TS.QHSE.PCD.10

Whistleblowing

Acronyms

Acronym	Description
ANAC	National Anti-Corruption Authority
AU	Sole Director
CCNL	National Collective Labour Agreement
GS	Whistleblowing Manager
HR	Human Resources
RI	Investigation Officer

Operational Procedures

Reporting of Violations

Internal Reporting Channel

Any individual — whether company personnel or third parties — who witnesses a violation has the right to report it.
The scope of reportable violations through the **TECHNOSCAVI S.R.L.** whistleblowing system is broader than that set out in **Legislative Decree No. 24 of 10 March 2023**, extending beyond the violations and offences referred to in the Decree to include alleged breaches of the internal regulations adopted by the Company (such as the Code of Ethics, the Anti-Corruption Guidelines, and the overall internal regulatory framework).

A dedicated e-mail address has been activated: **whistleblowingtechnoscavi@gmail.com**, managed by a specifically appointed **Whistleblowing Manager (GS)** with proven expertise in the field, formally designated by the **Sole Administrator (AU)** through the *Appointment of the Whistleblowing Manager* (Annex 1 to this Procedure).
By signing this document, the GS undertakes to guarantee the highest level of confidentiality towards the reporting person.

A dedicated **online form** has also been made available at the following link:
https://forms.gle/pLWMSGewLYxw6bLh9

Through this form, the reporting person may — **even anonymously** — report any misconduct they have witnessed or become aware of, providing all details deemed necessary.

It is possible to report violations of national or European Union law that harm the public interest or the integrity of Technoscavi, including:

- ✓ administrative, accounting, civil or criminal offences;
- ✓ offences falling within the scope of application of EU or national acts;
- ✓ acts or omissions that harm the financial interests of the European Union;
- ✓ acts or omissions concerning the internal market;
- ✓ acts or behaviours that undermine the purpose or objectives of EU provisions.

Reporting – External Channel (ANAC)

Reporting persons may use the **external channel (ANAC)** at the following link: **https://whistleblowing.anticorruzione.it/#/** when:

- ✓ the activation of an internal reporting channel is not required within the work context, or such a channel, even if required, is not active or does not comply with legal requirements;
- ✓ the reporting person has already made an internal report that was not followed up;
- ✓ the reporting person has reasonable grounds to believe that an internal report would not be effectively handled or could expose them to retaliation;
- ✓ the reporting person has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest.

Reporting – Public Disclosure

Reporting persons may make a **public disclosure** directly when:

- ✓ they have previously made both an internal and external report, or an external report only, and no feedback has been provided within the prescribed timeframe regarding the measures planned or taken in response;
- ✓ they have reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest;
- ✓ they have reasonable grounds to believe that the external report may expose them to retaliation or may not be effectively handled, due to specific circumstances — such as where evidence may be concealed or destroyed, or where there is a well-founded suspicion that the recipient of the report may be colluding with, or involved in, the violation itself.

Handling of the Report

Preliminary Verification of the Report

The **Whistleblowing Manager (GS)** evaluates the report received to determine whether it falls within the scope of violations established by **Legislative Decree No. 24/2023** and the Company's internal regulations.
Reports based on unfounded information, matters already in the public domain, or data obtained from unreliable sources are excluded from reportable violations.
Likewise, disputes, claims, or requests linked to personal interests connected to the individual employment relationship of the reporting person do not fall within the scope of whistleblowing.
Where the reporting person has voluntarily identified themselves, the GS shall:

- ✓ acknowledge receipt of the report within seven (7) days from the date of submission;
- ✓ maintain communication with the reporting person;
- ✓ ensure proper follow-up of the report;
- ✓ provide appropriate feedback.

Protection and Privacy of the Reporting Person

The identity of the reporting person, as well as any other information from which such identity may be inferred, may not be disclosed — without the express consent of the reporting person — to anyone other than those authorized to receive or follow up on the report and expressly authorized to process such data. Confidentiality is also guaranteed in judicial and disciplinary proceedings.

The reporting person and any other protected individuals shall not suffer any retaliation as a result of a report made (for example: dismissal, suspension, demotion, denial of promotion, change of duties, disciplinary sanctions, harassment, ostracism, discrimination, or any other unfavourable treatment).

The processing of personal data related to the receipt and management of reports is carried out by **Technoscavi**, as **Data Controller**, in compliance with European and national data protection principles. Appropriate information is provided to reporting persons and individuals involved in the reports, and adequate measures are adopted to safeguard the rights and freedoms of data subjects.

