NOVOTEMA SPA
Whistleblowing

REPORTS MANAGEMENT PROCEDURE
Issued on 29.04.2024.
(English version below, see pag.6)

Il presente documento rappresenta la procedura di gestione delle segnalazioni ricevute e gestite da parte di NOVOTEMA SPA (la Società), ai sensi della normativa Whistleblowing.
La procedura è conforme alle novità normative introdotte dal D.lgs. 10 marzo 2023, n. 24 di attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 (c.d. "Decreto Whistleblowing").
Il processo di gestione delle segnalazioni è parte integrante del Codice Etico di NOVOTEMA SPA.
Per l'invio e la gestione delle segnalazioni la Società ha implementato una piattaforma informatica dedicata, che costituisce il canale preferenziale per l'invio delle segnalazioni.
La procedura adottata dalla Società sarà revisionata in occasione di eventuali novità normative, con una verifica almeno annuale dell'esigenza di revisione.

1. Riferimenti normativi

Il Whistleblowing è stato introdotto in Italia con una legislazione specifica a fine 2017, con la legge n.179. Questa normativa regolamentava in modo completo l'istituto per la pubblica amministrazione, mentre introduceva alcune disposizioni anche per le organizzazioni del settore privato dotate di un modello organizzativo di gestione e controllo ex. D.Lgs. n.231/2001.
La legge n.179/2017 è stata superata dalla legge di trasposizione della Direttiva Europea in materia di whistleblowing (n.1937/2019).
La nuova legge, il D.lgs. 10 marzo 2023, n. 24, è l'attuazione della Direttiva UE n.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 (c.d. "Decreto Whistleblowing"). La nuova normativa prevede oneri in capo alle organizzazioni pubbliche e private, in particolare: tutti gli enti pubblici devono prevedere procedure interne per la gestione delle segnalazioni; lo stesso obbligo è in carico ai soggetti del settore privato che hanno un modello organizzativo ex D.Lgs. n.231/2001 e a tutte le organizzazioni private con almeno 50 dipendenti.

2. Chi può effettuare segnalazioni

Le procedure di whistleblowing incoraggiano a effettuare segnalazioni chiunque acquisisca, nel contesto dell'attività lavorativa, informazioni sugli illeciti commessi dall'organizzazione o per conto dell'organizzazione.
Lo scopo della procedura è quello di facilitare la comunicazione di informazioni relative a violazioni riscontrate durante l'attività lavorativa.
A tale scopo lo spettro delle potenziali persone segnalanti è molto ampio.
La procedura è volta a garantire questi soggetti, nel momento in cui segnalino una condotta illecita relativa alla Società.
Possono effettuare una segnalazione attraverso la procedura le seguenti categorie di soggetti:

- Dipendenti
- Collaboratori
- Fornitori, subfornitori e dipendenti e collaboratori degli stessi o Liberi professionisti, consulenti, lavoratori autonomi
- Volontari e tirocinanti, retribuiti o non retribuiti
- Azionisti o persone con funzione di amministrazione, direzione, vigilanza, controllo o rappresentanza
- Ex dipendenti, ex collaboratori o persone che non ricoprono più una delle posizioni indicate in precedenza
- Soggetti in fase di selezione, di prova o il cui rapporto giuridico con la Società non sia ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali.

La procedura protegge anche l'identità dei soggetti facilitatori, le persone fisiche che assistono una persona segnalante nel processo di segnalazione, operanti all'interno del medesimo contesto lavorativo.

3. Cosa può essere segnalato

All’interno di questa procedura possono essere segnalati fatti illeciti di cui si sia venuti a conoscenza nel contesto della propria attività lavorativa. Possono essere riportati anche sospetti, qualificati, di reati o altre violazioni di disposizioni di legge o potenziali rischi di commissione degli stessi.

Non viene richiesto alla persona segnalante di dimostrare in modo completo la commissione di un illecito ma le segnalazioni devono essere quanto più possibile circostanziate, al fine di consentire un accertamento dei fatti comunicati da parte dei soggetti riceventi. Allo stesso tempo, non si invitano i soggetti segnalanti ad attuare attività di investigazione che possano esporli individualmente.
Le segnalazioni possono riguardare:

- illeciti penali,
- illeciti civili,
- illeciti amministrativi o contabili,
- violazioni di normative comunitarie,
- violazioni del Codice Etico adottato dalla Società.

