



WHISTLEBLOWING PROCEDURE

REV.	DATE	APPROVED BY
0	31.03.2021	Board of Directors
1	06.12.2023	Board of Directors

WHISTLEBLOWING PROCEDURE IN FORCE SINCE 17.12.2023





CONTENTS

1	INTRODUCTION.....	3
2	REFERENCES AND DEFINITIONS.....	3
2.1	References.....	3
2.2	Definitions.....	3
3	RECIPIENTS.....	4
4	SUBJECT AND CONTENT OF REPORTS.....	5
4.1	Subject of Reports.....	5
4.2	Exclusions.....	5
4.3	Content of Reports.....	6
4.4	Anonymous reporting.....	6
5	PROTECTION OF THE REPORTING PARTY.....	7
5.1	Reporting party's protection system.....	7
5.2	Confidentiality.....	7
5.3	Prohibition of Retaliation.....	8
5.4	Limitations of liability.....	9
6	PROTECTION OF THE REPORTED PARTY.....	10
7	SUPPORT MEASURES FOR THE REPORTING PARTY.....	10
8	DESCRIPTION OF THE PROCESS AND RESPONSIBILITIES	10
8.1	Responsibility.....	10
8.2	Process.....	10
8.2.1	Reporting channels.....	10
8.2.1.1	Internal reporting channel.....	10
8.2.1.2	External reporting channel.....	11
8.2.1.3	Public disclosure.....	12
8.2.1.4	Complaint to the Authority.....	12
8.2.2	Preliminary analysis.....	13
8.2.3	Preliminary Investigation.....	14
8.2.4	Conclusion of the process.....	15
9	RECORD KEEPING AND PROCESSING OF PERSONAL DATA.....	15
10	FINAL PROVISIONS.....	16
11	ANNEXES.....	16



1. INTRODUCTION

On 30 March 2023, Legislative Decree no. 24 of 2023 headed '*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws*', which introduced a new system for reporting breaches, providing for a common discipline for public and private organisations.

Whistleblowing means the reporting of any information concerning the violations mentioned in Section 4.1 of this Procedure.

No negative consequences accrue to a person who has made a Report in good faith and the confidentiality of the identity of the reporting party is ensured, in accordance with the provisions of art. 12 of Legislative Decree. 24/23. Any act of retaliation against the reporting party is also forbidden, in accordance with article 17 of said decree.

2. REFERENCES AND DEFINITIONS

2.1 REFERENCES

- EU Data Protection Regulation 2016/679 ('General Data Protection Regulation - GDPR') and Privacy Code ('Privacy Code' or 'Code'): Legislative Decree 196/2003 amended and updated by Legislative Decree 101/2018 on "Provisions for the adaptation of national legislation to the provisions of EU Regulation 2016/679";
- Legislative Decree 231/2001;
- violations of the Code of Ethics;
- violations of the 231 Organisational Model, limited to offences relating to safety at work pursuant to art. 25 septies of Legislative Decree 231/2001;
- Criminal code;
- Legislative Decree No. 24 of 2023, with annexes;
- ANAC Guidelines, approved by Resolution No. 311 of 12.07.2023.

2.2 DEFINITIONS

<i>Company</i>	CSM TUBE spa unipersonale
<i>SB</i>	Supervisory Board appointed by the Company pursuant to Article 6 of Legislative Decree 231/2001.
<i>Reporting Officer</i>	Person in charge of receiving, analysing, verifying reports, also with the possible support of other corporate departments. In the present case: External subject, also SB CSM TUBE spa (Anita Scorza)
<i>Reporting party</i>	A person who makes a report of an offence or irregularity of which he/she has become aware in his/her work context
<i>Reported party</i>	Person attributed with committing the offence/irregularity that is the subject of the report

<i>Whistleblowing</i>	A tool that allows any individual to report misconduct, even alleged misconduct, of which he/she has become aware within his/her work context
-----------------------	---

3. RECIPIENTS

According to Legislative Decree No. 24 of 2023, the persons who can make the reports, the so called Reporting Parties, are:

- shareholders and persons with functions of administration, management, control, supervision or representation of the Company (the so-called Corporate Bodies, e.g. Shareholders' Meeting, Board of Directors, Board of Statutory Auditors, etc.);
- the Company's employees;
- workers or collaborators working for private-sector entities that provide goods or services or carry out works for third parties;
- self-employed workers and holders of a collaboration relationship working for the Company;
- freelancers and consultants working for the Company;
- volunteers and trainees, paid and unpaid, who work for the Company.

Protection for Reporting Parties operates even if the legal relationship has not begun, during the probationary period or after termination of the relationship, if the information is acquired in the course of the relationship.

