REPORT MANAGEMENT PROCEDURE - WHISTLEBLOWING

Index

1. PURPOSE

This procedure governs[1] the ways in which the companies fulfil their obligation to establish a system for handling Reports (channels, procedures, resources) and to guarantee Whistleblowers the Safeguards provided for by law and by the procedure itself.

This procedure is intended to facilitate the correct implementation of Community law (legal certainty) and thus ensure the 'well-being' of companies. The objective is the 'transparency' of private action, which is the way to a truly virtuous company.
Companies also handle Reports to avoid incurring detrimental effects related to Violations (e.g. negative publicity on the market).

This procedure does not limit the protection that applies on the basis of other laws, regulations or other regulatory sources.

2. DEFINITIONS AND SCOPE

2.1. Definitions

For the purposes of this Procedure, the following definitions apply:

ANAC - National Anti-Corruption Authority (or **Competent Authority**)	*Italian independent administrative authority designated to (i) receive External Reports and (ii) carry out the functions provided for by the Directive, including feedback to the Whistleblower, in particular with regard to the follow-up given to Reports, in the cases provided for by the Whistleblowing Decree.*
Sectoral Acts	*normative acts identified in **Appendix A** of this procedure*
Reporting Channels	*channels for making the Report, made available to the Whistleblower by the Companies, in the case of an Internal Report, or by ANAC, in the case of an External Report, respectively;* *These Internal Reporting Channels in turn are defined as Internal or External depending on whether they are managed directly by the companies or respectively by third parties authorised by them*
Work context	*work or professional activities, present or past, carried out within the framework of the Legal Relationship, through which, irrespective of the nature of such activities, a person acquires information on Violations and in the context of which he/she could risk being retaliated against in case of a Report or Public Disclosure or a complaint to the Judicial Authority*
Whistleblowing Decree	*Legislative Decree 24/2023 transposing the Whistleblowing Directive in Italy*

[1] In compliance with i) Article 6 paragraph 2 of Legislative Decree 231/01 as amended by Law no. 179 of 30 November 2017 on "Provisions for the protection of the authors of reports of offences or irregularities of which they have become aware in the context of a public or private employment relationship", ii) Legislative Decree 24/2023 implementing EU Directive 1937/2019 (the "Directive"), as well as iii) by the best practices applicable in this field (ISO 37002).

Public Disclosure	*making information on Infringements publicly available through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people (e.g. radio, television, blogs, internet, automated e-mail campaigns)*
Whistleblowing Directive	*EU Directive 2019/1937 on the protection of persons who report breaches of Union law*
Third Sector Entities	*Entities that have entered into agreements with ANAC to provide Support Measures*
Facilitator	*a natural person who assists a Whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential (e.g. a trade union representative or a workplace safety representative)*
Report Manager(s) (or '**Case Manager'** in the Portal/Software)	*person(s) designated by the Companies to receive the Report and carry out the further related activities provided for in Chapter 3.5 of this procedure*
GDPR	*EU Data Protection Regulation 679/2016*
Group	*The corporate group to which the Company(ies) belongs*
Information on Violations	*information, including well-founded suspicions, concerning:* *(i) Violations committed or which, on the basis of concrete evidence, could be committed in the organisation with which the Whistleblower or the person making the complaint to the judicial or accounting authority has a legal relationship; and* *(ii) elements concerning any conduct aimed at concealing such Violations*
Protection measures	*measures provided for in paragraph 2 of **Appendix B** of this procedure*
Support Measures	*measures provided for in paragraph 6 of **Appendix B** of this procedure*
Person involved (Reported)	*natural or legal person mentioned in the internal or external Report or in the Public Disclosure as a person to whom the Violation is attributed or as a person otherwise implicated in the reported or publicly disclosed Violation*
Portal/Software	*the third-party cloud portal, accessible on the Internet at **https://rmgwhistleblowing.integrityline.com**, which can be used by the reporter to make an Internal Report*
Procedures	*the set of directives, instructions, protocols and written procedures envisaged and implemented by the Company in order to prevent Violations, and/or to reduce their consequences or recurrence*
Legal relationship	*legal relationship between the reporter and the organisation in which a Violation has been committed or may be committed;* *the legal relationship may be direct or indirect (i.e. through a third party having a direct legal relationship with the Company(ies))*

Feedback	*communication to the Whistleblower of information on the Follow-up that is given or that is intended to be given to the Report*
Retaliation	*any conduct, act or omission, even if only attempted or threatened, committed by reason of the Report or of the complaint to the judicial authority or of the Public Disclosure and which causes or is likely to cause, directly or indirectly, unjust damage to the person making the Report or the complaint*
Administrative penalties	*administrative pecuniary sanctions to be imposed by ANAC in respect of the non-compliance provided for therein*
Disciplinary sanctions	*disciplinary sanctions applicable by the Companies in the event of non-compliance with the provisions of this procedure*
Whistleblower	*a natural person, as referred to in Chapter 2.2.3, who makes a Report or Public Disclosure of Infringement Information acquired in the course of his/her work context*
External Signalling	*written or oral communication of Violation Information by the Complainant submitted through the Reporting Channel activated by ANAC*
Internal Signalling	*written or oral communication of Violation Information, submitted through the Reporting Channels made available by the Companies*
Séguito	*action taken by the Reporting Manager to assess the existence of the reported facts, the outcome of the investigation and any measures taken*
Company	*the companies listed in Chapter 2.2.1 below*
Private Sector Subjects	*entities, other than those falling under the definition of Public Sector Entities*
Public Sector Stakeholders	*public administrations referred to in Article 1(2) of Legislative Decree 165/2001,* *public economic entities,* *bodies governed by public law referred to in Article 3(1)(d) of Legislative Decree 50/2016,* *public service concessionaires,* *publicly controlled companies referred to in Article 2(1)(m) of Legislative Decree 175/2016, even if they are listed,* *in-house companies referred to in Art. 2(1)(o) of Legislative Decree 175/2016, even if listed*
External Subjects	*Reporting Parties other than Internal Stakeholders*
Internal Subjects	*whistleblowers defined as internal in the table in Section 2.2.3 of this procedure*
Protected Subjects	*The persons envisaged in **para. 1 of Appendix B** to this Procedure, who are eligible for the Protections*
Safeguards	*the set of Protection and Support Measures provided for in the Whistleblowing Decree*

231 Violations	*acts or omissions detrimental to the public interest or integrity of the Companies and consisting of:* *a) unlawful conduct relevant under Legislative Decree No. 231/2001 (i.e. the commission of alleged offences or the reasonable danger of the commission of alleged offences, provided for in Legislative Decree No. 231/01 on the administrative liability of companies (so-called '231 offences'), or* *b) violations of the rules of conduct/procedures/protocols issued by the Company and/or any violation of Model 231,* *o* *(c) which frustrate the object or purpose of the regulations set out in Legislative Decree 231/2001, including any attempts to conceal such violations,* *which have occurred or which are very likely (on the basis of concrete elements) to occur in the organisation (possibly also different from the Companies, e.g. a supplier of the Companies) with which the Whistleblower has a legal relationship,* *including any conduct aimed at concealing such violations;* *regardless of the fact that:* *- the employment relationship with the companies has ended in the meantime (so-called former employee), or that* *- the facts were learnt during the selection process (e.g. candidate) or in other pre-contractual negotiations with the companies*
Violations of Sectoral Acts or **"Sectoral Violations"**	*conduct, acts or omissions that harm the public interest or the integrity of the Companies and that consist of offences falling within the scope of the Sectorial Acts identified in* ***Appendix A****,* *which have occurred or which are very likely (on the basis of concrete elements) to occur in the organisation (possibly also different from the Company(ies), e.g. a supplier of the same or a contact person of an auditing firm of the same) with which the Whistleblower has a legal relationship,* *including any conduct aimed at concealing such violations,* *regardless of the fact that:* *- the employment relationship with the companies has ended in the meantime (so-called former employee), or that* *- the facts were learnt during the selection process (e.g. candidate) or in other pre-contractual negotiations with the companies,* *regardless of whether, under national law, Whistleblowing Violations are administrative, criminal or purely civil violations (e.g. risk of damages).*