Non rientrano nell’oggetto di questa procedura le segnalazioni di carattere personale, per esempio inerenti al proprio contratto di lavoro, che sono regolate da altre procedure della Società.
Le segnalazioni possono essere effettuate nei confronti di:

- Azionisti o persone con funzione di amministrazione, direzione, vigilanza, controllo o rappresentanza;
- i dipendenti;
- i collaboratori;
- i consulenti;
- i lavoratori e i collaboratori delle imprese fornitrici di beni o servizi presso la Società;
- altri soggetti che a vario titolo interagiscono con la Società stessa.

4. Chi riceve e gestisce le segnalazioni

Il Responsabile dei Sistemi Interni di Segnalazione (RSIS) è il soggetto responsabile alla ricezione e gestione delle segnalazioni di illecito.
Il RSIS, nominato con atto interno dagli Amministratori, è coadiuvato da un soggetto del suo gruppo di supporto specificamente e similmente nominato in atto interno (Coadiutore del RSIS).
Il Responsabile dei Sistemi Interni di Segnalazione, o il coadiutore ove nominato, riceve le segnalazioni e dialoga con la persona segnalante per chiarire e approfondire quanto ricevuto.
Il dialogo con la persona segnalante continua anche durante le fasi di accertamento.
Il Segnalante può scegliere se inviare la propria segnalazione al RSIS, al Coadiutore, o a entrambi; questo per garantire una alternativa al segnalante ed inoltre per evitare una potenziale coincidenza tra soggetto Segnalato e soggetto Ricevente la segnalazione.
Il responsabile e/o il coadiutore, dopo una valutazione iniziale, svolgono un’attività di accertamento delle informazioni segnalate, anche richiedendo specifiche informazioni ad altri uffici e funzioni interni all’organizzazione.
Il Ricevente fornisce riscontri periodici alla persona segnalante e, al termine dell’attività di accertamento, comunica l’esito delle attività di accertamento. Nella comunicazione dell’esito non sono inclusi riferimenti a dati personali relativi all’eventuale soggetto segnalato.
Tra i possibili esiti che possono essere comunicati alla persona segnalante ci sono:

- Correzione di processi interni
- Avvio di un procedimento disciplinare
- Trasferimento dei risultati delle attività di accertamento alla Procura della Repubblica
- Archiviazione per mancanza di evidenze.

5. I canali di segnalazione interni

La Società mette a disposizione delle persone segnalanti canali diversi per le segnalazioni di violazioni ai sensi della presente procedura.
In particolare, è possibile effettuare segnalazioni in forma scritta o in forma orale.
Per quanto riguarda le segnalazioni in forma scritta, la Società mette a disposizione una piattaforma informatica crittografata; la piattaforma utilizza Whistleblower Software ApS..

La piattaforma informatica costituisce lo strumento preferenziale per l'invio e la gestione delle segnalazioni, in quanto maggiormente idoneo a garantire, da un punto di vista tecnologico, adeguate misure di sicurezza delle informazioni, la riservatezza dell'identità del Segnalante e dei soggetti menzionati nella segnalazione e del contenuto della stessa.
Sulla piattaforma è caricato un questionario che guida la persona segnalante nel percorso di segnalazione attraverso domande aperte e chiuse, di cui alcune obbligatorie.
Tramite la piattaforma è possibile nel dettaglio:

- selezionare la lingua dell'interfaccia (Italiano o Inglese, quest'ultima a beneficio di eventuali segnalatori esteri);
- scegliere il soggetto a cui si vuole indirizzare la segnalazione (Ricevente) tra quelli incaricati dalla Società;
- inviare una segnalazione;
- allegare documenti alla segnalazione;
- modificare o aggiornare una segnalazione inviata;
- consultare lo stato di una segnalazione inviata;
- ricevere riscontro sul seguito dato alla segnalazione.

La piattaforma consente di:

- separare i dati identificativi del Segnalante dal contenuto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima;
- mantenere riservato il contenuto della segnalazione durante l'intera fase di gestione della stessa, consentendo l'accesso ai soli soggetti autorizzati;
- adottare protocolli sicuri per il trasporto dei dati in rete nonché l'utilizzo di strumenti di crittografia per il contenuto della segnalazione e dell'eventuale documentazione allegata;
- interagire con il Segnalante, garantendone l'anonimato.

