

WHISTLEBLOWING PROCEDURE



RINO MASTROTTO

1. Summary

2. PURPOSE AND OBJECT.....	3
3. DEFINITIONS AND SCOPE.....	4
3.1. Definitions	4
3.2. Subjective Scope.....	9
3.3. Objective Scope of Application	11
4. REGULATION OF ACTIVITIES	13
4.1. Generalities	13
4.2. Subject of the Report	13
4.3. Types of alerts.....	13
4.4. Handlers of Alerts	18
4.5. Examination of alerts.....	21
4.6. Preliminary investigation.....	23
4.7. Actions following the Report	28
5. CONSERVATION	31
6. LEGAL PROTECTION	31
7. TRAINING	31
8. DISTRIBUTION	32
9. DISCIPLINARY MEASURES AND SANCTIONS	32
10. OTHER	33
11. MODIFICATIONS.....	33
APPENDIX A - SECTORAL VIOLATIONS	34
APPENDIX B - SAFEGUARDS.....	42
APPENDIX C - PROCESSING OF PERSONAL DATA.....	56
APPENDIX D - TRAINING	59
APPENDIX E - PORTAL/SOFTWARE MANUALS.....	59

2. PURPOSE AND SUBJECT MATTER

The purpose of this Whistleblowings Management Policy (hereinafter, the "**Policy**" or "**Procedure**") is to define and establish an adequate and efficient model for the operation of the Internal Information System (or "**Whistleblowings Management System**") that enables the receipt and processing of notifications of acts or omissions that may constitute Sectoral Violations, in accordance with

- the relevant legislation DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2019 on the protection of persons who report breaches of Union law (hereinafter, the "**Whistleblowing Directive**") (only for company with the RINOI MASTROTTO group based in the UE), and
- to Legislative Decree 24/2023 (only for Italy),
- the ANAC Guidelines (only for Italy),
- the Act 2021:1890 (only for Sweden), or
- the legislation on whistleblowing applicable from time to time in the different country in which the RINO MASTROTTO Group Company involved in the Report of a Violation is based.

This Procedure does not limit the protection that applies on the basis of other laws, regulations or other regulatory sources of non-EU states.

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

The purpose of this Policy is to **ensure the professional, confidential, impartial handling and adequate protection of the rights of data subjects** throughout the process of making, handling, processing, investigating and resolving Reports made through the Company's Internal Reporting Channel.

This Procedure **governs** the roles, processes and means of operation of the Company's Internal Reporting Channel, so as to **regulate matters relating to Reports made by Whistleblowers, as well as their handling and resolution** by the Case Managers.

The procedures for the processing, investigation and resolution and, in general, the management of the Reports received pursuant to this Procedure shall be governed by the utmost **objectivity and independence**, establishing in this Procedure the corresponding mechanisms in order to avoid the concurrence of possible conflicts of interest.

Furthermore, the rights to be informed of the actions or omissions attributed and the presumption of innocence of the Persons Concerned are guaranteed by this Procedure.

3. DEFINITIONS AND SCOPE OF APPLICATION

3.1. Definitions

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

ANAC - Autorità Nazionale Anticorruzione (or Competent Authority)	<i>Independent Italian administrative authority designated to i) receive External Reports and ii) carry out the functions provided for by the Directive, including the feedback to the Whistleblower, in particular with regard to the Follow-up given to the Reports, and the imposition of any sanctions, in the cases provided for by the applicable legislation</i>
Sectorial Acts	<i>Regulatory acts identified in Appendix A of this Procedure</i>
Reporting Channels	<i>Channels for making Reports, made available to the Whistleblower, respectively, by the Company, in the case of an Internal Report, or by the ANAC in the case of an External Report; Internal Reporting Channels are in turn defined as Internal or External depending on whether they are managed directly by the Company or by third parties authorised by it</i>
Reporting Committee	<i>Collegial body composed, for each Company, of: - the Supervisory Body 231 of RINO MASTROTTO GROUP S.P.A. or, if the reported Violation 231 concerns another Company of the RINO MASTROTTO Group which has designated its own Supervisory Body, the latter Body, - the HUMAN RESOURCES Manager of the Parent Company RINO MASTROTTO GROUP S.P.A., - the DPO of the Parent Company RINO MASTROTTO GROUP S.P.A. or, if the Violation concerns the legislation on the protection of personal data and concerns another Company of the RINO MASTROTTO Group which has designated its own DPO, the latter DPO, - the HR Manager of ELMO SWEDEN AB (if the Violation concerns the same Company), - any additional Case Managers appointed by any Company from time to time</i>
Work context	<i>Work or professional activities, present or past, carried out in the context of legal relations, through which, regardless of the nature of such activities, a person acquires information about Violations and in the context of which he/she could risk being retaliated against in the event of a Whistleblowing or Public Disclosure or a report to the Judicial Authority</i>
Whistleblowing Decree	<i>Legislative Decree 24/2023 implementing the Whistleblowing Directive in Italy</i>
Public Disclosure	<i>Placing information on Breaches in the public domain through the press or electronic media or in any case through means of</i>

	<i>dissemination capable of reaching a large number of people (e.g. radio, television, blogs, Internet, automated e-mail campaigns)</i>
Whistleblowing Directive	<i>EU Directive 2019/1937 on the protection of persons who report breaches of Union law</i>
Data Protection Officer	<i>The Data Protection Officer designated by RINO MASTROTTO GROUP SPA or, as the case may be, by another company of the RINO MASTROTTO group, pursuant to and for the purposes of Articles 37, 38 and 39 of the GDPR</i>
Third Sector entities	<i>Entities that have entered into agreements with ANAC to provide the specific Support Measures for which they are responsible under the Whistleblowing Decree. They never take on the role of Facilitator.</i>
Facilitator	<i>A natural person who assists a Whistleblower in the Whistleblowing process, operating within the same work context and whose assistance must be kept confidential, including a trade unionist if he assists the Whistleblower in his name and on his behalf, without using the trade union's initials</i>
FCA - False Claim Act	<i>A U.S. federal law designed to combat fraud against the U.S. government. It applies to anyone who submits false claims for payments or reimbursements to the U.S. government or uses artifice/deception to obtain public funds. It allows private citizens (called "relators") to sue on behalf of the government against those who committed the fraud.</i>
Case Manager(s)	<i>Person(s) designated under this Procedure to receive the Report and/or carry out the further management activities of the Report as set out in this Procedure</i>
GDPR	<i>EU Data Protection Regulation 679/2016</i>
Breach Information	<i>Information, including reasonable suspicion, concerning: (i) Violations committed or which, on the basis of concrete evidence, could be committed in the organisation with which the Reporting Person or the person making the complaint to the judicial or accounting authority has a legal relationship; and (ii) information concerning any conduct aimed at concealing such Breaches</i>
IRS	<i>Internal Revenue Service - Whistleblower Office - ICE, a U.S. public law entity, located at 1973 N Rulon White Blvd., M/S 4110, Ogden, UT 84404</i>
Whistleblowing Privacy Policy	<i>Disclosure by the Company to Data Subjects pursuant to Articles 13-14 of the GDPR</i>
Act 2021:890	<i>Sweden Act on the Protection of Persons Reporting Irregularities (in Swedish: Lag 2021:890 om skydd för personer som rapporterar om missförhållanden)</i>
ANAC Guidelines	<ul style="list-style-type: none">• ANAC Guidelines on the protection of persons who report violations of Union law and the protection of persons who report violations of national laws - Procedures for the submission and

	<p><i>management of external reports (approved by resolution No. 311 of 12 July 2023 - Outline of new guidelines on whistleblowing 07 November 2024), and</i></p> <ul style="list-style-type: none"> <i>• Regulations for the management of external whistleblowing and for the exercise of ANAC's sanctioning power in implementation of Legislative Decree 24/2023 (approved by Resolution No. 301 of 12 July 2023).</i>
Protection measures	<i>Measures provided for in paragraph 2 of Appendix B of this Procedure</i>
Support measures	<i>Measures provided for in paragraph 6 of Appendix B to this Procedure</i>
Organisational Model 231	<i>Organisational, Management and Control Model possibly adopted by a Company in Italy, pursuant to Italian Legislative Decree No. 231/2001, as amended</i>
Supervisory Board 231 (or "SB 231")	<i>Supervisory Body appointed by the Company in relation to the Organisational Model 231</i>
OSHA	<i>Labor Department's Occupational Safety & Health Administration, a U.S. public law body, located at 200 Constitution Ave NW, Washington, DC 20210, tel. 800-321-6742, 18003216742, reachable at https://osha.gov and call center https://www.dol.gov/general/contact/contact-phone-call-center#tty</i>
Involved (or Reported) Person	<i>Natural or legal person to whom is attributed, through or during the course of the Public Report or Disclosure or complaint to the Authority the responsibility in any capacity for the Violation reported or publicly disclosed or denounced</i>
Portal/Software	<i>The third-party cloud portal, accessible on the Internet at https://rmg.whistleblowing.integrityline.com, including user usable functionalities and its secure database</i>
Procedure	<i>This document</i>
Procedures	<i>The set of directives, instructions, protocols and written procedures provided for and implemented by the Company in order to prevent Violations, and/or to reduce their consequences or recurrence</i>
Legal relationship	<i>Legal relationship between the Whistleblower and the organisation in which a Breach 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).</i>
Register of Reports	<i>Software in which to register reports</i>
Feedback	<i>Communication to the Whistleblower of information on the Follow-up given or intended to be given to the Report, including the acknowledgement of receipt of the Report</i>

Retaliation	<i>Any conduct, act or omission, even if only attempted or threatened, carried out by reason of the Report or of the denunciation to the judicial authority or of the Public Disclosure and which causes or may cause to the person making the Report or having made the Report, directly or indirectly, an unjust damage</i>
Administrative sanctions	<i>Administrative pecuniary sanctions applicable (i) by the ANAC against the cases of non-compliance provided for by the Whistleblowing Decree, or (ii) by another public Authority against the cases of non-compliance provided for by local whistleblowing legislation</i>
Disciplinary sanctions	<i>Disciplinary sanctions applicable by the Company in the event of non-compliance with the provisions of this Procedure</i>
Whistleblower	<i>Natural person, who makes the Report or Public Disclosure of Information on Violations acquired in the context of his or her own work context</i>
External Reporting	<i>Disclosure of Information on Violations by the Reporting Party submitted through the Reporting Channel activated by ANAC or by another public competent Authority according to the whistleblowing legislation applicable from time to time to the Report</i>
Internal Reporting	<i>Communication of Information on Breaches, submitted through the Reporting Channels made available by the Company</i>
Follow-up	<i>Action taken by the Reporting Manager or the Reporting Committee to assess the existence of the facts reported, the outcome of the investigation and any measures taken</i>
Internal Information System	<i>Portal/Software</i>
Company	<i>Each Company indicated in Art. 3.2.1</i>
Private Sector Subjects	<i>Subjects, other than those falling within the definition of Public Sector Subjects</i>
Public Sector Subjects (Italy)	<ul style="list-style-type: none"> • <i>Public Administrations referred to in Article 1(2) of Legislative Decree No. 165/2001</i> • <i>Public Economic Bodies</i> • <i>Bodies governed by public law referred to in Art. 3, co. 1, lett. d), Legislative Decree 50/2016,</i> • <i>Public service concessionaires,</i> • <i>Publicly controlled companies referred to in Art. 2, co. 1, lett. m) Legislative Decree 175/2016, even if listed,</i> • <i>In-house companies referred to in Art. 2, co. 1, lett. o) of Legislative Decree 175/2016, even if listed</i>
External Parties	<i>Reporting Parties other than Internal Parties</i>
Internal Persons	<i>Whistleblowers defined as internal in this Procedure</i>

Protected Persons	<i>The persons referred to in paragraph 1 of Appendix B of this Procedure, who may benefit from the Safeguards.</i>
TFEU	<i>Treaty on the Functioning of the European Union</i>
Safeguards	<i>The set of Protection and Support Measures provided for Protected Persons under the applicable legislation</i>
231 Violations	<p><i>Acts or omissions which harm the public interest or the integrity of the Company and which consist of</i></p> <p><i>a) unlawful conduct relevant under Legislative Decree 231/2001 (i.e. the commission of predicate offences or the reasonable danger of the commission of predicate offences, provided for by Italian Legislative Decree 231/01 on the administrative liability of companies (so-called "231 offences"), or</i></p> <p><i>b) violations of the rules of conduct/procedures/protocols issued by the Company and/or any violation of the 231 Model,</i></p> <p><i>o</i></p> <p><i>c) that frustrate the object or purpose of the regulations set out in Legislative Decree 231/2001, including any attempts to conceal such violations,</i></p> <p><i>which have occurred or which are very likely (on the basis of concrete elements) to occur in the organisation (possibly even other than the Companies, e.g. a supplier of the same) with which the Reporting Person has a legal relationship, including any conduct aimed at concealing such violations;</i></p>
Violations of Sectorial Acts	<p><i>Behaviours, acts or omissions detrimental to the public interest or the integrity of the Company and consisting of offences falling within the scope of the Sectorial Acts identified in <u>Appendix A</u>, which have occurred or which are very likely (on the basis of concrete elements) to occur in the organisation (possibly even other than the Company, e.g. a supplier of the same or a contact person of an auditing firm of the same) with which the Reporting Person has a legal relationship, including any conduct aimed at concealing such violations, regardless of whether</i></p> <p><i>- the employment relationship with the Company has ended in the meantime (so-called former employee), or that</i></p> <p><i>- the facts have been learnt during the selection process (e.g. candidate) or in other phases of pre-contractual negotiations with the Company, regardless of whether, under national law, Whistleblowing Violations are administrative violations, criminal violations or violations of purely civil law (e.g. risk of damages).</i></p>

3.2. Subjective scope of application

3.2.1. This procedure, subject to approval by the competent administrative body. applies to 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
- **CONCERIA SUPERIOR SPA**, with registered office in Via San Tommaso 72 - 56029 Santa Croce Sull'Arno (PI), Italy
- **JACQART SRL**, with registered office in Via Roma 76 - 23892 Bulciago (LC), Italy
- **MAPEL TEXTILE SRL** with registered office in Via Vajone 12 - 21020 Galliate Lombardo (VA), Italy
- **MAPEL COMPONENTS SRL** with registered office in Via Vajone 12 - 21020 Galliate Lombardo (VA), Italy
- **MANIFATTURA TACCA SRL** with registered office in Via Vajone 12 - 21020 Galliate Lombardo (VA), 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**, with registered office 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
- **TANNERIE LIMOGES SAS**, with registered office at 65 Rte de Périgueux, 87170 Isle, France.

