# WHISTLEBLOWING: ORGANISATIONAL ACT FOR THE MANAGEMENT OF REPORTS

| ISSUE/REVISION | | |
|---|---|---|
| DATE | MODIFICATION INDEX | TYPE OF MODIFICATION |
| 14/12/2023 | 00 | First issue |
| | | |
| | | |

| Drafted by | Approved by |
|---|---|
| Signature<br>  <br>Elisa Scilhanick | Signature<br>See Resolution act for approval of the Organisational Act for the "Whistleblowing" of any company to which this document is applicable |

## 1. PURPOSE

The purpose of this Organisational Act is to regulate within the Marcegaglia Steel S.p.a. Organisation, which includes the following companies:

- Marcegaglia Carbon Steel S.p.A.
- Marcegaglia Specialties S.p.A.
- Marcegaglia Ravenna S.p.A.
- Marcegaglia Gazoldo Inox S.p.A.
- Marcegaglia Buildtech S.r.l.
- Marcegaglia Plates S.p.A.
- Marcegaglia Palini e Bertoli S.p.A.
- Trafital S.p.A.

the "whistleblowing" procedure, understood as a reporting or whistleblowing system regulated by the **European Directive of 23 October 2019 no. 193.**

The system provides for the reporting of alleged violations or threats to rights enshrined in the European Union, implemented by workers ("whistleblowers") who provide the Organisational Bodies responsible for supervision, or the external Supervisory Authorities, with detailed information on true (or well-foundedly real) facts, of which they have become aware during their employment relationship, useful for activating an investigation. This procedure is accompanied by whistleblower protection measures.

In implementation of Directive (EU) 2019/1937, **Legislative Decree no. 24 dated 10 March 2023** concerning the protection of persons who report breaches of Union law and national regulations was issued.

The provisions do not concern disputes, claims or requests related to a personal interest of the whistleblower or the person who filed a complaint with the judicial or accounting authority, nor reports already regulated by European Union or national acts.

## 2. DEFINITIONS

***"Reports"***: are defined as information, including well-founded suspicions, on violations already committed or not yet committed (but which, on the basis of concrete elements, could be), as well as on conduct aimed at concealing them (e.g. concealment or destruction of evidence).

These must then be behaviours, acts or omissions of which the whistleblower or the complainant has become aware in the public or private work context.

In the context of public and private entities, reports can be made by:

Salaried employees and self-employed persons
collaborators, freelancers, consultants
volunteers/trainees
shareholders and persons with management, administration and control functions.

Important to mention is the existence of a qualified relationship between the whistleblower and the public or private entity in which the first works, a relationship that concerns present or even past work or professional activities.

***"Internal reporting"***: the communication, written or oral, of information on violations, submitted through the internal reporting channel of the Organisation.

***"External reporting"***: the communication, written or oral, of information on violations, submitted through external reporting channels (platform, voice messaging, dedicated telephone lines) to the National Anti-Corruption Authority (ANAC).

***"Violations":*** conduct, acts or omissions that harm the public interest or the integrity of the public administration or private body and that consist of:

- administrative, accounting, civil or criminal offences;
- unlawful conduct, relevant pursuant to Italian Legislative Decree no. no. 231 of 8 June 2001, or violations of the Organisation and Management Models;
- offences falling within the scope of the European Union or national acts indicated in the annex to Legislative Decree March 10, 2023, no.24 or that constitute implementation of the acts of the European Union indicated in the annex to Directive (EU) 2019/1937, relating to 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; privacy protection and protection of personal data and security of networks and information systems;
- actions or omissions that affect the financial interests of the European Union;
- acts or omissions concerning the internal market in particular infringements of competition or tax rules.

***"Whistleblower":*** the natural person who makes the report or public disclosure of information on violations acquired within their work context.

***"Facilitator":*** a natural person who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential.

***"Person involved"***: the natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the violation is attributed or as the person in any case involved in the violation reported or publicly disclosed.

***"Retaliation":*** any behaviour, act or omission, even if only attempted or threatened, carried out by reason of the report, the complaint to the judicial or accounting authority or public disclosure and that causes or may cause the reporting person or the person who filed the complaint, directly or indirectly, unfair damage, to be understood as unjustified damage.