Al termine della segnalazione la persona segnalante riceve un codice univoco di 16 cifre, con il quale può accedere alla segnalazione e dialogare in maniera bidirezionale con il soggetto ricevente, scambiare messaggi e inviare nuove informazioni.
Tutte le informazioni contenute sulla piattaforma sono crittografate e possono essere lette solo dai soggetti abilitati alla ricezione della segnalazione.
Non è possibile gestire altre segnalazioni ricevute in forma scritta. Qualora queste fossero inviate, il soggetto ricevente, ove possibile, inviterà la persona segnalante a presentare nuovamente la segnalazione tramite la piattaforma informatica.
Per le segnalazioni in forma orale, la persona segnalante può contattare il soggetto ricevente (RSIS o suo Coadiutore), richiedendo disponibilità per un colloquio telefonico o incontro diretto. Le segnalazioni in forma orale vengono verbalizzate e il verbale deve essere firmato dalla persona segnalante, affinché sia processato.
È opportuno ricordare che le segnalazioni in forma orale non offrono la stessa riservatezza tecnologica delle segnalazioni effettuate in forma scritta tramite la piattaforma crittografata.

6. Tempistiche di gestione delle segnalazioni

Al termine del percorso di segnalazione scritta effettuata tramite Whistleblower Software ApS., la piattaforma mostra un codice di ricevuta a conferma che la segnalazione è stata consegnata e presa in carico dal soggetto ricevente.
Entro 7 giorni, il soggetto ricevente conferma alla persona segnalante la presa in carico della segnalazione e invita il soggetto segnalante a monitorare la sua segnalazione sulla piattaforma per rispondere a possibili richieste di chiarimenti o approfondimenti.
Entro 2 mesi dal giorno della segnalazione, il soggetto ricevente comunica alla persona segnalante un riscontro rispetto alle attività di accertamento svolte per verificare le informazioni comunicate nella segnalazione.
Il riscontro fornito entro 2 mesi può coincidere con l'esito delle attività di accertamento. Qualora queste non fossero concluse, il ricevente invita la persona segnalante a tenere monitorata la piattaforma fino a conoscere l'esito definitivo delle stesse.
La stessa tempistica nel riscontro viene garantita in caso di segnalazione orale.

7. Riservatezza e anonimato

Il soggetto ricevente è tenuto a trattare le segnalazioni preservandone la riservatezza. Le informazioni relative all'identità del soggetto segnalante, del soggetto segnalato e di ogni altra persona menzionata nella segnalazione sono trattate secondo i principi di confidenzialità. Allo stesso modo, sono trattate in modo confidenziale anche tutte le informazioni contenute nella segnalazione.
L'identità della persona segnalante non può essere rivelata senza il suo consenso. La conoscenza delle segnalazioni e dei relativi atti di accertamento sono sottratti anche al diritto all'accesso amministrativo da parte dei soggetti interessati.
L'unico motivo di possibile rivelazione dell'identità della persona segnalante può avvenire nel caso in cui gli atti di accertamento siano inoltrati presso una procura ordinaria o contabile e la conoscenza della stessa sia necessaria ai fini del diritto di difesa durante un procedimento giudiziario ordinario o contabile presso la Corte dei conti.
La riservatezza è garantita attraverso strumenti tecnologici, quali la piattaforma crittografata per le segnalazioni e un protocollo riservato, e all'interno di processi organizzativi volti a minimizzare la circolazione delle informazioni.
È consentito e garantito l'invio di segnalazioni anonime, che verranno comunque processate dal soggetto ricevente, e ritenute ammissibili qualora il contenuto della segnalazione sia circostanziato e corredato di evidenze.
In ogni caso, le segnalazioni vengono trattate secondo gli stessi principi di riservatezza.
Tuttavia, nel caso di segnalazioni anonime, il soggetto ricevente non ha conoscenza dell'identità della persona segnalante e potrebbe involontariamente esporlo durante le attività di accertamento.