2.2. Subjective scope

2.2.1. This procedure applies to the following companies:

- ✓ **RINO MASTROTTO GROUP SPA**, with registered office in Via Dell'Artigianato, 100 - 36070 Trissino (VI), Italy
- ✓ **NUOVA OSBA SRL,** with registered office in Via Dell'Artigianato, 100 - 36070 Trissino (VI), Italy
- ✓ **TESSITURA ORESTE MARIANI SPA**, with registered office at Via Alfredo Catalani, 75 - 20833 Giussano (MB), Italy
- ✓ **MORELLINO SRL**, with registered office in Via Caduti sul Lavoro, 1/3 - 56029 Santa Croce sull'Arno (PI), Italy
- ✓ **ELMO SWEDEN AB**, with registered office at Kyrkogatan 18, 512 50 Svenljunga, Sweden
- ✓ **BERMAS MARACANAU INDUSTRIA E COMERCIO DE COURO LTDA**, with registered office at Av. Sen. Virgílio Távora, S/N - Distrito Industrial I, Maracanaú - CE, 61939-160, Brazil
- ✓ **RMG LEATHER USA LLC**, headquartered at 1226 Fed Ex Drive SW, CONOVER, NC (North Carolina), Zip Code: 28613 - U.S.A.
- ✓ **BRUSAROSCO DE MEXICO SA**, with registered office at Industria Zapatera 168, Fracciones de Santa Lucia, 37490 León, Gto., Mexico.

2.2.2. In relation to the aforementioned companies, this procedure applies:

- for Companies that have not adopted a 231 Model pursuant to Legislative Decree 231/2021, to Whistleblowers who make i) Internal and/or External Reports or ii) Public Disclosures or iii) Complaints to the judicial authorities, in relation to Sectoral Violations only;
- for companies that have adopted a 231 Model pursuant to Legislative Decree no. 231/2021, to Whistleblowers who make:
  - i) Internal Reporting, in relation to 231 Violations only; and
  - ii) if they have reached an average of at least 50 employees in the previous year, Internal Reports or External Reports or Public Disclosures or Complaints to the Judicial Authority, including in relation to Sectoral Violations;
- to other Protected Subjects;
- other Data Subjects whose personal data are processed during the life cycle of the management of the Reports.

2.2.3. Whistleblowers may belong to the following categories:

ID	Subject category	Subject nature
A	Company employees, including casual workers	Internal Subject
B	Paid and unpaid volunteers and **trainees** working for the companies	Internal Subject
C	**Self-employed workers, including** self-employed relationships that have special rules pursuant to Article 2222 of the Civil Code (work contracts) (including **freelancers and consultants** working for companies) as well as **Holders of a collaboration relationship as referred to in Article 409 of the Code of Civil Procedure, who** work for the Companies, the latter being understood to mean: 1) those of private employment, even if not inherent in the exercise of an undertaking; 2) agency, commercial representation relationships; and 3) other collaborative relationships resulting in the provision of continuous and coordinated work, mainly of a personal nature, even if not of a subordinate nature	External Subject
D	**Employees and collaborators**, who work **for third parties Public or private sector entities that provide goods or services or carry out works in favour of the companies**	External Subject
E	**Shareholders**	External Subject
F	**Members of the administrative and/or management** or representative **bodies of** the Companies, including non-executive members (e.g. directors without or with delegated powers), even when such functions are exercised on a de facto basis	Internal Subject
G	**Members of the control or supervisory body of** the companies (e.g. Mayors, Auditors or Auditing Companies, Supervisory Board 231, DPO - Data Protection Officer)	Mayor-ODV 231: Internal Subject Auditor or contact person of auditing company - DPO: External Subject

In Italy

Even those who no longer belong to one of the categories of persons under A-B but who received or acquired the Information while within the organisation may validly make the Report.

Persons who have sought, applied for or otherwise made themselves available to carry out any of the activities under A-B-C-D may also make the Report, if they have acquired the Information during the time they have been in contact with the Companies for that purpose.

In Sweden

Anyone who no longer belongs to one of the above categories of persons (A-B-C-D-E-F-G) and who received or assimilated the Information while within the organisation may also make the Report.

Persons who have sought, applied for or otherwise made themselves available to perform, any of the activities under A-B-C-D-E-F-G, may also make the Report, if they have acquired the Information during the period in which they have been in contact with the Companies for that purpose.

2.3. Objective scope

The Reports subject to the Safeguards concern Violations that have occurred or are very likely to occur

- in the activity in which the Whistleblower is, has been or might be engaged; or
- in another organisation with which the Whistleblower is or has been in contact through his/her work.

Reporting is an obligation, which, by virtue of the general duties of good faith, loyalty and fidelity towards the Company, is incumbent on employees and collaborators, as well as, from time to time, on the other potential Whistleblowers indicated above.

Whistleblowers are obliged to communicate well-substantiated Infringement Information based on precise (adequately detailed) and concordant facts, and not facts of a general, confusing and/or blatantly defamatory or slanderous content.

Reports **may also be anonymous**, i.e. they may not show the identity of the reporter or allow the identity of the reporter to be reconstructed or found. They will be examined, provided they comply with the above requirements.

Complaints**, claims or demands linked to a personal interest of the whistle-blower** or the person lodging a complaint with the judicial authority **that relate exclusively to his or her individual employment relationships, or inherent to his or her employment relationships with hierarchically superior figures,** will not be taken into account.

The application remains unaffected:
(i) the provisions on (a) the exercise of the right of workers to consult their representatives or trade unions, (b) protection against unlawful conduct or acts carried out as a result of such consultations, (c) the autonomy of the social partners and their right to enter into collective agreements, and (d) the suppression of anti-union conduct (Article 28 L. 300/1970 and ss.mm.ii - Workers' Statute), and
(ii) the provisions of criminal procedure laid down by the applicable law (therefore, the Whistleblower shall always be entitled, in the event that he/she has information about an offence, to lodge a complaint with the competent criminal authority).

3. REGULATION OF ACTIVITIES

3.1. Generalities

The Report is:

a) **mandatory**, on the part of the **Internal Parties** (NB. by virtue of the **general duties of loyalty, diligence and good faith** connected with the legal relationship with the Companies, to be understood as expressly reaffirmed herein);

b) **compulsory**, by **External Parties** who are **contractually obliged to** the Companies to report;

c) optional, by **External Parties** to the Companies that are not contractually obliged towards the Companies to report.

3.2. Subject of the Report

In order to facilitate and allow the due verifications and preliminary investigation activities by the Companies, also in order to ascertain the merits of the Report, the Whistleblower is suggested to provide at least the **following** useful **elements:**

- the **identity** of the reporter (name, surname, tax code, position or function held), unless the reporter decides not to proceed with an anonymous Report;
- a description of the **reasons** related to the work performed that made the reported facts known;
- a clear and complete **description of the facts that are** the subject of the Report;
- the **circumstances of time and place** in which the acts were committed, if known;
- the **particulars** of the person to whom the violation is attributed or elements useful for identifying him/her, if known;
- an indication of any **other persons who may report** on the facts that are the subject of the Report;
- an indication of any **documents that** may confirm the facts that are the subject of the Report;
- any other **information** that may provide useful feedback on the existence of the reported facts.

3.3. Types of Reports

A **Report** is defined:

a) **Internal**, if directed to the Companies, in which case it may be through one or more of the **Reporting Channels** (in turn distinguished as **internal or external**, depending on whether they are managed by the Companies or by third parties), and/or

b) **External**, if executed **to the competent authority**, and/or

c) **Public disclosure** if carried out in the presence of the specific prerequisites laid down by the Whistleblowing Decree for the latter.

3.3.1. Internal Signalling Channels

3.3.1.1 Trade Union Hearing (Italy only)

The Internal Reporting Channels are to be implemented after hearing the company representations or trade unions (if any), to be activated by the date of entry into force of this Procedure and the Internal Reporting Channel provided for herein, without prejudice to

- the possibility of continuing the consultation until union feedback is received, and
- the non-binding nature of the opinion to be expressed by the representations themselves.

