Policy for whistleblowing management

Issued	Date approved
0	12/14/2023

Contents

1 OBJECTIVE

TENACTA GROUP S.p.A. *unipersonale* (the "**Company**") operates in compliance with the ethical principles of honesty, integrity, and transparency, and in accordance with relevant national and international regulations and best practices for its activities across all jurisdictions in which it operates.

In this context, the Company actively pursues the adoption of mechanisms for reporting misconduct and irregularities (the "**Reports**") that certain categories of individuals – whether belonging to the Company or not – who have a legal relationship with it ("**Whistleblowers**") come to learn of.

This Policy aims to encourage Reports, outline the protections the Company ensures to Whistleblowers, the persons who are subjects of reports, as well as other categories mentioned in paragraph 2 below, and to describe the methods for making and managing Reports.

The reporting system described in this Policy has the following characteristics:

1. It is accessible to anyone wishing to make a Report;
2. It ensures the highest levels of confidentiality regarding the information disclosed and the identity of both the Whistleblower and the person who is the subject of the Report;
3. It offers Whistleblowers the choice of alternative reporting methods: (i) a web platform, not residing in the Company's IT system, as it is hosted on an independent server; (ii) a recorded voice messaging system accessible via landline or mobile phone; and (iii) direct meetings with the Internal Whistleblowing Management Committee;
4. It allows interaction between the Company and Whistleblowers;
5. It is managed by beLab S.p.A. - a company wholly owned by BonelliErede, specialising in compliance management services and digital solutions - an autonomous body, dedicated and staffed by personnel specifically trained to manage the reporting channel ("*System Manager*");
6. It complies with the provisions of Italian Legislative Decree No. 24 of 10 March 2023, implementing EU Directive No. 2019/1937 on the protection of persons who report breaches of Union law.

The content of this Policy is disseminated to all employees and third parties in a legal relationship with the Company through publication on the corporate website and is the subject of dedicated training sessions.

2 CATEGORIES OF WHISTLEBLOWERS

The categories of Whistleblowers entitled to send Reports and who benefit from the protections provided by Italian Legislative Decree No. 24/2023 are the following:

a) employees;

b) self-employed workers and professionals (including volunteers and interns);
c) workers or collaborators of suppliers;
d) freelance professionals and consultants;
e) managers and members of supervisory bodies; and
f) shareholders.

Moreover, the protections granted to the categories of Whistleblowers listed above also apply if the Report is made:
a) When the legal relationship has not yet begun, if the information on breaches was acquired during the selection process or other pre-contractual phases;
b) During the trial period; and
c) After the termination of the legal relationship, if the information on breaches was acquired during the relationship.

Finally, these protections also extend to the following individuals:
a) Facilitators;
b) People in the same work environment as the Whistleblower who are linked by a stable emotional or kinship relationship within the fourth degree;
c) Work colleagues of the Whistleblower in the same work environment, who have a regular and ongoing relationship with such person;
d) Entities owned by the Whistleblower, or for which they work, as well as entities operating in the same work environment as such person.

3 SUBJECT OF THE REPORTS

There is no exhaustive list of misconduct or irregularities that can be reported.
The Report may concern actions or omissions, whether committed or attempted:

- Penal, civil, or administrative infringements, or accounting breaches;
- Involving legal representatives, administrators, executives, and/or employees of the Company [or subsidiaries, companies that are not subsidiaries in which the Company holds significant equity interests], joint ventures, or – in any case – anyone acting on behalf of the Company (e.g., consultants, suppliers, etc.);
- Carried out in violation of this Policy or corporate procedures involving punishment;
- Likely to cause financial or reputational damage to the Company;
- Potentially constituting conflicts of interest;
- Likely to cause harm to employee health or safety, or environmental damage;
- Likely to constitute a breach of regulations, including, but not limited to, the following areas:
  - Public contracts;
  - Services, products, and financial markets, and prevention of money laundering and terrorist financing;
  - Product safety and compliance;

- Environmental protection;
- Food and feed safety, animal health, and welfare;
- Public health;
- Consumer protection; or

- In general, national or European legislation.