3.2.2. In relation to each Company, this procedure applies:

- to persons who make i) Internal and/or External Reports or ii) Public Disclosures or iii) Complaints to the judicial authorities, in relation to **Sectorial Violations**;
- to persons who make Internal Reports or Reports to judicial authorities in relation to **231 Violations**;
- to other Protected Persons;
- other categories of Interested Parties whose data are processed in relation to Reports managed by the Company.

3.2.3. Whistleblowers may belong to the following categories:

ID	Subject Category	Subject Nature
A	Company employees , including casual workers, regardless of their position within the Company, the legal nature of their relationship and the area of activity or hierarchical level	Internal whistleblower
B	Paid and unpaid volunteers and trainees working for the Company	Internal whistleblower
C	<p>Self-employed workers, including self-employment relationships that have a special discipline pursuant to Article 2222 of the Italian Civil Code (work contract) (including freelancers and consultants working for the Company, <i>such as intellectual professions for which registration in special registers or lists is required, such as psychologists, architects, surveyors, etc.</i>).</p> <p>as well as</p> <p>Holders of a collaboration relationship referred to in Article 409 of the Italian Code of Civil Procedure, who carry out their work activity at the Company, by which is meant</p> <ul style="list-style-type: none"> ✓ those of private subordinate employment, even if not inherent to the exercise of a business (<i>e.g. domestic work, home work</i>) ✓ agency, commercial representation relationships; and ✓ other collaborative relationships resulting in the provision of continuous and coordinated work, mainly personal, even if not of a subordinate nature <p><i>e.g. lawyers, engineers, social workers, who provide their work for the company by organising it autonomously (para-subordinate relationship)</i></p>	External whistleblower
D	Employees and collaborators , who work for third parties Public or private sector subjects that supply goods or services or carry out works in favour of the Company	External whistleblower
E	Shareholders (if natural persons)	External whistleblower
F	Members of the administrative and/or management or representative body of the Company, including non-executive members (e.g. directors without or with delegated powers), even when such functions are exercised on a de facto basis	Internal whistleblower
G	<p>Members of the control or supervisory body of the Company (e.g.</p> <p>Statutory Auditors,</p> <p>Auditors or Auditing Firme,</p> <p>DPO - Data Protection Officer)</p>	<p>Statutory auditor, Auditor or contact person of auditing firm: External whistleblower</p> <p>DPO: Internal whistleblower</p>

In Italy

Even those who are no longer part of one of the categories of persons under A-B-C-D-E-F-G but who received or acquired the Information while they were within the Company or had a terminated legal relationship with it, may validly make the Report.

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

In Sweden, Brazil, Mexico and U.S.

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 carry out, any of the activities under A-B-C-D-E-F-G, may also make the Report, if they have acquired the Information while in contact with the Companies for that purpose.

3.3. Objective scope

The Whistleblower is obliged to communicate Information on Violations that is well substantiated and based on precise (adequately detailed) and concordant facts, and not facts of generic, confusing and/or blatantly defamatory or slanderous content.

Reports **may also be anonymous**, i.e. they may not mention 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.

They will not be taken into consideration, and will result in exclusion from the Safeguards provided for by this Procedure:

a) **disputes, claims or requests linked to a personal interest of the Whistleblower** or of the person who has filed a complaint with the judicial authorities or has made the Public Disclosure, **which relate exclusively to his/her individual employment relationships, or inherent to his/her employment relationships with hierarchically superior figures**

(e.g. reports concerning labour disputes, discrimination between colleagues, interpersonal conflicts or involving only the Reporting Person and another worker or the persons to whom the Report or Public Disclosure or complaint relates), and

b) **information contained in Reports that have already been rejected** by any Internal Reporting Channel or by the ANAC, and

c) **information already fully available to the public** or which constitutes mere **hearsay**, and

d) information that relates to **acts or omissions not expressly covered** by this Procedure.

This is without prejudice to:

- the application of 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 repression of anti-union conduct (e.g., by way of example but not limited to, Article 28 of Law 300/1970, as amended - Workers' Statute), and

- the application of the provisions of criminal procedure (**if the Whistleblower has information about a criminal offence, he may always lodge a complaint with the competent criminal authority**).

All Reports sent through the Internal Reporting Channel must be made in good faith.

This means that, at the time of submission, the reporting person must have reasonable and sufficient grounds to believe that the information provided is true, accurate and has not been obtained through potential violations (e.g. criminal offences).

In this sense, **malicious or grossly negligent reporting may give rise to the relevant sanctions by the Company**, without prejudice to the civil and criminal liabilities that may arise therefrom.

4. REGULATION OF ACTIVITIES

4.1. Generalities

Reporting is

- a) **mandatory**, on the part of **Internal Parties** (NB. by virtue of the **general duties of loyalty, diligence and good faith** connected to the legal relationship with the Company, to be understood as expressly reaffirmed herein);
- b) **mandatory**, on the part of the **External Parties** who **are contractually obliged** towards the Company to report;
- c) **optional**, on the part of **Persons External** to the Company who are not under a contractual obligation towards the Company to report.

4.2. Object of the Report

In order to facilitate and allow the due verification and preliminary investigation activities by the Company, also in order to ascertain whether the Report is well-founded, the Report must contain at least the **following information**

- **identity** of the Whistleblower (name, surname, number of a valid identity document), unless he/she intends to remain anonymous;
- **relationship** with the Company (candidate, employee/collaborator, director, shareholder, supplier/consultant, partner, etc.) and, if applicable, **position/qualification/company position** of the Whistleblower;
- as clear, detailed and complete **a description** as possible **of the facts** that are the subject of the Report;
- **the circumstances of time and place** in which the facts were committed, if known;
- identity of the **person to whom the violation is attributed** (so-called " Involved Person ") or elements useful to identify him/her (area/position/qualification/assignment), if known;
- indication of any **other persons who can report** on the facts that are the subject of the Report;
- indication of any **documents** that may confirm the truthfulness of the facts that are the subject of the Report;
- description of the **reasons** connected with the work activity carried out that made the reported facts known;
- any other **information** that may provide useful **evidence of the existence of the facts** reported;
- if applicable, a **means of communication** with the Whistleblower other than the Portal/Software (e-mail address, telephone or other) so that the Reporting Committee can communicate with the Whistleblower.

If, having assessed the content of the Report, it turns out to lack the minimum mandatory requirements for its proper assessment, the Reporting Committee will proceed to request the corresponding information and/or documentation from the Whistleblower through the communication methods indicated by the latter, proceeding as per Chapter 4.5.1 in the event that the necessary information is not available for the opening of the investigation phase.

4.3. Types of Reporting

4.3.1. Internal Reporting Channels

In Italy, the Internal Reporting Channels must be activated **after compulsorily informing the trade union representatives (RSA/RSU)**. Any comments made by the trade union have the value of a non-binding opinion.

In Sweden, according to the Employment (Co-determination in the Workplace) Act – Lag (1976:580), when implementing Internal Reporting Channels, the Company must **inform** and, **when requested, negotiate with the trade union** regarding the implementation of the whistleblowing system; ii) although the law does not impose a strict obligation of mutual approval, trade union involvement is generally expected as advisable.

The law stipulates that through a **collective agreement signed or approved by a central workers' organisation**, it is possible to **derogate from Articles 2–9 of Chapter 5 of Act 2021:1890**, which concern internal channels and reporting procedures, **provided that the rights of the whistleblower** established by Whistleblowing Directive are not removed or substantially restricted.

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

4.3.1.1. Communication of the Report

The following Internal Reporting Channels may be used by the Whistleblower:

- ✓ **ELECTRONIC**:
Portal/Software, accessible at https://rmg_whistleblowing.integrityline.com
- ✓ **ORAL** (*at the request of the Reporting person or if deemed useful and possible by the Reporting Manager(s) while respecting the Reporting person's wish for anonymity*): **Personal/direct meeting** with one or more Reporting Manager(s), also via remote videoconference session, if any.

The Case Managers ensure in this case, **subject to the consent of** the Whistleblower, that

- the meeting takes place **within a reasonable time** from the date of the said request, and
- a complete and accurate **record** of that meeting is **kept on a durable medium** that **allows access** to the Breach Information.

The Whistleblowing Committee is obliged to **document** the meeting **by** keeping **detailed minutes** of the meeting.

The Whistleblower has the right and obligation to **verify, rectify and approve the minutes** by his/her signature.

NB1: In the event that the companies decide at any time to activate any oral reporting channels other than and/or in addition to the direct personal meeting (e.g. voice messaging, telephone lines, etc.), it is understood that the oral channels will be reciprocal and not cumulative to the direct meeting. Only in such a case, the Whistleblowers' Committee may assess at its own discretion which oral channel to use towards the Whistleblower.

NB2: The use of electronic mail (ordinary or certified) must be considered in itself inadequate to guarantee the confidentiality of the identity of the Reporting person, given the peculiar system of logs associated with it.

✓ CARDS

In Italy:

- **Closed paper envelope** marked "**Confidentiality of personnel for the Whistleblowers' Committee**" on the outside, to the ordinary mail address: RINO MASTROTTO GROUP S.p.A., Via dell'Artigianato, n. 100, Trissino (VI) - Italy.

The secretarial staff receiving the envelope in the first instance are strictly forbidden to open it and must immediately deliver it to the Reporting 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).

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

HR personnel who receive 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 **diligently kept in a locked safe place** (room, cupboard, or drawer).

In countries other than Italy

The above paper communication should be addressed to the head office of the Company to which the Violation to be reported relates.

4.3.1.2. Reporting to erroneous person

Report to erroneous person

If **a person other than the competent Whistleblowings Committee** (e.g. the secretary/receptionist) **receives a Whistleblowing Report**, he/she must forward it to the competent Case Managers, within 7 (seven) days from its receipt, complete with any supporting documentation received, not retaining any copy and refraining from taking any independent initiative for analysis and/or investigation, and guaranteeing the confidentiality of the same at all times.

Failure or delay on the part of the first recipients of the Report to communicate it to the competent Managers constitutes a serious breach of this Procedure, as such punishable by disciplinary sanctions.

Reporting to more than one internal person

If **the Report is sent, at the same time, to several persons, all internal to the Company**, the Report must be considered as a Report sent to a non-competent person. Therefore, the person(s)

in charge of receiving such Reports should forward them, within 7 days from their receipt, to the competent internal subject, simultaneously notifying the Reporting Party.

Reports also sent to several external subjects

If, on the other hand, **the Report is sent not only to the internal subject in charge of handling it, but also to several persons outside the Company**, the Whistleblower should be asked for clarification of the circumstances that led to the Report, in order to ascertain whether the reporting person intended to proceed directly to public disclosure.

In such a case, given that there are no conditions for considering that the Internal Reporting was carried out correctly (since the reporting person chose not to turn solely and exclusively to the internal person in charge of handling the report), it is necessary to understand whether the Reporting can be qualified as a Public Disclosure and to ascertain whether or not one of the conditions set out in Article 15 of the Whistleblowing Decree itself is met.

4.3.2. External Reporting and Public Disclosure

4.3.2.1. External Reporting

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

- a) there is no mandatory activation of any Internal Reporting Channel within its working context, or
- b) the Internal Reporting Channel, even if theoretically envisaged as compulsory by the Company, **is not in fact active or, even if activated, does not comply with** the regulatory indications; or
- c) the Internal Reporting already carried out by the Whistleblower **has not been followed up**; or
- d) the Whistleblower has **well-founded reasons to believe** that, if he/she were to make an Internal Report, it would not be effectively followed up, or that the Report might give rise to the **risk of retaliation**; "well-founded reasons" should be understood as the presence of concrete factual elements, and not merely and generically feared, supporting the expectation of suffering Retaliation; or
- e) the Whistleblower has well-founded reasons to believe that the Breach may constitute an **imminent or obvious danger to the public interest**.

The External Report to the ANAC is made

- **in writing** through the Reporting Channel activated by ANAC (for further information on the contacts and instructions on the use of the External Reporting Channel, on the confidentiality regime applicable to External Reports, on the process for handling External Reports and any Retaliation, please consult the ANAC Guidelines available on the website <https://www.anticorruzione.it/-/whistleblowing>), or
- **orally** through (i) **telephone lines** or (ii) **voice messaging systems** or, (iii) at the request of the Reporting Person, through a **face-to-face meeting** set within a reasonable time.

4.3.2.1.1. Sweden

There is no requirement to use Internal rather than External channels or that reporting via External Channels must have been preceded by reporting via Internal Channels.

An External Report may be submitted directly to the following competent authorities, depending on the type of Breach to be reported:

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

4.3.2.1.2. Brazil and Mexico

No External Signalling channel is set forth by the local laws.

4.3.2.1.3. U.S.A.

The following External Reporting channels are active:

- **OSHA** channel, for Violations of **OSHA** regulations, as listed in **Appendix A**
- **IRS** channel, for Tax Violations as provided for and punished by the **Internal Revenue Act**, as listed in **Appendix A**,
- **DOJ** Channel for Violations contemplated and punished by the **Foreign Corrupt Practices Act**, as listed in **Appendix A**.

For details on how to use the External Reporting channels, and the protections afforded to them, please refer herein to **Appendix B**.