## 3. APPLICABILITY

The decree entered into force on 30 March 2023 and the provisions are effective from 15 July 2023.

- The decree applies to subjects in the public and private sectors. With particular reference to the latter sector, the legislation extends the protections to reporting Organisations that have employed, in the last year, an average of at least fifty employees or, even under this limit, to the Bodies that deal with the so-called "Sensitive sectors" (services, products and financial markets and prevention of money laundering or terrorist financing, transport security and environmental

protection) and those that adopt Organisation and Management Models pursuant to Legislative Decree 231/2001.

- Only for private sector entities that have employed, in the last year, an average of employees, with permanent or fixed-term employment contracts, up to two hundred and forty-nine, it is mandatory to establish an internal reporting channel starting from 17 December 2023.

***Within the company***

The protection of whistleblowers operating in the private sector, provided for by Legislative Decree 24/2023, imposes the obligation to prepare reporting channels for those Entities that meet at least one of the following conditions:

- have employed, in the last year, an average of at least fifty employees, with permanent or fixed-term employment contracts;
- deal with some specific sectors (services, products and financial markets and prevention of money laundering or terrorist financing, transport security and environmental protection), even if in the last year they have not reached the average of at least fifty employees with permanent or fixed-term employment contracts;
- adopt the Organisation and Management Models referred to in Legislative Decree 231/2001, even if in the last year they have not reached the average of at least fifty employees with permanent or fixed-term employment contracts.

***What can be reported***

Behaviours, acts or omissions that harm the public interest or the integrity of the public administration or private body and that consist of:

- administrative, accounting, civil or criminal offences;
- relevant unlawful conduct pursuant to D.Lgs.231/2001, or violations of the Organisation and Management Models provided for therein;
- offences falling within the scope of Union or national acts relating to the following areas: public procurement; financial services, products and markets and the 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 protection of personal data and security of networks and information systems;
- actions or omissions that affect the financial interests of the European Union;
- actions or omissions that affect the internal market;

- acts or conduct which undermine the object or purpose of the provisions of Union acts.

***Use of the instrument in Groups of Companies***

It should be noted that the reporting management tool **can be shared within the Groups of Companies**. Although there is no clear and specific definition of the concept of Group of Companies in the national legal system, the discipline introduced by Legislative Decree 24/2023, of European inspiration, formulates an express openness to the possible preparation of Internal Reporting Channels shared between subjects of the private sector who have employed, in the last year, an average of employees, with permanent or fixed-term employment contracts, not exceeding two hundred and forty-nine. It is also the right of these subjects to share the management aspects of the channel.
The sector legislation does not provide specific information on the concrete methods of sharing the Channels. However, the ANAC Guidelines and the Operational Guide of Confindustria have provided important operational indications regarding the obligations that, necessarily, must be put in place in order to guarantee a legitimate and functional **sharing of Internal Reporting Channels** within the **Groups of Companies**. They highlight, in particular, that:
- each entity belonging to the Group and involved in the sharing must be provided with **exclusive and autonomous access** to the reports under their responsibility, i.e. those relating to violations that have taken place within their organization or that are related to it;
- the Companies of the Group will inevitably have to stipulate an **agreement between the participating entities**, which clearly and precisely define the terms of the shared management of the reporting instrument. It is desirable that this organisational step be implemented through the preparation of a **Service Contract**, or through an action of integration and completion of Service Contracts already in place in the context of the Group of Companies. Through the aforementioned contract, the Companies must clearly and unequivocally regulate:

  - the **operating methods of** the shared reporting channel (how the written and oral reporting procedures will be structured; how access to the electronic reporting collection tools will be managed; how the phases of the reporting management process will be structured, how the composition of any Investigation Team will be determined, etc.);

- the **purposes and means of the processing of personal data** (strictly limited to the need to manage information and investigate the reported facts);
- the technical and organisational measures adopted so that the channel **guarantees confidentiality in the context of reporting**;
- the technical and organisational measures adopted so that the reporting channel **guarantees each entity access only to reports concerning them**;
- the **recipient of the reports** and the related **tasks** and **powers**;
- the procedures for receiving reports;
- the reporting management process;
- the provision and determination of **costs** as well as the methods of **reporting** them, in accordance with the operating practices of the application of the Service Contracts in force at the Group.

