

WHISTLEBLOWING POLICY

Caurum Srl

Sommario

1. OBJECTIVE	3
2. WHISTLEBLOWER CATEGORIES	4
3. SUBJECT OF WHISTLEBLOWING REPORTS	5
4. CONTENT OF WHISTLEBLOWING REPORTS	6
5. GENERAL PRINCIPLES	7
6. WHISTLEBLOWING SYSTEM	8
7. TRACEABILITY OF THE REPORT MANAGEMENT PROCESS	12
8. DISSEMINATION AND TRAINING	13

1. OBJECTIVE

Caurum Srl (the "Company") acts in accordance with the ethical principles of honesty, integrity and transparency and the national and international regulations and best practices applicable to its business in all jurisdictions in which it operates.

In this context, the Company promotes the adoption of tools for the reporting of offences and irregularities that have come to the attention of certain groups of natural persons - either inside or outside the Company - who have a legal relationship with the Company ("Whistleblowers").

The purpose of this Policy is to encourage whistleblowing, describe the protections that the Company guarantees Whistleblowers and reported persons and explain how whistleblowing reports are made and managed.

The whistleblowing system described in this Policy:

1. is accessible to anyone wishing to make a report;
2. guarantees the highest levels of confidentiality with regard to the information disclosed and the identities of the Whistleblower and the reported person;
3. offers Whistleblowers a choice of alternative reporting channels: (i) online platform, which does not reside in the Company's IT system, as it is hosted on an independent server; (ii) recorded telephone line/voice messaging system accessible by landline or mobile phone; and (iii) face-to-face meeting;
4. enables interaction between the Company and Whistleblowers;
5. them reports are managed by Avv. Michelangelo Scatena ("System Manager"), actual Supervisory body;
6. complies with the requirements of Italian Legislative Decree No. 24 of 10 March 2023 transposing EU Directive No. 2019/1937 on the protection of persons who report breaches of Union law.

The content of this Policy is shared with all categories of potential Whistleblowers through publication on the Company's website or in a specific notice, and is the focus of dedicated training sessions.

> > >



2. WHISTLEBLOWER CATEGORIES

The following categories of Whistleblowers are entitled to send reports and receive the protections provided for by Italian Legislative Decree No. 24/2023:

- a) employees;
- b) self-employed and non-employee workers (including volunteers and trainees);
- c) employees or non-employee workers of suppliers;
- d) freelance professionals and consultants;
- e) directors and members of the supervisory bodies; and
- f) shareholders.

In addition, the protections guaranteed to the Whistleblower categories listed above also apply if a whistleblowing report is made:

- a) when the legal relationship has not yet begun, if information on violations was acquired during the recruitment process or at other pre-contractual stages;
- b) during the trial period; or
- c) after termination of the legal relationship, if the information on violations was acquired in the course of that relationship.

Lastly, these protections also extend to the following parties:

- a) facilitators;
- b) persons in the same work environment as the Whistleblower who are linked to the latter by a stable bond of affinity or consanguinity up to the fourth degree;
- c) work colleagues of the Whistleblower who work in the same work environment as the Whistleblower and who have an ongoing, current relationship with that person;
- d) entities owned by the Whistleblower, or for which the Whistleblower works, or entities operating in the same work environment as that person.

3. SUBJECT OF WHISTLEBLOWING REPORTS

There is no complete list of offences or irregularities that can be reported. Whistleblowing reports may relate to committed or attempted actions or omissions that:

- > are punishable under criminal law or that constitute civil or administrative offences or accounting violations;
- > involve legal representatives, directors, managers and/or employees of the Company or subsidiaries, non-subsidiaries in which the Company holds significant interests, joint ventures or - in any case - anyone acting on behalf of the Company (e.g. consultants, suppliers, etc.);
- > are carried out in violation of the 231 Model or other Company policies or procedures;
- > could damage the Company's assets or image;
- > constitute potential conflicts of interest;
- > could cause harm to the health or safety of employees or to the environment;
- > could constitute a violation of the regulations laid down to, *inter alia*, protect the following sectors:
 - o public procurement;
 - o financial services, products and markets and the prevention of money laundering and the financing of terrorism;
 - o product safety and compliance;
 - o environmental protections;
 - o public health;
 - o consumer protections;
 - o protection of personal privacy and personal data; or
 - o in general, national or European legislation.

