RAFFMETAL

Procedure for the management of reports of unlawful conduct and protection of the reporting person

(so-called Whistleblowing)

PROCEDURE FOR THE MANAGEMENT OF REPORTS OF UNLAWFUL CONDUCT AND PROTECTION OF THE REPORTING PERSON

(so-called Whistleblowing)

In implementation of Legislative Decree no. 24/2023 concerning the protection of persons who report breaches of Union law and national regulations

Procedure in force from 15 July 2023 - First issue

2^ Edition - Approved by the Board of Directors on 31 March 2025

3^ Edition - Review of compliance with the current regulatory framework on 24 June 2026

PROCEDURE

PROCEDURE FOR THE MANAGEMENT OF REPORTS OF UNLAWFUL CONDUCT AND PROTECTION OF THE REPORTING PERSON (so-called Whistleblowing)

1. PURPOSE AND SCOPE

This document is intended to describe and regulate the organisational aspects and operational processes relating to reports of unlawful acts, or breaches of national or EU laws and regulations, and of unlawful conduct relevant pursuant to Legislative Decree No. 231/2001, as further detailed in paragraph 4 below, which internal or external persons[1] connected to Raffmetal S.p.A. hereinafter "Raffmetal" or the "Company" by employment or business relationships become aware of in a work-related context. This Procedure applies to such persons.

The document and the definition of the internal reporting channels described herein were subject to prior information to the comparatively most representative trade union organisations.

Any legal obligations remain unaffected, in particular with regard to the obligation to report to the Judicial Authority or to the Supervisory Authorities, as well as with regard to the processing of personal data and the protection of privacy under the legislation in force.

The Procedure also incorporates the principles and provisions of the Code of Ethics and of the Organisation, Management and Control Model pursuant to Legislative Decree No. 231/2001 adopted by the Company. It does not in any way amend, but rather supplements and regulates in greater detail, the methods for communicating to the Company's Supervisory Body any relevant acts or facts falling within its areas of responsibility, as provided for by the Organisation, Management and Control Model.

The possibility of submitting reports concerning workplace safety, as provided for by the procedures in force and by the applicable company collective agreements, is also confirmed.

This Procedure entered into force on 15 July 2023 and was subsequently updated on 31 March 2025 and on 24 June 2026 following approval by the Board of Directors.

Any further subsequent amendments and/or additions shall enter into force on the date provided for by laws or regulations or by resolution of the Board of Directors, or, in urgent cases, by decision of the Chair of the Board of Directors or the Chief Executive Officer.

[1] Specifically, it applies to all persons broadly connected to the organisation in which the breach occurred: employees, self-employed workers, freelancers and consultants, external collaborators, persons carrying out paid or unpaid traineeships, volunteers, persons working under the supervision and direction of contractors, subcontractors and suppliers, customers, shareholders, and persons with administrative, management, control, supervisory or representative functions.

2. REFERENCES

In implementation of EU Directive No. 1937/2019 of the European Parliament and of the Council of 23 October 2019, concerning the protection of persons who report breaches of Union law and containing provisions concerning the protection of persons who report breaches of national laws and regulations, the Italian legislature, through Legislative Decree No. 24/2023, extended the scope of application of the protection afforded to the reporting person. Such protection, previously limited to cases of unlawful conduct relevant pursuant to Legislative Decree No. 231/2001 or breaches relating to the Company's 231 Model and Code of Ethics, has been extended to breaches of further European and national legislation.

Article 6 of Legislative Decree No. 231/2001 provides that 231 Models shall include internal reporting channels, the prohibition of retaliation and the disciplinary system, adopted pursuant to Legislative Decree No. 24/2023.

This Procedure has been drafted taking inspiration not only from the applicable statutory provisions, but also from the following documents:

- Code of Ethics of Raffmetal S.p.A.;
- Organisation, Management and Control Model pursuant to Legislative Decree No. 231/2001 of Raffmetal S.p.A.;
- Legislative Decree No. 196 of 30 June 2003, as amended and supplemented, and Regulation (EU) 2016/679 on data protection;
- Guidelines for the Preparation of Whistleblowing Procedures issued by Transparency International Italia;
- Guidelines on the protection of persons who report breaches of Union law and on the protection of persons who report breaches of national legal provisions, approved by ANAC with Resolution No. 311 of 12 July 2023, as amended and supplemented by ANAC Resolution No. 479 of 26 November 2025[2];
- Operational Guide for private entities on the new whistleblowing rules, prepared by Confindustria in the edition updated to May 2026;
- ANAC Guidelines No. 1/2025 on whistleblowing concerning internal reporting channels, approved by Resolution No. 478 of 26 November 2025.

[2] On 7 November 2024, in order to complete and supplement the guidance provided, ANAC published the Draft New Guidelines on Whistleblowing, with the aim of providing clarifications on the methods for implementing and managing internal reporting channels. This document, which was subject to public consultation until 9 December 2024, was definitively approved under the title ANAC Guidelines No. 1/2025 on whistleblowing concerning internal reporting channels, by Resolution No. 478 of 26 November 2025, published on 12 December 2025. By the simultaneous Resolution No. 479 of 26 November 2025, ANAC also amended and supplemented Guidelines No. 311/2023 concerning external reporting channels.