8. Trattamento dei dati personali

Le segnalazioni ricevute, le attività di accertamento e le comunicazioni tra la persona segnalante e la persona ricevente sono documentate e conservate in conformità alle prescrizioni in materia di riservatezza e protezione dei dati.
Le segnalazioni contengono dati personali e possono essere trattate e mantenute solo per il tempo necessario al loro trattamento: questo tempo comprende l'analisi, le attività di accertamento e quelle di comunicazione degli esiti, oltre a una eventuale tempistica ulteriore per possibili commenti aggiuntivi. In nessun caso le segnalazioni saranno conservate oltre i 5 anni successivi alla comunicazione dell'esito delle attività di accertamento alla persona segnalante.
Per quanto riguarda l'accesso ai dati personali, questi sono conosciuti solo dal soggetto ricevente e, se indicato in specifico atto organizzativo, dai membri dello staff di supporto alla gestione della segnalazione.
Nel corso delle attività di accertamento il soggetto ricevente può condividere con altre funzioni della Società informazioni preventivamente anonimizzate e minimizzate rispetto alle specifiche attività di competenza di queste ultime.
Nell'ambito del processo di gestione delle segnalazioni i dati personali sono trattati nel rispetto della normativa vigente in materia (Regolamento EU 679/2016 e D.Lgs. 196/2003, così come modificato dal D.Lgs. 101/2018).
L'informativa sul trattamento dei dati personali è disponibile nell'apposita sezione della piattaforma Whistleblowing della Società.

9. Tutele e protezioni

La persona cui si fa riferimento nella segnalazione come responsabile del sospetto di illecito beneficia di misure di protezione dell'identità analoghe a quelle della persona segnalante e delle altre persone menzionate nella segnalazione.
La Persona Coinvolta viene informata dell'esistenza e del contenuto della segnalazione e ne riceve copia, ad eccezione del riferimento all'identità del Segnalante, che non potrà in ogni caso essere resa nota alla Persona Coinvolta, fatti salvi i casi espressamente previsti dalla legge.
La Persona Coinvolta ha diritto di essere informata dell'esito dell'istruttoria. Previa valutazione adeguatamente tracciata, l'informativa alla Persona Coinvolta può essere ritardata ovvero non effettuata in tutto o in parte qualora appaia necessario attendere l'azione di pubbliche autorità, o qualora sia ragionevole ritenere che, fornendo l'informativa, possa essere a rischio la riservatezza della identità del Segnalante tutelata secondo legge.
In aggiunta alla tutela della riservatezza dell'identità della persona segnalante e dei soggetti menzionati nella segnalazione, nonché del contenuto della stessa, esistono altre forme di tutela garantite attraverso questa procedura.
Viene infatti garantita protezione alla persona segnalante contro ogni forma di ritorsione o discriminazione che dovesse subire in seguito e a causa di una segnalazione. Per ritorsione si intende qualsiasi azione o omissione minacciata o reale, diretta o indiretta, collegata o derivante da segnalazioni di illeciti effettivi o sospetti, che causi o possa causare danni fisici, psicologici, danni alla reputazione della persona, perdite economiche.

Tra le possibili discriminazioni rientrano:

- il licenziamento, la sospensione o misure equivalenti, o la retrocessione di grado;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa; o note di merito o referenze negative; o misure disciplinari o altra sanzione, anche pecuniaria; o la coercizione, l'intimidazione, le molestie o l'ostracismo; o la discriminazione o un trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto a termine;
- danni, anche alla reputazione della persona, pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e di redditi;
- 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 in futuro;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; l'annullamento di una licenza o di un permesso; la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

10. Sanzioni

Il Decreto Legislativo n.24/2023 prevede sanzioni amministrative, irrogabili da parte dell'Autorità Nazionale Anticorruzione in caso di violazione delle norme sul whistleblowing.
Le sanzioni riguardano in modo specifico eventuali ritorsioni contro i soggetti segnalanti, violazioni dell'obbligo di riservatezza, il boicottaggio a un tentativo di segnalazione, la mancata presa in carico di una segnalazione o un'insufficiente attività istruttoria avviata in seguito alla stessa.
Sono altresì sanzionabili gli abusi del sistema di segnalazione, con possibili sanzioni per colui che calunnia o diffama un altro soggetto a mezzo della procedura.
L'amministrazione può procedere disciplinarmente contro i soggetti responsabili di queste condotte.

11. I canali esterni per le segnalazioni

Al di fuori della procedura interna per le segnalazioni, la legge permette di effettuare anche segnalazioni esterne all'Autorità Nazionale Anticorruzione.
La persona segnalante può segnalare esternamente alla Società, ma solo se ne sussistono le condizioni: qualora abbia già effettuato una segnalazione a cui non è stato dato seguito; qualora abbia fondati motivi di ritenere che a una segnalazione interna non sia dato seguito o che le prove della stessa possano essere distrutte o occultate o che questa possa determinare un rischio di ritorsione; qualora abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.
Le modalità di segnalazione all'Autorità Nazionale Anticorruzione sono disponibili alla pagina dedicata sul sito dell'ANAC anticorruzione.it/-/whistleblowing.