In any case, the Whistleblower must have well-founded reason to believe that the information on the reported violations was true at the time of the whistleblowing report. Should a report prove to be manifestly unfounded or defamatory, this would constitute a violation of this Policy, which could lead to disciplinary measures being taken and the Whistleblower being held liable.

Furthermore, reports must not relate to the Whistleblower's personal grievances, claims/complaints that fall within the scope of regulations applicable to employment, relationships with a hierarchical superior or colleagues, or customers' product/service complaints.

4. CONTENT OF WHISTLEBLOWING REPORTS

Whistleblowers must provide all useful information to enable the relevant units to carry out the necessary checks and investigations to assess whether the report is substantiated.

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

- a) a clear and complete description of the events being reported;
- b) the time and place in which they were committed;
- c) indication of any other parties who can provide information on the events being reported;
- d) any documents that may confirm these facts, to be attached to the report;
- e) any other information that may provide useful confirmation of the existence of the reported events.

This is subject to the requirement that the events or situations reported must be believed to be true, for the protection of the reported person.

5. GENERAL PRINCIPLES

The whistleblowing system is based on the following fundamental principles:

- > **Protection of the Whistleblower's identity and confidentiality of the information:** the Company guarantees that the Whistleblower's identity and the information contained in the report will remain confidential at every stage of the report management process, to the extent that anonymity and confidentiality are enforceable under the law. In particular, the confidentiality obligation is waived in cases where (i) in the context of disciplinary proceedings, the charge is based, in whole or in part, on the whistleblowing report and knowledge of the Whistleblower's identity is indispensable for the defense of the person who has been accused and (ii) disclosure of the Whistleblower's identity and the information from which the Whistleblower's identity may be directly or indirectly inferred is indispensable for the defense of the person concerned. In such cases, the Whistleblower shall be notified in writing of the reasons for the disclosure of confidential information.

- > **No tolerance for retaliation or discrimination against Whistleblowers:** the Company prohibits any form of retaliation or discrimination, even if it is only attempted or threatened, that is carried out as a result of the report and that directly or indirectly causes or could cause unfair harm to the Whistleblower. This protection is extended even when the report (even if it is later found to be unsubstantiated), was made in good faith, as the Whistleblower had well- founded reason to believe that the information on the reported violations was true at the time of the report and that they fell within the objective scope of application of paragraph 3.

Discrimination includes unjustified disciplinary action, harassment in the workplace and any other form of retaliation that results in intolerable working conditions for the Whistleblower.

Retaliating or discriminating against the Whistleblower could lead to disciplinary proceedings against the person who committed them and the related disciplinary action, in accordance with the applicable national labour law.

Whistleblowers who believe that they have suffered retaliation/discrimination for having made a report must file another report on the retaliation/discrimination suffered. The Company guarantees that the related investigations will be promptly carried out in such cases.

- > **Duty of independence and professionalism in the management of reports:** all parties involved, in any capacity, in the report management process must perform their tasks in accordance with the duties of independence and ensuring the proper and efficient management of all reports. In particular, the body responsible for handling whistleblowing reports is independent, dedicated to this activity and composed of personnel specifically trained for it.
- > **Protection of the reported person:** the Company protects reported persons by maintaining the confidentiality of the reports concerning them and any investigations carried out and prohibiting any retaliation and/or defamation against them.
- > **Protection of the integrity of reports:** the online platform ensures that no report (from when it is submitted to the decision) can be deleted and/or altered.

6. WHISTLEBLOWING SYSTEM

The Company's whistleblowing system consists of the following channels:

1. online platform accessible at the link present on the company website;
2. face-to-face meeting by sending a request to the System Manager.

The Company recommends sending whistleblowing reports via the online platform, as it has been specifically designed for the Whistleblowers' ease of use, privacy and confidentiality and - in the case of anonymous reports - to allow Whistleblowers to request clarifications,

¹ For example:

- dismissal, suspension or equivalent measures;
- demotion or lack of promotion;
- a change of duties, reassignment to a new work place, lower salary, change of work schedule;
- suspension of training or any restriction of access to training;
- negative reviews or negative references;
- disciplinary action or other penalties, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or, in any case, unfavorable treatment;
- non-conversion of a fixed-term contract into a permanent contract, if the worker had legitimate expectations that the contract would be converted;
- non-renewal or early termination of a fixed-term contract;
- damage, including to the person's reputation, particularly on social media, or economic or financial losses, including the loss of economic opportunities and the loss of income;
- inclusion in black lists on the basis of a formal or informal agreement in the relevant sector or industry that could make it impossible for the person to find a job 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;
- request for the person to undergo psychiatric or medical tests.

while maintaining their anonymity.