Reports and related documentation are retained for the period necessary to manage the report and, in any case, for no longer than **five (5) years** from the date of communication of the final outcome, in compliance with confidentiality obligations under European and national data protection law.

Opening of the Investigation

Appointment of the Investigation Officer

The **Sole Administrator** appoints the **Investigation Officer (RI)**, who conducts the investigation under strict confidentiality.
The appointment is accepted by the RI, who undertakes to comply with the criteria established and documented by the organization in the *Appointment of the Investigation Officer* (Annex 2 of this Procedure).

The RI must not be related by blood or marriage to the person under investigation and must not have been involved in the procedure during which the event under investigation occurred.

The investigation must be completed within **thirty (30) days** from receipt of the report, unless extended due to its complexity, in which case a written request from the RI must be approved by the Sole Administrator.

Assessment of Critical Factors in the Investigation

The Sole Administrator assigning the investigation shall take into account:

- ✓ applicable laws;
- ✓ staff safety;
- ✓ risk of defamation;
- ✓ administrative liability;
- ✓ financial losses;
- ✓ reputational damage.

Given the presence of these factors that may influence the investigation, the Investigation Officer declares that they are not in a position of conflict of interest with the organization or with any matters related to the investigation.

Conduct of the Investigation

Information Gathering

The Investigation Officer (RI) collects and documents all relevant information through interviews with individuals directly or indirectly connected to the report. The RI records this information in the **Investigation Report** (Annex 3).

Document Collection

The RI gathers company documentation that may confirm or refute the statements made by interviewed persons. This is also recorded in the **Investigation Report**..

Collection of Testimonies

The RI records the testimonies of individuals who, although not directly involved, may have knowledge of the facts due to their role or circumstances.
If a collaborator refuses to testify, the RI reports the case to the Sole Administrator for appropriate action.
All testimonies are documented in the **Investigation Report**.

Determination of Evidence

Based on the interviews, documentation, and testimonies, the RI identifies and documents:

- ✓ the evidence that confirms or disproves the reported suspicions;
- ✓ serious, precise, and consistent indications that, within a broader context, may confirm or refute the suspicions.

These findings are recorded in the **Investigation Report**.

Protection of Information

Information Protection

The information collected by the Investigation Officer (RI) in the confidential investigation file, together with any attached documents, must be protected through:

- ✓ access control;
- ✓ encryption of electronic files;
- ✓ backup copies stored on a secure cloud server.

Determination of the Investigation Outcomes

Submission of Evidence to the Sole Administrator

The Investigation Officer (RI) delivers the investigation documentation to the Sole Administrator in its original format.

Communication of the Investigation Outcomes

The possible outcomes of the investigation depend on the seriousness of the verified facts and the potential administrative liability of the organization:

- ✓ **If the reported fact is unfounded**, the investigation is closed;
- ✓ **If nonconformities** with company procedures or **civil irregularities** are identified, they are handled in accordance with applicable internal procedures, or, where no specific procedure exists, under the **Civil Code** or **CCNL**;

- ✓ **If a criminal offence** is established, the matter is reported to the judicial authorities, together with supporting documentation demonstrating:
  - the non-involvement of the organization;
  - the sole civil and criminal liability of the individual responsible.

The RI communicates the investigation outcome to the reporting person.
The final outcome is recorded in the **Investigation Report**.

Follow-Up Actions within the Organization

Planning of Follow-Up Actions Following the Investigation

The investigations and information gathered may alter the organization's risk scenario relating to the potential commission of unlawful acts (civil or criminal).
The **Sole Administrator** plans, based on the investigation outcome, the necessary follow-up actions regarding:

- ✓ the organization;
- ✓ internal personnel.

This planning is documented in the **Follow-Up Actions to the Investigation** form (Annex 4).

Implementation of the Planned Actions

The **Sole Administrator** ensures the implementation of the planned actions as outlined in the aforementioned document.

Initiation of the Disciplinary Procedure

Sanctioning of Responsible Parties

Company personnel found responsible shall be subject to disciplinary proceedings initiated by the organization.
The disciplinary procedure applies to all aspects of employee conduct within the company and is governed by the applicable legal and contractual provisions.
For individuals other than employees, the misconduct shall be formally contested by **registered letter with return receipt**, and, where the report is substantiated, the **civil remedies** provided by the **Civil Code** shall apply — such as **contract termination for non-performance** and **compensation for damages**.
For all matters not expressly covered by this Procedure, reference shall be made to **Legislative Decree No. 24/2023**, the **Civil Code**, the **Criminal Code**, and the **National Collective Labour Agreement (CCNL)**, where applicable.