NOVOTEMA SPA
Whistleblowing

REPORTS MANAGEMENT PROCEDURE
Issued on 29.04.2024.

This document represents the procedure for managing reports received and processed by NOVOTEMA SPA (the Company), pursuant to Whistleblowing legislation.
The procedure complies with the regulatory changes introduced by the Legislative Decree. 10 March 2023, n. 24 implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 (so-called "Whistleblowing Decree").
The reporting management process is an integral part of the NOVOTEMA SPA Code of Ethics.
For sending and managing reports, the Company has implemented a dedicated IT platform, which constitutes the preferential channel for sending reports.
The procedure adopted by the Company will be reviewed when any regulatory changes will occur, with at least an annual verification of the need for revision.

1. Regulatory references.

Whistleblowing was introduced in Italy with specific legislation at the end of 2017, with law n.179. This legislation comprehensively regulated the institute for public administration, while also introducing some provisions for private sector organizations equipped with an organizational model of management and control ex. Legislative Decree no. 231/2001.
Law n.179/2017 was superseded by the law transposing the European Directive on whistleblowing (n.1937/2019).
The new law, the Legislative Decree. 10 March 2023, n. 24, is the implementation of EU Directive n.2019/1937 of the European Parliament and of the Council of 23 October 2019, concerning the protection of persons who report violations of Union law and containing provisions concerning the protection of persons who report violations of national regulatory provisions (so-called “Whistleblowing Decree”). The new legislation provides for burdens on public and private organizations, in particular: all public bodies must provide internal procedures for the management of reports; the same obligation is incumbent on private sector entities that have an organizational model pursuant to Legislative Decree no. 231/2001 and on all private organizations with at least 50 employees.

2. Who can report.

Whistleblowing procedures encourage anyone who acquires, in the context of work, information on offenses committed by the organization or on behalf of the organization to report.
The purpose of the procedure is to facilitate the communication of information relating to violations found during work.
For this purpose, the spectrum of potential reporting persons is very broad.
The procedure is aimed at protecting these subjects when they report illegal conduct relating to the Company.
The following categories of subjects can make a report through the procedure:

- Employees
- Collaborators
- Suppliers, subcontractors and employees and collaborators of the same o Freelancers, consultants, self-employed workers
- Volunteers and interns, paid or unpaid
- Shareholders or persons with administrative, management, supervisory, control or representation functions
- Former employees, former collaborators or people who no longer hold one of the positions indicated above
- Subjects in the selection or probationary phase or whose legal relationship with the Company has not yet begun if the information on the violations was acquired during the selection process or in other pre-contractual phases.

The procedure also protects the identity of the facilitators, the natural persons who assist a reporting person in the reporting process, operating within the same working context.

3. What can be reported.

Within this procedure, illicit facts of which one has become aware in the context of one's work activity can be reported. Qualified suspicions of crimes or other violations of legal provisions or potential risks of their commission may also be reported.

The reporting person is not required to fully demonstrate the commission of an offense but the reports must be as detailed as possible, in order to allow the recipients to ascertain the facts communicated. At the same time, reporting entities are not invited to carry out investigative activities that could expose them individually.

Reports may concern:

- criminal offences
- civil wrongs
- administrative or accounting offences
- violations of community regulations
- violations of the Code of Ethics adopted by the Company.

Reports of a personal nature, for example relating to your employment contract, which are regulated by other Company procedures, do not fall within the scope of this procedure.

Reports can be referred to:

- Shareholders or persons with administrative, management, supervisory, control or representation functions
- employees
- collaborators
- consultants
- workers and collaborators of companies supplying goods or services to the Company
- other subjects who in various capacities interact with the Company itself.

4. Who receives and manages the reports.

The Manager of Internal Reporting Systems (MIRS) is the person responsible for receiving and managing reports of offences.

The MIRS, appointed by internal deed by the Administrators, is assisted by a person from its support group specifically and similarly appointed in the internal deed (MIRS Assistant).

The Internal Reporting Systems Manager, or the assistant where appointed, receives the reports and communicates with the reporting person to clarify and explore what has been received.