- In any case, each individual entity will have the task of:

- provide its employees with **adequate training** on whistleblowing legislation and the concept of "reporting" (including through concrete examples), on the correct use of the channel and on sanctions in the event of violations. Nothing prohibits, however, that instruments provided by the Group may be used for this purpose;
- **inform** (also through the website) of the existence of the channel;
- properly **keep** the documentation relating to the report;

- the **confidentiality** of reports must always be protected;
- in any case, each company must comply with the **information** (publication on the website, sharing of a circular, posting on the company notice board, etc.) and **training** obligations towards its staff.

## 4. REFERENCES

**Directive (EU) 2019/1937** of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law.

**Italian Legislative Decree no.24 of 10 March 2023** – Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law and laying down provisions concerning the protection of persons reporting breaches of national legal provisions.

**Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 _General Data Protection Regulation updated to the corrections published in the OJEU no. 127 of 23 May 2018.

**Confindustria _ New "Whistleblowing" discipline Operational guide for private bodies**_October 2023

**ANAC National Anti-Corruption Authority_ Regulation for the management of external reports and for the exercise of the sanctioning power of ANAC in implementation of Legislative Decree 10 March 2023, no. 24** _ Resolution no. 301 of 12 July 2023

## 5. RESPONSIBILITY

| | |
|---|---|
| The Management | Having heard the Representatives or Trade Unions referred to in art. 51 of Legislative Decree 81/2015 is responsible for activating its own reporting channels that guarantee, also through the use of encryption tools, the confidentiality of the reporting person, the person involved and the person in any case mentioned in the report as well as the content of the report and the related documentation. The Company Management shall ensure adequate information and training about the contents of **Legislative Decree no. 24 of 10 March 2023 and** the dissemination of this Organisational Act. |
| Report Handler | Appropriately trained person or autonomous internal office in charge and with personnel specifically trained for the management of the reporting channel or autonomous external subject and equipped with personnel specifically appointed for the purpose. Provides for the management of reports. |
| Consultant | -- |
| RL | -- |
| RA/RL | It provides adequate information about the contents of this Organisational Act to its collaborators. |

## 6. OPERATING PROCEDURES

### 6.1 Assumptions for internal reporting and related eligibility conditions

In the context of public and private entities, reports can be made by:

- Salaried employees and self-employed persons
- collaborators, freelancers, consultants
- volunteers/trainees
- shareholders and persons with management, administration and control functions.

It is important to note that the reporting of such offences or violations must take place in good faith and in accordance with established procedures. In addition, in the context of Legislative Decree 231/01, the reporting of a crime may be relevant to the Organisation in the context of the administrative liability of legal persons and companies. In this case, the reporting of internal violations could be essential to demonstrate that the Organisation has taken adequate measures to prevent and counter such behaviour, avoiding potential legal liability. **In this case, it is also essential that the report is shared with the Supervisory Body and that said body is involved and made aware of each subsequent phase of investigation and analysis of the report**.

The reports must be as detailed as possible, to allow the evaluation of the facts by the parties responsible for receiving and managing the reports.

The following essential elements of the report must be clear, also for the purposes of the admissibility careful inspection:

- the **identification data** of the reporting person (name, surname, place and date of birth), as well as an address to communicate subsequent updates;
- the **circumstances of the time and place** in which the fact subject to the report occurred and, therefore, a description of the facts subject to the report, specifying the details relating to the circumstantial news and where present also the methods by which the facts subject to the report were known;
- the **general information** or other elements that allow to identify the subject to attribute the reported facts.

It is useful that **documents are attached** to the report that can provide elements of substantiation of the facts subject to reporting, as well as the indication of other persons potentially aware of the facts.
**In accordance with the provisions of the Confindustria Guidelines (October 2023, p. 17), the anonymous report must have an accurate content, detailed and supported by suitable documentation, so that it is considered as an ordinary and valid report.**

The Organisation has appointed a "Whistleblowing Manager" at the company's registered office, located in via Bresciani no. 16, 46040, Gazoldo degli Ippoliti, reachable by written communication sent on an online platform * to which reports can be sent relating to information, including well-founded suspicions, on violations already committed or not yet committed (but which, on the basis of concrete elements, could be), as well as on conduct aimed at concealing them.

