metalplasma
CENTRO LAVORAZIONE LAMIERE

Whistleblowing Procedure

REVISION	SUBJECT	DATE
1	IMPLEMENTATION OF REGULATORY CHANGES AND UPDATE TO THE WHISTLEBLOWING REPORT MANAGEMENT PROCESS	03/07/2026
0	WHISTLEBLOWING PROCEDURE (PURSUANT TO LEGISLATIVE DECREE 24/2023)	15/12/2023

1. Purpose

This procedure is adopted by the Company in compliance with the provisions of Legislative Decree no. 24 of 10 March 2023 (hereinafter referred to as the "Decree" or "Legislative Decree 24/2023) – and subsequent amendments – which entered in force on 30 March 2023. It transposes Directive (EU) 2019/1937 of the European Parliament and Council of 23 October 2019, regarding the protection of persons who report breaches of the national and European Union legislation (the so-called Whistleblowing Directive), of which they have become aware in a work-related context. Said violations are detrimental to the public interest or to the integrity of the public administration or of a private entity.

This procedure has been approved by the Board of Directors together with the identification of the organisational roles involved in the whistleblowing reporting management process and the related responsibilities.

In addition to the provisions set out in this Procedure, please refer to the dedicated section of the Company's website (https://www.metalplasma.it/en/reporting/).

2. Scope

This procedure is applied to any report of information on breaches (<u>as more specifically defined in section 4</u>) acquired within the work-related context[1], when they are detrimental to the public interest or to the integrity of the public administration or of a private entity, and consist of:

1. offences falling within the scope of application of the relevant EU or national acts relating to[2]:
    I. public procurement (tendering procedures and appeal procedures);
    II. services, products and financial markets, money laundering prevention (regulatory and supervisory rules, and rules on consumer and investor protection);
    III. product safety and compliance (regulations on safety and compliance requirements, on the marketing and use of sensitive and hazardous products, the so-called military goods);
    IV. transport safety (railway sector, civil aviation, road and sea transport, inland transport of hazardous goods by road, rail or inland waterways, both within the national territory and between States of the European Community);
    V. environmental and climate protection (marine, air and noise pollution, waste management, soil and water resources, biodiversity, chemical substances and biological products);
    VI. nuclear safety (facilities, exposure to radiation, nuclear fuel and waste management, shipment of radioactive substances);

[1] to be understood as an employment relationship with the organisation or as a professional/working engagement, whether current or past

[2] Please refer to the annexes to Directive 2019/1937 and Legislative Decree 24/23.

VII. food and animal feed safety, health and welfare of animals;

VIII. public health (quality and safety standards relating to human tissues and cells, human blood and its components, organs intended for transplantation, medicinal products and medical devices, patients' rights in cross-border healthcare, and the manufacture and sale of tobacco products);

IX. consumer protection (product quality and safety, information and advertising, contract relationships, commercial practices);

X. protection of privacy and personal data, and the security of networks and information systems;

2. breaches (acts and omissions) which are detrimental to the financial interests of the EU (see art. 325 of Treaty on the Functioning of the European Union);
3. breaches (acts or omissions) of rules on competition and State aid (see art. 26(2) of the Treaty on the Functioning of the European Union);
4. breaches (acts or omissions) of corporate taxation regulations;
5. breaches of the European Union's restrictive measures referred to in Chapter I-bis of Title I of Book II of the Italian Criminal Code, as well as Article 12(1-bis) of Legislative Decree no. 286 of 25 July 1998.

The following are excluded from the scope of this procedure:

- disputes, claims or requests relating to a personal interest which pertain exclusively to individual employment relationships, i.e. employment relationships with hierarchically superior roles;
- breaches relating to national security, as well as tenders concerning defence or national security matters;
- breaches mandatorily governed by European Union or national[3] acts which provide for specific reporting procedures.

The information on breaches must be acquired within the work-related context[4] and must be carried out through the dedicated channels made available by the Company.

[3] Please refer to the annexes to Directive 2019/1937 and Legislative Decree 24/23.
[4] to be understood as an employment relationship with the organisation or as a professional/working engagement, whether current or past.

