GROUP GUIDELINES
LGG 009

MANAGEMENT OF INTERNAL REPORTS

(“WHISTLEBLOWING”)

CONTENTS

1.0 FOREWORD

(It.) Legislative Decree no. 24 concerning the protection of persons who report breaches of national laws (published in the Official Gazette of the Italian Republic, General Series No. 63 of 15 March 2023), implementing 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, came into force on 10 March 2023.

The law aims to incentivise the reporting of information on all types of breaches acquired in the work-related context in order to facilitate their emergence within public and private entities, with the provision of systems enabling the reporting persons to do so under conditions of adequate protection.

(It.) Legislative Decree No. 24/23 introduces the possibility of using an internal company reporting channel and an external one to the Italian National Anti-Corruption Authority (Autorità Nazionale Anticorruzione - ANAC). The latter external channel can only be used when specific conditions expressly laid down in the legislation are met (art. 6 “Conditions for external reporting”) and only for breaches other than those consisting of illegal conduct relevant under (It.) Legislative Decree No. 231/2001 or breaches of organisation and management models.

In addition to the external ANAC channel, the rule stipulates that the reporting person may also resort to public disclosure, only under the terms and conditions provided for in Article 15 “Public disclosures” or direct report to the Authorities, when there are criminal or accounting offenses.

The law also includes the following essential elements:

- objective and subjective scope;
- the obligation of confidentiality;
- the processing of personal data;
- record keeping;
- measures to protect the reporting person.

The value of whistleblowing, in the spirit of the European directive, contributes to an integrated compliance that not only provides adequate procedures in line with the law, but also constitutes a group instrument with a guarantee of transparency towards all stakeholders.
In this perspective, Arvedi Group (“Group”) has set up a Group Compliance and Governance department, whose head performs the role of Group Compliance Officer. He is an autonomous, dedicated, trained (art. 3 of Italian Legislative Decree No. 24/2023) figure who, in coordination with the Group’s General Counsel, has the function of supporting management and employees in compliance with rules, regulations and procedures.

The Group has adopted these Guidelines in order to regulate reports of unlawful (*contra legem)* conduct and conduct that does not comply with the internal regulatory system. It provides employees and all other stakeholders with suitable tools and procedures for managing reports, taking care to ensure the confidentiality of the reporting person’s identity and the correct use of such tools, which may not be used for purposes unrelated to the spirit of the law.

2.0 PURPOSE AND SCOPE

The purpose of these Guidelines is to establish the procedures for making an internal report of unlawful or illegal conduct or behaviour, where non-compliance is the result of an action or omission, which pertains to the following areas of application, in accordance with Italian Legislative Decree No. 24/2023:

- breaches of national provisions consisting of unlawful conduct relevant under (It.) Legislative Decree 231/2001 or breaches of organisation and management models;
- breaches of the competition and State aid rules of the Treaty on the Functioning of the European Union (e.g., antitrust);
- breaches of national and European provisions in specific areas: offences related to public and private procurement; financial services and products; product safety and compliance; transport safety; protection of the environment; radiation protection; public health; protection of privacy and personal data; security of network and information systems;
- breaches of the company's internal regulatory system (e.g., guidelines; procedures).

By way of a non-limiting example, such breaches may therefore concern:

- Labour law, health, safety and environmental standards and regulations
- Bribery or extortion
- Money laundering
- Competition law (antitrust)
- Fraud
- Conflicts of interest
- Privacy
- Disclosure of confidential information
- Code of Ethics and/or Code of Conduct;
- Human rights
- Unethical or unprofessional business behaviour
- Misuse of company resources
- Non-compliance with Group regulations and procedures

These Guidelines also aim to ensure the confidentiality and anonymity of the reporting person and the adequate protection of the person concerned.

It applies to all Italian Group companies (hereinafter also referred to as the "Company" or "Companies") and to any of the aforementioned breaches, which may prejudice the public interest and/or the integrity of the Company and/or the Group, where there are reasonable grounds for the reporting person to believe that the information is true.

The reports may therefore not be complaints, claims or requests of a personal nature or pertaining exclusively to one's individual relations or to one's working relations with hierarchically superior figures.