3.3.1.2 Generalities

Internal Reporting Channels are distinguished into Internal and External, depending on whether they are managed directly by the Companies or, respectively, by third parties authorised by them.

The following Internal Reporting **Channels** may be used by the Whistleblower.

✓ INFORMATORS:

- **Portal/Software**[2] , accessible at **https://rmgwhistleblowing.integrityline.com**,

✓ ORALS:

- **Voice recording** (to a registered voicemail/voicemail box) possible in the Portal/Software.
  The Handlers of the Report are obliged to document the oral Report by means of a **detailed account of** the conversation **written** by the staff handling the Report, which, after being dated and signed by the Handler of the Report, will be submitted to the Whistleblower, which will have the right to **verify, rectify and approve the** account by affixing its **signature.**

- *(at the request of the Whistleblower*) **Direct personal meeting** with one or more Handlers of the Report, including via remote videoconference session if necessary.

  The Handlers of the Alert ensure in this case, **subject to the consent of** the reporter, that
  a) the meeting takes place **within a reasonable period of time** from the date of the said request (maximum 14 working days), and
  b) a complete and accurate **record** of that meeting is **kept on a durable medium** that **allows access** to the Violation Information.

  Report Managers are obliged to **document** the meeting:
  a) **recording the conversation on a durable medium** that allows access to the Information; or
  b) by means of a **detailed minute of** the meeting drawn up by the Handlers of the Report. The Reporting Officer has the right to **verify, rectify and approve** the minutes by his/her signature.

[2] Instructions for using the Portal/Software can be viewed:
a) the Whistleblower: on the first online page of the Portal/Software;
b) for the role of Admin or Case Manager: in the Admin Manual and/or the Case Manager Manual respectively, referred to in Appendix E to this procedure

After the verbalisation of the face-to-face meeting, the receiving Reporting Managers must **record the verbalisation on the Portal/Software**.
The Reporting Managers then manage the Follow-up of the Reporting via the Portal/Software.

✓ PAPERS:

- **A sealed paper envelope** marked "**Personal confidentiality for the Reporting Committee**" on the outside, to the postal address: RINO MASTROTTO GROUP S.p.A., Via dell'Artigianato, n.100, Trissino (VI).

  Secretarial staff who receive the envelope in the first instance are strictly forbidden to open it and must immediately hand it over to the Whistleblowing Committee. If the delivery cannot be made immediately, the envelope must be **stored diligently in a secure locked place** (room, cupboard, or drawer)**.**

- Introduction of communication (in a sealed paper envelope marked "Confidential for the Signalling Committee" on the outside) in the **physical box located in the canteen/changing room corridor of the** RINO MASTROTTO GROUP S.p.A. headquarters, Via dell'Artigianato, no. 100, Trissino (VI).

  Personnel of the HR Department receiving the envelope in the first instance are strictly forbidden to open it and must immediately hand it over to the Whistleblowings Committee. In the event that the delivery cannot be made immediately, the envelope must be **stored diligently in a locked safe place** (room, cupboard, or drawer).

The Reporting Managers then manage the Follow-up of the Report as per procedure.

3.3.2. External Reporting and Public Disclosure

3.3.2.1. External Signalling

The reporter may only make an External Report (i.e. to ANAC) if, at the time of its submission, one of the following **conditions** is met:

a) there is no compulsory activation of any Internal Reporting Channel within its work context, or

b) the Internal Reporting Channel, although theoretically envisaged as mandatory for companies, is in fact **not active or, even if activated, does not comply** with regulatory requirements;

c) the Internal Report already made by the Whistleblower **had no Follow-up**[3] ;

d) the Whistleblower has **reasonable grounds to believe** that, if he or she made an Internal Report, it would not be effectively followed up or the Report might lead to the **risk of retaliation**;

[3] Therefore, if the Alert has been closed with a final decision, even if negative, an External Alert is not allowed.

e) the Complainant has grounds to believe that the Violation may constitute an **imminent or obvious danger to the public interest**.

External Signalling is carried out:

- in **writing** through the Reporting Channel activated by ANAC
  (for more information on contact details and instructions on the use of the External Reporting Channel, the confidentiality regime applicable to External Reports and the process for handling External Reports see https://www.anticorruzione.it/-/whistleblowing), or
- **orally** through (i) **telephone lines** or (ii) **voice messaging systems** or, (iii) at the request of the Whistleblower, through a **face-to-face meeting** set within a reasonable time.

In Sweden
It is also possible to submit an External Report directly to the competent authorities:

- Swedish Working Environment Authority Av.se
- The Economic Crime Authority The Economic Crime Authority.se
- Data Protection Authority Imy.se
- Swedish Chemicals Agency Kemi.se
- National Food Agency National Food Agency.se
- Västra Götaland County Administrative Council Lansstyrelsen.se/vastragotaland
- Swedish Tax Agency Skatteverket Skatteverket.se
- Swedish Energy Agency Energy Agency.se

3.3.2.2. Public Disclosure

The Whistleblower is **entitled** to make a Public Disclosure of the Violation, benefiting from the Legal Protections, only if the following prerequisites are met (the '**Public Disclosure Prerequisites**'):

- **first carried out the Reporting** (internal and external, or directly external), but
  - ✓ **appropriate action has not been taken in** response to the Report within the 3 month time limit (or, in Sweden, if there are separate requirements - i.e. special and demonstrable reasons, and the Reporting Subject has been informed of the requirements for such longer time limit - within the 6 month time limit), from the date of the acknowledgement of receipt of the Report, or
  - ✓ **no acknowledgement of receipt was sent** to the Whistleblower within 3 months of the expiry of the 7-day time limit;

  or when
- the Whistleblower has **reasonable grounds to** believe that:
  - ✓ the Violation may constitute an **imminent or obvious danger to the public interest**, such as where there is an emergency situation or the risk of irreversible harm (or, in Sweden, the Whistleblower has reasonable grounds to believe that the Violation may constitute an **imminent or obvious danger to life, limb or property, or a risk of serious harm to the public, or otherwise has a legitimate reason to disclose the Information**); or

- ✓ the External Report **entails a risk of retaliation or makes it likely that the Violation may not be effective due to the** circumstances of the case, such as where **evidence** may be **concealed or destroyed** or where there is reason to believe that **the recipient of the Report may be colluding with** or **involved in the Violation**.

3.4. Case Managers

3.4.1. Generalities

The management of the Internal Reporting Channels and the Follow-up is entrusted jointly to the following persons, who are guaranteed an **autonomous functional position for this purpose**, and who must be **specifically trained** for this management:

- the 231 Supervisory Body of RINO MASTROTTO GROUP S.P.A. (as the first recipients of the Reports, and, following the preliminary screening, exclusively if the Violation is classified as a 231 Violation);
- the HUMAN RESOURCES Manager of the Parent Company RINO MASTROTTO GROUP S.P.A., without the intervention of the 231 Supervisory Body, in the event that, following the screening, the Violation is classified as other than a 231 Violation;
- the DPO of the Parent Company RINO MASTROTTO GROUP S.P.A., without the intervention of the Supervisory Board 231, in the event that, following screening, the Violation is classified as concerning the protection of personal data;
- the HR GENERALIST of ELMO SWEDEN AB, in cases where as a result of the screening the Violation concerns that company; the HR GENERALIST of Elmo Sweden AB is the first recipient and responsible for case management and investigation of Reports. If the reported issue relates to HUMAN RESOURCES, the case management is passed to the next person who is the Head of SUSTAINABILITY at Elmo Sweden AB; in cases where the Head of SUSTAINABILITY cannot handle the case, it is passed to the Head of QUALITY at Elmo Sweden AB. In cases where the Head of QUALITY cannot manage the case, this is passed to the Head of HUMAN RESOURCES of RINO MASTROTTO GROUP SPA.

3.4.2. Budget

The body responsible for appointing the Reporting Managers, if different from the Supervisory Board 231, assesses the appropriateness of allocating to the Reporting Manager(s) an annual budget, which can be used to perform the task, provided that the Managers do not already have a budget for their own functioning.