3. References

- Legislative Decree 10 March 2023, no. 24;
- Directive (EU) 2019/1937;
- European Regulation 2016/679 (GDPR);
- Privacy Code (Legislative Decree 196/2003 and as subsequently amended);
- The ANAC (National Anti-Corruption Authority) guidelines on the protection of persons who report breaches of the Union's law and the protection of persons who report breaches of national legislative provisions – procedures for the submission and management of external reports.

4. Definitions

- **"reports":** any communication, whether written, oral or expressed in a conversation, also in an anonymous form, containing information on breaches;
- **"information on breaches":** all information, including well-founded suspicions, regarding breaches committed or which, based on concrete elements, may be committed in the organisation with which the reporting person or who lodges a complaint with the judicial or accounting authority has a legal relationship and also the informational elements relating to conduct aimed at concealing such breaches;
- **"internal report":** communication of the "reports" through the dedicated internal reporting channel;
- **"external report":** any written or oral communication of information on breaches submitted through the external reporting channel;
- **"public disclosure":** making information on violations available in the public dominion through the press or by electronic means or, in any case, through means of dissemination capable of reaching a large number of people;
- **"reporting person":** a natural person who makes a report or disclosure to the public information on breaches acquired within the scope of their work-related activities;
- **"facilitator":** a natural person who assists a reporting person in the reporting process, operating within the same work-related context and whose assistance must be kept confidential;
- **"work-related context":** past or current work or professional activities through which, regardless of the nature of such activities, a person acquires information on breaches and within which they may be exposed to the risk of retaliation in the case of a report or public disclosure or complaint to the judicial or accounting authority;
- **"person concerned":** a natural or legal person mentioned in the report to whom the breach is attributed or as a person otherwise involved in the reported breach;

- **"channel manager":** an external party, appointed by the Company, responsible for managing the reporting channel and report, with organisational and functional autonomy;
- **"internal contact person":** a person within the Company appointed by the administrative body. Should the internal contact be a person concerned in the report, the internal contact's role shall be performed by the administrative body;
- **"deputy channel manager":** a person appointed by the Company who replaces the channel manager in handling reports in case of prolonged absence;
- **"governing body"**: the body entrusted with administrative and organisational policymaking functions (e.g. the Board of Directors / Sole Director);
- **"retaliation":** any conduct, act or omission, including attempted or threatened conduct, brought about in relation to the report (and closely linked to it), the complaint to the judicial or accounting authority or the public disclosure and which causes or may cause, directly or indirectly, unjust damage to the reporting person or to the person who has lodged the complaint;
- **"follow-up":** the action or actions initiated by the subject to whom management of the reporting channel is entrusted;
- **"feedback":** communication to the reporting person of information on the follow-up that has been or is intended to be given to the report, including the measures taken, to be taken or proposed, as well as the reasons for the chosen course of action.
- **"platform":** internal reporting channel adopted by the Company (as more specifically defined in section 8) for submitting information on breaches;

5. Responsibilities

The channel manager, also through the use of the platform:

- makes available, including through this procedure, the information published on the platform, as well as clear information on the channel, on procedures and on requirements for submitting internal reports;
- provides the reporting person with an acknowledgement of receipt of the report within the prescribed time limits;
- assesses the admissibility criteria;
- shares the report with the internal contact person, as defined in this procedure, the initiation of any investigations, their outcome and the feedback to be provided to the reporting person;
- provides the reporting person with the feedback regarding closure of the report handling process;

- maintains communications with the reporting person and, where appropriate, manages requests for additional information and conducts any follow-up meetings with the reporting person, if required;
- files and retains the documentation relating to the report within the time limits prescribed by law;
- ensures compliance with the principle of confidentiality.

