MARMOLES MAN
CARRARA

MARMOLES MAN SRL

WHISTLEBLOWING REPORT MANAGEMENT PROCEDURE

WHISTLEBLOWING

Approved by the Board of Directors of MARMOLES MAN SRL on 15 January 2024

Index

1. Purpose and scope 4

2. Reports 5

2.1 Subject of the report 5

2.2 Content of the report 5

2.3 Anonymous reports 6

2.4 Report sent to a non-competent person 6

3. Regulatory requirements 6

4. Protections 6

4.1 Confidentiality protection 7

4.2 Protection against retaliation 7

4.3 Limitations of liability for persons who report, complain or make public disclosures 8

2. Frequency 10

3. Equipment, products and software used 11

4. Activities 11

5. Controls, records and reports 14

6. Operating instructions and related documents 14

1. DATA CONTROLLER 18

2. SOURCE OF THE DATA PROCESSED 19

3. TYPES OF DATA PROCESSED 19

4. PURPOSES AND LEGAL BASES OF PROCESSING 19

5. ANONYMOUS REPORTING 20

7. PROCESSING METHODS 21

8. TRANSFER OF DATA ABROAD 21

9. DATA RETENTION PERIODS 22

1. Purpose and scope

The Whistleblowing System is a tool through which employees or third parties of a company (such as suppliers or customers) can report, confidentially and in a protected manner, any wrongdoing of which they have become aware in the context of their work. Following the transposition of EU Directive 2019/1937 by Legislative Decree no. 24 of 10 March 2023, adoption of the tool has become mandatory for companies with at least 50 employees and/or that have adopted an Organisation and Management Model pursuant to Legislative Decree no. 231/2001. The new legislation requires the establishment of reporting channels **to be used progressively and subsidiarily (and NOT alternatively)**:

i. i. Internal Channel;

ii. ii. External Channel;

iii. iii. Public disclosure or complaint to the judicial authority.

The manager of the internal channels adopted by **MARMOLES MAN SRL** (hereinafter "MARMOLES MAN") is the Supervisory Body, a collegial body made up of members external to the Company, endowed with autonomy and independence and able to offer adequate guarantees of confidentiality and data protection. The purposes are:

- to introduce, in addition to ordinary controls, a system of mutual oversight extended to every single member of staff that can guarantee anonymity. The information is in fact sent to the Supervisory Body in the person of its pro tempore Chair, who will bear full responsibility for guaranteeing the anonymity of the person making the report;
- to adopt a monitoring and reporting system that enables the early identification of a solution to certain problems, as well as the prevention of others;
- to be compliant with the national and European legislation in force on the subject.

MARMOLES MAN is required to make clear information available to the various interested parties ("stakeholders") on the channels, procedures and prerequisites for making both internal and external reports.

Subjects

Stakeholders, and therefore beneficiaries of the protections and safeguards guaranteed by the legislation, are:

- Employees;
- Self-employed workers who carry out their work activity at the entity;
- Suppliers, sub-suppliers and their employees;
- Freelance professionals and consultants;
- Agency workers;
- Volunteers and trainees, regardless of whether they receive any reimbursement of expenses;
- Shareholders and persons with administrative, management, control, supervisory or representative functions, even where such functions are exercised de facto;
- Those who do not yet have a legal relationship with the entity (during pre-contractual negotiations), as well as those whose relationship has ended or who are on probation.

2. Reports

2.1 Subject of the report

- For the purposes of the Whistleblowing legislation, the subject of a report consists of **breaches** and any active or omissive conduct, actual or suspected, capable of constituting a breach of:
  i. i. the provisions contained in Legislative Decree 231;
  ii. ii. the provisions contained in the Company's Model 231, including the control protocols and procedures forming an integral part of it;
  iii. iii. the Company's Code of Ethics.