3.4.3. Tasks

The Reporting Managers, as a body deemed impartial and competent by the companies, have the **task** of

a) receive and take charge of Reports;

b) screen alerts (see Chapter 3.6.1);

c) provide the first Notice to the Whistleblower within the time limit provided for in Chapter 3.6.3; maintain contact with the Whistleblower for subsequent communications; diligently follow up the Report;

d) if it is competent to do so, ensure the proper investigation of the reported facts, through actions such as an internal investigation, enquiries, requests for supplementary information if necessary from the Whistleblower, requests to third parties;

e) if competent for the matter, decide on the outcome (validity) of the Reports, on the basis of the results of the investigation, and communicate it to the Whistleblower within the deadlines set out in Chapter 3.6.3;

f) if competent for the matter, cooperate with the other competent corporate functions to verify that the reported Violation is remedied, e.g. also through criminal prosecution, an action for the recovery of funds;

g) ensure the proper filing and storage of Reports;

h) coordinate with the Privacy Function, as well as with the designated DPO, where necessary or required, to meet the compliance requirements of the personal data processing operations covered by the Reports;

i) make available clear information on the Reporting Channels, procedures and prerequisites for making Internal and External Reports, by means of display in workplaces, publication on the Company's website or by any other means enabling Reporting Parties to access such information;

j) cooperate with the IT Manager, upon request, to ensure that the requirements for the protection of computerised Reporting Channels and the storage of Reports are met;

k) communicate to the administrative bodies of the companies to which the Reports received relate, by 31 January, an annual report on the Reports received and their outcome; the report is not necessary if there are no Reports during the year. The report may be interim if the managers of the Reports consider it necessary on account of the particular importance of the Reports.

NB: If a person other than the competent Reporting Managers receives a Report, he/she must immediately forward it to the competent Reporting Managers, complete with any supporting documentation received, not retaining any copy of it and refraining from taking any independent initiative for analysis and/or investigation.

Failure or delay on the part of the first addressees of the Reports received to communicate them to the competent Reporting Managers constitutes a breach of this procedure, as such punishable, in the event of wilful misconduct or gross negligence, by the disciplinary sanctions referred to in Section 9 below.

3.5. Examination of Reports

3.5.1. Switching / Protocoling

The Report received through Reporting Channels other than the Portal/Software is logged/entered immediately in the Portal/Software by the Reporting Manager who first receives it. This entry causes an ID Code to be assigned to the Report (protocolation).

3.5.2. Preliminary screening

Following receipt of the Report, the Reporting Managers take **charge of** the Report and carry out a **preliminary assessment of** it, aimed at ascertaining

- whether the Report contains the minimum mandatory information required, and is therefore to be considered admissible,
- the type of Violation reported (e.g. 231 Violation, Sectoral Violation), and
- the possible conflict of interest of the Handlers of the Alert with respect to the Alert itself.

(the '**Screening**').

If the Reporting Manager(s) consider(s) that the Alert is **admissible** and also falls within their **competence**, they proceed with the further steps (inquiry, etc., on which see below).

If, on the other hand, the Reporting Manager(s) assesses that the further handling of the Report is **beyond his/her** technical or legal **knowledge** (because it falls within the competence of other Reporting Manager(s) - e.g. 231 Supervisory Board, DPO, other legally competent subjects such as Board of Auditors, Auditors and Auditing Firm), **he/she shall forward the Report** to such other subject(s), giving simultaneous notice of the transmission to the Whistleblower.
In particular, this must be done at the first available meeting or, if urgent, without delay.

The Whistleblowing Manager(s), if deemed necessary or useful for the performance of his/her tasks, may delegate in writing to one or more persons (internal, in compliance with the delegate's powers as per the company's delegation system in force, or external) the performance of the investigative tasks under e) and/or f) above (e.g. if they require specialised technical or legal expertise) (the "**Co-optation**") and under a prior written obligation of strict confidentiality. To this end, the Reporting Manager(s) shall ensure in advance that the delegate is aware of this procedure.

This is without prejudice to the sole responsibility of the Reporting Manager(s) as regards the final decision on the merits of the Report, as well as in relation to measures to eliminate the consequences and causes of the reported Violation, if so provided for in the company's functional organisation chart.

3.5.3. Conflict of interest

The Handlers of the Report, if they consider the existence of a **conflict of interest** with respect to the Report they receive (*e.g. the subject of the Report concerns violations attributable to the Handlers themselves, or to the functional area in which the Handlers perform their usual duties*), are required to

- refrain from dealing with the Report, and
- immediately transfer the handling of the Report to other Reporting Managers not subject to a conflict of interest, or, in the absence of such a Reporting Manager not subject to a conflict of interest, to the Parent Company's Board of Auditors), communicating in writing the nature of the conflict detected.

In the event of any **doubt** as to the existence of his or her conflict of interest, the Reporting Manager must immediately notify the other Reporting Managers, who will then assess the same with him or her.
The nature of the conflict detected with respect to a Report must be declared within the "notes" field in the Portal/Software, by the Managers of the Report not in conflict of interest.

3.5.4. Feedback to the reporter

Within 7 days of **receipt of the non-anonymous Report, the Reporting Managers shall provide the Whistleblower** with **an acknowledgement of receipt of the Report**, by an appropriate means to ensure the confidentiality of the message (SaaS Portal/Software - using the 'Secure Inbox' function), or, if the Portal/Software cannot be used, an encrypted e-mail message).
The obligation to provide the Whistleblower with acknowledgement of receipt within 7 days of the Report, does not apply if the Whistleblower has refused the acknowledgement of receipt or the Reporting Managers have reason to believe that the acknowledgement of receipt would reveal the identity of the Whistleblower (e.g. where the Whistleblower has provided contact details which, if used by the Reporting Manager, would clearly entail the risk of disclosure of the identity of the Whistleblower who wishes to remain anonymous).

Acknowledgement to the Whistleblower on the outcome of the report must be provided within a period of **three months,** commencing within that period:

- **from the date of the acknowledgement of receipt of** the Report, or,
- if no initial notice was sent to the Whistleblower (e.g. because the Whistleblower remained anonymous), from the **expiry of the period of 7 days** from receipt of the Report.

NB: If **no Follow-up** (as defined in Chapter 2) of the Report **has been decided upon** at the end of this three-month period, the Whistleblower **must be informed of this**, as well as of any further feedback to be expected.

The Reporting Officer using the Report ID received can access the Portal/Software and interact with the Reporting Managers designated from time to time by the Companies.

3.6. Investigation

3.6.1. Generalities

If the Report is deemed *prima facie* **admissible**, the relevant Reporting Manager proceeds with the preliminary investigation of the facts that are the subject of the Report. To this end, he/she shall, by way of example but not limited to:

a) verifies whether, in order to protect against the risk of the Violation that is the subject of the Report, the Companies have adopted adequate Procedures in advance;

b) if it deems it necessary or appropriate, requests and receives further information, clarifications, and/or the production of deeds and documents from the Whistleblower - if known - or from other persons, including third parties (e.g. heads of function or any other internal or external person), in possession of information useful for the preliminary investigation, in particular, reasonably concerning the processes at risk of Violation.

   [N.B.: It is not necessary for the companies adhering to this Procedure **to obtain from third party suppliers a written commitment to report** and cooperate with the Reporting Managers in the investigation of their respective Reports, since the Clause 231 signed by the Company is already suitable to guarantee such cooperation also in relation to non 231 Violations that emerge in connection with the same operational processes to which the 231 risks refer.
   (NB: *Third parties may invoke professional secrecy to which they are legally bound - e.g. legal or medical - and/or because of any previous confidentiality agreements with other third parties*)]

c) With immediate promptness, moreover, the Reporting Managers receive from the Heads of the respective functional areas of the company any information they become aware of concerning:

   - measures and/or news coming from judicial police bodies and/or any other competent Authority, from which it is inferred that investigations are being carried out, even against unknown persons, for Violations;
   - requests for Legal Protection made by employees or directors of the Companies in the event of legal proceedings being initiated for Violations;
   - reports prepared by the Heads of function within the framework of their control activities and from which facts, acts, events or omissions may emerge with critical profiles with respect to the reported Violations;
   - requests made by the persons reported (i.e. charged with the Violations) in order to defend their rights allegedly violated through the Report received.