In any case, the Whistleblower must have reasonable grounds to believe that the information about the reported breaches was true at the time of the Report. Should the Reports, on the contrary, prove to be manifestly groundless or defamatory, such a condition would constitute a breach of this Policy, with the possible application of disciplinary measures and the acknowledgment of responsibility on the part of the Whistleblower.

Furthermore, the Reports should not concern personal grievances of the Whistleblower or claims/requests that fall within the scope of employment relations or relationships with superiors or colleagues, nor customer complaints about products.

4 CONTENT OF THE REPORTS

Whistleblowers must provide all useful elements to enable the competent functions to proceed with the necessary checks and verifications to assess the validity of the facts constituting the subject of the Report.

To this end, the Report must contain the following elements:

a) A clear and complete description of the facts being reported;
b) The circumstances of time and place in which they occurred;
c) Indication of any other subjects who can report on the facts being reported;
d) Attachment of any documents that can corroborate the facts;
e) Any other information that can provide useful confirmation about the reported facts.

The requirement of the presumed truthfulness of the facts or circumstances reported remains unchanged, to protect the reported subject.

5 GENERAL PRINCIPLES

The reporting system is inspired by the following fundamental principles:

- **Protection of the identity of Whistleblowers and the confidentiality of information**: The Company ensures the confidentiality of the identity of Whistleblowers and the confidentiality of the information contained in the reports at every stage of the management process, to the extent that anonymity and confidentiality are enforceable under the law. In particular, the obligation of confidentiality is waived in cases where (i) in the context of a disciplinary proceeding, the claim is based, in whole or in part, on the Report and knowledge of the Whistleblower's identity is indispensable for the defence of the accused person and (ii) the revelation of the Whistleblower's identity and of the information from

which it can be directly or indirectly inferred, is indispensable also for the defence of the person involved. In such cases, the Whistleblower is notified, by written communication, of the reasons for the disclosure of confidential data. Moreover, the Reports are exempt from the right of access provided, and as applicable to the private sector, by Articles 22 et seq. of Italian Law No. 241/1990, as well as by Articles 5 et seq. of Italian Legislative Decree No. 33/2013. Measures to protect the Whistleblower's confidentiality are aimed, inter alia, at ensuring that they are not subject to any form of retaliation.

- **Prohibition of retaliatory or discriminatory acts against Whistleblowers**: The Company prohibits any form of retaliation or discrimination, whether active or by omission, even if only attempted or threatened, carried out because of the Report and which causes or may cause the Whistleblower, directly or indirectly, unjust harm; such protection is guaranteed provided the Report (even if subsequently evaluated as unfounded) was communicated in good faith, as the Whistleblower had reasonable grounds to believe that the information on the reported breaches was true at the time of the report and that they fell within the scope of application as per section 3.
  Discriminatory measures are understood as unjustified disciplinary actions, harassment in the workplace, and any other form of retaliation that results in intolerable working conditions for the Whistleblower.[1]
  The commission of retaliatory or discriminatory acts against the Whistleblower may lead to the initiation of a disciplinary procedure against the perpetrator and the application of the related disciplinary measures, in accordance with the applicable national labour legislation.
  A Whistleblower who believes to have suffered retaliation/discrimination for having made a Report must submit a new Report concerning the retaliations/discriminations suffered. The Company ensures the timely execution of

[1] For example:

- Termination, suspension, or equivalent measures;
- Demotion or failed promotion;
- Change of job functions, change of workplace, salary reduction, alteration of working hours;
- Suspension of or any restriction of access to training;
- Negative performance evaluations or adverse references;
- Imposition of disciplinary measures or other punishments, including financial penalties;
- Coercion, intimidation, harassment, or ostracism;
- Discrimination or otherwise unfavourable treatment;
- Failure to convert a fixed-term employment contract into a permanent contract, where the worker had a legitimate expectation of such conversion;
- Non-renewal or early termination of a fixed-term employment contract;
- Damage, including to the person's reputation, particularly on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income;
- Inclusion in improper lists based on a formal or informal sectoral or industrial agreement, which can lead to the person being unable to find employment in the sector or industry in the future;
- Early termination or cancellation of a contract for the supply of goods or services;
- Cancellation of a license or permit;
- Demands for psychiatric or medical examinations.

the related investigations in such cases.