The following do NOT constitute breaches and therefore cannot be the subject of a report:

- reports that are manifestly unfounded;
- information that is already in the public domain;
- so-called “corridor gossip”, that is, information acquired solely on the basis of rumours or hearsay which, by their nature, are scarcely reliable;
- mere personal grievances of the reporting person;
- claims relating to the employment or collaboration relationship, or to relations with superiors or colleagues;
- so-called “irregularities”, to be understood as situations in which, in the course of administrative activity, improper conduct by a public official is found which, also in order to pursue their own interest or that of third parties, takes or contributes to a decision that deviates from the impartial pursuit of the public interest. Since the amendment, these were previously classed as breaches of national law and no longer constitute, in re ipsa, the subject of a report, but may be symptomatic elements attributable to Art. 2, para. 1, letter b), of Legislative Decree 24/2023, such as to lead the reporting person to believe that one of the breaches provided for by the decree could be committed.

2.2 Content of the report

To allow the correct reconstruction of the facts and irregular conduct, the report must be detailed as far as possible, and must therefore contain the following essential elements:

- the identity of the reporting person (save in the case of anonymous reports – see para. 2.3);
- the circumstances of time and place in which the facts reported occurred;
- a clear, complete and detailed description of the facts;
- the identity or other elements enabling the identification of the person to whom the reported facts are attributed, and of any other persons involved;
- where applicable, contact details for confidential follow-up.

It is useful to attach supporting documents so as to provide evidence of the facts reported, and to indicate other persons who may be aware of the facts. If the report is not adequately detailed, the report manager may, where possible (or where contact details are included in the report), request further supplementary information from the reporting person through the same dedicated channel, or in person if they have requested a direct meeting.

2.3 Anonymous reports

Anonymous reports are those from which the identity of the author cannot be determined. Anonymous reports are treated as ordinary reports and managed according to the same criteria, except as regards requesting further supplementary information (since no contact details have been provided).

2.4 Report sent to a non-competent person

Where an internal report is submitted to a person other than the one identified and authorised by the Company, and the reporting person declares that they wish to avail themselves of the Whistleblowing protections, or that intention can be inferred from the content of the report, the report will be considered a “Whistleblowing report” and will be forwarded to the Supervisory Body within 7 days of receipt, with the reporting person being notified at the same time.

3. Regulatory requirements

The Company, after consulting the trade-union representatives and the trade-union organisations most representative at national level, establishes internal reporting channels within itself, defining the procedures for receiving reports in a dedicated organisational document. The organisational document includes:

- the role and duties of the persons who manage reports;
- the methods and periods for retaining data, appropriate and proportionate in relation to the Whistleblowing procedure and to the provisions of law.

The management of internal reporting channels is entrusted, alternatively, to:

- an internal person or office with dedicated, autonomous staff specifically trained for this purpose;
- an external person, likewise autonomous and specifically trained;
- mandatorily to the Anti-Corruption and Transparency Officer (RPCT) in public-sector entities required to appoint such a figure.

MARMOLES MAN **has chosen to appoint an external person** in order to guarantee autonomy and independence in the management of reports.

4. Protections

Legislative Decree 24/2023 provides a system of protections that includes:

- 1) protection of the confidentiality of the reporting person, of the facilitator, of the persons involved and of those mentioned in the report;
- 2) protection against any retaliation adopted by the entity on account of the report, public disclosure or complaint made, and the conditions for its application;
- 3) limitations of liability with respect to the disclosure and dissemination of certain categories of information, which apply when certain conditions are met.

Waivers and settlements concerning the means of protection provided for by the decree are not valid unless signed in the protected judicial, administrative or trade-union venues pursuant to Art. 2113, para. 4, of the Civil Code. Given the broad scope of the subjective application of the

legislation, the following are also beneficiaries of the protections and safeguards guaranteed by it:

- Facilitator, that is, the natural person who may assist (providing advice or support) the reporting person in the reporting process, operating within the same work context;
- Persons from the same work context as the reporting person who are linked to them by a stable emotional bond or by kinship up to the fourth degree;
- Work colleagues who work in the same work context as the reporting person and who have a regular and current relationship with that person;
- Entities owned by the reporting person, either exclusively or in majority joint ownership with third parties;
- Entities for which the reporting person works;
- Entities operating in the same work context as the reporting person.

