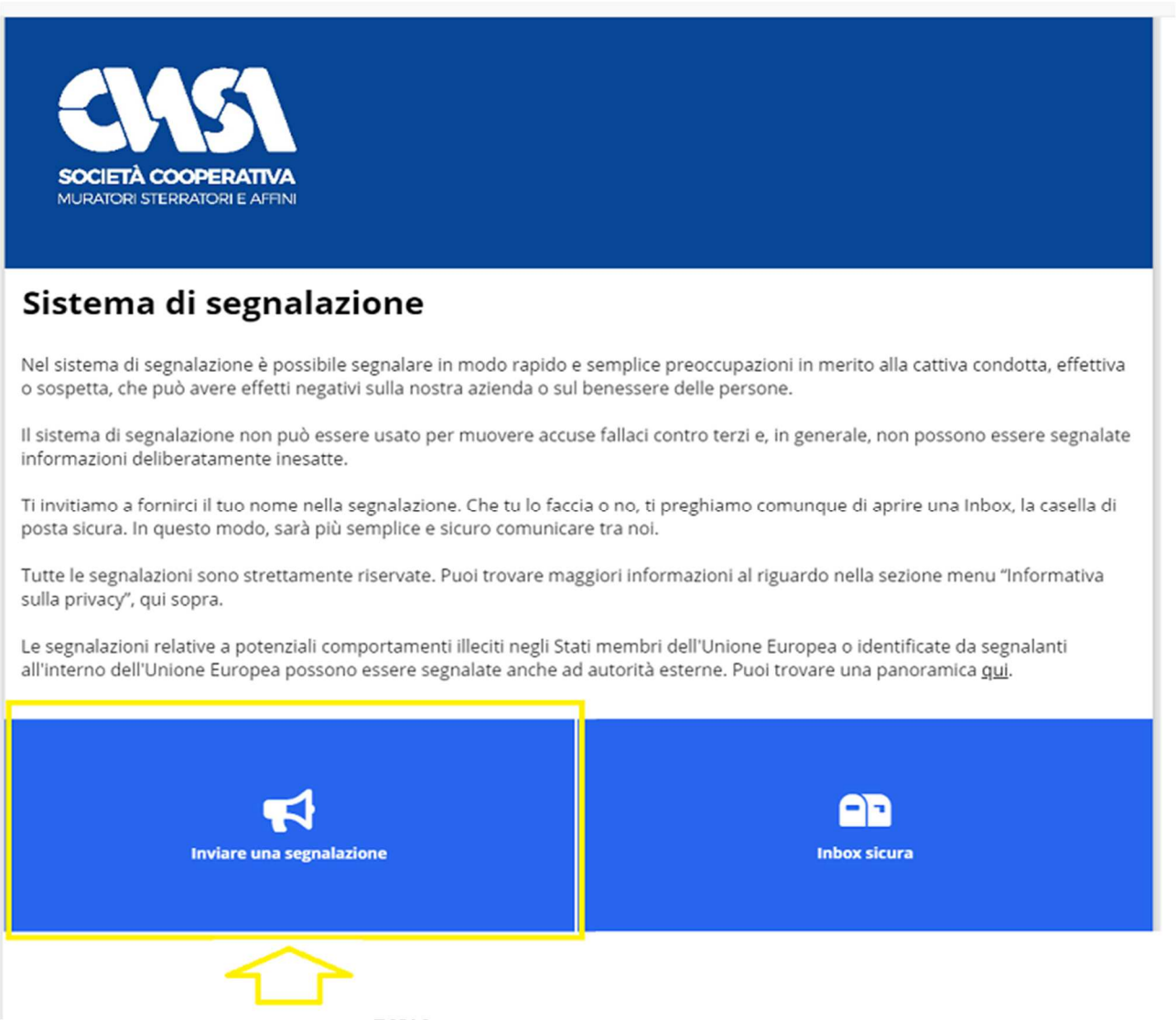
https://cmsa.integrityline.com/frontpage.