3. DEFINITIONS

Before setting out the substantive and operational aspects related to the management of reports, the following definitions are intended to clarify the meaning attributed to certain terms used in this Procedure:

Report

A written or oral communication by the Reporting Person, concerning information relating to a breach committed by the Reported Person and submitted through the channels established by the Company, concerning potential "breaches", as defined below. The Report may not concern information that is already entirely in the public domain, information acquired solely on the basis of poorly reliable rumours or hearsay, so-called "corridor rumours", nor may it consist of claims, disputes or requests of a personal nature by the reporting person or by the person who has filed a complaint with the judicial or accounting authority, relating exclusively to their individual employment relationships, or concerning their employment relationships with hierarchically superior persons.

Breaches

Conduct, acts or omissions that harm the public interest or the integrity of the private entity, i.e. Raffmetal, and which consist of:

a) Unlawful conduct relevant pursuant to Legislative Decree No. 231/2001 or breaches of the Company's Organisation, Management and Control Model;
b) Offences falling within the scope of application of the European Union or national acts indicated in the annex to Legislative Decree No. 24/2023, or of the national acts implementing the European Union acts indicated in the annex to EU Directive No. 1937/2019, even if not indicated in Legislative Decree No. 24/2023, relating to the following sectors: public procurement; financial services, products and 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; protection of privacy and personal data and security of network and information systems (List of European and national legislation referred to in Legislative Decree No. 24/2023, Annex a);
c) Acts or omissions that harm the financial interests of the Union;
d) Acts or omissions concerning the internal market, including breaches of EU rules on competition and State aid, as well as breaches concerning the internal market connected with acts that breach corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax legislation;
e) Acts or conduct that defeat the object or purpose of the provisions laid down in the Union acts in the sectors referred to in points b), c) and d) above);

f) Breaches of the restrictive measures of the European Union, according to the scope of application of the Whistleblowing Decree, as most recently amended by Legislative Decree No. 211 of 30 December 2025.

Reporting Person (or *Whistleblower*)

The directors, managers, employees, collaborators, as well as external persons who collaborate with the Company. The persons referred to in Article 3, paragraphs 3, 4 and 5 of Legislative Decree No. 24/2023 are also considered reporting persons, including: employees, self-employed workers, suppliers of goods or services, freelancers and consultants, volunteers and trainees, shareholders, candidates and employees during their probationary period, as well as former employees.

Reported Person

The person who, within the report, is identified as responsible for the unlawful act or breach that is the subject of the report.

Person Concerned

The natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the breach is attributed or as a person otherwise involved in the reported or publicly disclosed breach.

Report Managers

The person or autonomous internal office, or the external party, entrusted with the management of the internal reporting channel. The Report Manager is specifically trained in the management of the channel.

Substitute Report Manager

The person or autonomous internal office, or the external party, entrusted with the management of the internal reporting channel in the event of a conflict of interest involving the Report Manager or in the event of prolonged absence, i.e. more than 7 days. The Substitute Report Manager is specifically trained in whistleblowing matters for the management of the channel.

4. REPORTS

4.1 Subject and persons involved in the report

The breaches that may be reported pursuant to the Whistleblowing Decree must concern conduct, acts or omissions that harm the public interest or the integrity of the public administration or of the private entity, i.e. Raffmetal, of which the Reporting Person has become aware within the Company's work-related context, and which consist of:

- Unlawful conduct relevant pursuant to Legislative Decree No. 231/2001 or breaches of the 231 Model, including the Code of Ethics, which do not fall within the offences indicated below ("231 Reports");

- Offences falling within the scope of application of European Union or national acts, as referred to in the Whistleblowing Decree, relating to the following sectors:
  a) Public procurement;
  b) Financial services, products and markets, and prevention of money laundering and terrorist financing;
  c) Product safety and compliance; transport safety;
  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) Protection of privacy and personal data, and security of network and information systems.
- Acts or omissions that harm the financial interests of the European Union, as indicated in the Whistleblowing Decree;
- Acts or omissions concerning the internal market, including breaches of European Union rules on competition and State aid, as well as breaches concerning the internal market connected with acts that violate corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax legislation, as indicated in the Whistleblowing Decree;
- Acts or conduct that defeat the object or purpose of the provisions laid down in Union acts in the sectors indicated under points b), c) and d)
- Breaches of restrictive measures of the European Union falling within the scope of application of the Whistleblowing Decree as a result of the amendments introduced by Legislative Decree No. 211 of 30 December 2025.

Therefore, where falling within the categories indicated above and/or relating to breaches of the 231 Model or of the Code of Ethics, the scope of this Procedure also includes, by way of example and without limitation, reports concerning conduct relating to environmental matters, occupational health and safety, protection of personal rights, discrimination and harassment, personal data protection, cybersecurity and breaches of relevant company procedures.

Reporting Persons may include the Company's employees and managers, members of corporate bodies, collaborators, consultants and, in general, third parties who are connected to the Company by contractual relationships or work-related activities, such as business partners. In this regard, please refer to note 1 of this document.

Reports may not concern information that is already in the public domain, nor claims, disputes or requests of a personal nature by the Reporting Person relating exclusively to their individual employment relationships.

Reports may relate to:

- Employees, collaborators and managers of the Company;
- Members of corporate bodies, including the Board of Directors, the Board of Statutory Auditors, the Auditing Firm and the Supervisory Body;
- Third parties connected to the persons indicated above, including suppliers, subcontractors and consultants.

The Reporting Person is required to indicate in the report whether they have any private interest connected with the report and, if so, to specify the nature of such interest, and to declare their commitment to report what they know truthfully.

