

## POLICY WHISTLEBLOWING

|                                                     |    |
|-----------------------------------------------------|----|
| 1. PURPOSE .....                                    | 2  |
| 2. OBJECTIVE SCOPE OF APPLICATION .....             | 2  |
| 3. EXCLUSIONS .....                                 | 3  |
| 4. SUBJECTIVE SCOPE OF APPLICATION .....            | 4  |
| 5. PROTECTION OF THE WHISTLEBLOWER .....            | 5  |
| 6. INTERNAL REPORTING .....                         | 6  |
| 7. DISCIPLINARY ACTIONS .....                       | 9  |
| 8. PERSONAL DATA AND CONFIDENTIAL INFORMATION ..... | 9  |
| 9. EXTERNAL REPORTING .....                         | 10 |
| 10. DEFINITIONS .....                               | 11 |

| Version | DATE       | Approved by:        |
|---------|------------|---------------------|
| V1      | 04.03.2025 | Intern Legal Office |

## 1. PURPOSE

The ARSENALIA Group recognizes the importance of ethical values and business principles. In order to promote an internal culture of integrity—characterized by compliance with the law, honesty, transparency, and organizational accountability—and in accordance with the provisions of Legislative Decree 24/2023 implementing EU Directive 2019/1937, the ARSENALIA Group (hereinafter also referred to as the “Organization”) has adopted this Whistleblowing Policy. The purpose of this Policy is to promote a responsible and trustworthy business culture that benefits both the Organization and its stakeholders. To this end, the Organization is committed to ensuring the confidentiality of the whistleblower’s identity and guaranteeing that no retaliatory or discriminatory action—whether direct or indirect—will be taken against any individual who, in good faith, submits a report.

## 2. OBJECTIVE SCOPE OF APPLICATION

This Policy is valid for all companies within the ARSENALIA Group.

### **Subject of the Reports:**

All subjects addressed (Recipient) by this Policy are required to report Unacceptable Conduct, meaning any action or omission occurring during work activities or impacting them, which may cause harm or damage to the Group and/or its Employees.

In general, reports may concern:

- a) Unlawful conduct pursuant to Legislative Decree 231;
- b) Other illegal conduct relevant in EU law or national law, as specified in the first attachment to the Whistleblowing Decree. In particular:
  - a. Public procurement;
  - b. Financial services, products and markets and prevention of money laundering and terrorist financing;
  - c. Product safety and compliance;
  - d. Environmental protection;

- e. Radiation protection and nuclear safety;
- f. Food and feed safety and animal health and welfare;
- g. Public health;
- h. Consumer protection;
- i. Privacy, personal data protection, and network and information system security;

c) Acts or omissions that harm the financial interests of the European Union, as indicated in the Whistleblowing Decree. By way of example, but not limited to, this includes fraud, corruption, and any other illegal activity that damages the financial interests of the EU (e.g., pursuant to Article 325 TFUE);

d) Acts or omissions concerning the internal market, including violations of the EU competition and state aid rules, as well as violations of tax regulations intended to obtain a tax advantage inconsistent with the objectives of the applicable provisions (e.g., Article 26(2)TFUE);

e) Acts or conduct that undermine the objective or purpose of the provisions in the areas listed in (b), (c), and (d)

### 3. EXCLUSIONS

Pursuant to Legislative Decree 23/2024, this Policy does not apply to complaints or mere grievances regarding:

- Matters of a personal nature concerning the whistleblower, such as claims, disputes, or requests related to their individual employment relationship, interactions with colleagues, or relationships with hierarchical superiors, if they relate exclusively to the management of the employment relationship;
- National security violations, including those related to defense and national security procurement, unless such matters are covered by the European Union's secondary legislation;

- Violations regulated by European or national legislation, as provided for in Article 1, paragraph 2(b) of the Whistleblowing Decree (i.e. in the areas of financial services, products and markets, prevention of money laundering and financing of terrorism, safety and environmental transport);
- Reports based on unsubstantiated information;
- Information already publicly available;
- Information based solely on hearsay or rumors, lacking documentary support or concrete evidence.

Furthermore, reports shall not be considered relevant and shall not be subject to the protections of the Whistleblowing Decree if they:

- Use offensive language, contain personal insults, or express moral judgments intended to harm the honor and/or personal and/or professional reputation of the person(s) reported, without factual elements justifying an investigation;
- Are made with defamatory or slanderous intent;
- Are discriminatory, making reference to sexual orientation, religious, political belief, race or ethnic origin of the reported person;
- Are too vague or irrelevant to allow an understanding of the facts or their verification.

The Organization reserves the right to take disciplinary or legal action to protect persons and entities subject to reports falling under the above categories.

#### **4. SUBJECTIVE SCOPE OF APPLICATION**

The Whistleblowing Policy, including the protections provided in this policy, is addressed to anyone who reports violations perpetrated within the work context, including:

- Employees;
- Self-employed workers;
- Workers or collaborators performing activities for entities supplying goods or services or carrying out works on behalf of the Company;

- Freelancers and consultants;
- Volunteers and interns;
- Persons performing tasks involving administration, management, auditing, supervision or representation.