If the recorded telephone line/voice messaging system is used to make the report or if a face-to-face meeting with the Company is requested, the System Manager [or the person who will participate in the face-to-face meeting] may request, with the Whistleblower's consent, to document the report (by means of a verbatim transcript or by recording the conversation, preparing a detailed report or taking minutes, as the case may be).

The Whistleblower is given the opportunity to verify, rectify and approve, as appropriate, the transcript, report or minutes of the meeting.

It should be noted that the System Manager uploads the transcripts, reports or minutes of reports received through internal channels other than the online platform to such platform.

The subsequent steps in the management of these reports are described in the following paragraphs.

In any case, anyone who receives a report through channels other than those provided for by the whistleblowing system must promptly - and no later than 7 days after the report - forward it to the System Manager, who will upload it to the online platform, with the concurrent notice of transmission to the Whistleblower.

1.1 PLATFORM AUTHENTICATION AND SUBMISSION OF REPORTS

To access the online platform, the Whistleblower must click on the dedicated link on the Company's website.

The online platform will request authentication by the Whistleblower, whose identification information will be stored in a separate database to which the Company will not have access, so as to ensure the confidentiality of the Whistleblower's identity and make it impossible to identify the Whistleblower while the report is being managed.

The online platform also allows Whistleblowers to submit anonymous reports. The Whistleblower's confidentiality, privacy and protection are in any case guaranteed with both methods on the online platform.

After authentication, the Whistleblower reports the alleged violation, filling in all the required fields of the form, writing a precise description of the events and persons involved and attaching any supporting documentation.

The online platform facilitates interaction with the Whistleblower and requests for clarification from the latter, while also ensuring utmost protection and confidentiality as well as protection against reports made for the purposes of retaliation and/or defamation.

When a report is received, the online platform sends the Whistleblower an initial notice confirming that the report has been received and accepted. It also sends the Whistleblower a unique identification code for the report, which the Whistleblower may use to check any updates relating to the report on the online platform. The code does not in any way make it possible to identify the Whistleblower, whose identity will remain confidential. It is the duty of each Whistleblower to safeguard this code diligently, to not share it with others and to not allow third parties to access information on the report.

Once the report has been uploaded and the unique identification code has been received:

- a) the Whistleblower can check the progress of the report at any time by accessing the online platform;
- b) the System Manager may continue to dialogue with the Whistleblower in complete confidentiality on the online platform and request further details, if the report is found to be inadequately substantiated.

In the light of the above, the Company recommends that Whistleblowers periodically log onto the online platform to check for any requests for clarifications related to the report submitted.

1.1 ACCEPTANCE

When a report is received, the online platform sends a notice to the System Manager's mailbox that a new report has been received, without providing details on its content.

During this stage, the System Manager immediately dismisses reports that are obviously unfounded, pretextual or outside the scope of this Policy.

If, in the management of a report, potential conflicts of interest emerge involving the System Manager, the latter may not proceed with dismissing the report and must therefore notify the Supervisory body so that the measures deemed most appropriate can be taken to ensure that the report is properly handled.

The report acceptance stage is completed within five days of receipt of the report.

1.2 INITIAL ASSESSMENT AND INVESTIGATION

The System Manager verifies, for reports that are not immediately discarded, whether they are accompanied by sufficient information to assess their basis in fact.

If a report, without being obviously unfounded, pretextual or outside the scope of this Policy, includes insufficient details, the System Manager makes the appropriate requests for additional information/clarifications from the Whistleblower via the online platform.

Following this initial assessment and after receiving the clarifications deemed appropriate, the System Manager:

- a) dismisses reports that, based on the preliminary examination, prove to be unfounded and/or inadequately documented, despite the clarifications received; or
- b) classifies the reports that, following the initial assessment, appear to be reasonably well-founded and supported by sufficient elements to proceed with an investigation, considering the nature of the report and according to the categories indicated on the platform. The System Manager then performs the preliminary examination and informs the "Ethics Committee" (composed of the Head of Internal Audit and the Secretary of the Board of Directors) of the need to proceed with an investigation.

If the Ethics Committee decides to proceed with the investigation, it prepares a specific "investigation plan" with the support of the other internal units concerned due to the subject of the report. This plan includes:

- > the methods by which the investigation is to be conducted (requests for additional information/clarifications from the Whistleblower, performance of the assessments considered necessary, etc.);

- > the Company's internal units or external bodies appointed to conduct the investigations;
- > any other persons who can provide information on the reported facts, who must be questioned in accordance with the principles of impartiality, confidentiality and the protection of the Whistleblower's identity; and
- > the time limit for completion of the investigation.