*(*) ANAC, transposing the opinion of the Privacy Guarantor, points out that, for the purposes of establishing the internal reporting channel, "Ordinary email and PEC are considered to be inadequate tools to guarantee confidentiality".*

The Organisation has **prepared both the written channel - analogue and/or IT - and the oral one**, having to make both available to the whistleblower.

Among the topics that may be **the subject of reports** are indicated by way of example and not exhaustive:

**Financial fraud:** Any fraudulent activity involving the company, e.g. falsification of documents, misappropriation of funds, manipulation of financial statements, etc.
**Bribery:** Illegal offers, payments, gifts, or other practices to obtain improper benefits or favors.
**Violations of occupational health and safety regulations:** Failure to comply with occupational health and safety regulations, exposure to inadequately managed risks, lack of training or adequate equipment.
**Violence in the workplace:** Inappropriate behaviour, harassment, discrimination, or abuse in the workplace.
**Privacy violation and improper handling of data:** Unauthorised access to personal data, failure to protect sensitive information, or any other violation of data protection legislation.

**Environmental violations:** Company activities that cause damage to the environment, non-compliance with environmental regulations, pollution, improper disposal of waste, etc.
**Tax evasion:** Unlawful practices aimed at avoiding the payment of taxes or evading tax laws.
**Human rights violations:** Involvement of the company in activities that violate human rights, such as child labour, human trafficking, exploitation, etc.

### 6.2 Procedures that can be operated by the Organisation for the use of the internal/external reporting channel

For **PRIVATE SECTOR ENTITIES** that

**1) did not reach the average of 50 workers on an annual basis and adopted the MOG 231**.
Reports may concern illegal conduct or violation of model 231 and be made through the internal channel.

**2) employed an average of at least 50 workers and adopted MOG 231.**
Reports can:

- have as their object unlawful conduct or violation of model 231 and be carried out only through an internal channel;
- relate to violations of EU law and be carried out through internal or external channels, public disclosure or denunciation

**3) have employed an average of at least 50 workers and do not have Model 231 or fall within the scope of the Union acts referred to in Parts I.B and II of the Annex** (financial services, products and markets, prevention of money laundering, terrorist financing, transport safety and environmental protection) even if **they have not reached the average of 50 employees** .

Reports may relate to violations of EU law and be made through internal, external, public disclosure or complaint channels.

### 6.3 Procedure for handling the report

Internal reports are made as rule of practice through a **computer platform** suitably configured for reasons of confidentiality and security of the identity of the whistleblower and the contents of the communication.

The **choice between the online platform and the analogue/paper mode** is an **assessment left to the individual company**, according to different considerations attributable to the context, to the company size (see paragraph 6.2), the functionality with respect to the purpose and the level of security and confidentiality guaranteed by the solutions adopted.

Having chosen to use an **IT platform**, although the Decree and the ANAC LGs do not identify any particular obligations to be carried out during the reception phase, the Company Management has provided for the adequate configuration of this platform for reasons of confidentiality and security of the data transmitted and to guarantee adequate training to the subject/office entrusted with the management of reports.

***Reports received via "anomalous" channels***

Any report received **through different channels than the Internal Channel setup pursuant to art. 4 of Legislative Decree no. 24/2023** will be processed on the merits and the Company will recognise, in any case, the protections provided by the Decree in favour of the author of the report, both as regards respect for the rights to privacy and confidentiality, and as regards the prohibitions of discrimination and retaliatory actions against him. In any case, if reports formalised through unregulated channels are **received by subjects other than the person in charge of the internal channel**, they are required to share the content with the same Manager within seven days and, subsequently, to delete without delay any sensitive data collected through the unconventional channel and remaining in their availability. It will be the responsibility of the Head of the internal channel to ensure that the data transited is then stored in accordance with the provisions of Legislative Decree 24/2023, Legislative Decree 193/2003 and the GDPR.

### 6.4 Person entrusted with the management of reports, powers and obligations

The **management of the report**: it is entrusted to a group of dedicated trained personnel. In particular, the management of the report is entrusted to:

- group legal department (Corporate General Counsel);
- group Human Resource department (HR Manager);

- individuals internal to the individual companies (ref. resolution appointing the manager of the reports of each individual company).