The protection guaranteed to whistleblowers also apply in the following cases:

- If the legal relationship has not yet begun, provided that the information on violations was acquired during the selection process or other pre-contractual phases;
- During the probationary period;
- After the termination of the legal relationship, if the information on violations was acquired during the course of the relationship.

The Organization reserves the right to take disciplinary or legal action to protect individuals and entities subject to reports falling under the above categories.

## 5. PROTECTION OF THE WHISTLEBLOWER

The whistleblower is protected from any act of retaliation or discrimination arising directly or indirectly from the report.

The whistleblower shall not suffer any discrimination or retaliation as a result of the report submitted.

Discriminator actions against the whistleblower may be reported to the Department of Human Resources by the whistleblower.

The Organization ensures, within the limits of the law, the confidentiality of the whistleblower's identity and the protection of confidential information.

The report may be submitted anonymously by the whistleblower. In any case, the identity of the whistleblower will be kept confidential at all stages of the investigative procedure.

The identity of the whistleblower may be disclosed only when:

- Disclosure is required by law (e.g., if it is necessary to law enforcement or authorities, or if the reported person has the right to receive notification); or

- Disclosure is necessary to prevent or mitigate threats to public health, safety, or the environment.

The unauthorized, direct, or indirect disclosure of the whistleblower's identity, beyond the circumstances mentioned above, shall be considered a violation of this procedure and subject to disciplinary action.

The same protective measures guaranteed to the whistleblowers shall also apply, due to their role or close connection with the whistleblower, to the following categories of persons:

- **Facilitators**, i.e. natural persons who assists the whistleblower in the reporting process;
- **Individuals working in the same remote working environment** as the whistleblower, linked to them by a stable emotional bond or kinship up to the fourth degree, who have filed a compliant or made a public disclosure;
- **Colleagues of the whistleblower** who work in the same professional environment and maintain a habitual and ongoing working relationship with them.

## 6. INTERNAL REPORTING

The Report is managed by the "Reporting Committee", an internal commission of each Group Company, composed of the Reporting Officer of the relevant Company, personnel from the Human Resources department, and the Legal department.

If the Report concerns one of the members of the Reporting Committee, the matter will be handled by the other members of the Committee who are not directly affected.

### Reporting Channel

Reports may be submitted, in accordance with the procedures described below, through the platform designated for each Group Company, which is available online on the individual websites of ARSENALIA Group companies.

### GlobaLeaks Reporting Platform

The mandatory fields required by the reporting platform must be completed to submit the report. The whistleblower may also attach supporting documents, which will remain stored in the relevant case file.

Once the Report has been submitted, the system will generate a token, which the whistleblower must use to access the platform and check the status of their Report.

## **Handling of Reports**

The Internal Reporting Committee shall:

- Issue a notice of receipt of the report within seven (7) days of its submission. This notice will be published on the platform, where the whistleblower can access it using the unique identification code (token) assigned by the system.
- Conduct a preliminary evaluation of the report to assess whether the information provided is sufficiently detailed and useful for an initial assessment. If the report lacks sufficient details, the Committee shall request additional information from the whistleblower via a specific message posted on the platform .
- Dismiss the report if preliminary analysis reveals a lack of sufficient evidence and determines it to be unfounded or confirms that it was filed in bad faith. The decision to archive must be accompanied by written reasons.
- If the Report is deemed admissible as a whistleblowing case, the Internal Reporting Committee shall initiate an internal investigation into the reported facts or conduct, assessing their validity and proceeding with the investigative phase.

During the investigation, the Committee may communicate with the whistleblower, requesting clarifications, documents, and additional information through the dedicated platform channel. If necessary, it may also obtain documents from other departments, seek their support, involve third parties for hearings or other inquiries, always ensuring the confidentiality of both the whistleblower and the reported person.

If the Report appears to be credible, the matter should be immediately referred to the competent internal bodies or external authorities, each according to their jurisdiction.

It is not the responsibility of the Committee to establish individual liability or conduct legitimacy checks. These activities shall be performed by the competent authorities or judicial bodies within the applicable jurisdiction.

In carrying out its assessment, the Internal Reporting Committee may:

- Engage other corporate functions or consult external advisors;
- Conclude the investigation and archive the Report if the claims are found to be unfounded;
- Determine appropriate measures to protect the Group, such as suspension, contract termination, legal action, etc.;
- Request the HR department to initiate disciplinary proceedings against the whistleblower in cases of malicious or defamatory reporting.

All activities described above, as well as all documentation related to the reports, shall be recorded and retained on the platform for the period permitted by law. The platform shall summarize all information regarding the report, the investigation, and any findings.

At the conclusion of the investigation, which must be complete within three months from the date of Report submission, the Internal Reporting Committee shall provide feedback to the whistleblower. This feedback shall include information on how the report was handled, the findings of the investigation, and any measures taken.

The feedback may consist of:

- Notification of case closure;
- The opening of an internal inquiry and, if applicable, the related findings;
- Measures adopted to address the issue;
- Referral to a competent authority for further investigation.