The protections afforded to Reporting Parties are also extended:

- so-called facilitators (those who assist the worker in the reporting process within the same work context and whose assistance must be kept confidential);
- persons in the same employment context as the reporting party or the person who has filed a complaint with the judicial or accounting authorities or the person who has made a public disclosure and who are linked to them by a stable emotional or kinship relationship up to the fourth degree;
- to the colleagues of the reporting party or of the person who has filed a complaint with the judicial or accounting authorities or who has made a public disclosure, who work in the same work environment as the reporting party or who have a habitual and current relationship with that person;
- organisations owned by the reporting party or by the person who made the report to the judicial or accounting authorities or made a public disclosure, or for which the same persons work (e.g. an employee of a company performing a supply service), as well as entities operating in the same work environment as the aforementioned persons (e.g. the latter situation could occur in the private sector in the case of partnerships between companies).

4. SUBJECT AND CONTENT OF REPORTS

4.1 SUBJECT OF REPORTS

Reports may concern:

violations of national law

- administrative, accounting, civil or criminal offences occurring in the corporate context;
- unlawful conduct relevant to the application of Legislative Decree No. 231 of 2001, i.e. the offences for which Legislative Decree No. 231/2001 applies;
- violations of the Code of Ethics;
- violations of the 231 Organisational Model, limited to offences relating to safety at work pursuant to art. 25 septies of Legislative Decree 231/2001;

violations of EU law

- offences (always occurring in the business context) committed in breach of the EU legislation listed in Annex 1 to Legislative Decree no. 24/2023 and all the national provisions implementing them (even if these are not expressly listed in the aforementioned annex) and which relate to the following areas: public procurement, services, products and financial markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and network and information system security;
- acts or omissions affecting the interests of the European Union (art. 325 TFEU, fight against fraud and illegal activities affecting the EU's financial interests) as identified in EU regulations, directives, decisions, recommendations and opinions. Such as fraud, corruption and any other illegal activity related to EU expenditure;
- acts or omissions affecting the internal market that jeopardise the free movement of goods, persons, services and capital in the internal market, including violations of EU rules on: (a) competition; (b) state aid; (c) corporate tax and mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;
- acts or conduct that frustrate the object and purpose of the EU provisions in the areas mentioned above.

Information on violations must relate to conduct, acts or omissions of which the reporting party or whistleblower has become aware in the work context.

4.2 EXCLUSIONS

No reports with content other than that mentioned above are allowed.

In particular, the following **are not allowed**:

- a) disputes, claims or demands of a personal nature, which relate to individual working relations or relations with hierarchically superior figures, colleagues or co-workers. This excludes, for instance, reports concerning labour disputes and pre-litigation phases, discrimination between colleagues, interpersonal conflicts between the reporting party and another worker or with hierarchical superiors, reports concerning data processing

- carried out in the context of the individual employment relationship in the absence of injury to the public interest or to the integrity of the public administration or private body;
- b) reports of violations already regulated by special laws, already regulated by EU regulations or EU directives that have already been transposed, which already ensure appropriate reporting procedures. The European Union, in fact, has long recognised in a significant number of legislative acts, in particular of the financial services sector, the value of the protection of reporting parties with the obligation to activate internal and external reporting channels while also placing an explicit prohibition on retaliation (think, for example, of the market abuse reporting procedures set out in Regulation (EU) No 596/2014 of the European Parliament and of the Council to the Commission Implementing Directive (EU) 2015/2392 adopted on the basis of the aforementioned Regulation);
 - c) reports on security and defence, defence procurement and national security. Since national security is an exclusive competence of the Member States, the subject matter is not included in the scope of Directive (EU) 2019/1937 and, consequently, in Legislative Decree No. 24/2023, which implements it.

4.3 CONTENT OF REPORTS

Reports must be made in good faith, be well-founded or at least based on factual evidence.

The following must be clear:

- the circumstances of time and place in which the reported event occurred;
- description of the event;
- personal details or other elements enabling identification of the person that the reported events can be attributed to.

To this end, therefore, the reporting party must:

- precisely describe the event being reported;
- indicate the person(s) held responsible for the violation(s), as well as any other persons involved and/or who may report the event;
- describe the circumstances of time and place in which the reported event occurred;
- attach all available documents in support of the report;
- provide all useful elements for reconstructing the event and ascertaining whether the report is well-founded.

If what is reported is not adequately substantiated, the reporting officer may request additional information from the reporting party through the dedicated channel or even in person, if the reporting party has requested a face-to-face meeting.