4.3.2.2. Public Disclosure

In Italy and Sweden

The Reporting Party **may** make a Public Disclosure of the Breach, benefiting from the Safeguards provided by law, only if the following conditions (the "**Public Disclosure Conditions**") are met:

- **the Report** (internal and external, or directly external) **has first been made**, but
 - ✓ **no acknowledgement of receipt has been sent to the Reporting Party**, within the period of **7 working days** from the date of the Reporting, or
 - ✓ **appropriate action has not been taken** in response to the Report **within the period of 3 months** from the date of the acknowledgement of receipt of the Report

or

- the Reporting person has **reasonable grounds** to believe that:
 - ✓ the Violations may constitute an **imminent or obvious danger to the public interest**, such as where there is an emergency situation or a risk of irreversible harm (including danger to the physical integrity of a person); or

- ✓ in the case of an External Report, there **is a risk of retaliation or there is little likelihood of an effective Follow-up** due to the circumstances of the case, such as where evidence may be concealed or destroyed or there is reason to believe that the Reporting Authority may be in collusion with the author of the Breach or involved in the Violation.

In Brazil, Mexico and the U.S.A.

There is no Public Disclosure set forth by the applicable legislation.

4.4. Case Managers

4.4.1. Generalities

The Administrative Body of each respective Company is the body responsible for the appointment, removal or dismissal of any Case Manager, who, in turn, is responsible for the management and processing of Reports that enter the Internal Reporting Channel.

In the event that RINO MASTROTTO GROUP SPA designates a Case Manager, assigning him/her the responsibility to also manage Reports relating to other Companies of the RINO MASTROTTO Group, such designation is also deemed to be made in the name and on behalf of the administrative body of the beneficiary Company, based on a mandate automatically conferred by the latter through adherence to this Procedure.

The Case Manager may be a natural person or a collegiate body (Reporting Committee) that may delegate to one or more of its members (natural person), or to an external person, the powers to manage and process individual Reports.

The management of the Internal Reporting Channels and the Follow-up is entrusted collegially to the **Reporting Committee**, which is composed of the following persons

- the Supervisory Body 231 of RINO MASTROTTO GROUP S.P.A. (as first recipients of the Reports, and, following the preliminary screening, exclusively only if the Violation is classified as a 231 Violation);
- the HUMAN RESOURCES Manager of the Parent Company RINO MASTROTTO GROUP S.P.A., without intervention of the 231 Supervisory Body, in the event that, following the screening, the Breach is classified as other than a 231 Breach;
- the DPO of the Parent Company RINO MASTROTTO GROUP S.P.A., without intervention of the Supervisory Body 231, in the event that, following the screening, the Breach is classified as concerning the protection of personal data;
- the HR GENERALIST of ELMO SWEDEN AB, in case that as a result of the screening the Breach 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.

The Reporting Committee acts in a **functional position that is autonomous and independent from the rest of the corporate functions and from any hierarchical or functional subordination that may exist.**

In the remainder of this Procedure, the reference to the "Case Managers" or to the "Whistleblowings Committee" is to be understood as being limited to the sole Case Manager, in the event that the latter remains such according to the rules laid down therein.

In the event that the initially designated sole Case Manager operates the eventual Instructional Appointment provided for by Article 4.6.2.1.d, or in the event of the designation of more than one Case Manager, they act collectively as the "Reporting Committee" and any reference to the Case Manager must be understood as referring to the "Reporting Committee".

The Case Manager acts in a **functional position that is autonomous and independent from the rest of the corporate functions and from any hierarchical or functional subordination that may exist.**

Without prejudice to the generality of the foregoing, it is therefore strictly forbidden for anyone to exert pressure, send mandatory instructions, attempt to condition or hinder in any form whatsoever, and in general try to compromise the autonomy, impartiality and independence of the Reporting Committee.

Each Case Manager must be **specifically trained** for such management.

In particular, it is essential that the choice falls on a person who has all the knowledge and skills for an effective management of Reports.

Preferably, this should be a person with a good knowledge of law, ethics and integrity, and who has been adequately trained in the processing of personal data and whistleblowing processes.

The Case Manager must be guaranteed adequate knowledge of the Company's functional organisation chart.

The Case Manager who is temporarily absent or unable to perform his or her duties (due to holidays, illness, accident), must report this to the other members of the Whistleblowing Committee. In the case of holidays, moreover, if the Portal/Software does not allow the Case Manager to be notified automatically of receipt of the Report within the strict deadline of 7 days from the date of the Report, and the Reporting Manager cannot be temporarily replaced by other Case Managers, he/she shall give formal notice to potential Case Managers on the home page of the Portal/software, indicating the duration of the holiday.

4.4.2. Budget

The body of the Company responsible for appointing the Case Managers allocates them **an annual budget**, which they can use to perform their assigned tasks. The amount of the budget shall be deemed to be automatically renewed from year to year, unless otherwise quantified by the competent body.

4.4.3. Tasks

The Case Manager/Reporting Committee is **responsible** for

- a) **receiving and taking charge of Reports;**
- b) **screening** (content analysis and admissibility assessment) of Reports;
- c) **provide the Whistleblower with the Notice of Receipt of the Report within 7 days of the date of the Report**, unless this would compromise the confidentiality of the Report or the identity of the Whistleblower or the Whistleblower has waived its right to

communications relating to the investigation; maintain contact with the Reporting Party for further communications;

- d) **diligently follow up** the Report;
- e) determine, in coordination with area company contact persons if necessary, the advisability or necessity of taking immediate action to **prevent** (stop or mitigate) **further damage**;
- f) conduct or arrange for the **proper investigation** of the reported facts, in accordance with the rules and principles set out in this Procedure;
- g) **decide on the outcome (merits) of the Reports**, on the basis of the results of the investigation within the time limit prescribed by law; extend the termination period for reasons of complexity
- h) **propose the appropriate measures for the resolution of the Breach, as well as, where appropriate, the disciplinary measures** to be taken, with the possibility of delegating this power to another competent body;
- i) **communicate the outcome of the Report to the relevant persons** within the deadline laid down in this Procedure (unless, in the case of the Whistleblower, he/she has waived the right to avail him/herself of the communications relating to the investigation);
- j) in general, **maintain contact with the Whistleblower** throughout the follow-up to the Report;
- k) take care of the proper **filing and storage of Reports**;
- l) liaise with the Privacy Function and other corporate functions, where necessary or requested, to **meet the compliance requirements of the processing of personal data** covered by Reports ;
- m) make available **clear information on the Reporting Channels, procedures** and **prerequisites** for making Internal and External Reports, by means of the specific methods provided for in this Procedure and/or further identifiable; for this specific purpose, the HR Function is henceforth delegated to act also on behalf of the Reporting Committee;
- n) **manage the Internal Reporting Channels, guaranteeing the necessary protection requirements** of the system for managing and filing data on Reports, also by limiting access thereto, also **by availing itself of the skills and activities of the corporate IT and/or Privacy Functions**, without prejudice to the responsibilities and powers of the latter deriving from the corporate delegation system
- o) **resolve any doubts and requests for clarification** concerning the provisions of this Procedure;
- p) keep the Reporting Register up-to-date;
- q) ensure that adequate measures are taken to **prevent and avoid possible retaliation** against the Whistleblower and other Protected Persons.

In order to perform the above-mentioned tasks, and where it deems it necessary, the Reporting Committee may be assisted by an external consultant or even delegate to the latter some of the above-mentioned functions. In this respect, the Whistleblowings Committee will have to obtain a confidentiality agreement from the external consultants involved in the management and resolution of the communication.

Likewise, it must obtain the same from internal collaborators, when it considers it useful or necessary.

4.5. Examination of Reports

4.5.1. Screening

Following receipt of the Report, the Reporting Committee takes it in hand and carries out a **preliminary assessment**, aimed at ascertaining that the Report

- a) **concerns facts constituting a type of Violation** included among those listed in **Appendix A**,
- b) originates from **Whistleblowers belonging to one of the categories set out** in this Procedure,
- c) contains the **minimum mandatory information** required by the Whistleblowing Decree,
- d) does not contain **Information** that already upon summary examination appears to be **manifestly false or unreliable**,
- e) does not contain **Information** that already on summary examination appears **to be the result of an offence committed by the Whistleblower**,
- f) does not appear, already on summary examination, to have been made by the Whistleblower in **bad faith**, i.e. with the intention of damaging the Company or third parties connected to it
- g) **does not contain significant new information** on the Breaches **with respect to a previous Report** for which the relevant decisional procedure has been completed,

and therefore whether the Report is deemed to be **admissible** (the "**Screening**").

The results of the Screening must be documented.

The Whistleblowing Committee will have to issue a decision on whether or not the Report is admissible.

The Whistleblowing Committee if it assesses that the Report **is not procedural**:

- **must refrain from further follow-up to a Report**
- shall issue a decision to **dismiss** the Report on grounds of impropriety under the Whistleblowing Decree, **giving reasoned written notice**
- **to the Whistleblower**, unless the Whistleblower has waived the right to receive communications;
- **to the Board of Auditors**.

In the event that the Whistleblowing Committee during the Screening detects the possible absence of the conditions required by the Whistleblowing Decree to guarantee the Whistleblower the protection and support regime to which he/she is normally entitled, it will give written notice thereof, not only to the Whistleblower, but also to the Involved Subject and to the other competent internal subjects, as better indicated in Chapter 4.7.1 below.

Alternatively, **if the documentation is missing or in any way defective**, the Reporting Committee may not file the Report but, if it deems it necessary, request information from the Whistleblower.

Similarly, the Reporting Committee may, with the consent of the reporting person, transfer the report to a corporate function which may be competent to treat it as an ordinary report according to corporate policies (e.g. report from a customer, report on a conflict of interest of a member of the administrative body).

When the Report **is manifestly unfounded and there are, in the opinion of the Reporting Committee, reasonable grounds to believe that it was obtained through the commission of an offence**, in addition to inadmissibility, the Company assesses whether to send the Public Prosecutor's Office a detailed report of the facts alleged to be an offence (such a report is an obligation if the offence is prosecutable *ex officio*).

The Reporting Committee must immediately forward the information to the CEO (provided that there is no conflict of interest, in which case the transmission is made directly to the different competent body on the basis of the company's system of delegated powers) for any decision on whether to immediately forward it

- to the Public Prosecutor's Office **when the facts may be suspected of constituting a criminal offence**, or
- to the European Public Prosecutor's Office **when the facts concern the financial interests of the European Union**.

Finally, the Reporting Committee must forward the communication without delay to the authority, body or third party body that may be considered competent *ratione materiae* to handle the Report.

4.5.2. Conflict of interest

If the Reporting Committee considers the existence of a **conflict of interest** with respect to the Report received (*e.g. if the subject of the Report concerns violations attributable, even indirectly, to one of the members of the Reporting Committee itself, or to persons who are relatives or linked by a stable emotional bond, etc.*), it is required to

- inform the Whistleblower of the nature of the conflict of interest;
- refrain from dealing with the Report, and shall therefore not have access to the information deriving from the actions carried out in the management of the Report (unless he/she is an Involved Person); and
- Immediately devolve the handling of the Whistleblowing Report to another Whistleblowing Manager(s) not in conflict of interest, within the Whistleblowings Committee, or, in the absence of such Whistleblowing Manager(s) not in conflict of interest, to the additional person who will be designated and appointed without delay by the competent administrative body. In the event of a conflict of interest of the competent administrative body, the designation of the Whistleblower Manager will be made by the HR Manager, after hearing the Chairman of the Board of Auditors.

In the event that no Reporting Manager with no conflict of interest can be identified, the Whistleblower will be entitled to make an External Report (i.e., direct to the ANAC).

4.5.3. Acknowledgement of receipt and acknowledgement to the Whistleblower

4.5.3.1 Acknowledgement of receipt

Within the strict deadline of 7 calendar days from the receipt of the Report, the Reporting Committee shall communicate to the Reporting Subject an acknowledgement of receipt of the Report, by an appropriate means to ensure the confidentiality of the message.

The acknowledgement of receipt may be omitted if:

- a) the Reporting Party expressly objects, or
- b) there is reason to believe that confirmation of receipt of a written Report would compromise the confidentiality of the identity of the Reporting Party, or
- c) the Reporting Party has not provided an address to which the acknowledgement can be sent and cannot be reached anonymously via the Portal/Software.

In case c) the report received must be declared inadmissible by the Reporting Committee.

4.5.3.2 Acknowledgement

The subsequent acknowledgement to the Reporting Subject on the **outcome of the Report** must be provided within a period of **3 months**, starting

- **from the date of the acknowledgement of receipt of the Report**, or,
- if the initial acknowledgement of receipt has not been sent to the Reporting Party (e.g. because the Reporting Party has remained anonymous despite being guaranteed the possibility of receiving the acknowledgement through the Portal/Software, or because it has expressly waived the right to receive the said acknowledgement), **from the expiry of 7 calendar days** from the date of receipt of the Report.

NB: In cases of **particular complexity** requiring an extension of the investigation period, this may be extended, by decision of the Whistleblowing Committee, up to a maximum of a further three (3) months, in which case the **Reporting Officer must be informed** of the extension within the first 3 months.

NB: The aforementioned period of three months is not, by law, binding on the reporting person. Any exceptions, however, must be reasonably justified by the Reporting Committee.

4.6. Investigation

4.6.1. Generalities

Each Report assessed as admissible must be investigated to verify its merits.

The results of the Preliminary Screening are used by the Case Manager/Reporting Committee to determine the scope of the investigation (see e.g. Section 8.3 ISO 37008) and to define an investigation plan (see e.g. Section 8.4 ISO 37008).

If the Case Manager/Reporting Committee assesses that the Report **is admissible** (in particular, that **it falls within the scope of this Procedure**, as it relates to Violations of Sectorial Acts), it may

- a. assess whether the Report falls within the competence *ratione materiae* of other bodies or functions on the basis of mandatory provisions of the law** (e.g. Board of Statutory Auditors or Auditing Firm/Auditor in administrative, fiscal, accounting and financial statement matters subject by law to their control, RSPP, DPO, SB231) and therefore, **on the basis of a decision to be taken in agreement with such bodies and functions**; or
- b. transfer the management of the Follow-up to such bodies or functions, or share the management of the Follow-up with such bodies or functions, with**

the consequent assumption by them of the status - concurrent or exclusive, as the case may be - of Case Manager and of the consequent duties and responsibilities, subject to acceptance of this Procedure; or

c. (in the case of their competence *ratione materiae* according to this Procedure or to the corporate system of delegation of powers in force, e.g. privacy delegate, etc.) coordinate the management of the Follow-up with such bodies or functions, subject to acceptance of this Procedure, **with the first Case Manager/Reporting Committee retaining its original duties and responsibilities**;

in particular, such forwarding must take place at the first useful meeting or, if urgent, without delay; or

d. assess that the further handling of the Report **does not fall within the competence** - on the basis of mandatory provisions of law or the delegation system - **of any other corporate body or function**, and consequently

- ✓ **proceed with further investigative steps** (investigation, etc.), or
- ✓ **identify, by agreement with the competent Administrative Body, a different person competent** in relation to the Report, transferring **the management of the Follow-up**, including the final decision on the merits of the Report, **to the latter, without delay**, subject to acceptance of this Procedure, and giving simultaneous notice of the transmission to the Reporting person. **The different person identified must meet the requirements set out in this Procedure.**
- ✓ Assess the appropriateness of **taking immediate measures to prevent further harm** and, if necessary, implement them.