- **Duty of independence and professionalism in managing reports**: All parties involved in the report handling process, in any capacity, must perform their tasks respecting the duties of independence and ensuring accurate and efficient management of all reports. Specifically, the body responsible for managing reports is autonomous, dedicated, and composed of personnel specifically trained for this task.

- **Protection of the reported individual:** The Company protects those reported in terms of both the confidentiality of the Reports concerning them and any investigations conducted, as well as protecting them from potential retaliatory and/or defamatory actions.

- **Preservation of report integrity**: The web platform ensures that no Report (from the notification phase to the decision phase) can be deleted and/or altered:

6 THE REPORTING SYSTEM

The Company's reporting system consists of the following internal channels:

1. Web platform accessible at the following link: sistemasegnalazioneewhistle.mesacloud.tech/?cluster=8AFE5524-D42A-4605-A70B-443D6A7352A4;
2. Recorded telephone line/recorded voice messaging system accessible at the following phone number: +39 02 8737 7208; and
3. Direct meeting, upon request to the Internal Whistleblowing Management Committee – composed of the Head of Administration, Finance and Control, the Legal Office Manager, Human Resources Manager, and Information Systems and Organization Manager – via the following email address: whistleblowing@tenactagroup.com.

The Company recommends submitting Reports through the web platform, as it is specifically designed to ensure ease of use, confidentiality, and privacy for the Whistleblower.

To protect the Whistleblower's privacy without exposing the Company to potential GDPR breaches, it is not possible to use computer devices, telephone equipment, and/or company networks for making reports (both via the web platform and the recorded telephone line/voice messaging system).

The Company recommends using the web platform, unless for technical reasons it is not possible to access it, because:

1. The use of alternative channels cannot ensure the same level of protection for Whistleblowers and efficiency in managing the reports;

2. In the case of anonymous reporting, using the web platform is the only way that allows for requesting clarifications from the Whistleblower while maintaining their anonymity.

If the recorded telephone line/voice messaging system is used for Reporting, or a direct meeting with the Internal Whistleblowing Management Committee is requested, the latter has the right, with the Whistleblower's consent, to document the Report (via full transcription, recording of the conversation, detailed report, or minutes, as appropriate).
The Whistleblower is offered the opportunity to verify, amend, and approve, as applicable, the transcription, report, or minutes of the meeting.
It is specified that transcriptions, reports, or minutes related to Reports received through internal channels alternative to the web platform are subsequently entered into the web platform, under the responsibility of the System Manager.
For subsequent phases of managing oral reports, refer to the following paragraphs.

In any case, anyone who receives a Report through channels other than those provided by the reporting system must promptly - and no later than 7 days from the report - forward it to the System Manager, who will then enter it into the web platform, with simultaneous notification of the transmission to the Whistleblower.

6.1 AUTHENTICATION ON THE PLATFORM AND SUBMITTING REPORTS

The Whistleblower accesses the web platform through the dedicated link.
The web platform will request authentication by the Whistleblower, whose identification data will be collected in a separate database to which the Company will not have access. This ensures the confidentiality of the Whistleblower's identity and the impossibility of tracing it during the management of the Report. Access credentials to this separate database will be provided exclusively to an entity outside the Company, which will certify compliance with the requirements set out by regulations for accessing the Whistleblower's identification data.

The web platform also allows for anonymous reporting. Both methods of reporting via the web platform ensure confidentiality, privacy, and protection for the Whistleblower.

Once authenticated, the Whistleblower reports the detected breach, filling in all required fields and providing a precise description of facts and individuals involved, as well as attaching any supporting documentation.

The web platform facilitates interaction with the Whistleblower and requests for clarifications, while ensuring maximum protection, confidentiality, and safeguarding from retaliatory and/or defamatory reports.