3.2 *Modalità di segnalazione con comunicazione dati del segnalante*

Prima azione: Selezionare il tasto "Inviare una nuova segnalazione";

CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione

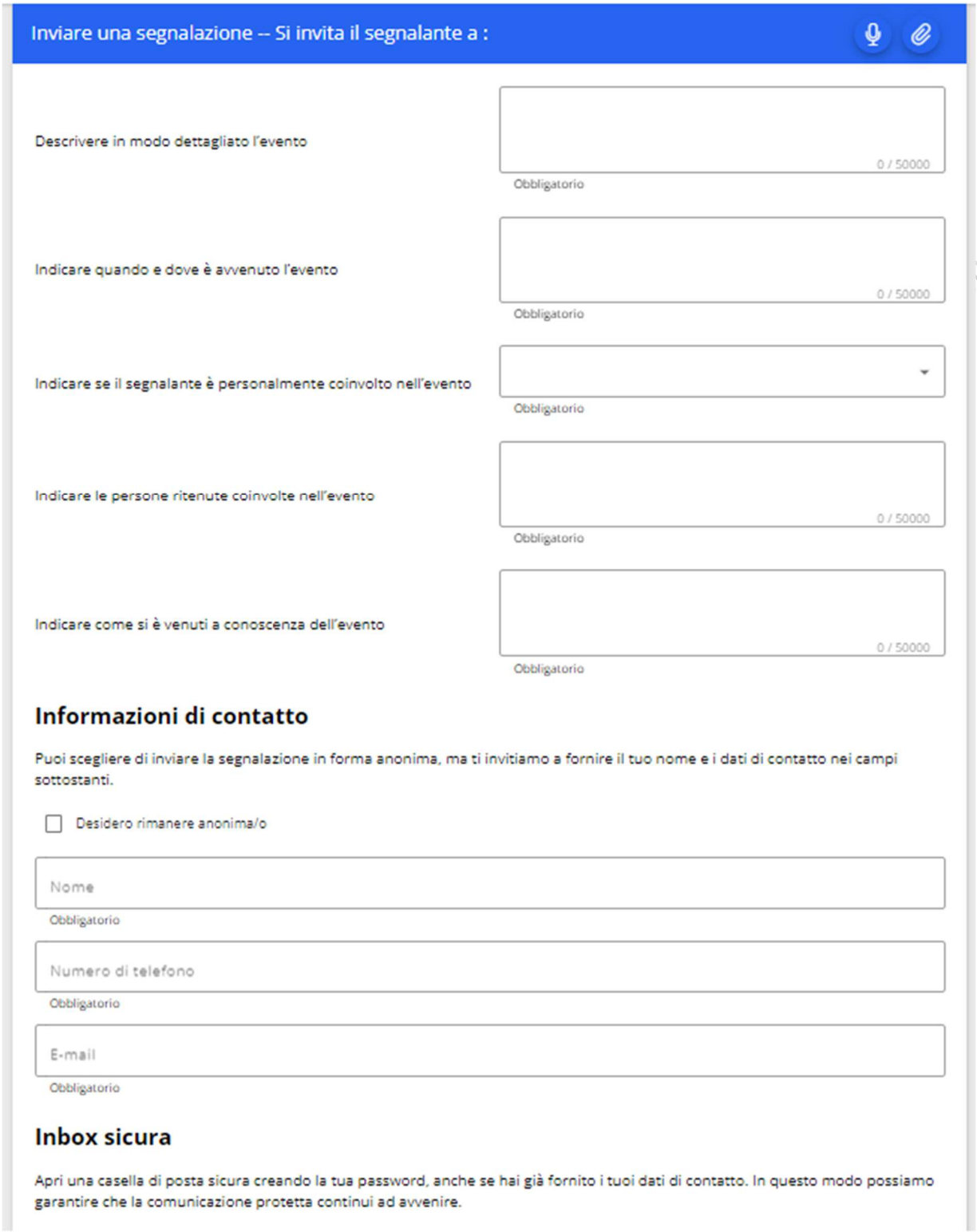


Seconda azione: Inserire le informazioni richieste (fare attenzione a quelle obbligatorie):

Terza azione: Inserire i propri dati di contatto, se il segnalante non vuole rimanere anonimo.