4.4 ANONYMOUS REPORTS

Reports from which the identity of the reporting party cannot be established are considered anonymous. Anonymous reports, where substantiated, are treated as ordinary reports and dealt with in accordance with the provisions of this procedure.

It should be noted that an anonymous reporting party, subsequently identified, who has informed ANAC that he or she has suffered retaliation may benefit from the protection that the decree guarantees against retaliatory measures.

5. THE PROTECTION OF THE REPORTING PARTY

5.1 THE REPORTING PARTY PROTECTION SYSTEM

The system of protections offered to reporting parties, public disclosures and whistleblowers consists of:

- ❖ protection of the confidentiality of the reporting party, the facilitator, the person involved and the persons mentioned in the report;
- ❖ protection against any retaliation taken by the Company on account of the report, public disclosure or grievance made;
- ❖ limitations of liability with respect to the disclosure and dissemination of certain categories of information operating under certain conditions.

5.2 CONFIDENTIALITY

Specifically, the identity of the reporting party, as provided for in article 12 of Legislative Decree No. 24 of 2023, is protected in every context, starting from the moment the report is sent.

Specifically, the rule states that:

- 1) reports may not be used beyond what is necessary for proper follow-up;
- 2) the identity of the reporting party and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the reporting party themselves, to persons other than those competent to receive or follow up the reports (expressly authorised to process such data pursuant to articles 29 and 32, paragraph 4, of Regulation (EU) 2016/679 and article 2-quaterdecies of the General Data Protection Regulation set out in Legislative Decree No. 196 of 30 June 2003);
- 3) Within the framework of criminal proceedings, the identity of the reporting party is covered by secrecy in the manner and within the limits provided for in article 329 of the Code of Criminal Procedure (this provides for the obligation of secrecy of the events covered in the preliminary investigation '*until the defendant is notified of them and, in any case, not beyond the closure of the preliminary investigation*').
- 4) In proceedings before the Court of Audit, the obligation of secrecy applies until the end of the preliminary investigation phase. Afterwards, the identity of the reporting party may be disclosed by the judicial authority for use in the proceedings themselves.
- 5) Within the framework of disciplinary proceedings, the identity of the reporting party may not be disclosed, where the allegation of the disciplinary charge is based on investigations that are separate from and additional to the report, even if consequent to it.

There are two hypotheses in which the identity of the reporting party must be disclosed:

- ✓ prior written notification of the reasons for the disclosure of their identifying data;
- ✓ prior express consent of the reporting party.

The first hypothesis occurs where, in the context of disciplinary proceedings initiated against the alleged perpetrator of the reported conduct, the identity of the whistleblower is indispensable for the defence of the person charged with the disciplinary offence.

The second scenario occurs, on the other hand, where in internal and external reporting procedures the disclosure of the identity of the reporting party is also indispensable for the defence of the person concerned. Also in this case, in order to disclose the identity of the

WHISTLEBLOWING PROCEDURE IN FORCE SINCE 17.12.2023

whistleblower, it is necessary to: obtain the whistleblower's express consent beforehand; notify him/her, in writing, of the reasons for the need to disclose his/her identity.

Therefore, the identity of the whistleblower may not be disclosed without his or her express consent and those who receive or are involved in the handling of the report, even accidentally, are obliged to protect the confidentiality of that information. Breaching confidentiality is a source of disciplinary liability, without prejudice to other forms of liability provided for by law.

5.3 PROHIBITION OF RETALIATION

The reporting party may not suffer retaliation.

Retaliation is defined as *'any conduct, act or omission, even if only attempted or threatened, occurring by reason of a grievance, a report made to the authorities or public disclosure and which causes or is likely to cause the reporting party or the person raising the grievance, directly or indirectly, unjust damage'*.

Retaliation can also be 'only attempted or threatened'.

Therefore, the Reporting Party shall not be subject to: (a) dismissal, suspension or equivalent measures; (b) downgrading or non-promotion; (c) change of duties, change of place of work, reduction of salary, change of working hours; (d) suspension of training or any restriction on access to it; (e) demerit notes or negative references; (f) adoption of disciplinary measures or any other sanction, including a fine; (g) coercion, intimidation, harassment or ostracism; (h) discrimination or any other unfavourable treatment; (i) failure to convert a fixed-term contract of employment into a contract of employment of indefinite duration, where the employee had a legitimate expectation of such conversion; (j) non-renewal or early termination of a fixed-term employment contract; (k) damage, including to a person's reputation, particularly on social media, or economic or financial loss, including loss of economic opportunities and loss of income (l) 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 or industry in the future; (m) early termination or cancellation of a contract for the supply of goods or services; (n) cancellation of a licence or permit; or (o) application for psychiatric or medical examinations.