The investigation is completed within 60 days of receipt of the report - except when reports relating to particularly complex situations require a longer investigation - in accordance with the principles of impartiality, competence and professional diligence.

1.1 DECISION

Once the investigation has been completed, the Supervisory body expresses its decision on the whistleblowing report, identifies - with the involvement of the Managing Director - any disciplinary measures and possible corrective action to be proposed and prepares a report on the results of the investigations conducted.

In any case, the Whistleblower must be informed of the decision on the report within three months of the notice of receipt of the report.

To this end, the Supervisory body shares its final report with the System Manager and the latter prepares the final reply to the Whistleblower.

Disciplinary measures

Disciplinary measures must be appropriate and proportionate to the assessed violation, taking into account any potential criminal liability, and must comply with the provisions of the applicable national labour law.

The disciplinary measures proposed following the assessment of the violation must be discussed with the units affected by the violation and with the relevant Human Resources Department. The measures are then definitively approved and adopted by the Human Resources Department. The person who committed the violation is informed of the measures, in compliance with the applicable national labour law.

Corrective Measures

The Supervisory body, in agreement with the Managing Director of Directors, informs the company units affected by the violation of the corrective measures to remedy the consequences of the violation and to prevent the risk of similar violations.

The units affected by the violation confirm that the identified measures have been implemented and inform the Supervisory body of their outcome. The Supervisory body informs the System Manager of the implementation of the corrective measures with a view to a possible follow-up with the Whistleblower.

1.1 REPORTING

At least once every year, the System Manager drafts a report on the whistleblowing reports that it has received and managed, to be forwarded to the Company's management.

In any case, at any stage in the report management process, the System Manager may inform the Company's management of any reports that could have a significant impact on the Company.

1.3 NOTICE TO THE REPORTED PERSON

In all stages of the report management process, the Supervisory body, with the support of the System Manager, considers which method to use to inform the reported person of the report submitted against them, the related investigation and its outcome.

In particular, the moment when the reported person is notified of the report must be assessed on a case-by-case basis, considering whether such notification could compromise the investigations necessary for the assessment of the events subject to the report or, on the other hand, whether the reported person must be involved in order to carry out the investigation.

In any case, the Company guarantees the reported person's right to a defense and to be informed (within a reasonable amount of time) of the charges and of any disciplinary measures against them.

7. TRACEABILITY OF THE REPORT MANAGEMENT PROCESS

The whistleblowing reports received (together with any attached documentation) are saved in the online platform's computer archive, which does not allow deletions and/or alterations of any kind.

This documentation must be kept for as long as necessary to process the report and, in any case, not more than five years from the date when the final decision on the whistleblowing procedure is notified.

Once the report has been assessed and/or dismissed or discarded, the System Manager will anonymize the personal/sensitive information in the report. In any event, personal data related to reports are processed in accordance with Regulation (EU) 2016/679 and Italian Legislative Decrees No. 196/2003 and No. 51/2018, and therefore the personal data that are not manifestly useful for the handling of a specific report are not collected or are immediately erased if they have been collected accidentally.

8. DISSEMINATION AND TRAINING

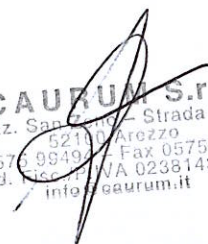
The Company ensures that this Policy is disseminated to all employees and third parties that have legal relationships with it and organizes training sessions on the subject. In particular, the Company provides clear information on the channels, procedures and conditions for making internal whistleblowing reports and on the channel, procedures and conditions for making external whistleblowing reports.

This information is:

- > displayed and made easily visible in workplaces, and made accessible to persons who, even if they do not visit the workplace, have a legal relationship with the Company; and
- > published in a dedicated section of the Company's website.

Training for all employees is carried out regularly and, in any case, when necessary and includes, insofar as possible, case studies and examples to avoid the recurrence of any situations that have already arisen.

In addition, newly hired employees are immediately made aware of the rules and procedures to protect employees who file whistleblowing reports.



CAURUM S.r.l.
Fraz. San Zeno - Strada A 36
52100 Arezzo
Tel. 0575 99494 - Fax 0575 959190
Cod. Fisc. 02381430517
info@caurum.it