4.2 Characteristics of the Report

The report must be made in good faith or on the basis of a reasonable belief and must contain useful elements enabling the persons responsible for its examination and assessment to carry out the appropriate investigations and checks regarding the merits of the facts and circumstances reported.

The report must therefore provide detailed information on the facts reported, indicating the time and place in which they occurred, the perpetrator or, where more than one, the perpetrators of the facts, as well as any documents proving the same.

Reports may also be submitted anonymously, provided that they meet the requirements of completeness, detail and substantiation set out in this paragraph and are adequately circumstantiated. Nevertheless, it should be borne in mind that submitting an anonymous whistleblowing report may make it more difficult to ascertain the reported conduct and to communicate between the Report Manager and the Reporting Person, and may therefore undermine the usefulness of the Report itself.

4.3 Recipients and Reporting Channels

Reports may be submitted through three different reporting channels:

a) Internal reporting channel;
b) External reporting channel;
c) Public disclosure.

The three types of reporting must be used progressively and subsidiarily, meaning that the Reporting Person may make:

- An external report only if they were unable to make an internal report or if the internal report was not followed up, as further described in the subsequent section "External Reporting";
- A public disclosure only after having made an internal and/or external report without any follow-up, as further described in the subsequent section "Public Disclosure".

The reporting channels available to the persons concerned are communicated through internal company communications and by publication on the Company's website.

The Reporting Person may at any time supplement, rectify or complete the report submitted, or add further evidence, including documentary evidence, in the same manner in which the original report was submitted.

Internal Reporting

The monitoring and management of the internal reporting channels are entrusted to the "Report Manager".

In this regard, it should be noted that, in order to ensure the protection of the confidentiality of the Reporting Person's identity, in accordance with the applicable regulations, the Company has deemed it appropriate to entrust the role of report manager pursuant to Article 4, paragraph 2, of Legislative Decree No. 24/2023 to an internal resource of the Payroll Department hereinafter also referred to simply as the Report Manager, who has adequate professional expertise and the necessary autonomy and independence in relation to the task of managing the internal reporting channels.

Furthermore, the Company has provided for the role of "Identity Custodian" by appointing an external consultant, namely the person authorised to disclose the details of the Reporting Person upon express and reasoned request, although the custodian is not able to view individual reports.

The Report Manager has received a formal appointment as the person responsible for managing the internal channels, which also includes the letter of designation as an authorised person pursuant to Article 29 of Regulation (EU) 679/2016, also the "GDPR", and Article 2-quaterdecies of Legislative Decree No. 196/2003, also the "Privacy Code". The letter provides specific instructions for the correct processing of personal data relating to the report, for which the Company acts as Data Controller pursuant to Article 4, paragraph 1, no. 7, of the GDPR.

From the time of designation of the Report Manager, the Company also identifies a substitute for the same, likewise possessing adequate professional expertise, autonomy and independence. The functions relating to the management of the internal channel are transferred to the substitute in cases where the Report Manager has a conflict of interest in relation to a specific report, or in the event of the Report Manager's absence or impediment lasting more than seven days.

Raffmetal has established the following internal reporting methods:

- Dedicated whistleblowing platform

This enables reports to be submitted electronically, in written and oral form, and ensures, including through encryption tools, the confidentiality of the identity of the Reporting Person, the Person Concerned and any person otherwise mentioned in the Report, as well as the confidentiality of the content of the Report and the related documentation.

The platform can be accessed from any browser through Raffmetal's website, in the dedicated section: https://raffmetal.wallbreakers.it/#/

Anonymous Whistleblowing Reports may also be submitted.

In this regard, it should be noted that the platform allows the Reporting Person to remain in contact with the Report Manager during the management of the Anonymous Report, enabling them to provide clarifications and/or additional documentation through a messaging system that guarantees their anonymity.

The reporting platform adopted, provided by a third party and equipped with appropriate technical security measures as required by Article 32 of the GDPR, provides for confidential registration, the use of encryption and a guided process for the Reporting Person, enabling them to enter the information necessary for the reconstruction and assessment of the facts.

The platform provider has signed a data protection agreement pursuant to Article 28 of the GDPR, under which it undertakes to comply with the instructions provided by the Company as Data Controller, including in the event of sub-processing.

When using the platform, the Reporting Person must complete a series of open and closed questions that will allow the Report Manager to carry out an initial examination of the subject matter of the report, even without establishing direct contact with the Reporting Person. The platform also allows the upload of any documentation that the Reporting Person considers appropriate to bring to the attention of the Report Manager in support of their report.

Through the use of the platform, exchanges of requests between the Reporting Person and the Report Manager may take place in order to further examine the matters reported or to arrange a direct meeting.

At the end of the reporting procedure, the platform will provide the Reporting Person with a code enabling them to access the system and, therefore, their report, in order to:

a) Monitor its progress;
b) Supplement their report with further factual elements or other documentation;
c) Have direct contact with the Report Manager, including by initiating a possible exchange of requests and information.

The platform used by the Company allows reports and the attached documentation to be stored electronically and in encrypted form, as well as in compliance with the applicable legislation on the protection of personal data. The data and documents covered by the Report are retained in accordance with the law. Encryption ensures the confidentiality not only of the Reporting Person, but also of the facilitator, the person concerned or otherwise mentioned in the report, as well as of the content of the report and the documentation.

- Direct meeting

To be held in person, in a confidential place, upon request by the Reporting Person to the Report Manager through the platform, and scheduled within a reasonable time. This oral report, subject to the prior consent of the Reporting Person, shall be documented by means of a recording on a device suitable for storage and playback, or by means of a full transcript. In the event of transcription, the Reporting Person may verify, rectify or confirm the content of the transcript by signing it. Failure to sign shall result in the report being inadmissible.