This list is not exhaustive.

The application of the protection regime against retaliation is subject to the following conditions and requirements:

- The person reported, complained or made the public disclosure based on a reasonable belief that the information on the reported, disclosed or reported violations was true and within the objective scope of the decree.
- The reporting or public disclosure was carried out in accordance with the rules laid down in Legislative Decree 24/2023.
- There must be a consequential relationship between the reporting, disclosure and grievance carried out and the retaliatory measures suffered.
- Mere suspicions or 'rumours' are not enough.

Neither the certainty of the facts nor the personal motives that led the person to report, complain or make the public disclosure are relevant.

The protection provided in the event of retaliation **shall not apply** in the event that the reporting party is found to be criminally liable for the offences of slander or defamation or, in any event, for the same offences committed in the report, i.e. civil liability, for having reported false information intentionally with malice or negligence. In cases where the aforementioned responsibilities are established, a disciplinary sanction shall also be imposed on the reporting party.

If the Reporting Party has suffered retaliation as a result of the report, he/she may communicate this **exclusively to ANAC** for the investigations attributed to it by law and for the possible application of an administrative sanction on the person responsible. It is important, therefore, that those who have suffered retaliation do not transmit the communication to parties other than ANAC so as not to nullify the protections that Legislative Decree No. 24/2023 guarantees, first and foremost, confidentiality.

In order to benefit from the aforementioned protection, there must be a link between the report, public disclosure and whistleblowing and the unfavourable conduct/act/omission suffered, directly or indirectly, by the person reporting, raising a grievance or making the public disclosure, for retaliation to occur. It is therefore necessary for the reporting party to provide ANAC with objective elements to deduce the consequentiality between the report, grievance, the public disclosure made and the alleged retaliation.

5.4 LIMITATIONS OF LIABILITY

Criminal liability and any other liability, including civil, administrative and disciplinary, is excluded in cases of disclosure of information covered by the obligation of secrecy.

The body or person protected under Legislative Decree No. 24/2023 does not incur any liability, including civil or administrative liability, for the acquisition of or access to information on infringements, provided that such acquisition does not constitute an offence 'per se'.

The limitations of criminal, civil, administrative liability operate only in cases where two conditions are met:

- i) The first requires that at the time of disclosure or dissemination there are reasonable grounds to believe that the information is necessary to discover the breach. The person must therefore reasonably believe, and not on the basis of mere inferences, that said information must be disclosed because it is indispensable for the infringement to come to light, to the exclusion of superfluous information, and not for further and different reasons (e.g. gossip, vindictive, opportunistic or scandalous purposes);
- ii) the second condition, on the other hand, requires that the report, public disclosure or grievance be made in compliance with the conditions laid down in Legislative Decree No. 24/2023 in order to benefit from protection from retaliation (well-founded reason to believe that the information on the breaches was truthful and fell within the breaches reportable under Legislative Decree No. 24/2023; internal and external reports, public disclosures made in compliance with the terms and conditions set out in Chapter II of the Decree).

6. PROTECTION OF THE REPORTED PARTY

Confidentiality must also be guaranteed for reported parties.

The protection of the identity of the person involved and of the person mentioned in the report must be guaranteed until the conclusion of the proceedings initiated as a result of the report and in compliance with the same guarantees provided for in favour of the reporting party. The reported party may be heard or shall be heard, at his or her request, also through paperwork, with the acquisition of written comments and documents. This person does not always have the right to be informed of the report concerning him or her, but only within the scope of any proceedings initiated against him or her following the conclusion of the handling of the report, and where such proceedings are based in whole or in part on the report.

7. MEASURES TO SUPPORT THE REPORTING PARTY

To further strengthen the protection of the reporting party, the legislator has provided for the possibility for ANAC to enter into agreements with third sector organisations so that the latter provide support measures to the reporting party. In particular, these organisations, included in a special list published by ANAC on its institutional website, provide assistance and advice free of charge:

- on how to report;
- on the protection against retaliation recognised by national and EU legislation;
- on the rights of the person involved;
- on the terms and conditions of access to legal aid.

8. DESCRIPTION OF THE PROCESS AND RESPONSIBILITIES

8.1 RESPONSIBILITY

It is up to the Company to set up two internal reporting channels, one in paper form and one in electronic form.

The Company has identified in a **person external to its Organisation**, who also holds the role of Supervisory Board in CSM TUBE spa unipersonale, the Reporting Officer (Anita Scorza), appointed to receive and manage Reports.