<u>The internal contact person:</u>

- identifies, within the Company, the persons to be involved and shares with them findings arising from the analysis carried out by the channel manager;
- is entrusted with providing the channel manager with feedback on the decisions taken by the Company regarding the further investigation of the matters reported;
- implements the recommendations issued by the channel manager to further investigate the matters reported;
- coordinates and monitors investigation phase, where applicable, with internal functions/appointed external teams;
- shares the initiation of any investigations with the channel manager, their outcome and the feedback to be provided to the reporting person;
- identifies improvement plans so to prevent the recurrence of incidents that are the subject of whistleblowing reports;
- ensures that all information relating to the reporting channel, procedures and the requirements for making internal reports is made available through the Company's internal communication channels;
- manages, with the support of the relevant Company functions, the actions required following any public disclosures in the circumstances provided for by applicable legislation;
- ensures compliance with the principle of confidentiality.

<u>The reporting person:</u>

- submits reports in accordance with this procedure;
- is required to provide detailed information regarding the matters reported;
- identifies any individuals who may be entitled to protection and support measures (e.g. facilitators).

<u>The legal representative:</u>

- liaises with the National Anti-Corruption Authority (ANAC) in the event of an external report being submitted or inspection activities being initiated by ANAC.

The governing body:

- assesses individual responsibilities and any subsequent measures or proceedings arising from the investigation of the report.
- ensures that any necessary measures are taken in accordance with the provisions of the Company's disciplinary system;
- approves this procedure together with the associated organisational role structure;
- provides prior information to trade unions and ensures that such communication is properly documented;
- provides specific training activities on Legislative Decree 24/2023;
- regulates its relationship with the channel manager through a contractual agreement.
- ensures the internal contact person/channel manager has access to the Company's services (e.g. the company's systems, databases, platforms);
- ensures compliance with the protection measures applicable to the reporting person;
- carries out general monitoring of the correct operation of the whistleblowing procedure.

6. Persons who may submit a report (the "reporting person")

The following persons may submit a report:

- employees;
- self-employed persons and collaborators who carry out their activities for public or private sector organisations;
- independent professionals;
- volunteers;
- consultants;
- shareholders;
- directors;
- suppliers providing services to third parties in any capacity, (regardless of the nature of such activities) and whether or not they receive remuneration;
- interns whether paid or unpaid;
- individuals performing administrative, management, control, supervisory functions, or representative functions, including where such functions are exercised in practice rather than by formal appointment.

This category further includes all individuals who, in any capacity, become aware of breaches in a work-related context connected with the Company, namely:

- before the employment relationship has commenced
- during the probationary period;
- after the termination of the employment relationship.

7. Internal contact person

The Company has designated Emilio Zanella, in his capacity as Board Member, as the internal contact person pursuant to this procedure.

8. Internal reporting channel

The Company has established an internal reporting channel which the reporting person must use for submitting information concerning breaches. The establishment of this channel enables more effective prevention and investigation of breaches. This approach reflects the Company's commitment to fostering a culture of open communication and corporate social responsibility, as well as to continuously improving its organisational framework.

The internal reporting channel provides for the submission of reports in either written or oral form through the "@Whistleblowing" platform, accessible via the following link: https://digitalroom.bdo.it/GabrielliGroup/home.aspx

By accessing the platform, the reporting person may also request a face-to-face meeting with the channel manager through a voice messaging system.

The internal reporting channel ensures the confidentiality of the identity of the reporting person, the facilitator (where applicable), the persons concerned and any other persons referred to in the report, as well as the content of the report and any supporting documentation submitted or subsequently integrated.

8.1 Person Responsible for Managing the Reporting Channel (the "Channel Manager")

Responsibility for managing the internal reporting channel is entrusted to:

- BDO Advisory Services S.r.l., acting through Giuseppe Carnesecchi

an external party meeting the requirements of autonomy, impartiality and independence, with sound knowledge in the legal, ethical and integrity matters, as well as a thorough understanding of the Company's organisational structure, and having received appropriate specialist training.

The relationship with the channel manager is governed by a specific contractual agreement.

The channel manager has exclusive responsibility for the receipt of reports and access to the platform. In handling the reports, the manager may be supported by a dedicated structure which is adequately trained and independent.