4.6.2. Investigation

4.6.2.1 General

Once the Report has been admitted for processing, the Reporting Committee proceeds with the investigation of the facts that are the subject of the Report, carrying out all the acts, procedures and checks necessary and aimed at verifying the truthfulness of the facts that are the subject of the Report, in compliance with the principles and rules set out in this Procedure.

To this end, he/she shall, by way of example but not limited to

- a) verifies whether the Company has adopted adequate Procedures to protect against the risk of the Breach that is the subject of the Report
- b) if he deems it necessary or appropriate, requests and receives further information, clarifications, and/or the production of deeds and documents from the Reporting Officer - if known - or from other persons (e.g. department heads or any other internal or external person) in possession of useful information for the preliminary investigation, in particular, reasonably concerning the processes at risk of Breach;
- c) has direct and timely access to the Company's administrative body and control bodies (e.g. Board of Statutory Auditors, auditing firm or auditors, Data Protection Officer if designated, etc.);

d) where deemed necessary, it may **delegate in writing to one or more** (internal/external) **persons** with adequate competences the performance of the aforesaid **investigative tasks sub a-b-c**) - within the limits of the powers vested in the delegate in accordance with the corporate delegation system in force (the "**Investigative Appointment**") and subject to the delegate's commitment to comply with this Procedure.

In this case, the delegating Reporting Committee **retains** the power to:

- assess the results of the preliminary investigation and **making a final decision on the merits of the Report**, and
- assess, as far as possible on the basis of the results of the preliminary investigation, of the possible **existence of wilful misconduct or serious misconduct on the part of the Whistleblower and/or of any Involved Persons**, as a **non-binding opinion** addressed to the function or body competent to manage the disciplinary or sanctioning proceedings against the Whistleblower or the Involved Person).

It is understood that the person to whom the Reporting Committee intends to delegate the aforesaid activities shall report to the Reporting Committee any prior situations of his or her workload that may cause the risk of non-diligent follow-up by the delegate *in pectore*.

4.6.2.2 Professional defence

The Reporting Committee assesses the advisability of discussing with the competent functions of the Company to assess whether it would be useful to engage a lawyer to conduct the investigation, in the light of the legal principle of the so-called legal privilege¹ which protects the confidentiality of communications between the assisted party and his lawyer, preventing them from being compulsorily disclosed to third parties (e.g. the Public Prosecutor) or used against the assisted party in judicial or investigative proceedings.

4.6.3. Obligations to cooperate

The personnel and any other internal and/or external contacts of the Companies are required to **cooperate loyally and with the utmost diligence** in the investigative activities carried out by the Whistleblowings Committee.

Internal staff supporting the investigative activities must have signed the prior appointment as "authorised persons" pursuant to Article 29 of the GDPR.

4.6.4. Collection, storage, analysis and review of electronic data

The collection, storage, analysis and review of data in electronic format by the Reporting Committee must comply with the rules of law on computer checks on employees and electronic evidence, under penalty of, *inter alia*, unusability of electronic evidence in labour and civil law.

¹ The protection is enshrined, in Italy

- by Art. 103 of the Italian Code of Criminal Procedure (secrecy of lawyer-client communications)
- by Art. 200 of the Italian Code of Criminal Procedure (secrecy of lawyer-client communications)
- by professional secrecy (arts. 622 and 623 of the Italian Criminal Code) and by the lawyer's deontological duty of confidentiality
- by the right of defence and cross-examination.

4.6.5. Interviews

It is recommended that the Reporting Committee conduct interviews in accordance with the relevant good practice (e.g. point 8.9 ISO 37008).

4.6.6. Coordination between parent company and subsidiaries

Through the Portal / Software shared between the Companies adhering to this Procedure, **the Whistleblower can freely identify, by using the autonomous sub-channel expressly available on the screen, the Company to which he intends to make the Report.**

If the **Report is addressed to the parent company RINO MASTROTTO GROUP SPA**, the latter shall receive and manage the Report, and may, if it deems it appropriate, avail itself of the support of the subsidiary to which the Report refers, after informing the Whistleblower and in compliance with confidentiality obligations.

On the other hand, if the Report **is addressed to a subsidiary Company**, it is handled as follows:

(a) **Subsidiaries up to 249 employees**: the receiving Company, where deemed appropriate, **may make use of the investigative capacity** (of the Case Manager(s)) **of the mother company**, after having informed the Whistleblower.

b) **Subsidiaries with more than 249 employees**: the receiving Company **must autonomously manage the Report**, without - therefore - being able to avail itself of the assistance (of the case manager(s)) of the parent company.²

In both cases, the obligation to maintain contact and provide information on the development of the Report to the Whistleblower lies solely with the individual subsidiary Company to which the Report refers.

4.6.7. Rights of the Involved Person

In the course of the investigation, the Whistleblower must be informed of the Report with a brief account of the acts or omissions attributed to him/her and has the right to be heard at any time.

This communication must be made at a time and in a manner deemed appropriate by the Whistleblowers Committee, according to its prudent discretion, to ensure the proper conduct of the investigation.

This information may be withheld during the hearing of the Involved Person, if it is considered that its prior disclosure may facilitate the concealment, destruction or alteration of evidence.

Without prejudice to the right to lodge written complaints, the investigation shall include, where possible, an interview with the Person Involved, in which, always in full respect of the presumption of innocence, he/she is invited to explain his/her version of the facts and to provide the evidence he/she deems appropriate and relevant.

In order to guarantee the right of defence of the Involved Person, he/she shall have access to the file (without revealing information that could identify him/her) and may be heard at any time. He/she must also be informed of the possibility of being assisted by a lawyer.

In addition, the investigator must listen to all the persons concerned and any witnesses, and must carry out all the procedures he/she deems necessary (examining documentation, obtaining

² However, this prohibition can be overcome, on a practical and formal level, if the subsidiary has separately designated a natural person coinciding with an external Case Manager designated by the parent company. In essence: the prohibition in question only concerns the use of internal Case Managers within the parent company.

information from external sources, etc.). The intervention of the witnesses and persons concerned shall be strictly confidential.

The investigator may also obtain any information and documentation he deems appropriate from any area or department of the organisation to corroborate the investigation.

Of all the acts of investigation and, in particular, of the explanations or statements provided by the persons involved in the investigation of the Report, a written record shall be drawn up (provided that their prior consent has been obtained), which shall be duly signed by the Persons Involved in order to certify its content and the conformity of their statements.

In the event that the presence of the Involved Person during the period of investigation may jeopardise the conduct of the investigation or the strict observance of the guiding principles of the procedure set out in this Procedure, the Involved Person may be granted, on the proposal of the investigator and by the competent corporate function, paid leave from work, without loss of remuneration, in order to ensure that the necessary investigative activities can be carried out without interference that could be detrimental to the person under investigation. Paid leave will be granted for the time necessary to carry out the investigative activities, but may in no case extend beyond the duration of the investigative process.

If the Reporting Committee deems it appropriate, the presence of external legal advisers is permitted at hearings and/or statements of the parties concerned, witnesses, etc.

4.6.8. Information flows to senior bodies

In order to guarantee the autonomy of the Reporting Committee, the administrative body is prohibited from deciding whether and how to follow up the Whistleblowing, requesting information, supervising the investigation carried out and/or taking decisions on the merits of the Whistleblowing and the Reporting Committee

4.6.9. Finalisation of the investigation

An investigation cannot be considered substantially complete if it does not reach the following results:

- the Reporting Committee is prepared to make findings supported by evidence, and these findings are sufficient for the administrative body to make a decision on the Report of non-compliance;
- the Reporting Committee is able to fully account for its work product;
- the result of the investigation provides a sufficient basis for initiating the necessary corrective action, if any.

4.6.10. Reporting Decision and Investigation Report

Upon completion of all investigative actions, the Whistleblowing Committee prepares a written report containing at least the following content (the '**Investigation Report**'), which is intended to be limited to the defined scope of the investigation:

- A statement of the relevant facts (descriptive information about the Report) together with the identification code of the Report and the date of registration.
- The actions taken to verify the plausibility of the facts and the limitations and constraints encountered during the investigation.

- The conclusions reached in the investigation and the evaluation of the proceedings and supporting evidence.
- The actions taken (if any).

4.6.11. Corrective measures

The Investigation Report **may also contain any proposals for potential corrective measures or improvements** to be implemented on the basis of the results of the investigation **to minimise the impact of the Violation** (so that the root causes of the Violation are appropriately, sufficiently and effectively addressed) and to **improve the internal controls of the Company's compliance programme** and/or the proposal of disciplinary measures.

The Company function(s) assigned to the policies or procedures corresponding to the breach should design a **remediation plan based on the Investigation Report**.

If requested, the Reporting Committee should report to the Company's compliance function to assist in developing an interim remediation plan. The plan should clearly state the compliance gaps or vulnerabilities and the objective(s) the measures are intended to achieve.

4.7. Actions following the Report

After the Report of the Investigation has been issued, the Reporting Committee makes one of the following decisions.

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

In this case, the Reporting Committee rejects the report and proceeds to dismiss it.

If the Reporting Committee finds evidence that, in its prudent judgement, points to bad faith or gross negligence on the part of the Whistleblower, it notifies the Whistleblower without delay in writing

- a) to the Whistleblower, expressly warning him/her of the consequences under the law (absence of Safeguards);
- b) to the Person Involved; and
- c) to the Head of the functional area to which the Whistleblower belongs, as well as to the HR Function (e.g. for the assessment of the application of possible sanctions against the Whistleblower).

4.7.2. Report confirmed by the investigation

If, at the outcome of the investigation, the Reporting Committee finds that the facts reported are **well-founded in substance**, it issues a documented **decision to accept the Report**.

The communication may contain, where appropriate, the relevant proposals for action and/or proposal of disciplinary measures against any Person Concerned.

The decision must be **communicated, without delay**

- a) to the Whistleblower, unless the Whistleblower has waived it or the communication is anonymous;
in the case of an external Whistleblower, the communication must be sent

- ✓ to the pro-tempore legal representative of the third organisation to which the Whistleblower himself/herself belongs (or, if the Handlers of the report consider that the Whistleblower is in a position of conflict of interest with respect to the Breach decided, to the Head of the different functional area of the third organisation that appears competent to receive such communication), and
- ✓ to the Head of the internal functional area that has contractual relations with that third party organisation;
- b) to the Whistleblower;
- c) to the Head of the functional area affected by the Violation, for the assessment and implementation of the appropriate remedial actions;
- d) to the HR Function, for the assessment and implementation of possible consequent disciplinary sanctions;
- e) to the Board of Directors which approved this Procedure,
- f) to the members of the Board of Statutory Auditors.

The aforementioned communication **may be delayed** in the event that, in the opinion of the Cas Manager, it **may hinder** further **investigations or judicial proceedings** (e.g. administrative, criminal) for the protection of the rights of the Company and/or third parties, after the investigation has been carried out.

4.7.3. Improvemental actional

In the event that the investigation carried out following the Report leads the Reporting Committee to ascertain

- the absence of specific Company's valid Procedures aimed at guaranteeing against the risk of Violations or
- the lack of adequate internal and/or external disclosure of the same, or
- the lack of internal training with respect to the rules envisaged by the Procedure,

the Case 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 GROUP SPA, for the appropriate remedies.

4.7.4. New Violations

If, following the investigation, **other facts are discovered which could constitute new irregularities** (whether or not they fall within the scope of the Whistleblowing Decree) presumably committed by the same Involved Person or by other persons, the Whistleblowing Committee will **ex officio open a new file** (in which case the relative Follow-up will take place, in the first case, outside this Procedure, in accordance with the applicable corporate procedures on internal investigations), and in the second case, in accordance with this Procedure) **or**, if it is related to what is already being investigated in the current Whistleblowing file, **will extend the investigation file** itself, if it deems it more discretionary (in which case the relevant Follow-up will take place in accordance with this Procedure only where this appears necessary for a unified handling of the matter).

4.7.5. Administrative, civil or criminal proceedings

The Whistleblowings Committee, if it considers that, although there is no initial indication that the facts may constitute a criminal offence, or that there may be grounds to initiate administrative or civil proceedings, this indication emerges from the course of the investigation,

- a) if already competent on the basis of the company delegation system, independently initiates such an action against any Involved Person and/or further responsible third party, otherwise
- b) informs without delay the internal person competent under the company delegation system to authorise or initiate such an action; that person then assesses whether to initiate the action

if the latter person has a conflict of interest in relation to the report, the Whistleblowings Committee shall consult with the HR Function to identify the most appropriate function or person to receive and implement the request to initiate the aforementioned administrative, civil or criminal proceedings, who is not himself in conflict of interest.

The Company will consider whether it should make a self-report to the Authorities, for instance to reduce liability or to exonerate itself or to protect any of its own rights that may have been infringed; in order to assess the legal consequences, it may consider seeking professional legal advice, in line with point 4.6.2.2 of this Procedure.

The Reporting Committee must immediately transmit the information to the administrative body (provided that there is no conflict of interest, in which case the transmission is made directly to the other competent body on the basis of the company's system of delegated powers) for any decision on whether to transmit it immediately

- to the **Public Prosecutor's Office when** the facts may be suspected of constituting **a criminal offence**, or
- to the **European Public Prosecutor's Office when** the facts **concern the financial interests of the European Union**.