8.2 PROCESS

The process, which involves the activities described below, will therefore be managed by that party.

8.2.1 REPORTING CHANNELS

The reporting channels provided for by Legislative Decree 24/2023 are:

- ✓ Internal reporting channel;
- ✓ External reporting channel;
- ✓ Public disclosure;
- ✓ Complaint to the Authority.

8.2.1.1 INTERNAL REPORTING CHANNELS

The Company is obliged to set up the internal reporting channel.

Indeed, anyone wishing to make a report can do so:

- orally, the reporting party may request a meeting with the Reporting Officer by e-mail, at segnalazioni.csmtube@studioscorza.com;
- in writing in the following manner:
 - to the e-mail address: segnalazioni.csmtube@studioscorza.com. For this purpose, the reporting party who is also an employee/collaborator of the Company should not use the company e-mail account, but a private ordinary e-mail address;
 - by registered mail with return receipt to the Reporting Officer - Supervisory Board, at the latter's office in Viale Verdi no. 32-36, 31100 - Treviso (TV) to the Attention of Anita Scorza.

The report received will be logged and stored in such a way as to ensure maximum security.

The Company provides a simplified reporting system through a special form, Annex A, the use of which makes both reporting and its handling easier.

The template can be downloaded from the institutional website, in the Whistleblowing section, where this procedure can also be consulted.

The Reporting Officer shall record the report received in a special register of reports, the so-called 'reports register', set up in digital format and accessible only to the Officer himself.

It is understood that the report may also be submitted by means of a declaration other than the one provided for in the form, provided that it contains the essential elements indicated in the latter.

Upon receipt of the report, the Reporting Officer will take care to cover the reporting party's identification data for the duration of the preliminary investigation. The anonymity of the reporting party will always be guaranteed as provided for in Legislative Decree No. 24 of 2023.

Reports received by any person other than the person identified and appointed by the Company must be promptly forwarded by the recipient to the latter; in the event that the report concerns the Supervisory Board of CSM TUBE spa unipersonal, the reporting party may send their report to the Administrative Body.

8.2.1.2 EXTERNAL REPORTING CHANNEL

The reporting party may submit a report directly to the ANAC (National Anti-Corruption Authority) in the cases expressly provided for (see summary table). The reporting party may only file said report if one of the following conditions is met at the time of its submission:

- a) there is no internal reporting channel in their work environment or even if there is one, it does not comply with the requirements of the decree;
- b) the reporting party has already made an internal report and the report has not been followed up;
- c) the reporting party has reason to believe that, if he or she made an internal report, the report would not be effectively followed up or that the report might give rise to the risk of retaliation;
- d) the reporting party has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

The report to the ANAC - to be made either in writing through the IT platform or orally through the telephone lines or the voice messaging system or through a direct meeting with an official -

guarantees in any case the confidentiality of the reporting party, the reported party, the person mentioned in the report, the content of the report and the documentation produced, including through the use of encryption tools.

ANAC's institutional website publishes all the information needed to make an external report (contacts, channels and instructions for making the report, how to handle it, etc.), as well as indications on how to manage and file it.

8.2.1.3 PUBLIC DISCLOSURE

Legislative Decree No. 24 of 2023 also provides for the possibility of reporting misconduct through public disclosure, to be understood as that activity by which the reporter aims to '*bring information on violations into the public domain through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people*'.

It should be noted, in this respect, that the reporting party will only benefit from the protection provided for in Legislative Decree No. 24 of 2023 if, at the time of public disclosure, one of the following conditions is met:

- the reporting party has previously made an internal and external report, or has made an external report directly, under the conditions and in the manner provided for, and no feedback has been given on the measures provided for or taken to follow up the reports;
- the reporting party has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- the reporting party has reasonable grounds to believe that the external report may involve a risk of retaliation or may not be effectively followed up because of the specific circumstances of the case.