Please note that, if one of the subjects responsible for the management/related to the Group identified above who is called upon to manage the report were to detect a **conflict of interest of** their own, as they appear to be involved in any way by the subject of the report (reported subject, manager of an office involved in the reported conduct, in close relationship with the reporting person, etc.), the same has the obligation to refrain from taking part in the activities of evaluating the report itself and in the entire process referred to in this procedure.

***The activities that the person managing the reports is required to carry out***

**Who handles reports:**

1. issue to the whistleblower a **notice of receipt** of the report within seven days from the date of receipt only to inform him/her of the correct **receipt.; the Notice of** Receipt: certifies correct receipt, not the execution of investigative activities on the merits.
2. ensures **correct follow-up** to the reports received: prosecutability, admissibility of the report and investigation; this implies an assessment:
   - compliance with the **objective/subjective assumptions (prosecutability)**
   - existence of the essential requirements **(admissibility)**
   - **adequate investigation** (request for information, access to documents, etc.) to assess the substantiation of the reported facts (*fumus of substantiation,* probable existence of the reported unlawful act).

   If what has been reported is not adequately substantiated, the manager may request additional elements from the whistleblower through the channel dedicated to this, or even in person, where the whistleblower has requested a direct meeting.
3. provides **feedback** to the whistleblower.
4. It proceeds to the drafting of a **final report**, which is transmitted to the administrative body so that it can make any necessary determination. The report must contain:
   - a summary description of the reported facts;
   - an indication of the documentation collected and examined with reference to the report;
   - a summary of the investigation activities carried out and the respective findings
   - any additional documentary annexes;

- the conclusions drawn by the person in charge with regard to the admissibility or not of the report and the inherent responsibility profiles.

***Receipt of the report***

The manager issues the **notification of receipt** to the whistleblower by forwarding it to the address indicated by the whistleblower in the report. In the absence of this indication, it is possible to consider the report as unmanageable pursuant to the whistleblowing regulation (leaving a trace of this reason) and possibly treat it as an ordinary report.
In the event of receipt of **anonymous reports,** also in the light of the indications of the ANAC, the same, if they are accurate, detailed and supported by suitable documentation, can be equated by the company with ordinary reports and can be treated in accordance with internal regulations, where possibly implemented.
In any case, **anonymous reports** are **recorded** by the reporting manager and the documentation received is **kept**. In fact, the Decree provides that where the anonymous whistleblower is subsequently identified and has suffered retaliation, the same must be guaranteed the protections provided for the whistleblower.

***Reporting processability***

In order to proceed with the procedure, the reporting manager, first of all, verifies the existence of the objective and subjective conditions: i) that the whistleblower is a **person entitled** to make the report and ii) that **the subject of the report falls within the scope of** the regulation.
In the event that the report concerns a **matter excluded** from the objective scope of application, it may be **treated as ordinary** and, therefore, managed according to any procedures already previously adopted by the institution for such violations by notifying the reporting party.
***Admissibility of the report***

Once the prosecutability has been verified, **the admissibility as a whistleblowing report is evaluated.**
In this regard, it must be clear:

- that the **circumstances of the time and place** in which the fact subject to the report occurred and, therefore, a description of the facts subject to the report, specifying the details relating to the circumstantial news and where present also the methods by which the facts subject to the report were known;

- the **general information or other elements** that allow to identify the subject to attribute the reported facts.

The report may, therefore, be **considered inadmissible** for:

- lack of the data that constitute the essential elements of the report;
- manifest unfoundedness of the factual elements attributable to the violations typified by the legislator;
- presentation of facts of general content such as not to allow them to be understood by the offices or the person in charge;
- production of only documentation without the actual reporting of violations.

In the event that the report is **inadmissible**, the manager of the report proceeds to **archive** it, guaranteeing in any case the traceability of the supporting reasons.

***Investigation and assessment of the report***

The whistleblower ensures that all **appropriate checks** are carried out on the reported facts, ensuring timeliness and compliance with the principles of objectivity, competence and professional diligence.