Warning: Reports concerning breaches of Legislative Decree No. 231/2001 may be made only through the internal channel.

Warning: In any case, it is emphasised that only reports concerning the breaches as defined above fall within the scope of application of this Procedure and, therefore, benefit from the protections indicated below.

It is understood that reports that are not deemed relevant for the purposes of this Procedure and therefore fall outside the scope of application of Legislative Decree No. 24/2023 shall be archived by the Report Manager as "non-whistleblowing reports" and forwarded to the competent Functions so that they may carry out their own investigative activities.

Nevertheless, it should be noted that it is always possible to report unlawful conduct not falling within the above categories to the email addresses of the Supervisory Body, as indicated in the Company's Organisation, Management and Control Model:

a) Supervisory Body email address: odv@raffmetal.it;
b) Confidential postal letters addressed to Raffmetal S.p.A., Supervisory Body pursuant to Legislative Decree No. 231/2001, Via Malpaga, 82 - 25070 Casto (BS), Italy.

The members of the Supervisory Body are required to comply with confidentiality obligations; however, in such cases, the protections and safeguards provided for under this Procedure shall not apply.

External Reporting

Only for breaches concerning offences falling within the scope of application of the European Union or national acts indicated above, paragraph 3, letters b), c), d) and e), the Reporting Person may submit an external report through the channel activated at ANAC, the Italian National Anti-Corruption Authority. The external reporting channel may not be used for reports concerning breaches of Legislative Decree No. 231/2001 or breaches of the Organisation and Management Model.

An external report may be submitted under the following conditions:

a) The internal reporting channel, even if mandatory, is not active or, even if activated, does not comply with the provisions of Article 4 of Legislative Decree No. 24 of 10 March 2023;
b) The Reporting Person has already submitted an internal report pursuant to Article 4 and no follow-up has been given to it;

c) The Reporting Person has reasonable grounds to believe that, if they submitted an internal report, it would not be effectively followed up, or that the report itself could give rise to a risk of retaliation;

d) The Reporting Person has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest.

The existence of the conditions for using the external reporting channel must be adequately justified by the Reporting Person; in particular:

- report is considered not to have been "followed up", see letter b) above, when it has remained entirely without response;
- The "reasonable grounds" referred to in letters c) and d) above must be objective and adequately substantiated.

External reports shall be submitted through the platform made available by ANAC, the Italian National Anti-Corruption Authority, designated as the authority responsible for receiving external reports from both the public and private sectors. The methods for using this channel are indicated on ANAC's website https://www.anticorruzione.it/-/whistleblowing.

Public Disclosure

Public disclosure means making information on breaches publicly available through the press, electronic means or, in any case, through means of dissemination capable of reaching a large number of people. Public disclosure may not be used for reports concerning breaches of Legislative Decree No. 231/2001 or breaches of the Organisation and Management Model.

Public disclosure may be made only if one of the following conditions is met:

- The Reporting Person has previously submitted an internal and external report, or has directly submitted an external report, under the conditions and in the manner provided for by this Procedure, and no response has been provided within the prescribed time limits regarding the measures envisaged or adopted to follow up on the reports;
- The Reporting Person has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest;
- The Reporting Person has reasonable grounds to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there is a reasonable fear that the person who received the report may be colluding with the perpetrator of the breach or involved in the breach itself.

As regards the definition of "reasonable grounds", please refer to the previous paragraph.

The Reporting Person who makes a public disclosure benefits from the protection provided for by Legislative Decree No. 24/2023 only if one of the three conditions indicated above is met.

Warning: The external reporting channel and public disclosure may not be used in the case of unlawful conduct relevant pursuant to Legislative Decree No. 231/2001 or breaches of the Company's Organisation and Management Model or Code of Ethics.

5. INTERNAL REPORT MANAGEMENT PROCESS

5.1 Receipt of the Report and Preliminary Assessment

When an internal report is received, the Report Manager confirms receipt thereof to the Reporting Person, if identified, within seven days. The Report Manager then carries out a formal examination of the report, verifying:

- Its completeness;
- Compliance with the criteria established in this Procedure;
- The existence of the legal and factual conditions for initiating the subsequent analysis phase, including with the support of specialised external consultants;
- The possible seriousness of the reported facts and their urgency.

Once the above preliminary assessment has been completed, the Report Manager:

a) If the report falls outside the scope of this Procedure, for example because it relates to a personal complaint or concerns facts that are in the public domain or circumstances already ascertained by the Judicial Authority, or if it lacks the necessary requirements referred to in paragraph 4.2 above, proceeds to archive the report, informing the Reporting Person, if traceable, and stating the reasons for the archiving;

b) If the report is excessively generic or incomplete, contacts/summons the Reporting Person, if traceable, in order to request useful elements for the preliminary assessment;

c) If a possible breach or unlawful conduct is identified, proceeds with the subsequent analysis phase, informing the Chair of the Board of Directors.

The duration of this preliminary investigation phase shall not normally exceed thirty days from receipt/commencement of the preliminary assessment and shall be documented in a specific register, hereinafter the "Reports Register", kept by the Report Manager in such a way as to ensure the confidentiality of the information collected and the confidentiality of the Reporting Person. The type of report received, the date of receipt, the date of completion of the preliminary assessment and its outcome, together with the relevant reasons, shall be recorded in the register. The person entrusted with the management of reports shall also delete any personal data that are not useful for the purposes of the report. The Reports Register may also be managed within the whistleblowing platform.