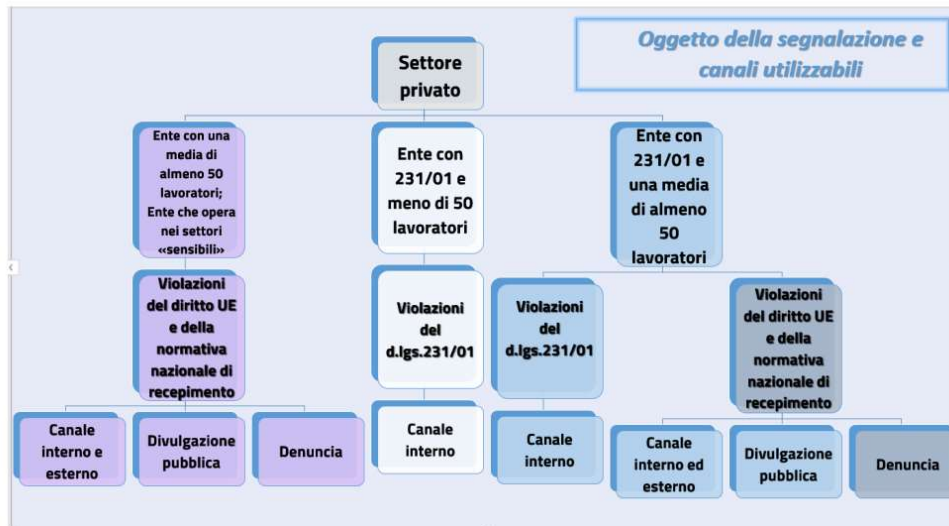
8.2.1.4 REPORTING TO THE AUTHORITY

The aforementioned decree also grants protected persons the possibility of turning to the judicial authorities to file a complaint of unlawful conduct of which they have become aware in a public or private employment context.

The same rules on the protection of confidentiality and the content of reports must be respected by the offices of the judicial authorities to which the report is made.

Summary table (from ANAC Guidelines, p. 47)

Settore privato



8.2.2 Preliminary analysis

Once the Reporting Officer receives the report, they:

- issue to the reporting party an acknowledgement of receipt of the report within seven days of its receipt;
- maintain communication with the reporting party and may request additions from the latter if necessary;
- diligently follow up on reports received;
- provide acknowledgement of the report within three months of the date of the acknowledgement of receipt or, in the absence of such notice, within three months of the expiry of the seven-day period from the submission of the report.

All Reports are subject to a preliminary analysis carried out by the Reporting Officer in order to verify the presence of useful data and information to allow an initial assessment of the legitimacy of the Report.

Therefore, this Officer carries out an assessment of the existence of the essential requirements of the report in order to assess its admissibility and thus be able to grant the reporting party the protections envisaged.

Following this initial assessment, they may dismiss the report:

- as manifestly unfounded due to the absence of factual elements capable of justifying findings;
- because the generic content of the report of misconduct does not allow the facts to be understood, or report of misconduct accompanied by inappropriate or irrelevant documentation.

If, at the end of the preliminary analysis phase, it emerges that there are no sufficiently circumstantiated elements or, in any case, that the facts referred to in the Report are unfounded, the Report is dismissed, with the relevant reasons.

Once the admissibility of the report has been assessed, the Officer initiates the internal preliminary investigation into the facts or conduct reported in order to assess their existence.

8.2.3 PRELIMINARY INVESTIGATION

With reference to each Report, where, following the preliminary analysis, useful and sufficient elements emerge or can be deduced for an assessment of the legitimacy of the Report itself, without prejudice to the right of defence of the reported party, the Officer shall:

- ✓ initiate specific analyses, possibly involving the departments concerned by the Report;
- ✓ terminate the preliminary investigation at any time if, in the course of the investigation, it is established that the Report is unfounded;
- ✓ make use, if necessary, of experts or surveyors from outside the Company.

The Officer then examines the reported facts and the documents (if any) received and, where he/she deems it necessary and/or appropriate, may:

- contact the reporting party and summon him/her for a personal and confidential interview in order to receive clarifications and/or additions to the information and documents provided;
- conduct a hearing of any other persons who may report on the reported events;
- carry out any other activity deemed appropriate for the purposes of investigating the report.

In carrying out the investigation activities, the Reporting Officer may involve other Company departments and/or appoint external consultants as necessary. The members of the working group involved in the examination of the report are subject to the same confidentiality constraints and responsibilities as the Reporting Officer. All these persons are also under an obligation to refrain from reporting in the event of possible conflicts of interest.

The Reporting Officer draws up and keeps minutes of any meetings relating to investigation activities conducted independently and/or with the assistance of the corporate departments involved.

If, following the conducted activity, elements of the report are deemed to be manifestly unfounded, it will be dismissed with adequate justification. Where, on the other hand, there is a prima facie case that the report is well-founded, it should be immediately referred to the relevant internal bodies or external bodies/institutions, each according to their purview.

It is not up to the person in charge of handling the report to ascertain individual responsibilities, whatever their nature, nor to carry out legitimacy or merit checks on acts and measures adopted by the reported entity, otherwise they risk encroaching on the purview of the persons in charge of such matters within each entity or of the courts.