The objective of the assessment phase is to carry out specific checks, analyses and assessments on the **substantiation or otherwise of the reported facts**, by way of example:

- directly acquiring the information elements necessary for the evaluations through the analysis of the documentation/information received;
- through the involvement of other company structures or even external specialised subjects (e.g. IT specialists) in consideration of the specific technical and professional skills required;
- hearing of any internal/external subjects, etc.

Once the assessment activity has been completed, the manager can:

1. **file** the report because it is unfounded, justifying the reasons;
2. **declare the report well-founded** and contact the competent internal bodies/functions for the related follow-ups (e.g. company *management* , General Manager, legal department or human resources).

**The manager of the report is not responsible for any assessment regarding individual responsibilities and any subsequent measures or consequent proceedings. Therefore, at the end of the reporting evaluation process, the Manager prepares a report summarising the activities carried out, the information collected and the conclusions drawn, which he sends without delay to the administrative body for any inherent evaluation of the remedial/disciplinary actions to be taken.**

***Response to the whistleblower***

A **response** must be provided to the whistleblower within **three months** of the date of the notice of receipt or, in the absence of such notice, within three months of the expiry of the seven-day period from the submission of the report.
It should be specified that **it is not necessary to conclude the assessment activity within three months**, considering that there may be cases that require, for the purposes of the verifications, a longer time.
The **feedback** may be **final or intermediate**.

The manager of the report may communicate to the whistleblower:

- **the archiviation** of the report, justifying the reasons;
- the **verification of the validity of the report** and its transmission to the competent internal bodies;
- **the activity carried out so far and/or the activity to carry out**.

In the latter case, it is advisable to notify the reporting person of the **subsequent final outcome** of the investigation of the report (filing or verification of the validity of the report with transmission to the competent bodies), in line with the LG ANAC.

## 7. THE NECESSARY ADJUSTMENTS PRESCRIBED FOR THE PROCESSING OF PERSONAL DATA

***Protection of whistleblower confidentiality***

- The identity of the whistleblower may not be disclosed to persons other than those competent to receive or follow up on the reports.
- The protection concerns not only the name of the whistleblower, but also all the elements of the report from which the identification of the whistleblower can be derived, even indirectly.

- The protection of confidentiality is extended to the identity of the persons involved and of the persons mentioned in the report until the conclusion of the proceedings initiated on the basis of the report, in compliance with the same guarantees provided in favour of the reporting person.

***Personal Data Protection***

- The processing of personal data relating to the receipt and management of reports is carried out by public and private sector entities, as Data Controllers, in compliance with European and national principles regarding the protection of personal data, providing suitable information to persons reporting persons and to the persons involved in the reports, as well as adopting appropriate measures to protect the rights and freedoms of the interested parties.
- In addition, the rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679 may be exercised within the limits of the provisions of Article 2-undecies of Legislative Decree no. 196 of 30 June 2003.
- The internal and external reports and the related documentation are kept for the time necessary for the processing of the report and, in any case, no later than 5 years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set out in European and national legislation on the protection of personal data.

## 8. CONDITIONS FOR RESORTING TO EXTERNAL REPORTING

**Whistleblowers may use the external channel (ANAC)** when:

- within the work context, the mandatory activation of the internal reporting channel is not foreseen or this, even if mandatory, is not active or, even if activated, does not comply with what is required by law;
- The whistleblower has already made an internal report and it has not been followed up;
- the reporting person has reasonable grounds to believe that, if it made an internal report, it would not be effectively followed up or that the same report could determine the risk of retaliation;
- The whistleblower has reasons for believing that the contravention may constitute an imminent or clear threat to the public interest.

**Whistleblowers may directly make a public disclosure** (by press or electronic means or means of dissemination capable of reaching a large number of people) when:

- the whistleblower has previously made an internal and external report or has made an external report directly and no response has been given within the established deadlines regarding the measures envisaged or adopted to follow up on the reports;
- The whistleblower has reasons for believing that the contravention may constitute an imminent or clear threat to the public interest.
- the whistleblower has reasonable grounds for believing that the external report may carry the risk of retaliation, or may not have been followed up properly due to the specific circumstances of the particular case. This would include instances where evidence may have been concealed or destroyed, or when there is a well-founded fear that the person who received the report may be colluding with the perpetrator or involved in the violation itself.
- The alert shall be removed from access to administrative acts and the right of general civic access.