As provided for by Article 4 of the Whistleblowing Decree, any Report submitted to a person other than the Report Manager must be forwarded immediately, and in any case within seven days, to the Report Manager, with simultaneous notice thereof to the Reporting Person.

5.2 Analysis and Assessment of the Report

If the preliminary assessment referred to in the previous paragraph is concluded positively, as indicated in point c) of the previous paragraph, the Report Manager immediately proceeds to the phase of analysis and assessment of the merits of the report.

In this phase, the Report Manager may:

- Liaise with other company functions and roles in order to request their cooperation, through the provision of data, documents or information useful for the analysis, obtaining operational support from the various company functions involved, while maintaining appropriate confidentiality regarding the identity of the Reporting Person and the Reported Person;
- Request further elements or clarifications from the Reporting Person, if traceable, recording any related interview in writing and keeping the minutes on file;
- Use external resources to conduct the necessary investigations;
- Carry out any activity deemed useful or necessary, including hearing the Reporting Person and/or any other persons who may provide information on the reported facts, in compliance with the principles of confidentiality and impartiality of judgment, the legislation on personal data protection and the applicable National Collective Bargaining Agreement.

In any case, the personal details of the Reporting Person and any other information from which such identity may be directly or indirectly inferred shall not be disclosed by the Report Manager without the consent of the Reporting Person, in order to protect them from possible retaliation or discrimination. It is specified that, even in the absence of consent, where necessary for investigative purposes and where other persons must also be made aware of the content of the report and/or the documentation attached thereto, the Report Manager shall redact the personal data of the Reporting Person, as well as those of the other persons whose identity must remain confidential, namely the facilitator, the Reported Person and the other persons mentioned in the report.

The Reported Person and any other persons mentioned in the reports have the right to be heard, in order to exercise their right of defence, either orally or through the submission of written observations.

The analysis phase ends with a written opinion by the Report Manager indicating:

- The details of the report, including the name of the Reporting Person, if known, and of the Reported Person or Persons, the place and date on which the facts occurred, and evidentiary or documentary elements;

- The checks carried out, their outcomes and the company persons or third parties involved in the analysis phase;
- A summary assessment of the analysis process, indicating the facts established and the related reasons;
- The outcome and conclusion of the analysis, namely archiving or confirmation of the merits of the report.

At the end of the analysis phase, the Report Manager:

- If the report is considered unfounded, proceeds to archive it, providing written reasons;
- If the report is considered well-founded and proven, communicates the outcome to the Chair of the Board of Directors for the adoption of the consequent decision-making measures, without disclosing the personal details of the Reporting Person.

The analysis phase referred to in this paragraph must be completed within sixty days from the date on which it is initiated, except in cases of particular importance and urgency, in which the Chair of the Board of Directors shall immediately inform the Board of Statutory Auditors and the Board of Directors without waiting for completion of the analysis phase.

Depending on the circumstances and the seriousness of the breach identified, the decisions to be adopted may include one or more of the following actions:

- Termination of contracts, suspension of projects or activities;
- Return, or request for return, of any improper benefit;
- Adoption of disciplinary measures against the personnel members involved;
- Reporting to the authorities;
- Adoption of actions aimed at avoiding or minimising any legal consequence of the breach identified, such as remediation of the damage, voluntary disclosure/remediation, etc.

In any case, the person entrusted with the management of reports must provide feedback to the Reporting Person, if traceable, within three months[3] from the date of the acknowledgment of receipt of the report or, in the absence of such acknowledgment, from the expiry of the seven-day period from submission of the report, on the status of the internal investigation and its outcome, if concluded, providing the reasons for any archiving.

With regard to 231 Reports and Reports concerning the Code of Ethics, the Report Manager carries out the above activities by involving the members of the Supervisory Body. In such case, the meetings of the Supervisory Body may also take place through the platform, in compliance with the confidentiality requirements provided for by the Whistleblowing Decree and by this Procedure.

Any powers of supervision or filtering by the management body over the investigation are expressly excluded: the Report Manager independently decides on the outcomes and on the internal/external recipients to whom the documents are to be transmitted.

[3] Starting from the expiry of the seven-day period following receipt of the report

Retention of Documentation

Reports, and the related documentation, even if anonymous[4], are retained through the platform for the time necessary for their processing and, in any case, in accordance with the provisions of Legislative Decree No. 24/2023, for no longer than five years[5] from the date of communication of the final outcome of the Report management process.

5.3 Reports Concerning Corporate Bodies

a) If the report concerns the Chair of the Board of Directors/Chief Executive Officer, the Report Manager shall forward it to the Deputy Chair of the Board of Directors, who may decide whether to proceed directly, on their own behalf, with the analysis phase referred to in paragraph 5.2, or whether to appoint the Report Manager and proceed in the ordinary manner, in any case informing the Chair of the Board of Statutory Auditors;

b) If the report concerns another member of the Board of Directors, the Report Manager shall forward it to the Chair of the Board of Directors, who may decide whether to proceed directly, on their own behalf, with the analysis phase referred to in paragraph 5.2, or whether to appoint the Report Manager and proceed in the ordinary manner, in any case informing the Chair of the Board of Statutory Auditors;