CMSA CMSA CMSA CMSA CMSA

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione



Inviare una segnalazione -- Si invita il segnalante a :

Descrivere in modo dettagliato l'evento
0 / 50000
Obbligatorio

Indicare quando e dove è avvenuto l'evento
0 / 50000
Obbligatorio

Indicare se il segnalante è personalmente coinvolto nell'evento
Obbligatorio

Indicare le persone ritenute coinvolte nell'evento
0 / 50000
Obbligatorio

Indicare come si è venuti a conoscenza dell'evento
0 / 50000
Obbligatorio

Informazioni di contatto

Puoi scegliere di inviare la segnalazione in forma anonima, ma ti invitiamo a fornire il tuo nome e i dati di contatto nei campi sottostanti.

Desidero rimanere anonima/o

Nome
Obbligatorio

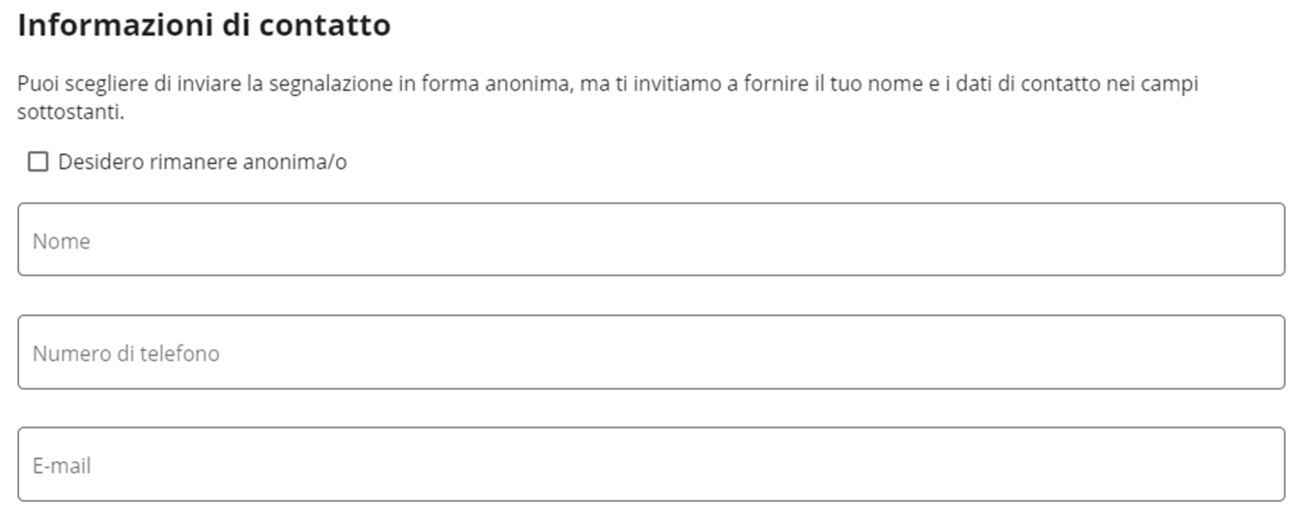
Numero di telefono
Obbligatorio

E-mail
Obbligatorio

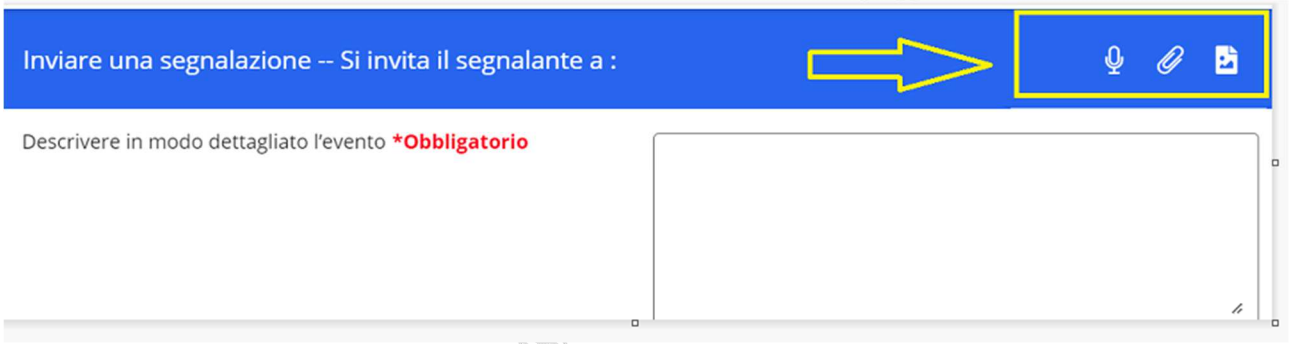
Inbox sicura

Apri una casella di posta sicura creando la tua password, anche se hai già fornito i tuoi dati di contatto. In questo modo possiamo garantire che la comunicazione protetta continui ad avvenire.