The dialogue with the reporting person also continues during the investigation phases.

The Reporter can choose whether to send his report to the MIRS, to the Assistant, or to both; this is to guarantee an alternative to the reporting party and also to avoid a potential coincidence between the Reported party and the receiving party.

The manager and/or assistant, after an initial assessment, carry out an activity to verify the information reported, also requesting specific information from other offices and functions within the organisation.

The Recipient provides periodic feedback to the reporting person and, at the end of the assessment activity, communicates the outcome of the assessment activities. The communication of the outcome does not include references to personal data relating to the individual reported.

Among the possible outcomes that can be communicated to the reporting person are:

- Correction of internal processes
- Initiation of disciplinary proceedings
- Transfer of the results of the investigation activities to the Public Prosecutor's Office
- Archiving due to lack of evidence.

5. Internal reporting channels.

The Company makes different channels available to reporting persons for reporting violations under this procedure.
In particular, it is possible to make reports in written or oral form.
As regards written reports, the Company provides an encrypted IT platform; the platform uses is Whistleblower Software ApS..
The IT platform constitutes the preferential tool for sending and managing reports, as it is most suitable for guaranteeing, from a technological point of view, adequate information security measures, the confidentiality of the identity of the Reporter and of the subjects mentioned in the report and its content.
A questionnaire is uploaded to the platform which guides the reporting person in the reporting process through open and closed questions, some of which are mandatory.
Through the platform it is possible in detail:

- select the interface language (Italian or English, the latter for the benefit of any foreign signallers);
- choose the person to whom you want to address the report (Recipient) among those appointed by the Company;
- send a report;
- attach documents to the report;
- modify or update a submitted report;
- consult the status of a sent report;
- receive feedback on the follow-up given to the report.

The platform allows you to:

- separate the identifying data of the Reporter from the content of the report, providing for the adoption of codes to replace the identifying data, so that the report can be processed anonymously;
- keep the content of the report confidential during the entire management phase of the same, allowing access only to authorized parties;
- adopt secure protocols for the transport of data over the network as well as the use of encryption tools for the content of the report and any attached documentation;
- interact with the Reporter, guaranteeing their anonymity.

At the end of the report, the reporting person receives a unique 16-digit code, with which he or she can access the report and communicate bidirectionally with the receiving party, exchange messages and send new information.
All information contained on the platform is encrypted and can only be read by those authorized to receive the report.
It is not possible to manage other reports received in written form. If these are sent, the receiving party, where possible, will invite the reporting person to submit the report again via the IT platform.
For oral reports, the reporting person can contact the receiving party (MIRS or his assistant, e.g. HR Manager), requesting availability for a telephone interview or direct meeting. Oral reports are recorded and the report must be signed by the reporting person in order for it to be processed.
It should be remembered that oral reports do not offer the same technological confidentiality as reports made in written form via the encrypted platform.

6. Timing for managing reports.

At the end of the written reporting process carried out via Whistleblower Software ApS., the platform displays a receipt code confirming that the report has been delivered and taken care of by the receiving party.
Within 7 days, the receiving party confirms to the reporting person that they have taken charge of the report and invites the reporting party to monitor their report on the platform to respond to possible requests for clarification or further information.
Within 2 months from the day of the report, the receiving party communicates to the reporting person feedback regarding the assessment activities carried out to verify the information communicated in the report.
The feedback provided within 2 months may coincide with the outcome of the assessment activities. If these are not concluded, the recipient invites the reporting person to keep the platform monitored until the outcome is known.
The same response time is guaranteed in the case of oral reporting.

7. Confidentiality and anonymity.

The receiving party is required to process the reports while preserving their confidentiality. Information relating to the identity of the reporting subject, the reported subject and any other person mentioned in the report is treated according to the principles of confidentiality. Likewise, all information contained in the report is also treated confidentially.

The identity of the reporting person cannot be revealed without his or her consent. Knowledge of the reports and the related assessment documents are also excluded from the right to administrative access by the interested parties.
The only reason for possible disclosure of the identity of the reporting person may occur if the assessment documents are forwarded to an ordinary or accounting prosecutor's office and knowledge of the same is necessary for the purposes of the right of defense during ordinary judicial proceedings or accountant at the Court of Auditors.
Confidentiality is guaranteed through technological tools, such as the encrypted reporting platform and a confidential protocol, and within organizational processes aimed at minimizing the circulation of information.
The sending of anonymous reports is permitted and guaranteed, which will in any case be processed by the receiving party, and deemed admissible if the content of the report is detailed and accompanied by evidence.
In any case, reports are treated according to the same principles of confidentiality.
However, in the case of anonymous reports, the receiving party does not have knowledge of the identity of the reporting person and could unintentionally expose him or her during the investigation activities.