3.6.2. Priorities

Alerts are processed in the following **order of priority**:

a) severity of the reported conduct / number of Violations reported;

b) reasons of urgency in order to prevent any further damage (e.g. to health) as a consequence of the events reported;

c) repeated commission of the facts already the subject of a previous Report;

d) involvement of several parties in the matter reported;

e) any further circumstances assessed at the discretion of the Reporting Manager.

3.7. Obligations to cooperate

The personnel and any other internal contact persons of the Companies are obliged to cooperate with the utmost diligence in the investigation activities of the Reporting Managers.

3.8. Archiving the Report

In the event that the outcome of the screening or subsequent more extensive investigation is found:

- the absence, even partial, of data constituting essential elements of the Violation Report; or
- the general content of the Report is such that it does not allow the reported facts to be understood; or
- the Violation Report is accompanied by inappropriate or irrelevant documentation; or
- unfoundedness due to the absence of concrete factual elements capable of justifying findings,

the Reporting Managers **declare** the Report received **inadmissible, and** consequently archive it through the Portal/Software.

Such filing is promptly **notified** through the Portal/Software:

- to the Whistleblower (if known or otherwise reachable via the Portal/Software's Secure Inbox),
- the other Handlers of the Alert, if they were not involved in the Screening or Investigation of the Alert,
- the administrative bodies of the companies to which the Reports refer, in the periodic report by the Reporting Manager.

3.9. Actions following the Report

3.9.1. Unfoundedness of the Report with wilful misconduct or gross negligence

In that case, Archiving must be carried out.

Should the Handlers of the Report find elements that, in its considered judgement, point to bad faith or gross negligence in the Report, it shall communicate this in writing:

- to the Reported; and
- the Head of the Whistleblower's functional area, as well as to the Human Resources/HR Department, for the assessment of the application of any sanctions against the Whistleblower.

3.9.2. Report confirmed by checks

In the event that, at the outcome of the investigations, the Reporting Officers responsible for the **merits of the Report** find that the facts of the Report are **well-founded**, they shall communicate the final outcome of the investigation in a traceable manner, for any assessment within their competence:

(a) to the Reported Party (unless this hinders investigations or judicial proceedings for the protection of the rights of the Companies; in any case, the Handlers of the Reported Party shall assess the advisability of delaying the aforesaid communication, depending on any confidentiality requirements concerning the conduct of the investigation); and

(b) the Head of the functional area to which the Whistleblower belongs, if the Violation relates to an offence concerning that area[4] ,

(c) the HUMAN RESOURCES Function/hr (unless the reported Violation is attributable to it); and

d) the administrative body of the Company to which the Violation relates (unless the Violation is attributable to it); and

(e) in the case of an external reporter:
(i) the legal representative pro tempore of the third party organisation to which the Whistleblower himself/herself belongs (or, if he/she is deemed to be in a position of conflict of interest with respect to the reported Violation, to the Head of the different functional area of the third party organisation that appears competent to examine the communication) and
(ii) the head of the internal functional area that has contractual relations with that organisation;

f) to the Board of Auditors of the Parent Company.

[4] On the other hand, it is not considered strictly necessary to inform the person in charge of the area to which the reported person belongs, as this could violate the confidentiality of the reporter beforehand [unlike in the other cases provided for in the text].

3.9.3. Non-compliance with Internal Procedures

If the investigation carried out following the Report leads the Reporting Managers to ascertain (i) the absence of specific corporate Procedures aimed at guaranteeing against the risk of Violations or (ii) the lack of adequate internal and/or external disclosure thereof, or (iii) the lack of internal training with respect to the rules laid down by the Procedure, the Reporting Managers shall report such circumstances to the Functional Managers of the Company to which the Violation refers and to the ESG Function of RINO MASTROTTO GRUOP SPA, for the appropriate remedies.

3.9.4. Report confirmed by verifications, but indeterminate in terms of damage suffered or insufficient evidence gathered

In such cases (*examples: reports in the media; cyber fraud, cartels in public tenders, conflicts of interest and other circumstances or conduct not easily detectable by internal controls, etc.*), additional investigative activities should be assessed, with an indication of the professional expertise required (e.g. specific legal or technical expertise on the reported facts or underlying processes).

On the basis of the results of these further investigations, should the reported facts be confirmed, the actions referred to in section 3.9.2 may be pursued.
Otherwise, further legal action must be taken or reports must be made to the competent authorities for any necessary investigations.

3.9.5. Reporting on facts that are plausible but cannot be verified

In these cases, too, the actions mentioned in section 3.9.2 above can be pursued.

4. CONSERVATION

The Report of Violations, and the related documentation, must be **archived** exclusively for the time necessary to process the Report and in any case **no longer than 5 years (in Sweden, 2 years) from the date of the documentation of the final outcome** of the reporting procedure (in compliance with the obligations of confidentiality of the information as well as of limitation of storage, provided for by the applicable regulations on the matter), and beyond that period for as long as necessary for the completion of administrative or judicial proceedings already initiated or for investigative proceedings pursuant to the Code of Criminal Procedure.

5. LEGAL PROTECTION

The Whistleblower and other Protected Persons are granted by the Companies the Safeguards set out in ***Appendix B***.

6. TRAINING

Training, communication and information activities are an indispensable component of the effective implementation of the Whistleblowing organisational model and are regulated in ***Appendix D***.

7. DISTRIBUTION

The Reporting Managers shall make available to the Addressees of this Procedure, clear information on the Reporting Channels, on the prerequisites for making internal and external Reports and public Disclosures, using the following methods:

- Posting in a visible place in the workplace (company notice board),
- Making available
  - ✓ hands and/or
  - ✓ by e-mail, or
  - ✓ via company intranet or
  - ✓ via another software application (e.g. personnel and/or payroll software or procedure distribution software),
- Publication in a special section of the company website (the URL of which is communicated by the company),
- Made available via link/icon on the first electronic page of the Reporting Portal/Software (see separate training slides).

8. SANCTIONS

Failure to comply with the provisions contained in this procedure may give rise - in addition to the civil and criminal consequences provided for by the legislation in force - to disciplinary sanctions by the Companies, as provided for:
i) in Italy, by the National Collective Labour Agreement and by the company Collective Bargaining Agreement, if any (therefore to be understood as expressly referred to herein) and by **paragraph 4** "***Penalty System"* contained in** the General Section of the company ***231 Organisational Model***;
(ii) in Sweden, by **paragraph 4** "***Penalty System"* contained in** the General Section of the company's ***231 Organisational Model.***

9. OTHER

It is prohibited to prevent or attempt to prevent a Report, or any subsequent evaluation of it;
It is forbidden to engage in or attempt to engage in acts of retaliation in response to a Whistleblowing Report or because someone approaches a trade union representative or workers' organisation for a consultation on Whistleblowing. Moreover, no one may prevent or attempt to prevent such a consultation.

For matters not expressly provided for in this Procedure, the following shall apply:

- **in Italy**
  the Whistleblowing Decree, and, if applicable, the ANAC Guidelines,
- **in Sweden**
  Law 2021:890.

APPENDIX A - SECTORAL VIOLATIONS

Sectoral Violations include:

a) **offences (actions or omissions) falling within** the **scope of the following sectoral Union acts**[5] :

Privacy and data protection E.g. Violations of privacy obligations such as information to data subjects, collection of consent on processing, data and processing protection measures, documentation, etc.
Environmental Protection E.g. violations of administrative prescriptions possibly punished with administrative fines and therefore not falling within the perimeter of offences 231 already to be reported under the company's 231 Organisational Model
Product safety and conformity E.g. obligations to ensure the quality and safety of marketed products intended for use by the consumer public
(only in Sweden) **any misconduct in a work context, which is in the public interest**

b) **acts or omissions affecting the financial interests of the Union** as referred to in Article 325 TFEU specified in the relevant EU secondary legislation;

c) **acts or omissions relating to the internal market**, as referred to in Article 26(2) TFEU, including:
   1. violations of EU competition and state aid rules, and
   2. internal market infringements related to acts violating corporate tax rules (in the case of Italy: IRES, IRAP) or
   3. mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;

d) **acts or omissions that frustrate the object or purpose of the provisions of** Union acts in the areas referred to in (a), (b) and (c).