In the event of the channel manager's absence, the report shall be automatically redirected by the platform to the deputy manager acting through Dr. Renato Marro – BDO Advisory Services S.r.l. Should the reporting person deem that the channel manager is in a situation giving rise to a conflict of interest, he may submit the report to the deputy channel manager through the platform. Should the deputy channel manager also be affected by a conflict of interest, the reporting person may submit the report to ANAC (National Anti-Corruption Authority) through the external channel. In all cases, the channel manager who is in a conflict of interest situation shall refrain from performing his duties and from making any decisions in order to ensure compliance with the principle of impartiality.

The conflict of interest situation must not be disclosed to the governing body.

8.2 Internal reporting channel characteristics

The Company's internal reporting channel is managed through a web-based "Whistleblowing" platform, which can be used by all devices (PCs, tablets, smartphones).

The data entered into the platform are segregated within a logical partition dedicated to the Company and are processed using a dedicated scripting algorithm before being stored. Secure communication protocols are used to ensure the security of data transmission.

Upon submission of a report (whether or not anonymous) the platform generates and provides a unique 12-character alphanumeric code, automatically and randomly generated by the IT system and not reproducible. This code enables the reporting person to monitor the progress of the report at any time and to communicate with the channel manager through a dedicated messaging tool.

In the case of a non-anonymous report the reporting person's details ("user data") cannot be accessed by the channel manager. The channel manager may, at his discretion, access such fields (the "clear-text fields") only where deemed necessary and subject to the recording of an appropriate justification within the platform, ensuring full traceability of the access.

The report may be accessed and managed solely by the channel manager. The manager is provided with unique access credentials which expire every three months. The password policy complies with international best practices.

Data Retention is governed by predefined retention periods with automatic reminders to the channel manager who shall delete the data upon expiry of the applicable retention period.

The Company BDO, which provides the platform services, is certified in accordance with ISO 27001.

Personal data processing must always consider and comply with the obligations set out in the GDPR and Legislative Decree 196/2003 as subsequently amended and supplemented. The Company, as data controller of the internal reporting channel, shall carry out a preliminary assessment of the organisational framework including a data protection impact assessment (pursuant to art. 35 of the GDPR).

8.3 Characteristics of reports and anonymous reports

Reports should be as detailed as possible in order to enable the persons responsible for receiving and handling reports to properly assess the reported facts. In particular, the following information should be clearly identified:

- the time, place and circumstances in which the reported conduct or incident occurred;
- the description of the reported facts;
- the identity of the person concerned, or other information enabling the individual to whom the reported facts are attributed to be identified.

Information relating to reported breaches must be truthful. Mere assumptions, unsubstantiated rumours (so-called “hearsay” or “office gossip”), information which is already in the public domain, inaccurate information (except when arising from a genuine mistake), information which is manifestly unfounded or misleading or information which is submitted solely to cause harm or offence, shall not be regarded as such. The reporting person is not required, however, to be certain that the reported facts have actually occurred, nor of the identity of the person responsible for them.

The reporting person should also provide any documentation that may substantiate the reported facts, together with the details of any other persons who may potentially have knowledge of the matters reported.

Anonymous reports that are sufficiently detailed shall be treated as ordinary reports and shall therefore be handled in accordance with this Procedure, including in relation to the protections available to the reporting person, if subsequently identified, and the applicable data and record retention obligations.

8.4 Process for handling reports

The reporting person submits the report through the dedicated internal channel.

The reporting person submits a report via the above-mentioned link, either in writing by completing a guided online form or orally through a voice messaging system. Where a face-to-face meeting is requested, the channel manager shall ensure that the meeting is held within a reasonable period of time (10–15 days), preferably at premises other than those of the Company.

Where the reporting person submits a report orally during a meeting arranged with the channel manager, the report, prior to the reporting person’s consent, shall be documented by the channel manager either via the recording on a device suitable for storage and playback of audio recordings or through the preparation of minutes of the meeting. In the latter case, the reporting person may review, amend and/or confirm the minutes of the meeting by signing them.

The report-handling process begins upon receipt of the report by the channel manager. The channel manager then processes the report in accordance with a predefined workflow.