However, it should be noted that the feedback, which must be provided within three months, may also be preliminary, including only an update on planned actions and the progress of the investigation.

## **Oral reporting**

A Report may also be made orally, upon request by the whistleblower, through a direct meeting with the officer designated by the Company to handle internal reports.

To request a meeting, which shall be scheduled within a reasonable timeframe from the receipt of the request, the whistleblower must send an email to [whistleblowing.cclera@arsenalia.onmicrosoft.com](mailto:whistleblowing.cclera@arsenalia.onmicrosoft.com), including the following subject line: "Whistleblowing – Request for Direct Meeting – Confidential Communication".

In such cases, and subject to the whistleblower's consent, the report shall be documented either by recording it on a secure device or by drafting a written record. In the latter case, the whistleblower shall have the right to review, correct, and confirm the transcript by signing it.

## **7. DISCIPLINARY ACTIONS**

The individual ARSENALIA Group company shall adopt the disciplinary measures applicable to its own employees who are whistleblowers.

Disciplinary measures will be taken against employees who have submitted unfounded reports maliciously or with gross negligence.

Sanctions shall also be imposed on those who violate the protective measures afforded to the whistleblower.

The Group company has the right to initiate legal proceedings where required by law.

## **8. PERSONAL DATA AND CONFIDENTIAL INFORMATION**

The information and any other personal data acquired are processed, including within the Platform, in compliance with EU Regulation 2016/679 (General Data Protection Regulation – GDPR). In particular, the Group ensures that the processing of personal data respects

fundamental rights and freedoms, as well as the dignity of the data subject, with particular regard to confidentiality and data security.

## **Protection and Documents storage**

In accordance with applicable legislation on personal data protection, the documentation related to reports is confidential and is stored securely. The documentation is stored on the Platform and is accessible only to members of the Internal Reporting Committee.

The documents related to the report and the whistleblower's data shall not be retained for more than five (5) years from the date of notification of the final outcome of the reporting procedure or for as long as necessary in accordance with the law in the event of legal proceedings.

## **9. EXTERNAL REPORTING**

### **Procedure for Reporting to ANAC**

Article 7 of the Decree assigns ANAC the responsibility of establishing a reporting channel that ensures, similarly to the initial channel, confidentiality of the whistleblower's identity, as well as that of the individuals involved in the report, the content of the report itself, and the related documentation, including through encryption tools.

However, in order to use the reporting channel established by ANAC, certain conditions must be met pursuant to Article 6 of the Decree.

Specifically, the whistleblower may resort to the external procedure only if at least one of the following conditions applies:

- The establishment of an internal reporting channel is not mandatory within their work environment or, if required, it has not been activated;
- The internal report has not resulted in any action;
- The whistleblower has reasonable grounds to believe that an internal report would not be acted upon or that they would face retaliation;

- The whistleblower has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest.

## **Procedure for Public Disclosure**

The legislation also introduces the possibility for the whistleblower to make a public disclosure while benefiting from protection.

To adopt this procedure, at least one of the following conditions must be met:

- The internal and/or external reporting channels have been previously used, but no response has been received or no action has been taken within the timeframe provided by the Decree;
- The whistleblower reasonably believes that there is an imminent and manifest danger to the public interest, defined as an emergency situation or a risk or irreversible damage, including to the physical safety of one or more individuals, requiring the immediate disclosure of the violation with broad public awareness to prevent its effects;
- The whistleblower reasonably believes that external reporting may result in retaliation or may not be effectively addressed because, for example, there is a risk of destruction of evidence or collusion between the authority responsible for receiving the Report and the perpetrator of the violation. In other words, the situation should involve particularly serious instances of negligence or international misconduct within the entity.

## **10. DEFINITIONS**

**Recipients:** Recipients include senior management, members or corporate bodies, all employees, collaborators (including interns or temporary workers), external consultants, suppliers, clients, contractors, and other collaborator, as well as individuals acting on behalf of and/or in the name of ARSENALIA Group companies based on an assignment or other contractual relationships.

**Internal Reporting Channel:** The Internal reporting Channel refers to the online platform made available for submitting Reports.

The tool is accessible through the website of the individual companies of the ARSENALIA Group for the submission, storage of reports and related documentation, as well as for the tracking and management of operational activities, at the following links:

<https://whistleblowing.alpenite.com/>;

<https://whistleblowing.actabase.com/>;

<https://whistleblowing.aboustrust.com/>;

<https://whistleblowing.amplize.com/>;

<https://whistleblowing.cclera.com/>;

<https://whistleblowing.oblics.it/>;

<https://whistleblowing.altitudo.com/>;

<https://whistleblowing.arsenalia.com/>

**Report:** A report consists of information regarding Unacceptable Conduct provided by the Whistleblower through the available reporting channels.

**Whistleblower:** A person who reports Unacceptable Conduct, illegal activities, or non-compliant behavior occurring within the ARSENALIA Group.

**Reported Party:** The individual identified in the Report as responsible for Unacceptable Conduct.