NB. For a detailed description of these relevant areas, see the ***Annex (Part I and Part II) of the Whistleblowing Decree*** available at www.normattiva.it.

[5] See Annex to EU Directive 1937/2019

APPENDIX B - SAFEGUARDS

1. PROTECTED SUBJECTS

Protected Subjects include,

- the reporter (even anonymous, whose identity is discovered at a later stage),
- those who lodge a complaint with the judicial authorities in relation to a Violation,
- those who make a Public Disclosure, and
- the following categories of persons:
  - **Facilitators**,
  - **Persons** in the same employment context as the Whistleblower, the person who filed a complaint with the judicial authority or the person who made a Public Disclosure and who are related to them by a stable emotional or kinship link up to the fourth degree (cousins),
  - **Co-workers** of the Whistleblower, of the person who has filed a complaint with the judicial authority or made a Public Disclosure, who work in the same work context as the Whistleblower and who have a usual and current relationship with that person,
  - **Entities that own, or are employers of, or operate in the same employment context as the aforementioned persons.**

2. PROTECTION

In the event of a Report, **all Protected Persons** are guaranteed the following three mandatory categories of legal protection:

- PROTECTIVE MEASURES,
- SUPPORTING MEASURES,
- RIGHT TO CONFIDENTIALITY,

as detailed below.

In addition, **with regard to Whistleblowers only**, the Safeguards also apply if the Reporting or Public Disclosure occurs in the following cases:

a) **when the legal relationship** with the Companies **has not yet started**, if information on Violations was acquired during the selection process or in other pre-contractual stages;

(b) during the **probationary period**;

(c) **after termination of the legal relationship**, if the Information was acquired during the course of the legal relationship.

The **reasons** that led the person to report or publicly disclose **are irrelevant for** the purposes of Protection.

3. PROTECTIVE MEASURES[6]

The following **Protection Measures** apply to Protected Persons:

- Prohibition of Retaliation,
- Protection from Retaliation,
- Limitations of liability,
- Waivers and conditional settlements.

NB: Protective Measures also apply:

(a) in cases of anonymous Reporting or Public Disclosure, if the Whistleblower was subsequently identified and retaliated against, and

(b) in cases of External Alerts for Violations of Sectorial Acts submitted to any of the competent institutions, bodies, offices and agencies of the European Union that have set up External Alert channels and procedures for this purpose (*e.g. the European Anti-Fraud Office*), provided that the Whistleblower executes the Alert in accordance with the conditions for External Alerts,

(c) (in Sweden) even if someone reports internally by means other than the Internal Reporting governed by this Procedure, if

- there are no such channels or the available channels and procedures do not meet legal requirements; or
- Reporting occurs before the person has started working in the organisation.

3.1. Prohibition of retaliation

Protected Persons may not be subjected to any Retaliation (meaning *any conduct, act or omission, even if only attempted or threatened, carried out by reason of the Reporting or Whistleblowing or Public Disclosure and that causes or may cause the Whistleblower, directly or indirectly, unjust damage)* (**prohibition of retaliatory acts**).

Retaliation' is to be **understood broadly**, including **but** not limited to;

(a) **dismissal**, **suspension** or equivalent measures;

(b) downgrading or **non-promotion**;

(c) change of duties, **change of place of work**, **reduction of salary**, **change of working hours**;

(d) **suspension of training** or any restriction of access to it;

(e) **demerit notes or negative references**;

(f) the adoption of **disciplinary measures** or other sanctions, including fines;

(g) **coercion**, **intimidation**, **harassment** or **ostracism**;

(h) **discrimination** or otherwise **unfavourable treatment**;

(i) **failure to convert** a fixed-term employment contract into an employment contract of indefinite duration, **where the employee had legitimate expectations of** such conversion;

(j) **non-renewal** or **early termination of** a fixed-term employment contract;

[6] The protection afforded to the Whistleblower will be guaranteed only in the case of reports made by clearly identified persons. Disclosure of the identity by the Whistleblower may take place at any time even after the Report, without prejudice to the protection granted above.

(k) **damage**, including to a person's reputation, particularly on social media, or **economic or financial loss**, including loss of economic opportunities and loss of income;

(l) inclusion on improper lists (e.g. **black lists**) on **the** basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;

m) the **early** termination (termination) or **cancellation of the contract for the supply of goods or services**; **the introduction of detrimental changes** to the service or supply contract;

(n) **cancellation of a licence or permit;**

(o) a request to undergo **psychiatric or medical examinations**.

3.2. Protection from Retaliation

3.2.1 **Complaint to ANAC (in Italy)**

Whistleblowers may **report retaliation they believe they have suffered to ANAC**.

In order to acquire preliminary elements that are indispensable for ascertaining the retaliation, the ANAC may avail itself of the cooperation of the Civil Service Inspectorate and of the INL, within the limits of their respective competences, without prejudice to the exclusive competence of the ANAC as regards the assessment of the elements acquired and the possible application of administrative sanctions.

3.2.2 **Invalidity of Acts**

In the event of non-application or non-observance, even partial, of the Safeguards by the Companies, the Protected Person may invoke, even cumulatively:

- The **nullity ex lege of the acts of retaliation**, resulting in the re-establishment of the situation prior to them.
- **Reinstatement in the employee's job** in accordance with the legislation applicable to the employee, if the Protected Person has been dismissed because of the Report.

In Sweden

Proceedings pursuant to Articles 1 and 2 of Law 2021:890 (i.e. initiated in the face of violation of the prohibition of obstructive or retaliatory measures) will be dealt with in accordance with the Labour Disputes Act (1974:371), even if the measure relates to

1. a person inquiring or looking for work,
2. a person carrying out a voluntary activity,
3. a person undertaking or completing an apprenticeship
4. a person who is otherwise available to carry out or perform work under the control and direction of an operator; or
5. a person who belonged to one of the above categories of persons and who received the information while within the organisation.

In this case, the persons mentioned in points 1 to 5 are also considered workers. The Company Elmo Sweden AB shall be regarded as the employer. This also applies when the dispute negotiation provisions of the Act (1976:580) on co-determination in working life apply.

The following provisions of the Act on Co-Determination in Working Life (1976:580) apply in the above-mentioned cases:

- ✓ Article 64 on the time limit for requesting a hearing,
- ✓ Article 65 on the time limit for bringing an action
- ✓ Article 66 on the extension of the time limit for persons not represented by a workers' organisation, except that the time limit referred to in the first sentence of the first subparagraph of Article 66(1) shall be two months; and
- ✓ Article 68 on loss of the right of action due to prescription

An arbitration agreement concluded before the dispute arose pursuant to Law 2021:890, which provides that the dispute shall be settled by arbitrators without reserving to the parties the right to challenge the award, may not be invoked.

3.2.3 **Burden of Proof**

In Italy

In the context of judicial or administrative proceedings or extrajudicial disputes concerning the ascertainment of the conduct, acts or omissions, constituting Prohibited Retaliation, it shall be presumed that the same have been committed as a result of the Reporting or Public Disclosure.

The burden of proving that they are motivated by reasons unrelated to the Reporting or Public Disclosure lies with the person who has carried them out.

In the event of a **claim for damages submitted to the judicial authorities by the** Whistleblower (and not, therefore, by other Protected Persons), if he/she proves that he/she has made a Whistleblowing Report or a Public Disclosure under the Whistleblowing Decree and has suffered damage, it **shall be presumed, unless proven otherwise, that the damage is a consequence of such** Whistleblowing **Report or Public Disclosure**.