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione

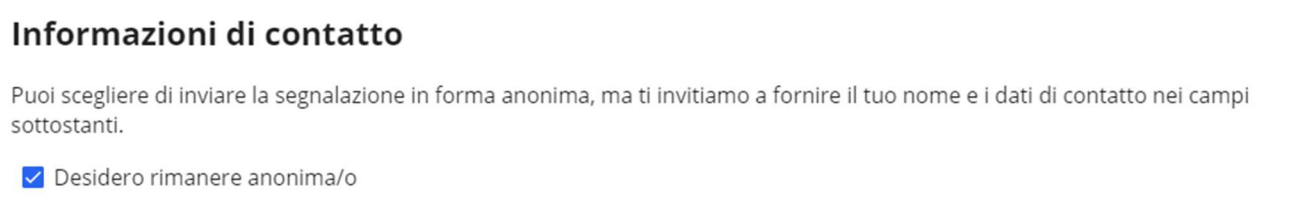


Quarta azione: Sarà inoltre possibile allegare registrazioni , file attraverso i tasti dedicati :



3.3 *Modalità di segnalazione anonima*

E' anche possibile inviare una segnalazione anonima, in questo caso dopo la prima e la seconda azione, ed a scelta la terza azione, deve essere selezionato il campo specifico seguente:



In questo caso, per poter interagire con l'azienda è necessario attivare una ***InBox sicura*** come di seguito illustrato.

3.4 *InBox Sicura*

Per l'attivazione della InBox sicura, inserire una password a propria scelta nello specifico campo :

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione

Inbox sicura

Si prega di aprire una casella di posta elettronica sicura creando una propria password, anche se si sono già inseriti i propri dati di contatto. In questo modo, sarà più semplice e sicuro comunicare tra noi.

Utilizza la Inbox - casella postale se desideri inviare ulteriori informazioni o rispondere a potenziali domande.

Quando crei la Inbox, ti sarà assegnato un numero della segnalazione e sceglierai una password. Usa il numero della segnalazione e la password per accedere alla Inbox e vedere se hai ricevuto domande. Se lo desideri, tutte le nostre comunicazioni saranno anonime.

Una volta che la tua segnalazione è stata trattata, puoi trovare la risposta nella Inbox - casella postale. Sarai informato via email. Nel caso di una registrazione che non richieda un'approvazione, ti contatteremo solo in caso di domande.

Inserisci la tua password

La password deve:

- Avere una lunghezza minima di 8 caratteri.
- Deve contenere almeno una lettera minuscola e una maiuscola.
- Contenere almeno un numero.

Password

Inserisci nuovamente la password

☐ Ho letto e capito l'Informativa sulla privacy e accetto.

Il sistema risponderà comunicando un codice univoco che , insieme alla pasword , consentirà di verificare l'avanzamento della propria richiesta ed interagire con l'azienda.

Conferma

Grazie. Abbiamo ricevuto la tua segnalazione. Inizieremo a trattare il tuo caso il più presto possibile.

Una volta che la tua segnalazione è stata trattata, puoi trovare la risposta nella Inbox - casella postale. Sarai informato via email. Nel caso di una registrazione che non richieda un'approvazione, ti contatteremo solo in caso di domande.