This incorporates and updates the contents of the Whistleblowing Policy Rev. 0 of 8/3/2021 issued by Finarvedi S.p.A., which is therefore annulled and replaced.

3.0 REFERENCE DOCUMENTS AND STANDARDS

- Code of Conduct of Finarvedi S.p.A.
- Code of Ethics
- Organisation, Management and Control Model pursuant to Italian Legislative Decree No. 231/01 as amended and supplemented.
- General Data Protection Regulation (EU) 2016/679 (“GDPR”)
- (It.) Law of 30 November 2017, no. 179
- EU Directive 2019/1937
- Confindustria Guidelines
- Italian Legislative Decree no. 24/2023 (“Whistleblowing Decree”)
- Assonime Circular No. 12 of 18 April 2023
- ANAC guidelines

4.0 RECIPIENTS

The recipients of these Guidelines (hereinafter also referred to as reporting persons) are:

- top management and members of the corporate bodies of the Companies, e.g., shareholders and persons in administration, control, supervision and representation roles;
- employees and internal collaborators of the Companies, e.g. volunteers, paid and unpaid trainees;
- all stakeholders, who, for whatever reason, have relations with the Companies, e.g. employees of different parties, such as customers, suppliers, associates; self-employed workers, such as freelancers and consultants;
- facilitators, as defined below;
- those entrusted with the management of reporting channels (hereinafter also referred to as “Reporting Officers”), who are in charge of following up the reports;
- people concerned, as defined below (or reported subjects/persons).

5.0 ABBREVIATIONS AND DEFINITIONS

5.1 Abbreviations

AA Acciaieria Arvedi S.p.A.
AST Acciai Speciali Terni S.p.A.
CFO Chief Financial Officer
HR Human Resources

5.2 Definitions

Breach	shall mean any conduct, act or omission, occurring in the course of or having an impact on the work activity and involving unlawful conduct as defined in para. 2.0.
Report	the written or oral communication of information on breaches, which can be submitted through the appropriate reporting channels.
Anonymous report	any report in which the identity of the reporting person is not made explicit or traceable.
Reporting in "bad faith"	unsubstantiated reports made for the purpose of harming or being detrimental to employees, internal collaborators, members of corporate bodies or third parties in business relations with the Group.
Reporting person	the natural person reporting information on breaches acquired in their work-related context.
Facilitator	an individual who assists a reporting person in the reporting process, operating within the same work environment and whose assistance must be kept confidential.
Work-related context	current or past work or professional activities carried out in the context of the relationships referred to in para. 3.0, through which, irrespective of the nature of such activities, a person acquires information about breaches and in the context of which they may risk retaliation in the event of reporting.
Person concerned	the natural or legal person mentioned in the report as the person to whom the breach is attributed or as a person otherwise involved in the reported breach.
Retaliation	any conduct, act or omission, even if only attempted or threatened, committed by reason of the report and causing or likely to cause the reporting person, directly or indirectly, unjust damage.
Follow-up	the action taken by the person entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the investigation and any measures taken.
Feedback	Provision to the reporting person of information on the follow-up given or intended to be given to the report.

6.0 PRINCIPLES OF CONDUCT

These Guidelines, consistent with (It.) Legislative Decree 24/2023, are based on the following principles of conduct aimed at defining ex ante the governance of the whistleblowing management process, identifying and assessing suitable organisational solutions for Arvedi Group.

The Group, within its own organisation, has a centralised department of Corporate Compliance and Governance, with adequate autonomy and independence from corporate operational departments, coordinated by a Group Compliance Officer, with professionalism and experience in the management of whistleblowing systems prior to the entry into force of Italian Legislative Decree No. 24/2023.

Through this function, the Group intends to guarantee its internal and external stakeholders a systematic and homogeneous approach, completeness and timeliness of reporting to the High Management, collaborating with the Supervisory Bodies, appointed pursuant to Italian Legislative Decree No. 231/2001.

The management of internal reporting channels take into account the regulatory requirements regarding the size limit of 250 employees and, therefore, for each Company of the Group a specific dedicated channel is established, which provides two e-mail boxes for each Company (Annex 1). In particular, these boxes are addressed both to the Company's Supervisory Body and to the Group Compliance Officer who works jointly in the "preliminary verification of the report" (par. 7.4) and independently in the next "investigation" phase (par. 7.5).