4.7.6. Report confirmed by verifications carried out, 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 investigation activities should be assessed, with an indication of the professional expertise needed (e.g. specific legal or technical expertise on the reported facts or underlying processes).

On the basis of the results of these further investigations, if the reported facts are confirmed, the actions set out in section 4.7 may be taken.

Otherwise, further action should be taken for legal protection or reporting to the competent authorities for any necessary investigations.

4.7.7. Report of facts that are plausible but cannot be verified

In these cases too, the actions referred to in 4.72 above may be taken.

4.7.8. Referral

The Reporting Committee may decide to refer the report to the authority, body or third party body considered competent to deal with it (e.g. UIF).

Whatever the decision, it must be communicated to the reporting person without delay, unless the reporting person has opted out or the communication is anonymous, as well as to all other interested parties.

4.7.9. Communication

The Reporting Committee works with the relevant corporate functions (e.g. management, compliance functions, human resources, public relations, etc.) to define who is competent to communicate with the various relevant stakeholders, and effectively plan the manner and content of such communications.

The Reporting Committee plans communication with governmental authorities on the specific issues under investigation, if applicable.

Before communicating with them, corporate legal counsel (internal or external) and any existing guidelines should be consulted to ensure that the interests and rights of the organisation are fully protected.

5. CONSERVATION

The Company will keep a Register of all Reports received, by means of the Portal/Software.

The Whistleblowing Register is not public, therefore the records and data contained therein will be kept confidential.

Records will not be kept longer than necessary and, in any case, for as long as necessary to comply with any applicable legal requirements at any given time.

Reports of irregularities or other cases that do not qualify as Violations included in this Procedure must be deleted, unless an obligation to further preserve the same arises from other Procedures in force at the Company, or from the law, in which case they will be handled within the limits provided for by the same.

Once the investigation of the Report has been concluded and the appropriate actions have been taken, as the case may be, the Report data that have been followed up will be duly blocked in order to comply with the legal obligations that may be applicable in each case.

In no case may the data (report, related documentation) be retained for a period longer than **5 years (in Sweden, 2 years) from the date of the documentation of the final outcome** of the reporting procedure .

If it is decided not to follow up the Report submitted, the information may be kept anonymously.

The aforementioned term of 5 years is without prejudice to the different term provided, on the other hand, for the preservation of data, deeds and documents relating to the proceedings (e.g. disciplinary proceedings) initiated and to the initiatives (e.g. corrective measures, compensation, etc.) taken by the Company in total or partial dependence on the Report.

6. LEGAL PROTECTION

The Whistleblower and the other Protected Persons are guaranteed by the Company the Protections indicated in *Appendix B*.

7. TRAINING

Training on the subject of whistleblowing, and its periodical updating, by the internal recipients of this Procedure (employees, collaborators) is mandatory for the Company, as it constitutes an essential element to ensure a conscious and accurate handling of Reports.

Training, communication, and information activities, in particular, i) represent an essential component for the effective implementation of the whistleblowing management system, ii) demonstrate the organization's genuine commitment to actively prevent the reported crimes, and iii) encourage collaboration among stakeholders in effectively achieving the objective of legality.

The Human Resources Department, in consultation with the person responsible for this Procedure, must make clear information easily accessible to the entire organizational structure—differentiated according to the users' roles—at least on the requirements and procedures for reporting violations, the protections afforded to whistleblowers, and their limitations.

The Human Resources Department, in consultation with the person responsible for this Procedure, prepares and periodically updates a ***Whistleblowing Training Plan***, which forms an integral part of **Annex D**.

8. DISTRIBUTION

The Whistleblowers shall make available to the addressees of this Procedure, clear information on the Whistleblowing channels, on the prerequisites for internal and external Whistleblowing and public disclosures, using the following methods:

- Publication in a separate and easily identifiable section of the Company's website (the URL address of which shall be communicated by the Company to the main addressees, if reasonably possible),
- Making available
 - ✓ by hand and/or
 - ✓ via e-mail or intranet or other document distribution application software.

9. DISCIPLINARY MEASURES AND SANCTIONS

9.1) This Procedure is a mandatory rule for all members of the Company.

Its violation may give rise - in addition to the other civil and criminal liabilities provided for by the laws in force - to **disciplinary sanctions** by the Companies, against the responsible persons, as set forth:

i) in Italy, by the National Collective Labour Agreement and/or the Company Collective Bargaining Agreement, if any (therefore to be understood as expressly referred to herein) and by **paragraph 4 "Sanctioning system" contained in the General Section of the Company 231 Organisational Model**

Violations of the Procedure may give rise - in addition to other civil and criminal liability under applicable law - to the imposition by the Company, against the responsible employee, of **disciplinary sanctions** as provided for:

i) in Italy, by the National Collective Bargaining Agreement and/or any company Collective Bargaining Agreement (therefore to be understood as expressly referred to herein), as well as

- by **paragraph 4 "Sanctions System" contained in the General Section of the company's 231 Organizational Model**, if the violation concerns RINO MASTROTTO GROUP SPA; or
- by the **"Sanctions System" contained in the General Section of the company's 231 Organizational Model**, if the violation concerns NUOVA OSBA SRL; or

ii) in other countries, by the applicable legislation and employment contract.

9.2) **When it is determined that the reported conduct constitutes a labour offence**, the Company may take the appropriate measures in accordance with the applicable disciplinary regime and, in particular, with the provisions of the collective agreement and labour regulations applicable to the Company and, in the case of the adoption of an *Organisational Model 231*, by the sanction system therein.

Notwithstanding the adoption of disciplinary measures, if the facts may be suspected of constituting an offence, the relevant information shall be immediately forwarded to the Public Prosecutor's Office. If the facts concern the financial interests of the European Union, the matter is referred to the European Public Prosecutor's Office.

In Italy, the following **sanctions** are also provided for:

Whoever:

- **obstructs or attempts to obstruct** the Whistleblower or the other Protected Persons, in connection with any Reporting, or
- **adopts a retaliatory act**,
- **violates confidentiality provisions**,
- **fails to verify and analyse the Reports** received

commits an **administrative offence** and, unless the offence is punished with a more severe penalty by another provision of law, is punished by ANAC - the National Anti-Corruption Authority - with a **fine** ranging from 10,000.00 to 50,000.00 EUROS.

The Company's governing body is liable for the penalty jointly and severally with its individual members, without prejudice to the recourse action to be brought against all the persons responsible for the violation, in accordance with Article 6 of Law 689/1981.

10. OTHER

For all matters not expressly provided for in this Procedure, the further regulations referred to therein shall apply.

- in Italy, the Whistleblowing Decree and the ANAC Guidelines;
- in Sweden, Law 2021:890 and the additional regulations referred to therein.
- in other countries, the applicable local legislation on whistleblowing.

11. AMENDMENTS

This Procedure may be amended or updated, at any time, in accordance with operational, legislative or regulatory requirements, and on the basis of lessons learned during its actual application. Such amendments shall be promptly communicated to all persons involved and shall become binding from the moment of their communication or, if necessary, from the effective date established by the Company.

If the amendments are substantial, they shall be subject to approval by the competent bodies of the Company.

APPENDIX A - SECTORAL VIOLATIONS

The Violations of Sectorial Acts related to the Companies of the RINO MASTROTTO Group with registered offices in Italy and Sweden, include:

a) **offences** (acts or omissions, even if only attempted or concealed) **that fall within the scope of application of the following Sectoral Acts of the Union³**, regardless of their qualification under national law:

SECTOR
<p>Privacy and data protection</p> <p>Examples</p> <ul style="list-style-type: none">• Omitted or inaccurate privacy notices to employees, applicants, visitors, customers, potential customers, suppliers, agents• Omitted or inaccurate privacy policy on the company website (so-called privacy policy) and/or cookie policy• Omitted or inaccurate privacy policy on whistleblowing• Absence or inaccurate privacy policy on video surveillance or automated monitoring and decision-making systems• Failure to obtain the prior specific consent of the data subject in cases provided for by law (in particular:<ul style="list-style-type: none">✓ use of the employee's image for advertising purposes✓ use of the image of guests at company events for advertising purposes✓ processing of personal data for direct marketing, profiling or market research purposes)• Failure to obtain a trade union agreement or administrative authorisation for video-surveillance or automated monitoring and decision-making systems• Failure or deficiency of register of processing operations• Failure or deficiency of appointment of external data controllers• Failure or deficiency of co-ownership agreements for processing in cases required by law• Failure to distribute written appointments and instructions to employees on the processing of personal data• Failure to comply with the privacy clauses of the corporate Whistleblowing Procedure• Failure to adopt organisational (e.g. physical, managerial) or technical (in particular, IT) protection measures suitable to avoid/reduce the risk of unauthorised access, loss or alteration, even accidental, of personal data processed by the company• Failure to draw up a DPIA (assessment of the impact of a given processing operation or set of processing operations on the rights of data subjects) in the mandatory cases provided for by law• Failure or delay in handling requests received by the company to exercise data subjects' rights
<p>Protection of the environment</p> <p>E.g. so-called environmental offences, such as the discharge, emission or other release of hazardous materials into the air, soil or water or the unlawful collection, transport, recovery and disposal of hazardous waste.</p>

³ See Annex to EU Directive 1937/2019

E.g. violations of administrative requirements punished by administrative fines.

Product safety and compliance

E.g. violation of obligations aimed at ensuring that any product manufactured or marketed by the Company [...], under normal or reasonably foreseeable conditions of use, including duration and, where appropriate, commissioning, installation and maintenance, does not present any risk or only presents minimal risks, compatible with the use of the product and considered acceptable in compliance with a high level of protection of the health and safety of persons [...].

E.g. Infringement of the producer's obligation to provide the consumer with all information relevant to the assessment and prevention of risks arising from normal or reasonably foreseeable use of the product.

E.g. Infringement of the producer's obligation to take measures proportionate to the characteristics of the product supplied to enable the consumer to be informed of the risks.

NB: A product is defective when it does not offer the safety that may legitimately be expected taking into account all the circumstances, including:

(a) the manner in which the product was put into circulation, its presentation, its obvious characteristics, and the instructions and warnings provided;

(b) the use for which the product may reasonably be intended and the behaviour which may reasonably be expected in connection therewith; the time during which the product was put into circulation.

A product is defective if it does not offer the safety normally offered by the others in the same series.

N.B. The scope of risk relevant here goes beyond the mere presence of flaws and defects in the product (e.g. damage, failure to function, appearance not corresponding to the agreed description, etc.) that do not, however, result in a real safety risk for the purchaser/user even though they affect the suitability for use or the promised qualities.

Consumer protection

E.g. prohibition of unfair/aggressive commercial practices in the promotion of services/products

Anti-money laundering and terrorist financing

The offence of money laundering exists when, apart from cases of complicity in the offence, a person replaces or transfers money, goods or other utilities originating from a crime, or carries out other transactions in connection with them, in such a way as to obstruct the identification of their criminal origin.

The offence of financing terrorism exists when any person (i) collects, disburses or makes available property or money intended to be used, in whole or in part, for acts of terrorism, or (ii) deposits or keeps property or money intended for such purposes (even if not subsequently used).

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

According to Article 2 of the relevant directive, 'financial interests' include all revenue and expenditure covered by the Union budget, including VAT revenue.

Examples of infringements: fraud involving Community resources; cross-border VAT fraud; breaches of customs law.

- c) **acts or omissions relating to the internal market**, as referred to in Article 26(2) TFEU, including
 - a. violations of EU **competition rules** (e.g. abuse of a dominant position, agreements between undertakings restricting competition in the internal market, merger rules)
(N.B.: these regulations, as a norm, do not apply to the Companies to which this Procedure is addressed, and are therefore relevant only in the event that the companies, in their capacity as suppliers and/or partners of third parties, detect any violations in this matter exclusively referable to the activity of the latter)
 - b. violation of the Union rules on **State aid**
(e.g. falsification of data and information in order to obtain state aid that is not due, use of state aid for purposes other than those for which it was granted, false reporting)
 - c. internal market violations related to acts in breach of **corporate tax** rules
(e.g. any accounting/tax irregularity aimed at distorting the correct assessment of IRES, IRAP, such as under-declaration of turnover, over-declaration of costs, invoicing of non-existent transactions, deduction of non-deductible costs, creation and use of slush funds), or
 - d. **practices whose purpose is to obtain a tax advantage that distorts 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 mentioned under (a), (b) and (c).

E.g. abusive practices as defined by the case law of the EU Court of Justice. Consider, for example, an undertaking operating in a dominant market position: the law prevents such an undertaking from gaining, through its own merits and abilities, a dominant position on a market, or from ensuring that less efficient competitors remain on the market. However, such an undertaking could jeopardise, by its own conduct, effective and fair competition in the internal market by resorting to so-called abusive practices (adoption of so-called predatory pricing, target rebates, tying) in violation of the protection of free competition.

NB. For a detailed description of these relevant sectors, please refer to the Annex (Part I and Part II) of the Whistleblowing Decree available at www.normattiva.it.

In Sweden

Any further "misconduct in a business context that is in the public interest", is also a Violation to be reported under this Procedure.

This wide category of events is described under the Act 2021:890 as "Information about illicit conducts in a working context, whose reporting is of public interest " (Capitolo 1, Sezione 2, Paragrafo 1).

If the matter only concerns me as an individual, it's usually not in the public interest. For there to be a public interest,

- it should apply to **serious** conditions (e.g. systematic misconduct),
- **affect** a group that can be described as the **general public** (many people, the community), or fundamental (e.g. health, safety, environment, justice, public finances)
- there is a **legitimate interest** in exposing abuses, that is to say, a public interest in **correcting or stopping** them.