With reference to the 'acknowledgement' to be made within the three-month time limit, it should be noted that this may consist of the announcement of the closure, the opening of an internal investigation and possibly its findings, measures taken to deal with the matter raised, or referral to a competent authority for further investigation. However, it should be noted that the same feedback, to be given within three months, may also be merely interlocutory, as information may

WHISTLEBLOWING PROCEDURE IN FORCE SINCE 17.12.2023

be provided on all the activities described above that are intended to be undertaken and the progress of the investigation. In the latter case, once the investigation has been completed, the results must in any case be communicated to the reporting party.

8.2.4 CONCLUSION OF THE PROCESS

At the end of the preliminary investigation, the Reporting Officer will:

- a) agree with the Head of the Department concerned by the Report, on any "action plan" necessary for the removal of the control weaknesses detected, also ensuring the monitoring of the implementation;
- b) take note of any initiatives that the Departments concerned intend to take to protect the interests of the Company (e.g. legal action, suspension/cancellation of suppliers);
- c) suggesting the initiation of disciplinary proceedings against the reporting party, in the case of Reports in relation to which the reporting party's bad faith and/or merely defamatory intent is established, possibly also confirmed by the lack of grounds of the Report itself;
- d) submit the results of the investigation of the Report, if it relates to employees and is well-founded, to the relevant Department for assessment, so that the most appropriate measures may be taken against the reported employees.

Also in these cases, the Reporting Officer shall record in the aforementioned 'reports register' the outcome of the procedure and the possible imposition of penalties against the reported party or the author of the offence (if not the same), as well as the possible initiation of legal proceedings against him/her. Grievances and reports received by the Reporting Officer are accessible only to the latter - and to the persons (as indicated above) involved by him/her in the subsequent verification and assessment process - and are kept for the period of time strictly necessary for the handling of the report.

9. RECORD KEEPING AND DATA PROCESSING

In order to ensure the management and traceability of Reports and related activities, the Reporting Officer ensures the archiving of all related supporting documentation for the time necessary to process the report and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set out in Article 12 of Legislative Decree 24/2023.

The Reporting Officer is therefore responsible, at each stage of the process described above, for the safekeeping of the documentation received by them and for filing it in a manner that guarantees its integrity and completeness.

In this respect, it should be noted that when, at the request of the reporting party, the report is made orally during a meeting with the appointed staff member, it is documented by said staff member, with the reporting party's consent, by recording it on a device suitable for storage and listening or by means of a report. In the case of minutes, the reporting party may verify, rectify and confirm the minutes of the meeting by signing them.

The processing of the data of reporting party and reported party will be carried out in compliance with the personal data protection legislation in force, expressly referred to in Legislative Decree No. 24 of 2023. Data will only be kept for the period strictly necessary to process the report, and in any case no longer than necessary to follow up the report. In cases where the report is considered worthy of further attention by the Company, and consistent with the Data Retention WHISTLEBLOWING PROCEDURE IN FORCE SINCE 17.12.2023

policy on Personal Data Protection, the report and related documentation are retained for up to 5 years after the report is closed. Naturally, if a possible judgement arises as a result of the report, the time limit will be extended until the conclusion of the judgement itself.

It should be noted that, in order to protect the confidentiality of the reporting party, the rights set out in articles 15 to 22 of the GDPR (e.g. the right to erasure) cannot be exercised. In such cases, the rights in question may be exercised through the Data Protection Authority.

The processing of personal data relating to the receipt and handling of the report is carried out by the Reporting Officer, a person external to the Organisation, specifically appointed as external data controller pursuant to article 28 of Reg. EU 2016/679.

10. FINAL PROVISIONS

Violations of the obligations laid down in this procedure constitute disciplinary liability, if, depending on the case, more serious disciplinary offences cannot be identified. The procedure identified in this act for whistleblowing, as well as the whistleblower protection profiles, will be reviewed periodically.

11. ANNEXES

- A) Reporting form
- B) Privacy policy

ANNEX A

<u>FORM FOR</u> <u>REPORTING MISCONDUCT</u> (so-called <i>whistleblowing</i>)	
<p>Persons who wish to report suspected misconduct of which they have become aware, as provided for in Legislative Decree No. 24 of 2023, may use this form.</p> <p>It must be mentioned that the system under Legislative Decree No. 24 of 2023, protects reporting parties. This rule regulates the protection of persons who report violations of national or European Union law that harm the public interest or the integrity of the public administration or private entity, of which they have become aware in a public or private employment context.</p>	
NAME AND SURNAME OF THE REPORTING PARTY	
TAX CODE OF THE REPORTING PARTY	
PROFESSIONAL QUALIFICATION OR POSITION	
PLACE OF WORK	
TEL/CELL	
E-MAIL	
AREA THAT THE REPORT REFERS TO	
DATE/PERIOD IN WHICH THE EVENT OCCURRED	
PLACE WHERE THE EVENT OCCURRED	<input type="checkbox"/> Company _____ <input type="checkbox"/> outside the Company, _____ (indicate place and address)
I BELIEVE THAT THE ACTIONS OR OMISSIONS COMMITTED OR ATTEMPTED CONSTITUTE	<input type="checkbox"/> predicate offences under Legislative Decree 231/2001) <input type="checkbox"/> violation of the Organisational Model 231 of CSM TUBE spa unipersonale <input type="checkbox"/> violation of the Code of Ethics <input type="checkbox"/> violations of EU law