In Sweden

If a person who believes that he or she has been prevented from reporting, or subjected to an attempt to prevent reporting, or subjected to retaliation in breach of the whistleblowing legislation, alleges circumstances that give reason to suppose that this is the case, the burden of proving that such measures have not been taken lies with the defendant.

3.3. Limitations of liability

The Whistleblower shall not be criminally liable, and any further civil or administrative liability, for the disclosure or dissemination of Violation Information is also **excluded**:

- breaches covered by **secrecy** obligations (official, corporate, professional, scientific, commercial or industrial) (examples punished by Articles 326, 622, 623 of the Italian Criminal Code),
- copyright infringements,
- **personal data protection** (privacy) violations,
- violations that offend the reputation of the person involved or reported (Reported)

provided, however, that there were reasonable grounds to believe that the disclosure or dissemination of the same Information was necessary to disclose the Infringement and the Reporting, Public Disclosure or the reporting to the judicial authorities.

The aforementioned criminal, civil and administrative exemption, however, does not apply:

a) in the event of **criminal conduct engaged in by the Whistleblower in order to acquire or access the Information that is the** subject of the Report

(e.g. the offence of unauthorised access to a computer system exists in relation to the act of a person who intentionally hacked into the e-mail system of a work colleague to obtain evidence in support of a report), and

b) **for conduct, acts or omissions not** related to the Report, the judicial report or the Public Disclosure or not strictly necessary to disclose the Violation.

The Companies may also impose **disciplinary sanctions against** persons who decide to retaliate, in accordance with the following documents:

In Italy

- ***National Collective Bargaining Agreement*** and any ***company Collective Bargaining Agreement*** (therefore to be understood as expressly referred to herein), and/or
- ***231 Organisational Model*** adopted, in the event that the conduct of the retaliator is relevant pursuant to and for the purposes thereof.

In other countries

- ***National Collective Bargaining Agreement*** and any ***company Collective Bargaining Agreement*** concluded or approved by a representation or central organisation of employees (therefore to be understood as expressly referred to herein), and/or other similar documents governing the employment relationship;
- any ***additional and/or different company policies governing this matter***.

3.4. Prohibition of transactions (only in Italy)

The rights and protections provided for in favour of the Signatory **may not be waived or settled, in whole or in part,** which shall therefore be deemed invalid, unless they are made in the form and manner provided for in Article 2113(4) of the Civil Code.

4. SUPPORTING MEASURES

In Italy

The Whistleblower is also entitled to **support measures** consisting of **free information, assistance and counselling** on the modalities of Whistleblowing and on the protection from retaliation offered by national and European Union law provisions, on the rights of the Whistleblower, and on the terms and conditions of access to legal aid.

These support measures are provided by Third Sector Entities that have entered into agreements with ANAC. The list of Third Sector Entities is published on the website: https://www.anticorruzione.it/-/whistleblowing.

Such free information, assistance and advice may be requested at any time by the Whistleblower from these Third Sector Bodies, even before the actual communication of the Report.

In Sweden

The local law does not provide for any other measure of support.

5. CONFIDENTIALITY

5.1. Generalities

Alerts may not be used beyond what is necessary to adequately follow them up.

The non-anonymous Whistleblower must be guaranteed confidentiality by the Companies, the Handlers of the Whistleblowing and anyone else involved in receiving and dealing with a Whistleblowing:

- **his identity and** that of **persons close to him facilitating** the Report (right to anonymity), throughout the entire Reporting process, to anyone other than the Reporting Manager, and
- **the content of the Report**, including the **documentation** attached thereto, to the extent that its disclosure, even indirectly, may allow the identification of the Whistleblower.

At all stages of the activity, it is forbidden to **disclose** the identity of the Whistleblower to **the Whistleblower or to other persons not expressly authorised to do so**, **without the** express **consent of** the Whistleblower.

The Internal Reporting Channels adopted by the Company must therefore guarantee the aforementioned confidentiality.

5.2. Exclusion of confidentiality

The obligation of confidentiality does **not apply** in the following cases:

(i) when the **disclosure of** the identity of the Whistleblower is a **necessary and proportionate obligation** imposed by Union or national law **in the context of investigations by national authorities or judicial proceedings**, including for the purpose of safeguarding the rights of defence of the person reported.
To this end, the person reported **must be warned without delay by the Handlers of the Report of an unfounded Report made in bad faith or with gross negligence against him/her** in order to be able to assess whether to exercise any rights against the person reported[7]; or

(ii) the existence of an obligation to communicate the name of the reporter to the **judicial or police authorities**, or

(iii) any **voluntary waiver** in writing of confidentiality at any time by the reporter, or

(iv) if knowledge of the identity of the Whistleblower is indispensable for the **accused's defence**, only if the Whistleblower has expressly consented to the disclosure of his/her identity.

[7] In order to enable the reported person to file a complaint-complaint (if necessary, even against unknown persons) for the offence of slander, defamation or other offences that may be found in the specific case, and also in view of the fact that the reported person may entrust a lawyer with the task of carrying out "preventive defensive investigations" (pursuant to Articles 327 bis and 391 nonies of the Code of Criminal Procedure, institutes that may also serve the person unjustly accused of a crime to identify the identity of the person who made an anonymous report against him/her).
On the other hand, the protection of the Whistleblower's confidentiality must be ensured where he/she is not in bad faith; in fact, the purpose of 'whistleblowing' could be frustrated if it expressly provided for the disclosure to the Whistleblower of an unfounded but not in bad faith report, especially in the case of minor negligence (not punishable even at disciplinary level, but theoretically - although it is rare - actionable in civil law).

In any case, the Whistleblower **must be informed in writing** by the Handlers of the Report or by the competent authority of the reasons for **disclosing** confidential data **before his/her identity is disclosed**, unless this would prejudice the relevant investigation or judicial proceedings[8].

The Companies, the Handlers of the Report and anyone else involved in the receipt and processing of a Report also have to protect **the identity of the Persons involved and of the other persons mentioned in the Report** until the conclusion of the proceedings initiated on account of the Report, in compliance with the same guarantees of confidentiality provided for in favour of the Whistleblower.

6. PREREQUISITES FOR PROTECTION. UNFOUNDED, BAD FAITH OR GROSSLY NEGLIGENT REPORTING

Protection Measures apply if the following **conditions are** met:

(a) at the time of the Report or Complaint to the Judicial Authority or Public Disclosure, the Whistleblower had **reasonable grounds to believe that the** Violation **Information** reported or publicly disclosed **was true** and fell within the objective scope of Section 2.3;

(b) the **Report** or Public Disclosure **was made on the basis of the provisions of this procedure**.

The Protection of Protected Subjects also exists in the event of a **Report or Disclosure that later turns out to be unfounded**, if the Whistleblower, at the time of the Report or Public Disclosure, had **reasonable grounds to believe that the Report was necessary to disclose the Violation** and the Report or Public Disclosure or report to the judicial authority that the Information was within the scope of this Procedure.

Safeguards in favour of the Protected Subjects are not guaranteed, and a disciplinary sanction is also imposed on the Whistleblower, when it is **ascertained, even by a judgment of first instance,**

i) **the criminal liability** of the Whistleblower **for offences of slander or defamation** in relation to the facts reported, or

ii) the Whistleblower's **civil liability, for the same reason** (pursuant to Article 2043 of the Civil Code, which provides for the right to compensation for damages in favour of anyone who is the victim of an extra-contractual damage caused by a third party), in cases of **wilful misconduct or gross negligence**.

Reports made in the **knowledge of** the **abuse/exploitation of** the Reporting procedure, e.g. those that are manifestly unfounded, **opportunistic** and/or made for the **sole purpose of harming** the reported person or other persons mentioned in the Report (employees, members of corporate bodies, suppliers, partners, group companies, etc.) shall be considered in **bad faith/grievous misconduct** (and therefore a source of liability, in disciplinary and other competent fora).

8 When informing the Whistleblower as above, the competent authority shall send him/her a written explanation of the reasons for disclosing the confidential data in question.