Reports to ANAC can be made through the services portal at the link **https://whistleblowing.anticorruzione.it**
The ANAC portal through the appropriate application issues the whistleblower a unique identification code, "key code", which must be used for communications in a depersonalized way and to be constantly informed about the processing status of the report sent.

## 9. THE PROHIBITION OF RETALIATORY ACTS

There is **a prohibition on retaliatory acts** (by "retaliation" we mean what is defined in par. 2).

Examples of retaliatory behaviour are:

- dismissal, suspension or equivalent measures;
- demotion or non-promotion;
- change of functions, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- negative notes of merit or negative references;

- adoption of disciplinary measures or other sanctions, including financial penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- failure to convert a fixed-term employment contract into a permanent 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, in particular on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income;
- listing improperly on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in the sector or industry in the future;
- early conclusion or cancellation of the contract for the supply of goods or services;
- cancellation of a license or permit;
- the request to submit to psychiatric or medical investigations.

The whistleblower may **communicate to the ANAC the retaliation** they believe they have suffered. If committed in the private context, ANAC informs the National Labour Inspectorate.

**Acts of retaliation** taken in violation of the aforementioned legislation **are null and void.**

***Competence to ascertain retaliation***

The management of retaliatory communications in the public and private sectors is the responsibility of ANAC, which may avail itself, to the extent of its respective competence, of the collaboration of the Public Service Inspectorate and the National Labour Inspectorate.
The declaration of nullity of the retaliatory acts is the responsibility of the Judicial Authority.

***Extension of protection to other parties***

The protection is also extended to the following subjects:

- **the facilitator** (natural person who assists the whistleblower in the reporting process and operates within the same work context);

- **to persons in the same working context as the reporting person**, the person who filed a complaint or the person who made a public disclosure and who are linked to them by a stable emotional bond or kinship within the fourth degree;
- to the work colleagues of the reporting person or of the person who filed a complaint or made a public disclosure, who work in the same working context as the same and who have a habitual and current relationship with said person;
- **to the Bodies owned by the reporting person** or for which the same persons work as well as to the Bodies operating in the same working context as the aforementioned persons.

***Loss of protections***

**Assumptions for protection**

Protections are granted when:

- the whistleblower, at the time of the report, had **reasonable grounds to believe** (no rumours or assumptions) that the information on the violations was true and fell within the objective scope of the legislation;
- **the discipline/procedure of use of the different channels has been respected** .

The protections **are not guaranteed** when it is ascertained, even with a judgment of first instance, the criminal liability of the reporting person for the crimes of **defamation** or **slander** or in any case for the same crimes committed with the complaint to the judicial or accounting authority or his/her civil liability, for the same title, in cases of wilful misconduct or gross negligence; in such cases the whistleblower or reporting person may be subject to a disciplinary sanction.

## 10. UPDATE OF MOG 231

As the organisation has adopted an Organizational Model based on D.Lgs.231/01, the MOG is updated a) with the indication of the **internal reporting channels** adopted by the entity; b) with reference to the **prohibition of committing any act of retaliation**; c) with respect for the **duties of confidentiality** in the processing of information regarding the management of reports; d) integrating the **disciplinary system** by providing for sanctions against those responsible for violations for which the ANAC applies administrative fines.

## 11. TRAINING AND INFORMATION

In order to ensure an informed, accurate and professional management of reports, the Organization is responsible for:

- **training costs**: the identified group entrusted **with the management** of the reporting channel receives **specific training** relating to the management of the channel and the reference legislation;
- **information costs**: the identified group entrusted with the management of the reporting channel provides the reporting person with clear information on the channel, procedures and conditions for making internal or external reports.