DESCRIPTION OF THE EVENT (conduct and event)	
AUTHOR(S) OF THE EVENT	
ANY OTHER PERSONS WITH KNOWLEDGE OF THE EVENT AND/OR ABLE TO REPORT ON IT	
ANY ATTACHMENTS IN SUPPORT OF THE REPORT	





REPORTING CHANNELS

- orally, the reporting party may request a meeting with the Reporting Officer by e-mail, at segnalazioni.csmtube@studioscorza.com;
- in writing in the following manner:
 - to the e-mail address: segnalazioni.csmtube@studioscorza.com. For this purpose, the reporting party who is also an employee/collaborator of the Company should not use the company e-mail account, but a private ordinary e-mail address;
 - by registered mail with return receipt to the Reporting Officer - Supervisory Board, at the latter's office in Viale Verdi no. 32-36, 31100 - Treviso (TV) to the Attention of Anita Scorza.



ANNEX B**POLICY CONCERNING THE PROCESSING OF PERSONAL DATA
OF THE PERSONS REPORTING VIOLATIONS OF EU LAW OR NATIONAL LEGISLATION, OF THE
PERSONS INVOLVED, NAMED PERSONS AND FACILITATORS**

CSM TUBE spa unipersonale, in its capacity as data controller (hereinafter 'CSM TUBE'), issues this information notice to the reporting party, the persons involved, the persons mentioned and the facilitators in compliance with the European and Italian regulations on personal data protection.

Purposes and legal basis of processing.

CSM TUBE processes personal data for the purpose of carrying out the necessary preliminary investigative activities aimed at verifying the legitimacy of the reported fact and taking the consequent measures.

Consent is not required because processing is necessary for the fulfilment of CSM TUBE's regulatory obligations under Legislative Decree. 10 March 2023, no. 24.

Categories of data and their sources.

CSM TUBE processes data of common nature (name, surname, qualification, etc.), data of special nature (data concerning health, trade union membership, etc.) and/or data concerning criminal convictions, offences and security measures: this information may be collected directly from the person it refers to (hereinafter referred to as the "Data Subject") and/or from third parties (e.g. when the reporting party provides information on the reported person and/or on other persons mentioned and/or on the facilitator, or when further information/documents are acquired from other CSM TUBE structures during the preliminary investigation).

Data retention period.

The collected data are retained for the time necessary to process the report and for the period necessary to complete the related administrative procedure or any legal proceedings initiated, and in any case no longer than 5 years from the date of communication of the final outcome of the reporting procedure.

Nature of the provision of data and consequences in the event of refusal.

The provision of personal data is optional, but necessary for the handling of reports and related activities, with the consequence that any refusal to provide such data prevents such handling.

Target categories.

During the handling of the report, personal data may be processed by internal persons specifically authorised for the purposes indicated, as well as service providers or other external parties (e.g. platform operators used for the handling of reports), who will process the data as data controllers on behalf of CSM TUBE.

Where applicable, personal data may be passed on to third parties to whom disclosure is required by law (e.g. judicial authorities, national anti-corruption authorities, etc.).

Under no circumstances will personal data be disseminated.

Transfer of data to another Country and/or an international organisation

The personal data shall not be transferred to non-EU Countries or to international organisations.

Rights of the data subjects.

Data subjects have the right to obtain access to their personal data, to have them updated (or corrected, if inaccurate), to have them deleted or to have the processing concerning them restricted, subject to the respective conditions and in particular within the limits of the provisions of art. 2-undecies of Legislative Decree No. 196/2003.

To exercise your rights, you may use the form available at <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924> and forward it to the subject in charge of handling the report, by contacting them through the channel used for the report, i.e. at CSM TUBE with registered office in Cimavilla di Codognè (TV), via del Lavoro n. 60. The Data Subject also has the right to lodge a complaint with the competent supervisory board, the Italian Data Protection Authority (www.garanteprivacy.it).