Reportable events include offenses or irregularities that affect the community (not just strictly private or internal matters), as, not exhaustively:

1. Risks to life, health, and safety

- Violations of workplace safety regulations
- Hazards to the health of workers or citizens
- Lack of safety measures that put human lives at risk
- Lack of safety of product

2. Environmental protection

- Serious polluting discharges or emissions
- Illegal disposal of hazardous waste
- Corporate conduct that significantly damages the ecosystem

3. Corruption and abuse of power

- Bribes or favoritism in public procurement
- Misuse of public funds
- Conflicts of interest that harm the community

4. Financial irregularities and fraud

- Systematic tax evasion or serious accounting fraud
- Manipulation of financial statements with an impact on the market or investors
- Abuses in banking and financial services

5. Discrimination and violations of fundamental rights

- Serious violations of anti-discrimination laws in the workplace
- Systematic abuse (e.g., large-scale harassment or mobbing)
- Treatment contrary to human dignity, with effect beyond the individual

If the offense constitutes a crime with a custodial sentence or is comparable in severity, it falls within the traditional definition of "allvarliga missförhållanden." This remains a strong indicator of seriousness.

NB: Many of these offences also simultaneously fall within areas covered by EU law, as Violation of Sectorial Acts.

In the U.S.

In relation to the activity carried out by the Company **RMG LEATHER USA LLC**, this Procedure covers the reports relating to the following REGULATORY VIOLATIONS.

REGULATORY VIOLATIONS FOR WHICH THE WHISTLEBLOWER PROTECTION REGIME IS MANAGED BY OSHA - Occupational Safety & Health Administration

False Claim Act (FCA) (31 U.S.C. - Articles 3729-3733)

The most important Violations relevant under the FCA are the following:

- ✓ Malicious submission of a false or fraudulent claim for payment to the federal government (or action intended to cause another person to submit such a claim).
- ✓ Fraudulent submission of a document or statement to obtain payment of a false or fraudulent claim to the federal government.
- ✓ Conspiracy to cause a false or fraudulent claim to the federal government to be paid.
- ✓ Malicious use (or action intended to cause another person to maliciously use) a false document or statement to conceal or diminish a debt owed to the federal government or to avoid a transfer of property for the benefit of the government.

A 'demand' or 'claim' is any request, whether under contract or otherwise, to obtain money or property, and whether or not the US has any rights to the money or property.

NB: The FCA does not punish the mere sending of false statements to the government, but there must be knowledge that the information sent is false. Proof of intent to defraud the Government is not required.

The FCA does not apply to tax returns reported under the Internal Revenue Code (any related reports are governed by the Internal Revenue Code and/or related legislation).

Clean Air Act (CAA)

Violations of statutory provisions relating to air quality and air pollution standards

Federal Water Pollution Act (FWPCA)

Violations of the Water Pollution Act

Safe Drinking Water Act (SDWA)

Violations of the Drinking Water Act

Solid Waste Disposal Act (SWDA)

Violations of the Waste Disposal Act

Toxic Substance Control Act (TSCA)

Violations relating to chemicals manufactured in or imported into the U.S.

Comprehensive Environmental Response, Compensation and Liability Act (CERCLA)

Violations of provisions relating to accidents, spills and other emergency releases of pollutants into the environment

Taxpayer First Act (TFA)

Failure to pay taxes, potential violations of domestic tax laws, potential violations of any provision of federal law relating to tax fraud

Anti-Money Laundering Act (AMLA)

Potential violations related to anti-money laundering laws or violations of Sections 1956, 1957 or 1960 of Title 18 of the U.S. Code (or any rules or regulations under those provisions).

The aforementioned **Section 1956 - Money Laundering** punishes

(a)

(1) Whoever, knowing that property involved in a financial transaction represents the process of some form of unlawful activity, conducts or attempts to conduct such financial transaction which in fact involves the process of a specific unlawful activity:

(A)

(i) with the intent to promote the conduct of specified unlawful activity; or

(ii) with the intent to engage in conduct constituting a violation of Section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B) knowing that the transaction is designed in whole or in part

(i) to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specific illegal activity; or

(ii) to avoid a transaction reporting requirement under state or federal law,

(...).

For the foregoing purposes, a financial transaction is considered a transaction involving the process of a specific illicit activity if it is part of a set of parallel or dependent transactions, each of which involves the process of a specific illicit activity, and all of which are part of a single plan or arrangement.

(2) Whoever transports, transmits, or transfers or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States

(A) with the intent to promote the conduct of certain illegal activities; or

(B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of illegal activity and knowing that such transportation, transmission, or transfer is designed in whole or in part

(i) to conceal or disguise the nature, location, source, ownership or control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under state or federal law,

(...)

(3) Whoever, with the intent

(A) to promote the conduct of specified unlawful activity;

(B) to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified illegal activities; or

(C) to avoid a transaction reporting requirement under state or federal law,
conducts or attempts to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, or property used to conduct or facilitate specified unlawful activity,

(...)

Section 1957 - Engaging in monetary transactions in property derived from specified illegal activities also punishes:

(a) Whoever, in any of the circumstances set out in subsection (d), knowingly engages or attempts to engage in a monetary transaction in criminally derived property valued in excess of \$10,000 and derived from specified unlawful activity, (...).

(B)

(...)

(c) In a prosecution for an offence under this section, the Government is not required to prove that the defendant knew that the offence from which the criminally derived property was derived was specified unlawful activity.

(d) The circumstances referred to in subsection (a) are:

(1) that the offense referred to in this section takes place in the United States or in the special maritime and territorial jurisdiction of the United States; or

(2) that the offense under this section takes place outside the United States and such special jurisdiction, but the defendant is a person of the United States (as defined in section 3077 of this title, but excluding the class described in paragraph (2)(D) of such section).

NB: For purposes of such section 1957,

(1) the term "**monetary transaction**" means the deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument (as defined in section 1956(c)(5) of this title) by, through, or to a financial institution (as defined in section 1956 of this title), including any transaction which would be a financial transaction within the meaning of section 1956(c)(4)(B) of title 18 of the U.S. Code, but such term shall not include any transaction necessary to preserve a person's right to representation as guaranteed by the Sixth Amendment to the Constitution;

(2) the term "**criminally derived property**" means any property that constitutes, or is derived from, proceeds obtained from a crime; and

(3) the terms "**specified unlawful activity**" and "proceeds" shall have the meanings given to those terms in Section 1956 of this title.

Section 1960 finally punishes:

Prohibition of unlawful money transfer activities

(a) Whoever conducts, controls, manages, supervises, directs, or owns all or any part of a business, knowing the business to be an unlawful money transmission business, shall be fined under this title or imprisoned for not more than 5 years, or both.

(b) As used in this section

(1) The term "**unlawful money transmission activity**" means a money transmission activity that affects interstate or foreign commerce in any manner or degree and

(A) is intentionally operated without an appropriate money transfer license in a state in which such operation is punishable as a misdemeanor or felony under state law; or

(B) fails to comply with the business registration requirements for money transmission under section 5330 of title 31, U.S. Code, or the regulations prescribed in that section;

(2) the term "**money transmission**" includes but is not limited to the transfer of funds for the account of the public by any means, including but not limited to transfers within this country or to foreign locations by wire transfer, check, draft, facsimile, or courier; and

(3) the term "State" means any state of the United States, the District of Columbia, the Northern Mariana Islands and any commonwealth, territory or possession of the United States.

REGULATORY VIOLATIONS FOR WHICH THE WHISTLEBLOWER PROTECTION REGIME IS ADMINISTERED BY THE VETERANS EMPLOYMENT AND TRAINING SERVICES

Uniform Services Veterans Employment and Reemployment Rights Act (USERRA)

Violations of the law protecting military service members and veterans from employment discrimination on the basis of their service and allowing them to return to civilian employment after a period of uniformed service.

REGULATORY VIOLATIONS FOR WHICH THE WHISTLEBLOWER PROTECTION REGIME IS ADMINISTERED BY THE DEPARTMENT OF JUSTICE

Foreign Corrupt Practices Act (FCPA)

Violations of provisions that make it unlawful for a U.S. person or company to offer, pay or promise to pay money to any foreign official for the purpose of obtaining or retaining business.

In Brasil

The following Violations may be reported:

- (limited to companies with an Internal Commission for Accident Prevention and Harassment - CIPA) conduct relating to sexual harassment and other forms of violence in the workplace (such as violations under Brazilian Law 14.457/2022), and
- Violations under Law 14.611/2023 of June 3, 2023, concerning equal pay and remuneration between women and men for work of equal value or in the performance of the same function.

APPENDIX B - SAFEGUARDS

1. PROTECTED PERSONS

Protected Persons include,

- the **Whistleblower** (even anonymous, whose identity is discovered at any time),
- 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 making a complaint to the judicial authority or the person making a Public Disclosure and who are **related to them by a stable emotional or kinship relationship up to the fourth degree** (cousins),
 - **Co-workers** of the Whistleblower, of the person who has reported the matter to the judicial authority or made a Public Disclosure, who work in the same work context as the Whistleblower and who have a regular and current relationship with the Whistleblower,
 - **Legal representatives of employees in the exercise of their functions in advising and supporting the Whistleblower**,
 - **Entities owned, or which are employers, or which work in the same Work Context, as the aforementioned persons, or with which the aforementioned persons have any other type of relationship in the work context, or in which they hold a significant interest.**

For this purpose, an interest in the capital or voting rights attached to shares or participations is considered "significant" when, by virtue of its proportion, it enables the person holding it to **exercise influence over the legal person** in which the interest is held.

2. PROTECTIONS

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

- **PROTECTION MEASURES**,
- **SUPPORT MEASURES**,
- **RIGHT TO CONFIDENTIALITY**,

as set out below.

With regard, moreover, to the **Whistleblowers only**, the Safeguards also apply if the Whistleblowing or the report to the judicial authorities or the Public Disclosure occurs in the following cases:

- a) **when the legal relationship** with the Company **has not yet commenced**, if information on Breaches has been 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 Breach 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 the Safeguards.

3. PROTECTIVE MEASURES⁴

The following **Protection Measures** apply to Protected Persons, provided they are bona fide:

- Prohibition of Retaliation,
- Protection from Retaliation,
- Limitation of Liability,
- Waivers and conditional settlements.

NB: The Protection Measures also apply

- (a) in cases of anonymous Reporting or Public Disclosure, if the Reporting Person was subsequently identified and retaliated against, and
- (b) in cases of External Reports submitted to the competent institutions, bodies, offices and agencies of the *European Union* (e.g. *the European Anti-Fraud Office*), in accordance with the conditions for External Reports themselves.

3.1. Prohibition of Retaliation

Protected Persons may not be subjected to any Retaliation (prohibition of retaliatory acts). The Company undertakes to strictly enforce this prohibition.

"Retaliation" is to be **understood extensively**, 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 on access to it;
- (e) **demerits or negative references**;
- f) the adoption of **disciplinary measures** or any other sanction, including a fine;
- (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) the **non-renewal** or **early termination** of a fixed-term employment contract
- (k) **damage**, including to a person's reputation, in particular on social media, or **economic or financial** loss, including loss of economic opportunities and loss of income

⁴ The protection envisaged for the Whistleblower will only be guaranteed in the case of reports made by clearly identified persons. The disclosure of the identity by the Whistleblower may take place at any time even after the Report, without prejudice to the protection granted above.

- (l) inclusion on improper lists (e.g. **blacklists**) on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- m) the **premature** termination (termination) or **cancellation of a contract for the supply of goods or services; the introduction of deteriorative changes** to the service or supply contract
- n) the **cancellation of a licence or permit**;
- (o) the request to undergo **psychiatric or medical examinations**.

3.2. Protection from Retaliation

3.2.1. Retaliation

In the event that a member of the Company, in contravention of the provisions of this Procedure, engages in direct or indirect retaliatory acts, the Company itself shall take the necessary measures to ensure that such acts cease as soon as possible and, where appropriate, shall take the necessary disciplinary or liability measures against those responsible.

3.2.2. Invalidity of acts

In the event of non-application or non-observance, even partial, of the prohibition of retaliatory acts by the Company, the Protected Person may invoke, even cumulatively

- **The nullity ex lege of the acts of Retaliation**, as well as of the administrative acts aimed at preventing or hindering the submission of Whistleblowings, resulting in the restoration of the situation prior to the same.
- The **reinstatement in the workplace** under the same conditions ex ante, pursuant to the legislation applicable to the worker, if the Protected Person was dismissed because of the Report.

Non-exhaustive examples of remedial actions

- ✓ *Equal access to any promotion and training that may have been denied*
- ✓ *Withdrawal of litigation against the Whistleblower*
- ✓ *Deletion of any record/data/document that could constitute a file for a blacklist or subsequent retaliation*
- ✓ *Reopening of a tender procedure*
- ✓ *Reinstatement of a cancelled contract*
- ✓ *Apology*
- ✓ *Acknowledgement for upholding the values or interest of the Company through the Violation Report*
- ✓ *Financial compensation for past, present and future losses*
- ✓ *Financial compensation for pain and suffering, including medical expenses*
- **Compensation for damages**, if any.

In Sweden

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

1. a person inquiring or seeking employment
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 has been in one of the above categories of persons and who has received the information while within the organisation.

In this case, the persons mentioned in points 1 to 5 are also considered to be workers. The Company Elmo Sweden AB is considered to be an 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 Codetermination in Working Life (1976:580) shall apply in the aforementioned 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 sentence of paragraph 1 of Article 66 shall be two months; and
- ✓ Article 68 on the loss of the right of action due to prescription.

An arbitration agreement entered into 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 appeal the award, may not be invoked.

In the U.S.

Major disparities between whistleblower protection statutes

Each private sector whistleblower law differs somewhat in scope and application. A careful reading of the law is necessary to ensure a complete understanding of applicable rights. Below are the main discrepancies to keep in mind:

- ✓ **Limitation** periods - The period of time a whistleblower has to file a retaliation complaint
- ✓ **Protected Persons categories** - Who is protected from retaliation?
- ✓ **Due process** - The process through which individuals assert their rights. For example, some laws allow whistleblowers to file their complaint in federal court only after a certain period of time.
- ✓ **Burden of proof** - This requirement refers to the amount of evidence needed to prove retaliation and win a case
- ✓ **Remedies** - The relief and compensation to which a whistleblower is entitled once a lawsuit resulting from the retaliation complaint is won.

Violations handled by OSHA

The **statutes enforced by OSHA are listed in Appendix A**. They contain whistleblower anti-retaliation provisions that generally provide that organizations may not fire or otherwise retaliate against an employee because the employee has filed a whistleblower complaint or exercised any other right provided to employees under the statute.