## 12. PROCESSING OF PERSONAL DATA

The Organization has provided that all processing of personal data is carried out in accordance with Reg. Reg. 2016/679, Legislative Decree 30 June 2003, no. 196 and Legislative Decree no. 51 of 18 May 2018.
The types of data processed are of a common nature, of a particular nature ("sensitive data") and judicial (eg criminal convictions and crimes) possibly contained in the report and in the documents connected to them.
The interested parties are the subjects to whom the personal data being reported refers (Whistleblower, Facilitator, Reported Person, people in various capacities involved in the report, e.g. any witnesses to the reported fact). All these subjects enjoy the protections and rights provided for by the regulations on the protection of personal data, albeit with differences.
In this regard, reference is made to the **General Principles of Data Protection** taken into particular consideration for the purposes of this Organisational Act (Articles 5 and 25 GDPR) in particular: **limitation of purpose**, **relevance and minimisation**; **accuracy and updating of data**; **limitation of storage** (no later than 5 years from the communication of the outcome of the procedure); **security** (guarantee against the risks of breaches of confidentiality, availability and integrity of data) on the basis of the impact assessment (DPIA) (the security measures adopted must in any case be periodically examined); **transparency** (providing for the obligation to provide full information to interested parties pursuant to Articles 13 and 14 of the GDPR in addition to the obligation to publish); data protection from design **onwards and** data protection by default of information about the channel, procedures and conditions for making internal or external reports (Articles 25 GDPR); **responsibility for processing (art.**

**24 GDPR Accountability, it is the responsibility** of the data controller to verify, guarantee and be able to demonstrate the correspondence of the implemented system, especially in terms of correctness, security, clarity of exposure, with the protection requirements imposed by the GDPR); **protection of the confidentiality of the reporting party (the confidentiality of** identity is guaranteed by pseudonymisation), **of the reported party and of the other parties involved.**

The Data Controller is responsible for receiving and managing reports.

The Organization considers the preliminary DPIA (Data Protection Impact Assessment) necessary (with reference to Articles 13.6 Legislative Decree n.24/2023 and 35 GDPR) as a precondition for the adoption of appropriate technical and organisational security measures (criteria that define high risk are the vulnerable nature of the Whistleblower, the sensitivity of the information Articles 9) and 10 of GDPR).

It is **forbidden to track the reporting channels** both on the platform and in any network equipment used (no retention of the whistleblower's LOGS), while it is necessary to track the activities of those who manage the reports as a measure to safeguard the obligations due, within the limits of the Workers' Statute.

**Access to the dedicated platform is provided through multi-factor authentication** as a further measure to strengthen protection measures.

If a **paper report** is used, it will be subject to the mechanism of the three envelopes and confidential protocol.

**The mapping of processing activities and updating of the register of processing activities** must be carried out dynamically following the changes that have occurred.

The sanctioning regime directly provided for violations of Legislative Decree Whistleblowing is in addition to the sanctions provided for in the field of Privacy and recalled by the Guarantor through Ordinances prior to the Decree (e.g. absence of information, failure to update the processing activity register, failure to adjust the relationship with the service provider and between it and subcontractors, failure to carry out DPIA, inadequacy of security measures such as encryption, unsuitable credential management methods, etc.)

## 13. REPORTING CHANNEL SHARING

In the event that the company subject to the specific procedure decides to entrust the management of the reports to the same (external) subject, it is contractually guaranteed that each Institution exclusively accesses the reports of its own responsibility, also taking into account the attribution of the relative responsibility. Therefore, technical and

organisational measures are taken to ensure that each Institution has access only to reports within its competence.

To this end, for the sharing of the reporting channel, it is necessary to stipulate agreements/conventions between the Bodies, in which the terms of the management of the reports are defined, which must in any case take place without prejudice to the obligation to guarantee confidentiality, to provide feedback and to manage the reported violation.

In groups with companies with more than 249 employees, it is possible to hypothesise solutions that take into account the characteristics of the business groups for the purpose of sharing platforms for the presentation and management of reports.

To this end, for the corporate reasons pertaining to Marcegaglia Steel S.p.A., the solution was adopted which provides for:

a) **the assignment to the Parent Company, as a third party with respect to the subsidiaries, of activities related to reporting**. In this case, in addition to the use of a single IT platform (possibly with dedicated and segregated channels for each company) prepared by the Parent Company, in line with the provisions of art. 4, par. 2 of the Decree, each subsidiary may entrust the management of the reporting channel to the third party, identified in the Parent Company. This model is governed by specific service contracts, signed between the individual subsidiary and the Parent Company. For the purposes of the management of the report, and to guarantee the so-called "proximity", the channel manager can make use, from time to time, of the support of the offices of the subsidiary – in compliance with the confidentiality obligations – or establish ex ante a dedicated structure that ensures the participation of subjects internal to the subsidiary to which the report refers.