Upon receipt of the report, the channel manager shall acknowledge receipt to the reporting person within seven days of receiving the report and confirm that the report has been accepted for handling.

The acknowledgement does not imply any assessment by the channel manager of the matters reported. Its purpose is solely to inform the reporting person that the report has been received and accepted for handling.

The channel manager handling the report first verifies whether the reporting person has correctly followed the procedure and the content of the report, both with reference to the scope of application defined in this procedure (the so-called consistency of the content of the report) and to its verifiability on the basis of the information provided.

In particular, a report shall be deemed admissible where:

a) it is submitted by one of the persons entitled to make a report;

b) the matters reported fall within the scope of Legislative Decree no. 24/2023;

c) it is based on sufficiently precise facts;

d) it contains a description of the matters reported and, where applicable, an indication of how those facts came to the reporting person's knowledge;

e) it contains the identity of the person concerned, or other information enabling the individual involved in the report to be identified.

Where the report is found not to fall within the scope of this procedure, the channel manager shall formally record the outcome of the assessment, notify the reporting person within a reasonable timeframe (and in any event no later than three months) and close the report.

In any event, the manager may forward the report to the competent person or department within the Company, that, where appropriate, shall handle it as an ordinary report, while simultaneously informing the reporting person. The Company may nevertheless decide, in order to afford greater protection to the reporting person, to maintain the confidentiality of their identity even where the report does not qualify as a whistleblowing report.

The channel manager shall promptly inform the internal contact person, while ensuring compliance with the principle of confidentiality. The internal contact person shall in turn share the relevant information with the Company.

Where it is necessary to obtain additional information, the channel manager shall contact the reporting person via the platform.

In particular, the channel manager may request clarifications, documents and further information from the reporting person, either through the dedicated channel, or in person. Where necessary, he may obtain records and documents from other Company departments, seek their assistance, involve third parties in interviews and other requests, while always ensuring that the confidentiality of both the reporting person and the person concerned is not compromised.

Should the reporting person fail to provide additional information within three months of the request for further information, the channel manager shall close the report, notify the reporting person accordingly, and inform the internal contact person.

Once the channel manager has verified that the report falls within the scope of this procedure and has gathered all relevant information, he shall, in compliance with the principle of confidentiality, inform the internal contact person in order to determine how the investigation phase should be initiated.

The investigation activities may be carried out, always in compliance with the principle of confidentiality, with the involvement of other internal functions of the Company or, where deemed necessary, specialised external parties taking into consideration the specific technical and professional expertise required for the case. These parties must be autonomous, appropriately trained, formally appointed and authorised to process personal data.

Upon completion of the investigation the internal contact person shall share the outcome with the channel manager so that he may provide feedback to the reporting person. Feedback to the reporting person must be provided within three months of the acknowledgement of receipt, or rather within three months calculated from the expiry of the seven-day period following the submission of the report. Only in exceptional circumstances, should the complexity of the report require this, or in consideration of the time taken by the reporting person to respond, may the channel manager, having informed the reporting person before the expiry of the relevant deadline and provided appropriate reasons, continue the investigation phase for the time necessary while providing periodical updates to the reporting person.

The internal contact person shall, on a case-by-case basis, assess with the Company whether, and if so which, Company function should be appropriately involved in the relevant review and in any consequent measures, always in compliance with the principle of confidentiality.

In the event of defamation or malicious false reporting, established by a criminal conviction, including at first instance, the Company shall act in accordance with its disciplinary and sanctions framework against the reporting person.

It is specified that from the receipt of a report until its closure, any person who finds themselves in a conflict of interest situation must refrain from taking decisions in order to ensure compliance with the principle of impartiality.

Reporting persons shall be informed (e.g. through the platform or other means) that a report may be forwarded to the Judicial Authorities.

8.5 Reports submitted to the wrong recipient

Where a report is submitted to a subject other than the one designated to receive it, the recipient shall be required to forward it to the competent person within seven days and to inform the reporting person that the report has been forwarded, while ensuring a custody chain of the information in compliance with confidentiality requirements and the provisions set out in Section 8.2. The Company shall apply disciplinary measures in the event of non-compliance with the obligation forward the report.