c) If the report concerns a member of the auditing firm/statutory auditor or of the Board of Statutory Auditors, the Report Manager shall forward it to the Chair of the Board of Directors, who may decide whether to proceed directly, on their own behalf, with the analysis phase referred to in paragraph 5.2, or whether to appoint the Report Manager and proceed in the ordinary manner, in any case informing the Board of Directors;

d) If the report concerns the Supervisory Body itself, the Report Manager shall not involve that body, even if the report concerns matters falling within its competence, and shall instead inform the Chair of the Board of Statutory Auditors and the Chair of the Board of Directors, who may decide whether to proceed directly, on their own behalf, with the analysis phase referred to in paragraph 5.2, or whether to appoint the company function deemed most competent;

e) If the report concerns the Report Manager, one of the conditions for using the external reporting channel to ANAC is deemed to exist, since it cannot be ensured that the report will be effectively followed up. If the report is forwarded to persons other than the Report Manager, such persons must forward it to the Chair of the Board of Directors, who may decide whether to proceed directly, on their own behalf, with the analysis phase referred to in paragraph 5.2, or whether to appoint the company function deemed most competent, in any case informing the Chair of the Board of Statutory Auditors

[4] The provision for the recording and retention of anonymous reports as well is intended to allow them to be linked to any subsequent reports of retaliation.
[5] With distinction from the documents of judicial proceedings, which may be subject to their own time limits.

and without prejudice to the involvement of the Company's Supervisory Body, insofar as matters falling within its competence are concerned.

6. DISCIPLINARY MEASURES

6.1 Disciplinary Measures against Employees

Upon receipt of the report from the person who carried out the analysis of the report, the Chair of the Board of Directors decides whether to initiate disciplinary proceedings against the reported persons deemed responsible for the breach or unlawful conduct, following the analysis carried out and the assessment performed.

Where the Reporting Person is jointly responsible for the facts covered by the report, they shall receive more favourable treatment than the other jointly responsible persons, provided that this is in compliance with the applicable legislation and National Collective Bargaining Agreement, as well as with the protections provided for under the Workers' Statute.

The Chair of the Board of Directors also assesses, with the assistance of the Human Resources Manager, whether to initiate disciplinary proceedings:

- Against the Reporting Person who has acted with wilful misconduct or gross negligence, duly ascertained and proven, or whose criminal liability for the offences of defamation or slander has been established, including by a first-instance judgment;
- Against any persons responsible for retaliatory/discriminatory conduct against the Reporting Person;
- Against the persons involved in the process of assessing and analysing the report who have breached confidentiality obligations or have failed to examine the report received.

The disciplinary proceedings adopted shall be those provided for by the applicable National Collective Bargaining Agreement, imposed on the basis of the Workers' Statute and in compliance with the company disciplinary system.

In addition to disciplinary sanctions, any power of attorney granted to the employee may also be revoked.

Under no circumstances shall proceedings be initiated solely on the basis of the report, in the absence of concrete findings regarding its content. This may occur, where applicable, on the basis of other evidence identified and ascertained starting from the report itself.

Any retaliatory or discriminatory dismissal of the Reporting Person is null and void. Any change of duties pursuant to Article 2103 of the Italian Civil Code, as well as any other retaliatory or discriminatory measure, as further defined in paragraph 7.2 below, adopted against the Reporting Person, shall also be null and void. In the event of disputes relating to the imposition of disciplinary sanctions, or to demotions, dismissals, transfers, or the Reporting Person being subjected to any other organisational measure having direct or indirect negative effects on working conditions after submission of the report, the burden shall be on the employer to prove that such measures are based on reasons unrelated to the report itself.

6.2 Measures against Corporate Bodies

Where the breach or unlawful conduct concerns a member of the corporate bodies, the Board of Directors and/or the Board of Statutory Auditors, depending on the case and according to their respective areas of competence, shall take the most appropriate and adequate initiatives in view of the seriousness of the breach and in compliance with the law and the Articles of Association.

In the most serious cases, the Board of Directors, after consulting the Board of Statutory Auditors, may propose to the shareholders' meeting that the office of the director concerned be revoked. In the event of a breach by statutory auditors, the Board of Directors, after consulting the shareholders' meeting, may apply to the Court for revocation of the mandate of the statutory auditor concerned.

In the case of breaches or unlawful conduct committed by a director who is also an employee of the Company, the applicability of the different disciplinary actions arising from the employment relationship shall in any case remain unaffected.

6.3 Measures against Third Parties

In the event of a breach or unlawful conduct by third parties, such as consultants, collaborators, agents, suppliers, subcontractors, etc., the Company may rely on the termination clauses contained in the contracts/engagement letters for breaches of the Organisation, Management and Control Model pursuant to Legislative Decree No. 231/2001, of which this Procedure forms an integral part.

6.4 Consequential and Additional Measures

The Chair of the Board of Directors may inform the judicial authority and/or the supervisory authorities of the facts covered by the report if they determine that such facts have the characteristics of a criminal offence or of a civil or administrative offence.

The Chair of the Board of Directors, in coordination with the Human Resources Manager, defines the implementation of any prevention measures that may become necessary in order to promote a culture of legality and transparency within the Company, and promotes the adoption of any amendments and additions to this Procedure and to the control systems, in light of constant monitoring of its application and of the results achieved.