The protection of the reporting person and of all the other subjects (the person concerned or other persons identified as reporting persons or mentioned in the report) is always guaranteed. Technical measures, including the use of encryption tools, are in fact implemented to ensure the confidentiality of the whistleblower identity as well as of the contents of the report.

Based on the principle of transparency, the operating procedures in which the process of handling reports is articulated are defined below, regulating the process of analysis and management of reports received.

Together with the Guidelines published on the web portals and summarised in English for possible foreign stakeholders, training on whistleblowing is provided to employees at the time of recruitment and on a regular basis (at least every two years).

7.0 GENERAL REQUIREMENTS FOR THE MANAGEMENT OF REPORTS

7.1 General information and assumptions

The Group is committed to ensuring that all its employees, at all levels and regardless of their hierarchical position within the Group, comply with the applicable regulations and these Group Guidelines on report management.

7.2 Liability

The Supervisory Bodies of the Companies and the Group Compliance Officer are responsible for managing the various internal reporting channels. They are bound by the same principles and terms as set out in this Guideline.

In addition, the General Counsel is responsible for supervising and coordinating the process.

7.3 Sending the report

Any person wishing to make a report can use any of the following channels.

Web platform

The platform, which is managed by an independent third party on an external domain, is available on the website of each Company of the Group. It has logical segregation per Company to which the report refers and it provides a guided form compilation path for the reporting person who can decide whether to remain anonymous.

Once the submission procedure is completed, the reporting person receives a unique code associated with the report. This code can later be used to monitor progress and to anonymously communicate, as well as to provide additional information and for clarifications after the report.

On the platform there will be:

- the date of taking over of the report (by the Reporting Officers, within seven days from the date of submission);
- information on the action taken or intended to be taken on the report, within three months from the date of the acknowledgement of receipt or, in the absence thereof, from the expiry of the period of seven days from the submission of the report.

Access to the platform is subject to the “no-log” policy in order to prevent the identification of reporting persons who wish to remain anonymous; this means that the company’s IT systems are not able to identify the access point to the portal, even if it is made from a device connected to the company network.

Only the subjects listed in Annex 1 have access to the information collected through the platform.

The whistleblowing platform is the preferred channel for reporting, ensuring confidentiality and protection of the reporting person as well as better traceability of information managed by the platform itself with efficient feedback for the reporting person.

In addition, the following alternative channels are available which, however, due to their technical features, do not offer the same guarantees of confidentiality and protection for the reporting person:

E-mail

It is possible to address the report, both jointly and separately, to the two e-mail boxes indicated for each Company in Annex 1.

In order to ensure greater confidentiality, it is recommended to use a text as an attachment to the e-mail and to indicate “confidential” in the e-mail subject.

In-person meeting

It is possible to arrange a meeting with one or both of the Reporting Officers indicated in Annex 1, for each Company, after sending an e-mail in response to which the necessary information will be provided.

In all cases of sending report through the channels indicated above, the identity of the reporting person cannot be revealed without their express consent, without prejudice to legal

obligations. All those involved in the management of the report are required to protect the confidentiality.

If a report should reach a subject other than those indicated in Annex 1, the latter must immediately instruct the whistleblower to report it to one of the indicated subjects.

7.4 Preliminary verification of the report

All reports received are subject to a preliminary check to determine whether they fall within the scope of these Guidelines and whether data and information that make it possible to make an initial assessment have been provided. In the event that a report received via the whistleblowing platform proves to be inadequately substantiated, the Reporting Officers, again and only by means of the relevant unique identification code, may request further details from the reporting person.

Similarly, the protection of the reporting person will be ensured in case of the need for preliminary investigation of reports received through other channels.

At the conclusion of the preliminary verification phase, the Group Compliance Officer updates the report card generated in the whistleblowing platform (or equivalent document, for reports received through other channels) and: i) in the event of a decision not to proceed, the report is archived, keeping track of the relevant reasons; ii) in the event of a preliminary assessment of the merits of the case, the investigation shall be initiated in accordance with par. 7.5.

7.5 Investigation

The Reporting Officers, based on the results of the joint preliminary analysis, define whether the subsequent investigation is potentially linked to 231 crimes or not.