In the event of a **Public Disclosure,** the Whistleblower benefits from Legal Protection if, in addition to the basic condition, one of the Public Disclosure Prerequisites set out in Chapter 3.3.2.2 of the Procedure is also fulfilled.

APPENDIX C - PROCESSING OF PERSONAL DATA

1.1 Any processing of personal data carried out for the purpose of handling the Report must be carried out in accordance with the legislation on the protection of personal data (GDPR, Supervisory Measures, Legislative Decree 196/2003)[9] .
Accordingly, anyone involved in the receipt and processing of non-anonymous Reports **is required to comply with all the procedures, protocols and written security instructions laid down in the** Companies' **privacy system**, without prejudice to the further rules laid down in this procedure.

1.2 **Personal data that appear to be not reasonably relevant and useful for the processing of a specific Report shall not be collected or, if received or collected accidentally, shall be promptly deleted** by the Case Manager(s).

1.3 The aforementioned processing operations must be carried out by the Company (data controller) in compliance with the general principles set out in Articles 5[10] and 25[11] of the GDPR, and by taking appropriate measures to protect the rights and freedoms of the data subjects.

1.4 The ESG Function, in coordination with the IT Function:

- defines, by means of this procedure and the annexes thereto, its own model for receiving and managing Internal Reports, identifying technical and organisational measures suitable for ensuring a level of security appropriate to the specific risks arising from the processing operations performed,
- carries out the Data Protection Impact Assessment (DPIA) carried out by the Privacy Function itself, and

---

[9] E, by the competent authorities for the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, of Directive (EU) 2016/680.
10 1. Art. 5 GDPR: Personal data are:
(a) processed lawfully, fairly and transparently vis-à-vis the data subject ('lawfulness, fairness and transparency');
(b) collected for **specified, explicit and legitimate purposes,** and subsequently processed in a way that is not incompatible with those purposes ('purpose limitation');
(c) **adequate, relevant and limited to what is** necessary in relation to the purposes for which they are processed ('data minimisation');
(d) **accurate** and, where necessary, **kept up to date**; all reasonable steps must be taken to delete or rectify in a timely manner data that are inaccurate in relation to the purposes for which they are processed ('accuracy');
(e) **kept in a** form which permits identification of data subjects **for no longer than the purposes** for which they are processed ('limitation of storage');
(f) processed in such a way as to **ensure appropriate security of** personal data, including protection, by appropriate technical and organisational measures, against unauthorised or unlawful processing and accidental loss, destruction or damage ('integrity and confidentiality')
11 Art. 25 GDPR: Article 25 Data protection by design and data protection by default
1. Taking into account the state of the art and the cost of implementation, as well as the nature, scope, context and purposes of the processing, and taking into account the risks to the rights and freedoms of natural persons represented by the processing which are likely and likely to vary in severity both when determining the means of the processing and at the time of the processing itself, the controller shall implement appropriate technical and organisational measures, such as pseudonymisation, to implement effectively the principles of data protection, such as minimisation, and to integrate in the processing the necessary safeguards in order to meet the requirements of this Regulation and to protect the rights of data subjects.
2. The controller shall implement **appropriate technical and organisational measures** to ensure that only personal data necessary for each specific purpose of the processing are processed by default.
This obligation applies to the amount of personal data collected, the scope of processing, the storage period and accessibility. In particular, these measures ensure that, by default, personal data are not made accessible to an indefinite number of natural persons without the intervention of the natural person.

- governs the relationship with any external suppliers that process personal data on behalf of the Company(s) pursuant to Article 28 of the GDPR (e.g., external Reporting Manager(s) designated by the Company, third-party Portal/Software Managers);
- provides, and/or identifies the different corporate functions responsible for providing, appropriate information to the Whistleblower and the Persons concerned (pursuant to Articles 13 and 14 of the GDPR).

1.5 The Reporting Managers shall ensure that Internal Reporting Channels other than the 'Portal/Software' are set up and operated in a secure manner that guarantees the confidentiality of the identity of the Whistleblower and any third parties named in the Report and the protection of the Report from the risk of unauthorised access, loss of integrity and/or availability.

The security measures applied to the Portal/Software are set out in the Contract between the Companies and the third party provider of the same, and in the related documentation, including ***Admin Manuals*** and ***Case Manager (Appendix E)***.

Configuration of the basic functionality of the Portal/Software is the responsibility of the designated Admin role(s), while technical maintenance is the responsibility of the third-party provider of the Portal/Software (EQS/Adacta).

1.6 It is understood that this Procedure also represents, pursuant to and for the purposes of Article 13 paragraph 5 of the Whistleblowing Decree, an internal agreement between the Group Companies, aimed at

i) regulate the **sharing of resources** (e.g. Portal/Software) for the receipt and management of Reports and

ii) determine their respective **responsibilities** with regard to compliance with data protection obligations, pursuant to Article 26 of the GDPR, as follows:
   - **privacy**: each company acts as a co-owner with regard to the processing of data related to:
     - **sharing the** internal reporting **channel** consisting of the Saas Integrity Line Portal/Software; and
     - the **Whistleblowing Procedure** for the communication/collection and management of reports.
   - **information to interested parties pursuant to Art. 13** GDPR:
     a) The privacy notice to Whistleblowers is made available to the data subject by the relevant Whistleblower Managers, as follows:
        - ✓ by means of a special link/text viewable on the landing page, if the reporter (even anonymous) **uses the Portal/Software** to send the Report;
        - ✓ by hand delivery, at the earliest opportunity, in the case of a **personal meeting** with the Whistleblower not preceded by the use of the Portal/Software for sending the Report;
        - ✓ if the Whistleblower **telephones** the Company to make the Report: by means of a verbal notice to the Whistleblower about the availability of the Information on the Portal/Software;

- ✓ by means of a specific document/link/viewable hypertext made available within the Secure Inbox, if the **Report is anonymous** and is received by the Company through an **offline** mode (e.g. personal meeting) and is then **entered autonomously in the Portal/software by the person receiving the Report**;

b) the privacy notice to Affected Persons (natural persons charged with the reported Violation) is made available to the data subject by the Reporting Managers, in the following manner:
   - ✓ by hand delivery, at the earliest opportunity, in the case of a **personal meeting** with the person concerned;
   - ✓ by means of a special link/text viewable on the landing page, if the Involved Party **uses the Portal/Software** to interact with those evaluating the Report;
   - ✓ in the event that the contact with the Involved Party is made by **telephone**: by verbal notice to the Whistleblower of the availability of the Information Notice on the Portal/Software;

- **response to the exercise of the data subject's rights**: each company acts as an independent data controller, in accordance with its own procedures for handling the exercise of data subjects' rights, to which reference is made here;
- **personal data breaches**: each company acts as an independent data controller in accordance with its own data breach management procedures, to which reference is made here ;
- **security measures**: each Group Company is required to comply with the security measures provided for by i) this Procedure, ii) the functional specifications of the Portal/Software, ii) its own privacy system, iv) the data protection legislation applicable to it;
- **Operational interface with the third party supplier of the Portal/Software**: the Parent Company acts as a centralised technical interface to the supplier, on behalf of the other Group Companies, on the basis of a mandate with representation to be understood as conferred herein.

APPENDIX D - TRAINING

Training, communication and information activities (i) represent an indispensable component for the effective implementation of the Whistleblowing organisational model, (ii) constitute proof of the real will of the entity to be an active part of the prevention of the offences subject to whistleblowing, on the other hand, (iii) stimulate the cooperation of individuals in the effective realisation of the objective of legality.

The person in charge of this Procedure must make easily accessible to the entire organisational structure - in a manner differentiated according to the role of the users - clear information about, at the very least, the prerequisites and procedures for reporting violations, the protections afforded to whistleblowers and the limits of such protections.

The HR Department, in agreement with the Head of this Procedure, draws up and periodically updates a ***Whistleblowing Training Plan*** which forms an integral part of this Appendix.

APPENDIX E - PORTAL/SOFTWARE MANUALS

- ***Admin User Manual***
- ***User Case Manager Manual***
- ***Synoptic table "Manual Entries" vs "Privileges/accesses in the back-end".***