8. Processing of personal data.

The reports received, the verification activities and the communications between the reporting person and the receiving person are documented and stored in compliance with the provisions on confidentiality and data protection.
The reports contain personal data and can be processed and maintained only for the time necessary for their processing: this time includes the analysis, assessment activities and communication of the results, as well as any additional time for possible additional comments. In no case will the reports be kept longer than 5 years following the communication of the outcome of the investigation activities to the reporting person.
As regards access to personal data, these are known only by the receiving party and, if indicated in a specific organizational act, by the members of the staff supporting the management of the report.
During the assessment activities, the receiving party can share information previously anonymized and minimized with respect to the specific activities of the latter's competence with other functions of the Company.
As part of the reporting management process, personal data are processed in compliance with current legislation on the matter (EU Regulation 679/2016 and Legislative Decree 196/2003, as amended by Legislative Decree 101/2018).
The information on the processing of personal data is available in the specific section of the Company's Whistleblowing platform.

9. Safeguards and protections.

The person referred to in the report as responsible for the suspected wrongdoing benefits from identity protection measures similar to those of the reporting person and the other persons mentioned in the report.
The Person Involved is informed of the existence and content of the report and receives a copy of it, except for the reference to the identity of the Reporter, which cannot in any case be made known to the Person Involved, except in the cases expressly provided for by law.
The Person Involved has the right to be informed of the outcome of the investigation. After a properly traced assessment, the information to the Involved Person may be delayed or not carried out in whole or in part if it appears necessary to wait for the action of public authorities, or if it is reasonable to believe that, by providing the information, the confidentiality of the identity of the Reporter protected by law.
In addition to protecting the confidentiality of the identity of the reporting person and of the subjects mentioned in the report, as well as of its content, there are other forms of protection guaranteed through this procedure.
In fact, protection is guaranteed to the reporting person against any form of retaliation or discrimination that they may suffer following and as a result of a report. Retaliation means any act or omission threatened or real, direct, or indirect, connected to or resulting from reports of actual or suspected wrongdoing, which causes or may cause physical or psychological harm, damage to a person's reputation, or economic loss.
Possible discrimination includes:

- dismissal, suspension or equivalent measures, or demotion;
- change of functions, change of place of work, reduction of salary, modification of working hours;
- the suspension of training or any restriction of access to it; o notes of merit or negative references; o disciplinary measures or other sanctions, including pecuniary; or coercion, intimidation, harassment or ostracism; or discrimination or unfavorable treatment;
- failure to convert a fixed-term employment contract into a permanent one, where the worker had a legitimate expectation of such conversion;
- failure to renew or early termination of a fixed-term contract;
- damage, including to the person's reputation, economic or financial prejudice, including loss of economic opportunities and income;

- improper listing on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector in the future;
- the early termination or cancellation of the contract for the supply of goods or services; the cancellation of a license or permit; the request to undergo psychiatric or medical tests.

10. Sanctions.

Legislative Decree no. 24/2023 provides for administrative sanctions, which can be imposed by the National Anti-Corruption Authority in case of violation of the rules on whistleblowing.
The sanctions specifically concern any retaliation against the reporting parties, violations of the obligation of confidentiality, the boycott of a reporting attempt, failure to take charge of a report or insufficient investigative activity initiated following it.
Abuses of the reporting system are also punishable, with possible sanctions for anyone who slanders or defames another person through the procedure.
The administration can take disciplinary action against those responsible for these conducts.

11. External channels for reporting.

Outside of the internal reporting procedure, the law also allows external reporting to be made to the National Anti-Corruption Authority.
The reporting person can report externally to the Company, but only if the conditions exist: if he has already made a report which has not been followed up; if he has reasonable grounds to believe that an internal report will not be acted upon or that the evidence thereof may be destroyed or hidden or that it may cause a risk of retaliation; if he has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.
The methods of reporting to the National Anti-Corruption Authority are available on the dedicated page on the ANAC website anticorruzione.it/-/whistleblowing.