The Supervisory Body, within the scope of its autonomy and competences with reference to potential 231 crimes:

- initiates specific analyses, deciding on a case-by-case basis on the degree of involvement of the Corporate departments of any external consultants and of the company functions concerned by the report, while respecting the anonymity and/or confidentiality of the reporting person and of the persons concerned;
- ensures that the investigation is thorough, has a reasonable duration and in any case envisages a report of the preliminary analysis within three months from the date of taking charge of the report, together with all supporting evidence[1];
- once the assessment process has been concluded, draws up a specific formalisation document, together with all supporting evidence[1].

During the various stages of the investigation, the General Counsel is constantly informed of the progress to ensure compliance with this Guideline, with particular reference to the time limits provided by the standard.

The Group Compliance Officer, for their area of residual jurisdiction in relation to the previously regulated:

- initiates specific analyses, using the relevant structures, possibly including external consultants, as well as involving the company functions concerned by the report, while

[1] The competent Supervisory Body can be supported by the *Group Compliance Officer* to manage the reporting on the platform.

respecting anonymity and/or confidentiality of the reporting person and of the persons concerned;

- ensures that the investigation is thorough, has a reasonable duration and in any case envisages a report of the preliminary analysis within three months from the date of taking charge of the report;
- once the assessment process has been concluded, draws up a specific formalisation document, together with all supporting evidence.

For all areas of competence, the investigation is discontinued if it proves to be unfounded, based on the evidence that emerges.

7.6 Outcome of the investigation

At the end of the investigation, the Supervisory Body or the Group Compliance Officer, within their respective areas of competence, draw up a report with the following contents:

- the course of the investigation and the evidence collected;
- conclusions reached;
- recommendations and suggestions for actions to be taken to remedy the breaches found and to ensure that they do not occur in the future.

They inform the reporting person, in writing, of the conclusions reached.

For investigations following reports within the scope of Legislative Decree No. 231/2001, the competent Supervisory Body informs the Board of Directors of the conclusions reached.

For all other investigations, the *General Counsel* informs:

- the Chief Executive Officer of the Company concerned and that of the Parent Company;
- the Statutory Auditors of the Company concerned;
- the Chief Financial Officer (CFO) of the Company concerned;
- the HR Department of the Company concerned.

Group Companies may take the most appropriate disciplinary measures and/or legal action to protect their rights, assets and image against any person who has committed or has been involved in a breach. Any disciplinary measures will be taken in agreement with the HR Department and in compliance with the relevant National Collective Bargaining Agreement and/or any contractual measures as regards internal collaborators.

A person who has committed or has been involved in a breach will not be immune from possible disciplinary and/or legal action merely because they have reported their own or another's breach under these Guidelines. However, this circumstance may be taken into account when assessing the measures to be taken.

In the event of a report made in bad faith, appropriate action may similarly be taken by Group Companies against the reporting person.

Otherwise, if at the end of the analysis it is found that there are no sufficiently circumstantial elements or, in any case, that the facts referred to in the report are unfounded, the report will be archived together with the relevant reasons and it will be destroyed after six months.

7.7 Corrective measures and monitoring

The corrective measures shall be formalised in an action plan drawn up by Group Internal Auditing (or by a person otherwise designated for investigation) in cooperation with the head of the department to which the report refers and with the General Counsel of Arvedi Group.

The respective deadline for corrective action and the name of the person responsible for implementing the corrective action must also be defined for each finding.

In case of urgency, corrective measures will be immediately implemented, followed by formalisation in the action plan.

The Group Compliance Officer, with the support of the contact persons identified for each Group Company, ensures that the progress of the action plan is monitored for each finding. The persons responsible for the implementation of the action plan for the individual findings may agree with the Group Compliance Officer on possible extensions of the deadline, giving detailed reasons.

The Group Compliance Officer and/or the Supervisory Body may provide for follow-up actions to verify the actual resolution of critical issues or the progress of the relevant action plan, by requesting information from the identified persons responsible.

Upon conclusion of the follow-up activity, the Group Compliance Officer shall update the Report Form on the whistleblowing portal or an equivalent formalisation document[2].