Upon receipt of the Report, the web platform provides an initial confirmation of receipt and acknowledgement of the report and sends the Whistleblower a unique identifier code linked to the Report. This code can be used to check for updates on the report by accessing the

web platform. The unique identifier code does not allow for the identification of the Whistleblower, whose identity remains confidential. It is the duty of each Whistleblower to safeguard it diligently, not to disclose it to others, and not to allow third parties to access information about the Report.

Once the Report is uploaded and the unique identifier code received:

i. the Whistleblower can check the progress of the report at any time by accessing the web platform;
ii. the System Manager can continue to communicate confidentially with the Whistleblower via the web platform and request further detailed elements if the Report is not adequately detailed.

Considering the above, the Whistleblower is recommended to periodically access the web platform to check for any requests for clarification regarding the submitted report.

6.2 TAKING CHARGE

Upon receipt of the Report, the web platform sends a notification of a new Report to the System Manager's email address, indicating its nature but without providing detailed information about its content.
Upon receipt, the System Manager carries out a preliminary assessment and classifies the report based on its nature.

Specifically, upon receipt, the System Manager carries out a preliminary assessment and classifies the report based on its nature.

At this stage, the System Manager immediately archives Reports that are clearly unfounded, instrumental, or outside the scope of this Policy.

Should potential conflicts of interest emerge during the handling of the report, the System Manager cannot archive the Report and must therefore communicate it to the Internal Whistleblowing Management Committee for the adoption of measures deemed most appropriate to ensure that the Report is correctly managed.

6.3 INITIAL ASSESSMENT AND INQUIRY

The System Manager verifies, for Reports that have not been immediately discarded, whether they are corroborated by sufficient elements to assess their validity.

If the Report, although not clearly groundless, instrumental, or outside the scope of this Policy, is not sufficiently detailed, the System Manager makes the appropriate requests for additions/clarifications to the Whistleblower.

After this initial assessment and having obtained the necessary clarifications, the System Manager decides to:

i. archive Reports that, following the preliminary examination, are found to be

unsubstantiated and/or inadequately documented, despite the clarifications obtained; or

ii. for Reports that, following the initial assessment, appear reasonably substantiated and supported by sufficient elements to proceed with the inquiry phase, classify the Report based on its nature using the categories available on the platform, conduct a preliminary assessment, and communicate to the Internal Whistleblowing Management Committee the need to proceed with the inquiry phase.

Should the Internal Whistleblowing Management Committee decide to proceed with the investigation, it sets out – with the support of the functions that may be involved based on the subject of the Report (e.g., Internal Audit, Human Resources, etc.) – a specific "investigation plan," which includes:

- the method of conducting the investigation (requests for additions/clarifications to the Whistleblower, carrying out the necessary checks, etc.);
- the functions, inside or outside the Company, tasked with conducting the investigations;
- the functions that might be affected by the breach, based on the subject matter;
- any other persons who can report on the facts, whose hearing must be conducted respecting the principles of impartiality, confidentiality, and protection of the Whistleblower's identity; and
- the timelines for concluding the investigation.

The inquiry phase is completed within 60 days of receiving the report - except in cases where Reports concerning particularly complex situations require longer evaluation times - in compliance with the principles of impartiality, competence, and professional diligence.

Should the revelation of the Whistleblower's identity become indispensable for the defence of the person involved during the inquiry, the Company is required to explain the reasons for the disclosure of confidential data to the Whistleblower and thereafter must request their consent for the disclosure of their personal data.

6.4 DECISION

At the end of the investigation/inquiry phase, the Function responsible for conducting the investigations submits a report on the results to the System Manager.

Following the evaluation of the results, the Internal Whistleblowing Management Committee formulates its decision on the report, identifies any disciplinary measures and possible corrective actions to propose, and instructs the System Manager regarding the feedback to be provided to the Whistleblower.

In any case, feedback to the Whistleblower on the results of their Report must be provided within 3 months of the date of the receipt notification of the Report or - if such notification is not given - within 3 months of the expiry of the seven-day term for such notification. If the inquiry has not been concluded due to circumstances that require more than three months for verification, an interim response must still be provided to the Whistleblower at the end of the specified term.