In all cases, the confidentiality of the reporting person and the protection of their personal data shall be ensured.

In the event that a report is inadvertently submitted to a person other than the one authorised to receive it, the reporting person must demonstrate that the misdirection was due solely to negligence and that they had no personal interest in the erroneous transmission.

8.6 Retention of documentation relating to internal reports

Internal reports, together with all related documentation, whether attached to the report or subsequently supplemented, shall be retained, subject to an appropriate digital chain of custody, for as long as necessary for the handling of the report.

In any event, the documentation shall be retained only for a period not exceeding five years from the date on which the final outcome of the reporting procedure is communicated.

Acts and documents related to proceedings initiated and actions taken by the employer (for example disciplinary proceedings, the referral of documents to the competent authorities, etc.) which arise, in whole or in part, from the report may be retained beyond the above-mentioned retention period.

In all the cases referred to above, it is necessary that the retention procedure of internal reports and related documents comply with applicable European Union and national requirements on the processing of personal data as well as the measures provided for to safeguard confidentiality.

8.7 Information and training obligations

Information regarding the reporting channel, the applicable procedures and the conditions for submitting reports is made available in the workplace through Company noticeboards and on the Company's intranet. In addition, such information is published in the dedicated section of the Company's website.
The Company has established its internal reporting channel having consulted the employees' representatives or the trade unions organisations.

8.8. Sharing of the reporting platform within the Group

It should be noted that the Company shares its reporting platform with the other companies within its Group, the platform being structured into as many dedicated sub-channels as there are Group companies. Each sub-channel has its channel manager.
Any person who wishes to submit a report shall access the platform from a single link and then, from the home page, select the relevant Group company to which they belong and/or to which the report is addressed.
Each Group company shall nevertheless remain responsible for maintaining communications with the reporting person and for providing information on the progress of the procedure.

9. External report

Where any of the following conditions apply, the reporting person may submit a report to the National Anti-Corruption Authority (ANAC) through the external channel:

- where, within the relevant work-related context, the establishment of an internal reporting channel is not mandatory, or where such channel has not been established, or does not comply with the legally prescribed requirements;
- where the reporting person has already submitted an internal report but no follow-up has been provided;
- where the reporting person has reasonable grounds to believe that, if an internal report were submitted, it would not be effectively followed up, or that the submission of the report would expose them to retaliation;
- where the reporting person has reasonable grounds to believe that the reported breach may constitute an imminent or manifest danger to the public interest.

The National Anti-Corruption Authority (ANAC) is the external body authorised to receive external reports in accordance with the procedures and arrangements it has established for that purpose (www.anticorruzione.it).

10. Public disclosure

As a measure of last resort and subject to the conditions set out below, the reporting person may make a public disclosure in the following circumstances:

- where they have previously submitted an internal report or an external one, or has directly submitted an external report without feedback within the prescribed time limits;
- where they have reasonable grounds to believe that the breach constitutes an imminent or manifest danger to the public interest;
- where they have reasonable grounds to believe that submitting an external report would expose them to a risk of retaliation, or that the report may not be effectively followed up due to the specific circumstances of the concrete case, such as those in which proof may be concealed or destroyed or where there are reasonable grounds to believe that the person receiving the report may be colluding with the perpetrator of the breach or may be involved in the breach itself.

11. Duty of confidentiality

All reports and related attachments shall not be used for longer than is necessary to follow up on the report.
The identity of the reporting person along with any other information from which that identity may be directly or indirectly inferred, shall not be disclosed without the reporting person's express consent to any persons other than those competent to receive or follow up reports and expressly authorised to process such data pursuant to articles 29 and 32(4) of Regulation (EU) 2016/679 and art. 2-quaterdecies of Legislative Decree no. 196 of 30 June 2003, the Italian Personal Data Protection Code.
The Company shall protect the identity of the persons concerned, facilitators and persons mentioned in the report until the conclusion of any proceedings initiated as a result of the report, in accordance with the same safeguards afforded to the reporting person.