7.8 Periodic reporting

The *Group Compliance Officer* shall prepare periodic reports containing an account of the reports received from internal and external parties and shall submit them to the Board of Directors at least once every six months.

Copies of these reports are also shared with the supervisory bodies (Statutory Auditors and Supervisory Board) of the Company concerned and the Parent Company, as evidence of the compliance system.

Reporting duties by the Supervisory Body according to the Italian law 231 are unchanged.

7.9 Filing

The documentation relating to the reports must be filed ensuring adequate storage security and in compliance with the Group's rules on the processing of information.

Such filing is carried out by the Group Compliance and Governance department, for a maximum period of five years from the date of notification of the final outcome (art. 14 of the Whistleblowing Italian Decree).

8.0 PROTECTIVE MEASURES ENVISAGED

8.1 Protecting the reporting person

Persons reporting in good faith are always protected by the Company concerned and by the Parent Company against any form of retaliation, discrimination or penalisation, which also

[2] In the case of reports transmitted by channels other than the platform

guarantee, where reasonably possible, the fulfilment of any request for transfer to another office.

Group Companies guarantee the anonymity of the reporting person, without prejudice to legal obligations and except in cases where the reporting person consents to disclosure.

Unauthorised disclosure of the reporting person's identity or information from which the identity of the reporting person can be inferred is considered a breach of these Guidelines.

8.2 Obligations of the reporting person

The reporting person has a duty to report on the basis of a reasonable belief (that an offence is about to occur, for example) and never to discredit someone. This duty is an essential safeguard against harmful or offensive reports and it ensures that those who have deliberately and knowingly reported incorrect, unsubstantiated or misleading information are not protected.

Failure to comply with the reporting person's duties is considered a prerequisite for disciplinary sanctions or for legal actions aimed at protecting the Company in the appropriate office.

8.3 Rights of the person concerned

During the verification and detection of possible breaches, the individuals to whom reports have been received, may be involved or notified of this activity, but under no circumstances will proceedings be initiated solely on the ground of the report, in the absence of concrete evidence of its content.

If there are concrete findings, proceedings could be initiated instead; the person concerned will always be guaranteed the right to their own defence for the facts ascribed to them.

9.0 DATA PROTECTION

Given the particular nature of the information that may be contained within the reports, these must be collected, processed and transmitted exclusively by persons entrusted with the processing and competent to initiate the verification procedure or to take the necessary measures depending on the findings. In any case, the recipients of the information must ensure that it is always handled confidentially and that appropriate security measures are applied.

10.0 DISTRIBUTION TO EXTERNAL PARTIES – WAIVER OF LGG 001

As an exception to the provisions of par. 5.2.1 of the LGG 001 Group Guidelines, this document is made available to parties outside the Arvedi Group through publication on the website of the individual companies.

The distribution is therefore according to code "A" provided in the LGG 001 (par. 5.2).

ANNEX 1 – Reporting Officers

These channels do not guarantee the same degree of confidentiality and data protection as the platform.

Company	Supervisory Bodies	Compliance Officer
Finarvedi S.p.A.	odv@arvedi.it	CPL@arvedi.it
Acciaieria Arvedi S.p.A.	odv@ast.arvedi.it	CPL@arvedi.it
Arinox S.p.A.	odv@arinox.arvedi.it	CPL@arvedi.it
Arvedi Tubi Acciaio S.p.A.	odv@ata.arvedi.it	CPL@arvedi.it
Ilta Inox S.p.A.	ilta-odv@ilta.arvedi.it	CPL@arvedi.it
Metalfer S.p.A.	odv@metalferspa.it	CPL@arvedi.it
Siderurgica Triestina S.r.l.	odv@siderts.arvedi.it	CPL@arvedi.it
Centro Siderurgico Industriale S.r.l.	odv@csindustriale.it	CPL@arvedi.it
Centro Siderurgico Adriatico S.r.l.	odv@csadriatico.it	CPL@arvedi.it
Euro-Trade S.p.A.	odv231@euro-trade.it	CPL@arvedi.it
Acciai Speciali Terni S.p.A.	odv.ast@acciaiterni.it	CPL@arvedi.it
Terninox S.p.A.	odvtix@acciaiterni.it	CPL@arvedi.it