Importante:

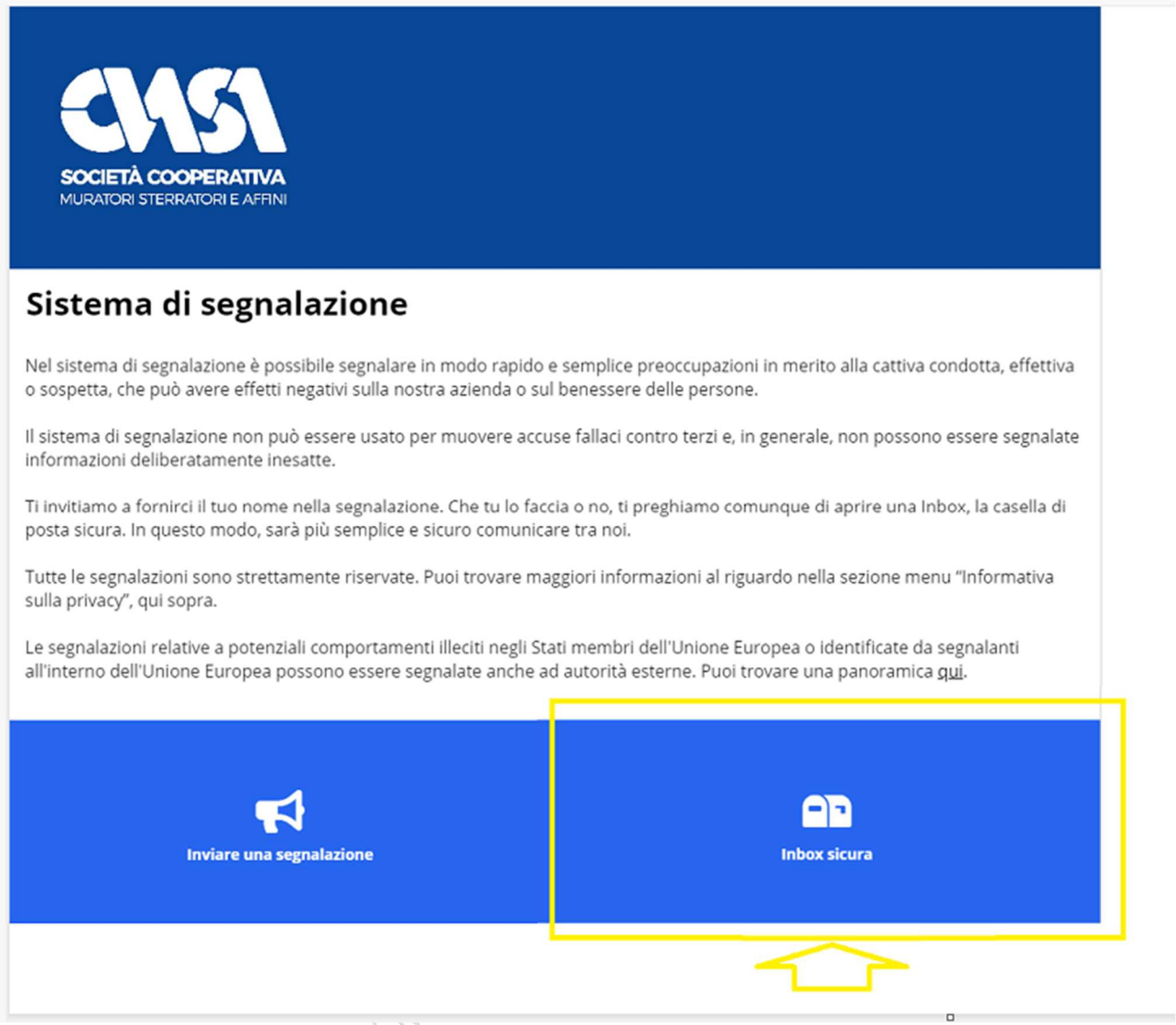
Ti suggeriamo di accedere all'interno della Inbox sicura (Casella postale) e prendere nota del numero della segnalazione e della Password. Questo ti consentirà di effettuare il login in un secondo momento.

Il numero della tua segnalazione è : XXXXXXXX

Hai aperto una Inbox - casella postale sicura. Per accedere alla casella postale, devi utilizzarela password che hai appena digitato. Se si dimentica una delle credenziali (Numero della segnalazione / Password), è necessario inviare una nuova segnalazione. Per motivi di sicurezza e di tutela dell'anonimato, non possiamo recuperarle.