Circumstances in which the protection of the right to confidentiality may be limited include the following:

- in the context of criminal proceedings, the identity of the reporting person is protected by investigative secrecy in the manner and within the limits provided for by Article 329 of the Italian Code of Criminal Procedure. The confidentiality of the preliminary investigation records must be maintained until such time as the suspect acquires the right to be informed thereof and, in any event, no later than the conclusion of the preliminary investigation phase;
- in the context of the proceeding before the Court of Auditors, the identity of the reporting person may not be disclosed until the conclusion of the preliminary phase;

- in the context of the disciplinary proceedings, 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 itself, even where such findings arise as a result of the report;
- where the disciplinary charge is based, in whole or in part, on the report and knowledge of the reporting person's identity is indispensable for the defence of the person concerned, the report may be used for the purposes of the disciplinary proceedings only where the reporting person has expressly consented to the disclosure of their identity;
- in the event that disciplinary proceedings are initiated against an alleged perpetrator of the reported conduct, the reporting person shall be notified in writing of the reasons for the disclosure of the confidential information where such disclosure is indispensable including for the purposes of defence of the person concerned.

Without prejudice to the limitations on confidentiality set out above, the person concerned shall, upon request, be given the opportunity to be heard, including through a written procedure involving the submission of written observations and supporting documents.

The obligations of confidentiality include:

- the exemption of the report and any attached documentation from the right of access of administrative documents under articles 22 et seq. and law no. 241/1990 and from the right of general civic access under articles 5 et seq. of Legislative Decree no. 33/2013;
- the authorities and entities involved in the handling of reports shall ensure confidentiality during all stages of the report process, including any transfer of reports to other competent authorities.

12. Personal data protection

All personal data processing, including the exchange of information between competent authorities, shall be carried out in compliance with:

- Regulation (EU) 2016/679;
- Legislative Decree no. 196 of 30 June 2003, as subsequently amended and supplemented.

The disclosure of personal data by institutions, bodies, offices and agencies of the European Union shall be carried out in accordance with Regulation (EU) 2018/1725.

Personal data processing relating to receipt and handling of reports shall be carried out by the data controller in compliance with the principles set out in articles 5 and 25 of Regulation (EU) 2016/679, by providing appropriate information in advance to reporting persons and to persons concerned, and by adopting appropriate measures to safeguard the rights and freedoms of data subjects.

The privacy notice for data subjects, which also provides a summary of their rights and the procedures for exercising them, is available at the following address: https://www.metalplasma.it/en/reporting/.

13. Protection and support measures

Appropriate measures are in place to protect Reporting Persons, as well as the other individuals identified under Legislative Decree 24/2023, from both direct and indirect retaliation.

Protection measures shall apply where, at the time of making the report, the reporting person had reasonable grounds to believe that the information on the breaches reported was true (see section 8.3), that it fell within the material scope of legislation and that the reporting process has been complied with.

In the event of defamation or malicious false reporting, established by a civil or criminal judgment, including a judgment at first instance, the protections shall not apply.
Protection measures shall also apply to:

a) facilitators;

b) persons within the same work-related context as the reporting person and/or complainant who are connected to them through a stable emotional relationship or are related to them up to the fourth degree of kinship;

c) work colleagues of the reporting person/complainant who work in the same context and have with said person an ongoing and regular relationship;

d) legal entities owned by the reporting person/complainant or for which people work, as well as entities operating the same work-related context as those persons.

13.1 Prohibition of retaliation and obstruction of reporting

Obstructing (or attempting to obstruct) a person who intends to make a report is prohibited.