Administrative Pecuniary Sanctions Applied by ANAC

ANAC may apply the following administrative pecuniary sanctions to the person responsible:

- From EUR 10,000 to EUR 50,000 where retaliation is established, or where it is established that the report has been obstructed, that an attempt has been made to obstruct it, or that the confidentiality obligation provided for by the Whistleblowing Decree has been breached;
- From EUR 10,000 to EUR 50,000 where it is established that reporting channels have not been established in accordance with the requirements provided for by the Whistleblowing Decree, that no procedure for making and managing reports has been adopted, that such procedure is not compliant with the Whistleblowing Decree, or where the reports received have not been verified and analysed;
- From EUR 500 to EUR 2,500 where the whistleblower's criminal liability for the offences of defamation or slander is established.

7. PROTECTION OF THE REPORTING PERSON

7.1 Confidentiality and Privacy

The Company guarantees the confidentiality of the Reporting Person and of the data/information transmitted, in order to protect the Reporting Person from any form of retaliation or discrimination.

With regard to access to internal reporting channels, the Company adopts appropriate technical and organisational measures to prevent the identity of the Reporting Person from being reconstructed through browsing logs, firewalls, proxies, DNS, authentication systems, access from the corporate network or other technical tracking tools.

This is without prejudice to the possibility of collecting and retaining any technical and security logs, where strictly necessary for cybersecurity, business continuity, abuse prevention, incident management, protection of the integrity of information systems and fulfilment of applicable obligations, including those provided for by Legislative Decree No. 138 of 4 September 2024.

Such logs are processed in accordance with the principles of minimisation, purpose limitation, segregation of access and proportionate retention, and may not be used to identify the Reporting Person, nor for retaliatory, disciplinary or otherwise incompatible purposes with the protection provided for by Legislative Decree No. 24/2023.

Access to the above-mentioned logs is permitted exclusively to persons formally authorised for cybersecurity purposes, in accordance with the principle of purpose separation referred to in Article 5, paragraph 1, letter b), of Regulation (EU) 2016/679. Any correlation between technical logs and the identity of the Reporting Person is also prohibited, unless this is required by a legal obligation or by an order of the competent Authority.

As a further precautionary measure to protect confidentiality, the Company recommends that the Reporting Person, where possible, access the internal channel from non-corporate networks and devices.

The identity of the Reporting Person and any other information from which such identity may be directly or indirectly inferred may not be disclosed, without the express consent of the Reporting Person, to persons other than those competent to receive or follow up on reports and 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 Personal Data Protection Code referred to in Legislative Decree No. 196 of 30 June 2003, except where disclosure is requested by the judicial or administrative authority and where there is a specific legal obligation in this regard, for example in cases where:

- The report submitted and the subsequent investigations reveal the commission of a civil or criminal offence[6] by the Reporting Person;
- Knowledge of the identity of the Reporting Person is necessary and indispensable for handling the report or for the purposes of exercising the right of defence of the Reported Person;
- The Reporting Person is notified of the disclosure of their identity by written communication, stating the relevant reasons.

Only personal data that are relevant and strictly necessary for the assessment of the report may be processed by the persons involved in the phases of this Procedure.

Such persons must also ensure that access to the information contained in the reports by other company functions or third parties that may be involved in the above-mentioned phases and processes never entails access to the personal data of the Reporting Person or of the Reported Person, without prejudice to the exceptions indicated above. In any case, the personal details of the Reporting Person and any other information from which such identity may be directly or indirectly inferred shall not be disclosed by the Report Manager without the consent of the Reporting Person, in order to protect them from possible retaliation or discrimination. It is specified that, even in the absence of consent, where necessary for investigative purposes and where other persons must also be made aware of the content of the report and/or of the documentation attached thereto, the Report Manager shall redact the personal data of the Reporting Person, as well as those of the other persons whose identity must remain confidential, namely the facilitator, the Reported Person and the other persons mentioned in the report. For the purposes of this Procedure, the personal data of the Reporting Person shall be retained, in compliance with Legislative Decree No. 196/2003, as amended and supplemented, Regulation (EU) 2016/679, the GDPR, and the company procedures in force, for the time strictly necessary for their processing and, in any case, for a period not exceeding five years from the date of communication of the final outcome[7], without prejudice to cases in which it is necessary to retain them for a longer period, subject to adequate justification and limited to the duration of such necessity.

[6] In criminal proceedings, the identity of the Reporting Person is protected by confidentiality in the manner and within the limits provided for under Article 329 of the Code of Criminal Procedure.

[7] As stated in the opinion of the Italian Data Protection Authority on the draft legislative decree implementing Directive (EU) 2019/1937 of the European Parliament.

The Company applies the same principles and protections set out in this paragraph also to the personal data of the Reported Person pending the internal analysis and assessment process, without prejudice to any liability and communication obligations that may be imposed by law or by the judicial authority. Similar confidentiality safeguards are granted to any other persons involved or mentioned in the reports, until the conclusion of the proceedings.

Within the scope of any disciplinary proceedings initiated against the Reported Person, the identity of the Reporting Person may not be disclosed where the disciplinary charge is based on findings that are separate from and additional to the report, even if consequent upon it. Where the charge is based, in whole or in part, on the report and knowledge of the identity of the Reporting Person is indispensable for the defence of the accused person, the report may be used for the purposes of the disciplinary proceedings only with the express consent of the Reporting Person to the disclosure of their identity.

All documentation relating to reports is considered confidential and therefore accessible only to authorised persons. During the activities aimed at verifying the merits of the report, all necessary measures shall be adopted to protect the data against accidental or unlawful destruction, loss and unauthorised disclosure.

7.2 Protection against Retaliatory Acts

In order to protect the Reporting Person, the legislation provides that they may not suffer any retaliation and establishes specific protection measures and limitations of liability.