A **current list of whistleblower protection statutes** for which OSHA has jurisdiction and which are applicable to **RMG LEATHER USA LLC** can be found at <https://www.whistleblowers.gov/statutes>.

Each statute requires that complaints be filed **within a certain number of days** of the alleged retaliation (ranging from 30 to 180 days).

Any person who believes that he or she has been retaliated against under a statute in connection with which a whistleblower protection scheme that falls within OSHA's jurisdiction applies may file a complaint of retaliation, as appropriate, with OSHA or with the other governmental authority with jurisdiction over whistleblower protection.

Complaints against the employer may be made **orally or in writing** (by fax, e-mail, regular mail) by the Whistleblower or his/her delegate (who will then serve as the point of contact with OSHA) and OSHA will accept the complaint **in any language**. **Anonymous complaints are not allowed**.

If the OSHA standard form template is used for the complaint, the complainant must complete all fields indicated as mandatory; the other fields are optional. Specific instructions on filling in the standard form can be found at: <https://www.osha.gov/whistleblower/WBComplaint>.

In the remainder of this chapter, the reference to OSHA should be understood as a reference to the competent public authority.

Filing a complaint

When a whistleblower files a retaliation complaint with OSHA, he or she becomes a "whistleblower". After the complaint is filed, OSHA investigators will conduct a preliminary review of the complaint to ensure that it was filed within the scope of the Act and the statute of limitations. Investigators may also interview the complainant to obtain the information necessary for an initial determination as to whether the conditions are met in order to initiate a subsequent investigation.

NB:: Although many protections for private sector whistleblowers are administered by OSHA, substantial portions of the underlying statute are enforced by what OSHA calls 'partner agencies'. For example, OSHA investigates allegations of retaliation under the Taxpayer First Act, but the IRS enforces the other parts of the law, including the rewards program.

Investigation of retaliation allegations

If the complainant passes the initial merits assessment, OSHA investigates to determine whether unlawful retaliation occurred.

At this stage, the complainant, the subject of the complaint, and the partner agency, if applicable, are informed that OSHA has initiated an investigation. Both parties are required to participate in the investigation, providing documentation and statements to the investigator upon request.

Once the investigation is complete, OSHA will decide whether the subject of the complaint has suffered unlawful retaliation and will issue a remedy as permitted by the violated statute. Depending on the applicable law, whistleblowers may appeal to an administrative law judge.

NB: The investigation process can vary in length depending on the nature of the complaint and the relevant law. Several statutes allow the whistleblower to 'give OSHA the boot' and appeal directly to federal court if the investigation does not result in a final decision a certain number of days (180 or 210 depending on the statute in question).

For a full explanation of the rules of the investigation process, OSHA's Whistleblower Investigation Manual can be found at: https://osha.gov/sites/default/files/enforcement/directives/CPL_02-03-011.pdf.

Alternative Dispute Resolution Option

If appropriate, the two parties can agree to participate in OSHA's free Alternative Dispute Resolution (ADR) programme, which suspends the ongoing investigation. This programme is only offered in some regional offices. In addition, the parties can reach their own independent alternative dispute resolution agreement, to be submitted to OSHA for approval.

ADR allows the parties to agree on a mutually acceptable remedy in lieu of the investigation and resolution process. If the parties cannot agree, the investigation resumes.

If you have any questions about filing a complaint with OSHA or the investigation process, you can call 1-800-321-OSHA (6742) or contact your local OSHA office.

Violations handled by the DOJ under the FCPA

The procedure for filing an anonymous whistleblower complaint under the FCPA is as follows.

First, the whistleblower must hire a US-licensed attorney.

Second, the whistleblower must provide the lawyer with his original information and must sign an official SEC form ("TCR" or "Tip, Complaint or Referral").

Third, the signed form is provided to the lawyer, who must keep it in his files.

Fourth, the lawyer deletes all identifying information about the whistleblowers and signs the form verifying the filing under oath. The lawyer then files the form directly with the DOJ. Therefore, although the US government does not know the name of the whistleblower, the whistleblower's lawyer can be held liable for any misconduct by the lawyer or the whistleblower.

3.2.3. Complaint to ANAC (in Italy)

Whistleblowers may report to the ANAC any retaliation they believe they have suffered.

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

3.2.4. Burden of proof

In Italy

In the context of judicial or administrative proceedings or, in any case, of extrajudicial disputes concerning the ascertainment of the conduct, acts or omissions, constituting a prohibited Retaliation, it is presumed that the same have been put in place because of the Reporting or the Public Disclosure itself.

The burden of proving that they were motivated by duly justified reasons unrelated to the Report or Public Disclosure rests on the Whistleblower.

In the event of a **claim for damages brought before the court by the Whistleblower** (not, therefore, also by other Protected Persons), if he reasonably proves that he has made a Report or

Public Disclosure and has suffered damage, it **is presumed, unless the accused proves otherwise, that the damage is a consequence of such Report or Public Disclosure.**

In Sweden, Brazil and Mexico

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 violation of the whistleblowing legislation, alleges circumstances that give reason to suppose that this is the case, the burden of proving that such measures were not taken is **on the defendant**.

3.3. Limitations of liability

3.3.1. In Italy, Sweden, Brazil, Mexico

The reporting entity or person shall not be criminally liable, and **any further civil or administrative liability**, in judicial proceedings, for the disclosure or dissemination of Infringement Information is also **excluded**:

- covered by **secrecy** obligations (official, corporate, professional, scientific, commercial or industrial) (e.g. punished by Articles 326, 622, 623 of the Italian Criminal Code)
- relating to the protection of **copyright**,
- relating to **the protection of personal data** (privacy),
- offending the reputation of the Involved Person (**defamation**), or

provided, however, that there were **reasonable grounds to believe that** the Public Reporting or Disclosure of the same Information **was necessary** to disclose the Infringement.

The above-mentioned criminal, civil and administrative exemption, however, does not apply

- a) in the case of **criminal conduct that the Whistleblower engages in 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 breaches the e-mail system of a work colleague in order to obtain evidence in support of the Report, and

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

The Company may also order the imposition of **disciplinary sanctions** against the persons who decide the Retaliation, in accordance with the following documents:

- National Collective Labour Agreement and the Company Collective Bargaining Agreement, if any (to be understood as expressly referred to herein), and/or
- 231 Organisational Model.

3.3.2. In the U.S.

On a voluntary basis, the same limitations of liability as set out above are granted by **RMG LEATHER USA LLC** to the Whistleblower.

Any mandatory provisions of applicable local law, if any, remain unaffected.

3.3.3. Mandatory Form of Waiver and Settlement

The rights and protections envisaged in favour of the Reporting Party **may not be subject to waiver or settlement**, in whole or in part, which, therefore, shall be considered invalid, **unless they are made in the form and manner set forth in Article 2113, fourth paragraph, of the Italian Civil Code**.

4. SUPPORT MEASURES

In Italy

The Whistleblower is also entitled to **support measures** consisting of **free information, assistance and advice** on how to report and on the protection from retaliation offered by national and EU legislation, 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 (ETS) 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 Reporting Party from these Third Sector Entities, even before the actual communication of the Report.

NB: The activity of the ETS is to provide information, assistance and advice in the terms set out above, also during the Whistleblowing process; however, the actual Whistleblowing has to be done personally by the Whistleblower, and in any case the activities of the ETS have to be kept separate from the actual examination of the Whistleblowing, which is the sole responsibility of the Whistleblowing Committee.

In Sweden

Organizations eligible for government grants (employer and employee organizations, non-profit organizations that address workplace safety and environmental issues, or combat corruption and other abuses in the workplace) **must provide information and advice to individuals protected by the Act 2021:1890.**

The information and advice must address:

- What protections do you have as a whistleblower?
- How and to whom to report misconduct?
- How your personal data will be processed.
What information is subject to confidentiality or secrecy.

However, there is not a central official list published by the government with specific names of such entities (e.g. NGOs, trade unions, environmental or anti-corruption organizations) to which the whistleblower can turn to receive.

If you're looking for the contact information of a reliable organization to contact, we suggest two practical approaches:

- **Check the website of the organization that received funding** (e.g., NGOs, unions, foundations): they often clearly indicate the whistleblowing channels and mandatory

information, and already have a contact person or internal contact to ask "what to do and who to contact."

Per maggiori informazioni sui soggetti che ricevono fondi governativi, puoi consultare il link: <https://www.av.se/arbetsmiljoarbete-och-inspektioner/lagar-och-regler-om-arbetsmiljo/visselblasarlagen/statsbidrag/>

- **Contact the relevant authorities directly:** the Swedish Work Environment Authority can provide advice and support to those who are considering making a complaint (link: <https://www.av.se/om-oss/kontakta-oss/>).

In the U.S.

The Office of the Whistleblower Ombuds has developed a general guide for Whistleblowers, with resources and information available on the following webpage: <https://whistleblower.house.gov/whistleblower-audience>.

People who wish to whistleblow should first **consult a lawyer experienced** in representing whistleblowers and/or an organisation that works with whistleblowers and has their best interests in mind.

At <https://whistleblower.house.gov/whistleblower-support-organizations> you will find a list of non-profit organisations that have extensive experience working with whistleblowers. You can consult them for support. Some of the organisations also offer legal representation and guidance resources available to the public.

At <https://www.pogo.org/legal-and-advocacy-resources-for-whistleblowers> you will find a list, developed by the Project On Government Oversight, of US law firms that have experience working with whistleblowers.

5. CONFIDENTIALITY

5.1. Generalities

Whistleblowers may not be used beyond what is necessary for the purpose of proper follow-up.

The non-anonymous Whistleblower shall be guaranteed, by the Company, the Whistleblowers' Committee and anyone else involved in receiving and processing a Whistleblowing, confidentiality regarding

- **his or her identity and that of the Facilitators** (right to confidentiality), throughout the process of handling the Report, to anyone who is not the Report Manager or otherwise authorised, and
- **the content of the Report**, including the **documentation** attached to it, to the extent that its disclosure, even indirectly, may allow the identification of the Whistleblower.

In all phases of activity, **it is forbidden to reveal the identity of the Whistleblower to the Reported Subject and to other subjects not expressly authorised, without the express consent of** the Whistleblower.

The Internal Reporting Channels adopted by the Company must, therefore, guarantee the aforementioned confidentiality, which also extends to the identity of any other interested person

mentioned in the Report (e.g. Involved Person, witnesses, etc.) or whose name is identified in the course of the assessments and investigations following the Report.

In this regard, specific confidentiality undertakings will also be signed with the persons in charge of handling them.

5.2. Exclusion of confidentiality

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

(i) when the **disclosure of** the identity of the Alerts **is a necessary and proportionate obligation** imposed by Union or national law **in the context of investigations** by national authorities **or judicial proceedings**, including in order to safeguard the rights of defence of the person reported.

To this end, **the Alerted Person should be warned without delay by the Handlers of the Report of an unfounded Report made in bad faith or with gross negligence to his/her detriment** in order to be able to consider whether to exercise any rights against the person making the Report⁵ ; or

ii) the existence of an **obligation to communicate** the name of the Whistleblower **to the judicial authorities** (Court, Public Prosecutor's Office), **or the Police**, or

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

(iv) where **knowledge of** the identity of the **Whistleblower is indispensable for the accused's defence**, only where the Whistleblower has given his/her express **consent** to the disclosure of his/her identity.

Such disclosures are subject to the guarantees provided for by the applicable rules. 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** the disclosure of confidential data **before** his/her identity **is disclosed, unless this would prejudice the related investigation or judicial proceedings** .⁶

The Company, the Handlers of the Report and anyone else involved in receiving and processing a Report must also protect **the identity of the Persons Involved and of the other persons mentioned in the Report** until the conclusion of the proceedings initiated as a result of the Report, in compliance with the same guarantees of confidentiality provided for in favour of the Whistleblower.

In the U.S.A.

In the U.S.A., the anonymity of the Whistleblower is always guaranteed.

⁵ In order to allow the reported person to file a complaint-complaint for the offence of slander, defamation or any other offence that may be detectable in the specific case, and also in view of the fact that the reported person, in Italy, 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).

⁶ The competent authority, when informing the Whistleblower as above, sends the reporter a written explanation of the reasons for disclosing the confidential data in question.

6. ASSUMPTIONS OF THE PROTECTIONS. WHISTLEBLOWING IN BAD FAITH OR WITH GROSS NEGLIGENCE

The Protection Measures described above 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 Information** about the Reported or Complained or Publicly Disclosed Violations **was true**, even if no conclusive evidence is provided, and fell within the objective scope of Section 2.3; and
- b) the Report or Public Disclosure was made on the basis of the provisions of this Procedure and applicable law.

The Protection of the Protected Persons also exists in the case of **Reports or Disclosures that later prove to be unfounded**, if the Reporting Party, at the time of the Report or Public Disclosure, had **reasonable grounds to believe that the Report was necessary to disclose the Breach** 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 Persons are not guaranteed, and a Disciplinary Sanction shall also be imposed on the Whistleblower, if **it is established, even by a first instance judgement**

- i) **criminal liability of** the Whistleblower **for the offences of slander or defamation** in relation to the facts reported, or
- ii) **the civil liability** of the Whistleblower, 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 with the **awareness of** the **abuse/instrumentalisation** of the Reporting procedure, e.g. manifestly unfounded, **opportunistic** and/or made for the **sole purpose of damaging** the Reported Person or other persons mentioned in the Report (employees, members of corporate bodies, suppliers, partners, group companies, etc.) are to be considered in **bad faith/gross negligence** (and therefore a source of liability, in disciplinary and other competent fora).

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

7. LIMITATIONS OF THE PROTECTIONS IN THE CASE OF NON-EU COMPANIES, AND/OR EU COMPANIES WITH LESS THAN 50 EMPLOYEES

The present Procedure is applied, not as a regulatory obligation but on an exclusively **voluntary** basis, also to the Companies of the RINO MASTROTTO Group with headquarters outside the European Union, and/or to Companies with headquarters in the EU but with a number of employees, calculated as the average of the last 12 months, of less than 50.