Furthermore, the persons identified in Section 5 shall not be subjected to any form of retaliation. By way of illustration and without limitation, the following shall be considered “retaliation”:

- dismissal, suspension or equivalent measures;
- demotion or failure to promote;
- a change in duties;
- a change in place of work;
- a reduction in salary;
- a change in working hours;
- the suspension of training or any restriction on access to training;

- negative performance assessments or negative references that are not adequately justified;
- the imposition of disciplinary measures or other sanctions (including financial penalties);
- coercion;
- intimidation;
- harassment;
- ostracism;
- discrimination or any other unjustified unfavourable treatment;
- the failure to convert a fixed-term employment contract into a permanent employment contract where the employee had a legitimate expectation that such conversion would take place;
- the non-renewal or early termination of a fixed-term employment contract;
- harm suffered by the person, including damage to their reputation, particularly through social media;
- economic or financial detriment, including loss of economic opportunities and loss of income;
- inclusion on improper lists based on a formal or informal sectoral or industry-wide agreement, which may result in the person being unable to secure employment in the sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the revocation of a licence or permit;
- requiring the person to undergo psychiatric or medical examinations.

Any acts taken in breach of the prohibition of retaliation shall be null and void.

In judicial or administrative proceedings, as well as in out-of-court disputes concerning the determination of prohibited conduct, acts or omissions against Reporting Persons, it shall be presumed that such conduct, acts or omissions were carried out as a consequence of the report. The burden of proving that such conduct or acts were motivated by reasons unrelated to the report shall rest with the person who carried out the retaliatory acts.

Reporting persons may advice the National Anti-Corruption Authority (ANAC) any retaliatory measures that they believe they have suffered, including attempted or threatened retaliation.

The National Anti-Corruption Authority (ANAC) shall inform the National Labour Inspectorate (Ispettorato Nazionale del Lavoro) for the purposes of any measures falling within its competence.

13.2 Support measures

The reporting person may also seek assistance from Third-Sector organisations included in the list published in the National Anti-Corruption Authority (ANAC) website. These organisations carry out activities of general interest, on a non-profit basis, pursuing civic, solidarity and social welfare objectives ("*the promotion of a culture of legality, peace among peoples, non-violence and non-armed defence; the promotion and protection of human, civil, social and political rights, as well as consumers' rights and those of the users of activities of general interest, the promotion of equal opportunities and of initiatives of mutual support initiatives, including time banks and collective purchasing groups),* which have entered into agreements with the National Anti-Corruption Authority (ANAC).

The support measures provided consist of free-of-change information, assistance and advice on reporting procedures and on the protection against retaliation afforded by the national and European Union legislation, on the rights of the person concerned, and on the procedures and conditions for accessing legal aid at the State's expense.

13.3 Limitation of the reporting person's liability

No liability (including civil or administrative liability) shall arise for any person who discloses or disseminates information concerning breaches where:

- the information disclosed is covered by confidentiality obligations,
- the information disclosed is protected by copyright,
- covered by personal data protection legislation;
- which adversely affect the reputation of the person concerned,

provided that, at the time of the disclosure or dissemination, there were reasonable grounds to believe that such disclosure or dissemination of the information was necessary to reveal the breach and that the report had been made in accordance with the conditions for protection.

In addition, the following protective measures shall apply:

- the rights to make a report and the related protections may not be limited or waived by any contractual provision;
- the exclusion of any other form of liability, including civil and administrative, arising from the acquisition of or access to information concerning breaches, except where the conduct constitutes a criminal offence;
- the exclusion of any other form of liability in respect of conduct, acts or omissions carried out provided that they are connected with the report and strictly necessary to reveal the breach.

14. Sanctions framework

The disciplinary system adopted by the Company provides for sanctions to be imposed – in accordance with the principles of proportionality and graduality – on those whom the Company determines to be responsible for misconduct relating to:

- the commission of retaliatory acts or the proposal to adopt such acts, the obstruction or attempted obstruction of reporting, or breaches of confidentiality obligations;
- the failure to establish reporting channels, the failure to adopt procedures for the handling of reports, the adoption of procedures which do not comply with the requirements of the decree, or the failure to carry out activities for the assessment and investigation of reports;
- civil or criminal liability of the reporting person, established by a judgment, including a judgment at first instance, for defamation or malicious false reporting committed with intent or gross negligence; as well as any breach of this procedure by any person.

For the same infringements, the National Anti-Corruption Authority (ANAC) may impose administrative pecuniary sanctions ranging from Euro 500 to Euro 50.000 where such infringements are established.

Appendices

Legislative Decree no. 24 of 10 March 2023