Quando il segnalante seleziona quindi il tasto "Inbox Sicura"

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione

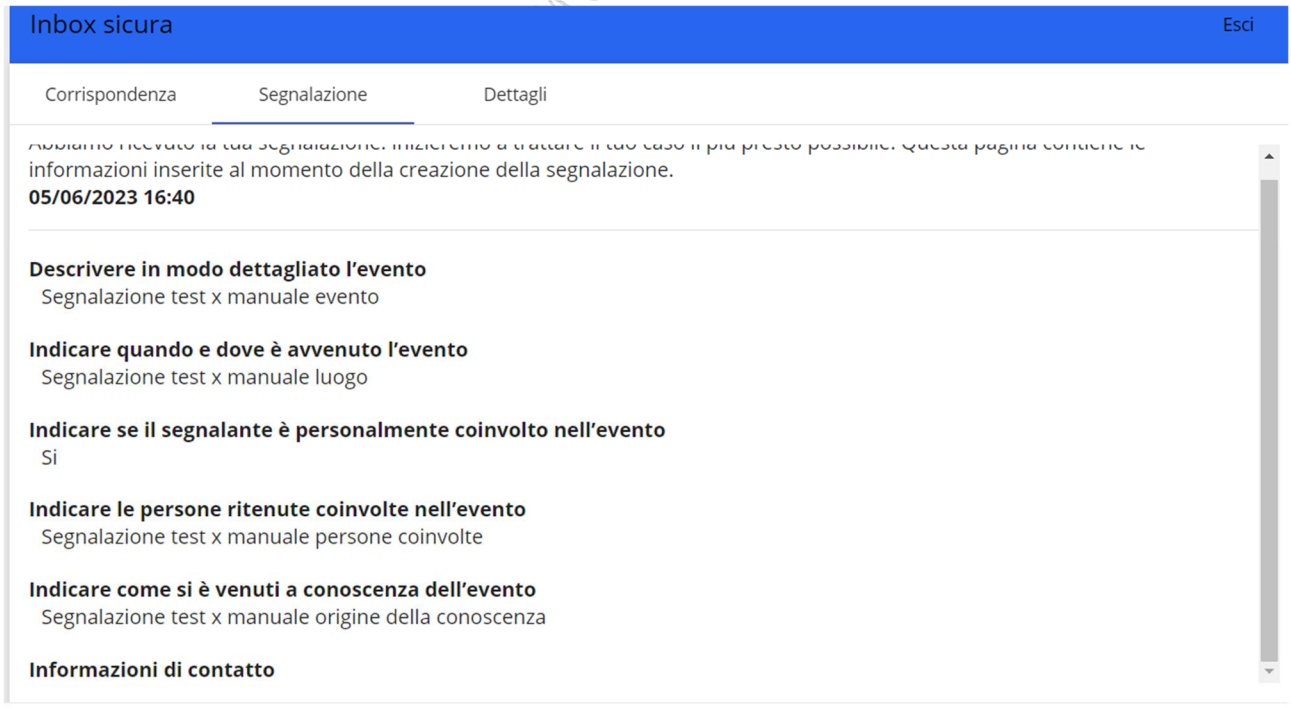


appare una schermata in cui viene richiesto il codice di segnalazione (numero della segnalazion) e la password di accesso inserita, come di seguito:

CMSA CMSA CMSA CMSA CMSA CMSA

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione

Dopo aver inserito le credenziali, sarà possibile accedere allo storico della segnalazione e inviare nuovi messaggi e/o allegare nuova documentazione.



4 CONCLUSIONI

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione

Riassumendo la piattaforma consente l'invio di segnalazioni verso le funzioni incaricate da CMSA alla ricezione sia comunicando le generalità del segnalante sia omettendo le stesse scegliendo la modalità anonima; in ogni caso sarà possibile monitorare la pratica (sia da parte del segnalante che della persona incaricata da CMSA) che interagire a mezzo chat ed inserire documentazione aggiuntiva.

CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione

5 NOTE

_____

_____

_____

_____

_____

_____

_____

_____

CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA CMSA

Questo documento è di proprietà CMSA; ne è vietata la riproduzione o la consegna a Terzi senza autorizzazione