In such cases, some protections and/or support measures provided for by the applicable laws, and in particular those falling under the exclusive competence of third party Authorities (e.g. ANAC) and/or third parties, will not be applicable in favour of the Protected Persons; in any case the Company will voluntarily guarantee to them the following protections

- it shall process whistleblowing data in accordance with criteria of **confidentiality** and in compliance with **personal data protection** legislation, and
- undertakes to respect and enforce, to the extent of its competence, **all the provisions of this Procedure**, it being understood that, with regard to the Protections due to the Whistleblower, to the other Protected Persons, and to the reported person, the same shall be **waived** as follows:
 - ✓ There is no obligation for the Company to inform the union in advance about the activation of the Whistleblowing Procedure,
 - ✓ **It will not be possible to send a Report to ANAC** in the specific cases provided for by the Whistleblowing Decree, **and/or to complain to ANAC, any retaliatory acts** (NB: the same, however, can always be complained to the Judicial Authority, e.g. Court).
 - ✓ **It will not be possible to have recourse, in a further subordinate way, to Public Disclosure**, if the specific prerequisites which are otherwise provided for by the Whistleblowing Decree are met (the company's interest in confidentiality having to be considered prevailing).
 - ✓ There are no exemptions from civil, criminal or administrative liability in favour of whistleblowers who breach laws on industrial secrets, privacy, copyright.
 - ✓ **No support measures are** available free of charge in favour of the whistleblower.
 - ✓ The obligation to waive and settle one's rights exclusively through the procedures provided for in the Italian Code of Civil Procedure will not apply.
 - ✓ **The regime of reversal of the burden of proof will not apply** in the event of legal action to enforce possible retaliatory acts against the Whistleblower and the other Protected Persons, or possible damages and compensation.

This is in any case **without prejudice to the right to report the matter to the judicial authorities**, if provided for by law (e.g. lawsuit).

8. REWARDS TO WHISTLEBLOWERS

8.1. Remuneration based on the False Claim Act

In the event of a Report of a False Claim Act Violation, the Whistleblower shall be entitled to remuneration calculated on the total amount that the Federal Government recovers as a result of the Report, as follows.

The Whistleblower may obtain from the Government, in addition to the **reimbursement of the legal costs**, a remuneration - in some cases absolutely guaranteed - calculated on the total amount that could be recovered thanks to the Report, as follows.

The remuneration varies **between 15 and 25% of the amounts recovered** through the penalty imposed on the convicted person or the settlement reached between the Government and the reported taxpayer.

If the Government does not intervene in the so called *qui tam action* against the taxpayer, the percentage will be **between 25% and 30%** of the amounts recovered.

The Court may **reduce** the remuneration, but **to no less than 10%** of the amounts recovered, if it finds that the case is based primarily on the disclosure of specific information (other than the information provided by the person bringing the case) revealed in a criminal, civil or administrative

hearing, in an administrative or federal office or through the media (subject to the reimbursement of legal costs to the complainant by the defendant).

Remuneration **is not due** if the complainant (relator in the qui tam case) is convicted of the reported violation in criminal proceedings.

Remuneration may be **reduced below the limit of 10 per cent of the proceeds recovered, or even be disallowed**, where the whistleblower has planned and given rise to **violations under Section 3729**.

8.2. Remuneration based on the Internal Revenue Code

In the case of a Whistleblower Report containing information about a Violation of tax or other laws that the IRS may handle, enforce, or investigate, the Whistleblower may obtain from the IRS Whistleblower Office remuneration - in some cases absolutely guaranteed - calculated on the total amount the IRS recovers as a result of the Report, as follows.

The remuneration depends on various factors, but as a rule, according to the **Internal Revenue Code**, varies **between 15 and 30% of the amounts recovered** by the IRS attributable to the information contained in the Whistleblower's documented and articulated whistleblowing. This requires that **the amount evaded by the Reporting Taxpayer** in the Whistleblower's complaint to the IRS **must exceed \$2 million**, including taxes, penalties and interest.

If this prerequisite is not met, the award of remuneration by the IRS **will be discretionary** (subject to case-by-case assessment) **and in any event not exceeding 15%** of the amount recovered.

The remuneration is payable only after the issuance of a final decision and until the obligated taxpayer has exhausted any right of appeal and can no longer file for refund or otherwise oppose the administrative procedure.

More details on how to report violations of tax laws or other laws within the jurisdiction of the IRS **to the IRS** - Whistleblower Office through an **Application for Award for Original Information** by the Whistleblower, as well as on the criteria for determining the remuneration due to the Whistleblower, can be found at the link: <https://www.irs.gov/compliance/whistleblower-office>.

The same website mentioned above also provides a link to **Publication 5261, The Whistleblower Claim Process and Timeline**, which contains a general description of the IRS Whistleblower Claim Process.

8.3. Remuneration based on the FCPA

The Foreign Corrupt Practices Act provides rewards to whistleblowers who provide original information leading to successful recovery of bribes paid to foreign government officials by U.S.-based companies.

Whistleblowers are entitled to financial remuneration of between 10% and 30% of all sanctions obtained by the government⁷. These rewards are available to non-US citizens for bribes paid outside the United States.

8.4. Anti-Money Laundering Act (AMLA) - FinCEN Whistleblower Program

The Anti-Money Laundering Act (AMLA) provides rewards to whistleblowers who report violations of anti-money laundering laws.

⁷ The DOJ has an intervention rate (including settlements) of almost 25% in qui tam False Claims Act cases submitted by whistleblowers.

Whistleblowers are entitled to financial remuneration of between 10% and 30% of sanctions in excess of \$1 million.

The body administering the rewards is the Financial Crimes Enforcement Network (FinCEN).

APPENDIX C - PROCESSING OF PERSONAL DATA

1.1 Any processing of personal data carried out for the purposes of the management of the Report must be carried out in accordance with the legislation on the protection of personal data (GDPR, Supervisory Measures, Legislative Decree 196/2003) . ⁸

Accordingly, anyone involved in the receipt and processing of non-anonymous Reports **is required to comply with all the policies, delegations, appointments, authorisations, procedures, protocols and written security instructions set out in the Company's privacy system**, without prejudice to the further rules set out in this procedure.

1.2 Personal data that appear not reasonably pertinent 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 appropriate Report Handlers with respect to the Breach.

Similarly, **any personal data reported and referring to conduct not included in the scope of the law and/or this Procedure will be deleted**.

If the information **received contains personal data included in the special categories of data referred to in Article 9 of the GDPR, it will be deleted immediately**, without being recorded and processed.

1.3 If it is established that the information provided or part of it is untrue, it must be deleted immediately as soon as this circumstance emerges, **unless the untruthfulness may constitute a criminal offence**, in which case the information will be retained for as long as necessary during the legal proceedings.

1.4 The aforementioned processing operations must be carried out by the Company (data controller) in compliance with the general principles set out in Articles 5⁹ and 25¹⁰ of the GDPR, as well as by taking appropriate measures to protect the rights and freedoms of the data subjects.

⁸ And, by 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.

9 Art. 5 GDPR: Personal data shall be:

(a) processed lawfully, fairly and transparently towards the data subject ("lawfulness, fairness and transparency");
(b) collected for **specified, explicit and legitimate purposes**, and further 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**; every reasonable step must be taken to ensure that data which are inaccurate in relation to the purposes for which they are processed ('accuracy') are erased or rectified without delay
(e) **kept** in a form which permits identification of data subjects **for no longer than is necessary for the purposes for which** they are processed ('limited storage'); and
(f) processed in a way that **ensures 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')

10 Article 25 GDPR: Article 25 Data protection by design and data protection by default

1. Taking into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing, as well as risks of varying likelihood and severity to the rights and freedoms of natural persons posed by the processing 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 processing are processed by default. This obligation shall apply to the amount of personal data collected, the scope of the processing, the storage period and the 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.

1.5 The Reporting Committee of each Company, in coordination with the IT Function and the ESG Function

- defines, by means of this procedure and the annexes thereto, its own model for the receipt and management of Internal Reports, identifying technical and organisational measures suitable to guarantee a level of security appropriate to the specific risks arising from the processing operations performed,
- regulates the relationship with any external suppliers that process personal data on behalf of the Company pursuant to Article 28 of the GDPR (e.g. external Data Processors appointed by the Company, third party technical managers of the Portal/Software)
- provides, and/or identifies the different corporate Functions, if any, in charge of providing, to the Whistleblower, to the Involved Persons and to the other relevant categories of data subjects, appropriate *information on the processing of personal data* (pursuant to Articles 13 and 14 of the GDPR), in compliance with the texts approved by the competent administrative body of the Company.

1.6 Access to the personal data contained in the Portal/Software shall be limited, within the scope of their respective competences and functions, exclusively to:

- a) the System Managers (Admin) who directly manage it, within the limits of the privileges attributed to the same;
- b) the Case Managers designated on the basis of this Procedure, and, upon their authorisation, the external consultants delegated in the investigation, with whom prior confidentiality agreements will be signed;
- c) any appointed Data Processors (which include the Supervisory Board 231 when it acts as Case Manager limited to Reports concerning 231 Breaches) and/or any external data processors designated by the Company (which include the Supervisory Board 231 when it acts as Case Manager in relation to Reports not concerning 231 Breaches).

1.7 This Procedure also represents, pursuant to and for the effects of art. 13 paragraph 5 of the Whistleblowing Decree, an **internal co-ownership agreement** between the Companies of the RINO MASTROTTO Group, aimed at

- a. Discipline the **sharing of resources** (e.g. Portal/Software) for the receipt and management of Reports.
Further persons in charge are designated by the Company according to the criteria better illustrated in the section "Communication of personal data" below.
- b. Determine the respective **responsibilities** and privacy vestiges with regard to compliance with the obligations on the protection of personal data, pursuant to Article 26 of the GDPR, as follows:
Co-processors are the companies of the RINO MASTROTTO Group indicated in point 3.2.1, with regard to the processing of data related to:
 - **the reciprocal sharing of the internal reporting channel** consisting of the Portal/Software; and
 - **the Whistleblowing Procedure** for the communication/collection and management of reports;

- the possible **use/intervention of Case Managers designated centrally** by RINO MASTROTTO GROUP SPA in relation to the management of Reports concerning a Subsidiary Company.

In particular, each Company is to be considered as autonomous owner of the personal data treatment in relation to Reports of Violations concerning the same, except for the following: the aforesaid centralised service for the collection and management of Reports involves the **processing of personal data in partial sharing between RINO MASTROTTO GROUP SPA** (and its Admins and/or Case Managers and/or other authorised subjects if centrally designated, when the same manage the Reports in outsourcing on behalf of the single Companies) **and the single Subsidiary** (in relation to the activities of the respective Case Managers and/or other authorised subjects, if the same do not coincide with those centrally designated by RINO MASTROTTO GROUP SPA to act also in the interest of the single Subsidiary), with consequent application of a **co-ownership** regime among them pursuant to art. 26 of the GDPR.

c. **Determine the rules on information to data subjects pursuant to Articles 13-14 GDPR:**

The *Whistleblowing Privacy Notice* must be made available to Data Subjects, by the relevant Whistleblowing Committee or Whistleblowing Manager, in the following main ways:

- by means of a **link/text that can be viewed on the landing page of the Portal/Software**;
- by hand delivery, or as an attachment to a chat via videoconference, at the first useful opportunity, in the case of a **personal meeting** with the Reporting Subject who has not used the Report Portal/Software
- in the event that the first useful contact with the person concerned takes place by telephone (in particular in the event that the Whistleblower requests a personal meeting by telephone): by verbal notice of the availability of the *Privacy Policy* on the landing page of the Portal/Software and/or in the separate "whistleblowing" section in the footer of the website of each of the Companies.

d. **response to the exercise of the rights of the data subject:** each Company acts as an independent data controller, in accordance with its own procedures for managing the exercise of the rights of data subjects, to which reference is made herein;

e. **personal data breaches:** each Company acts as an autonomous data controller in accordance with its own procedures for managing data breaches relating to personal data connected to the Reports, to which reference is made herein; and

f. **security measures:** each Company of the Group is required to comply with the security measures provided for i) by this Procedure, ii) by the technical-functional specifications of the Portal/Software, iii) by its own privacy system, iv) by the personal data protection legislation applicable to it;

the security measures applied to the Portal/Software are illustrated in the mandatory DPIA document prepared by the Company as well as in the additional documents referred to therein from time to time; and

g. **operative interface with the third party supplier of the Portal/Software:** RINO MASTROTTO GROUP SPA acts as exclusive centralised technical interface towards the supplier, on behalf of the other Companies, on the basis of a mandate with representation to be intended as conferred herein by the same.

APPENDIX D - TRAINING

Training of Case Managers

Specific training, to be updated periodically, must be provided, first and foremost, to those involved in the management of Reports, with the aim of providing them with the fundamental skills necessary for the implementation and effective management of whistleblowing processes, as well as knowledge of the issues covered by the reports (see ANAC Guidelines, point 5).

It is advisable that these individuals receive detailed training on the various aspects of report management with a view to promoting autonomous, ethical and professional conduct. Therefore, staff must be trained on at least the following topics:

- the regulatory framework governing whistleblowing (both European legislation and the provisions contained in Legislative Decree No. 24/2023), with particular attention also to the issue of personal data protection, in order to ensure maximum security and confidentiality of information;
- procedures and operating methods, with a specific focus on the duties to be performed by Report Managers, including the management of conflicts of interest;
- general principles of conduct (confidentiality and privacy, ethics and integrity, active listening, communication skills and collaboration).

As an alternative to the above training, the aforementioned specific skills and knowledge may be demonstrated by the Reporting Managers through CVs, certificates or similar documentation.

Training for all employees and non-employees of the organisation

The training must involve all employees and collaborators of the Company in order to provide a clear and comprehensive overview of the new regulations (clarifying, for example, who the Whistleblower is, what can be reported and through which channels, what protections the law guarantees to the whistleblower and which reports, on the other hand, are not covered by such protections, as well as specifying the involvement - also guaranteed by the protections - of the various persons operating in the same working environment as the Whistleblower).

APPENDIX E - PORTAL/SOFTWARE MANUALS

- EQS v3 Manual