Disciplinary measures

Disciplinary measures must be appropriate and proportionate to the established breach, also considering the potential criminal relevance of the behaviours implemented and must comply with the applicable national labour legislation.

The disciplinary measures proposed following the verification of the breach must be shared with the functions affected by the breach and with the competent Human Resources function. The measures are then definitively approved and adopted by the Human Resources function and are communicated to the person responsible for the breach, in accordance with the applicable national labour legislation.

Corrective measures

The Internal Whistleblowing Management Committee shares the corrective measures suitable to remedy the consequences of the breach and to prevent the risk of similar breaches to the one reported with the company functions affected by the breach.

The Functions affected by the violation confirm the implementation of the identified measures and inform the Internal Whistleblowing Management Committee of the results. The Internal Whistleblowing Management Committee informs the System Manager of the implementation of the corrective measures for any follow-up towards the Whistleblower.

6.5 REPORTING

The System Manager prepares at least an annual report on the Reports received and managed, to be transmitted to the corporate administration and control bodies.

In any case, the System Manager, at any stage of the Report management process, may inform the corporate administration and control bodies about any Reports that may have a significant impact on the Company.

6.6 NOTICE TO THE REPORTED PERSON

In all phases of the management of the Reports, the Internal Whistleblowing Management Committee assesses the manner in which to inform the reported individual about the transmission of the Report against them, the conduct of the related investigation, and its outcome.

In particular, the timing of when the reported person is informed of the Report against them must be evaluated on a case-by-case basis, checking whether sending such notice may prejudice the conduct of the necessary investigations to ascertain the facts reported or whether, on the other hand, the involvement of the reported individual is necessary for the progress of the investigation.

The Company ensures, in any case, the right of the reported person to defend themselves

and to be informed (within a reasonable time) of the accusations and any disciplinary measures against them.

7 TRACEABILITY OF THE WHISTLEBLOWING MANAGEMENT PROCESS

Reports received (together with any related documentation attached) are saved in the electronic archive of the web platform, which does not allow any form of deletion and/or alteration.

This documentation must be kept for the time necessary to process the Report and in any case no longer than five years from the date of communication of the final outcome of the Reporting procedure.
Once the Report has been evaluated and/or archived or rejected, the System Manager will proceed with the anonymization of personal/sensitive information contained in the Report.
In any case, personal data related to the reports are processed in accordance with Regulation (EU) 2016/679, and Legislative Decrees No. 196/2003 and No. 51/2018, and therefore personal data that are not manifestly useful for processing a specific report are not collected or, if accidentally collected, are immediately deleted.

8 EXTERNAL REPORTING

While the Company has established suitable internal reporting channels that comply with Legislative Decree 24/2023, as illustrated in this Policy, external reporting is allowed through the channel activated by the National Anti-Corruption Authority ("ANAC"), only if the Whistleblower:

(i) has already made an internal report and it has not been followed up;
(ii) has reasonable grounds to believe that, if an internal report were made, it would not be effectively followed up, or the report could lead to a risk of retaliation;
(iii) has reasonable grounds to believe that the violation may constitute an imminent or clear danger to the public interest.

In the absence of the above conditions, the report is not managed by ANAC, and the person does not benefit from the protections of Legislative Decree 24/2023.
The external reporting channel activated by ANAC is available at the following link: https://whistleblowing.anticorruzione.it.

9 DISSEMINATION AND TRAINING

The Company ensures the dissemination of this Policy to all employees and third parties who have legal relationships with it, as well as the organisation of training sessions on the subject.
In particular, the Company provides clear information on the channels, procedures, and prerequisites for making internal reports, as well as on the channel, procedures, and prerequisites for making external reports.

Such information is:

- displayed and made easily visible in the workplaces, and accessible to people who,

despite not frequenting the workplaces, have a legal relationship with the company; and

- published in a dedicated section of the company website.

Training, aimed at all employees, is carried out regularly and whenever necessary, and includes, where possible, case studies and examples aimed at avoiding the recurrence of any situations that have already emerged.
Furthermore, new employees are promptly made aware of the rules and procedures for protecting employees in case of reporting.