Such protections are granted where, at the time of the report, the Reporting Person had reasonable grounds to believe that the information on the breaches was true and fell within the objective scope of application of the legislation, even where the report ultimately proves to be unfounded.

Furthermore, reports and public disclosures must have been made in compliance with the rules and the procedure governing the use of the different channels.

The protection measures for the Reporting Person do not apply, however, where the Reporting Person's criminal liability for the offences of defamation or slander is established, including by a first-instance judgment, or where civil liability on the same grounds is established in cases of wilful misconduct or gross negligence. In such cases, disciplinary action is initiated, as indicated in paragraph 6.1 above.

Where the conditions for the application of the protections are met, retaliatory acts against the Reporting Person are prohibited, including, by way of example and without limitation:

- Dismissal, suspension or equivalent measures;
- Demotion or failure to promote;
- Detrimental change of duties, workplace, salary or working hours;
- Suspension of training or any restriction of access thereto;
- Negative performance notes or negative references;
- Adoption of disciplinary measures or other sanctions, including financial sanctions;

- Coercion, intimidation, harassment or ostracism;
- Discrimination or otherwise unfavourable treatment;
- Failure to convert a fixed-term employment contract into an open-ended employment contract, where the worker had a legitimate expectation of such conversion;
- Non-renewal or early termination of a fixed-term employment contract;
- Damage, including to the person's reputation, particularly on social media, or economic or financial prejudice;
- Inclusion in improper lists on the basis of a formal or informal sectoral or industry agreement, which may make it impossible for the person to find employment in the future in the relevant sector or industry;
- Early termination or cancellation of a contract for the supply of goods or services;
- Cancellation of a licence or permit;
- Request to undergo psychiatric or medical examinations.

Retaliatory acts adopted in breach of the above legislation are null and void.

Communications concerning retaliation suffered, or presumed to have been suffered, must be submitted exclusively to ANAC, in accordance with the methods set out in the previous paragraph "External Reporting". In order to acquire the investigative elements necessary to ascertain retaliation, ANAC may avail itself of the cooperation of the National Labour Inspectorate, without prejudice to ANAC's exclusive competence in assessing the elements acquired and the sanctions to be imposed.

It is therefore important that anyone who has suffered retaliation does not send the communication to persons other than ANAC, so as not to undermine the protections guaranteed by Legislative Decree No. 24/2023, first and foremost confidentiality. Where, by mistake, the Company receives a communication concerning retaliation, it is required to guarantee the confidentiality of the identity of the person who sent it and to forward it to ANAC, simultaneously informing the person who made the communication of such transmission. Persons who have suffered retaliation have the right to be reinstated in their workplace.

In judicial or administrative proceedings or in out-of-court disputes concerning the assessment of retaliatory conduct, such conduct is presumed to have been carried out as a result of the report, complaint or public disclosure. The burden of proving that such acts were based on different reasons lies with the person who carried them out. Furthermore, in the event of a claim for damages submitted by Reporting Persons who prove that they have suffered harm as a result of a report, public disclosure or complaint to the authorities, the damage is presumed, unless proven otherwise, to be a consequence of the report.

The Reporting Person shall also not be punishable where they disclose or disseminate information on breaches covered by confidentiality obligations, relating to the protection of copyright or the protection of personal data, or information that harms the reputation of the person concerned or reported, where, at the time of disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of such information was necessary to reveal the breach.

Protection against retaliatory acts cannot, for obvious reasons, be guaranteed in the case of anonymous reports.

The protections also apply to:

- The so-called "facilitators", defined as natural persons who assist a Reporting Person in the reporting process, operating within the same work-related context and whose assistance must be kept confidential;
- Other persons connected to the Reporting Person who may suffer retaliation in a work-related context, such as co-workers who have a habitual or recurring relationship with that person;
- Persons in the same work-related context who are linked to the Reporting Person by a stable emotional relationship or by kinship up to the fourth degree;
- Entities owned by the Reporting Person or for which the Reporting Person has worked, as well as entities operating within the same work-related context.

Finally, protection also applies where the report is made:

a) When the employment relationship/contract has not yet begun, if the information on the breaches was acquired during the selection process or in other pre-contractual phases;
b) During the probationary period;
c) After termination of the legal relationship, if the information on the breaches was acquired during the course of that relationship.

8. REPORTING

On an annual basis, the Report Manager prepares a summary report concerning the reports received during the year, the analyses carried out and the outcome thereof.

The annual report must contain at least:

- An indication of all reports received, distinguishing between those under analysis and those archived or concluded, the criteria and methods used for assessing the reports accepted, and their outcomes, including archiving, initiation of disciplinary proceedings and sanctions applied;
- A proposal for any corrective or supplementary criteria to the Procedure.

The above-mentioned report is sent to the Chair of the Board of Directors, who informs the Board of Directors and the Board of Statutory Auditors thereof.

9. INFORMATION AND TRAINING

Information on this Procedure is made accessible and available to everyone, displayed in a clearly visible manner in the workplace and also published on the website, and is therefore available to all potential stakeholders who become aware of the breaches described above.

Information on the Procedure is also made available when an employee is hired.

Training on whistleblowing and, more generally, on the provisions set out in this Procedure is also included in the staff training plans provided by the Company in relation to compliance.

The staff training plans provided by the Company in relation to compliance also include dedicated and periodic training for the Report Manager and the substitute, covering legislation, privacy, conflicts of interest, management of complex cases, etc.

For more information contact us:
info@raffmetal.it