4.1 Confidentiality protection

The Supervisory Body, which receives and manages reports, adopts all measures necessary to guarantee the confidentiality of the identity of the reporting person; the principles of limitation and minimisation laid down by the legislation on the protection of personal data are observed, and the data collected may not be used beyond what is necessary to follow up the report. Without the consent of the person directly concerned, neither the identity of the reporting person nor any other information from which that identity may be directly or indirectly inferred may be disclosed to persons other than those competent to receive the report. In criminal proceedings, the identity of the reporting person is covered by secrecy in the manner and within the limits provided for by Art. 329 of the Code of Criminal Procedure, which imposes secrecy on the acts of preliminary investigations until the suspect has the right to know them, and in any case no later than the close of that stage. In proceedings before the Court of Audit, the identity of the reporting person may not be disclosed until the close of the investigation stage. In disciplinary proceedings, the identity of the reporting person may not be disclosed where the disciplinary charge is based on investigations distinct from and additional to the report, even if they follow from it. Where the charge is based wholly or partly on the report and knowledge of the reporting person's identity is indispensable for the defence of the accused, the report may be used for the purposes of disciplinary proceedings only with the express consent of the reporting person to the disclosure of their identity. The report is exempt from access to administrative documents under Arts. 22 et seq. of Law no. 241/1990 and from generalised civic access under Arts. 5 et seq. of Legislative Decree no. 33/2013. Confidentiality is likewise ensured for the facilitator assisting the reporting person and for persons other than the reported person who are mentioned in the report.

4.2 Protection against retaliation

The reporting person is protected against any retaliation against them, meaning “any conduct, act or omission, even if only attempted or threatened, carried out on account of the report, of the complaint to the judicial authority or of the public disclosure, and which causes or may cause the reporting person or the complainant, directly or indirectly, unjust harm”. A reversal of the burden of proof is also provided for as regards the retaliatory nature of the conduct and the harm suffered. By way of non-exhaustive example, the following may be classified as retaliation:

- dismissal, suspension or equivalent measures;
- demotion or failure to promote;
- change of duties, change of place or working hours, reduction of salary;
- suspension of training or restrictions on access to it;
- negative performance notes or negative references;
- adoption of disciplinary or other measures, including financial ones;
- coercion, intimidation, harassment or ostracism;
- discrimination or similar unfavourable treatment;
- failure to convert a fixed-term employment contract into an open-ended contract, where the worker had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage to the person's reputation or financial or economic harm, such as loss of income or business opportunities;
- inclusion in improper lists on the basis of a formal or informal sector or industry agreement, which may prevent the person from finding future employment in the sector or industry;
- early termination or cancellation of a contract for the supply of goods or services;
- cancellation of a licence or permit;
- request to undergo psychiatric or medical examinations.

To benefit from protection against retaliation, the report/public disclosure/complaint to the judicial authority must:

- have been made on the basis of a reasonable belief that the information reported, disclosed or complained of is true and falls within the objective scope of application of the decree;
- have been made in compliance with the rules of Legislative Decree 24/2023;
- be causally linked to the retaliatory measures suffered;
- not be based solely on mere suspicions or corridor gossip.

Without prejudice to the specific cases of limitation of liability (see below – 4.3), the protection provided in case of retaliation is **not** guaranteed when the criminal liability of the reporting person for the offences of false accusation and defamation, or for the same offences committed through the complaint to the judicial or accounting authority, is established, even by a first-instance judgment, or when their civil liability for the same reason is established in cases of wilful misconduct or gross negligence.

4.3 Limitations of liability for persons who report, complain or make public disclosures

In addition to the protections granted to the reporting/complaining/disclosing person, the law recognises certain limitations of liability following the disclosure or dissemination of certain categories of information which, in different circumstances, would entail civil, criminal or administrative liability on the part of the author. Specifically, the act does not constitute an offence, if committed in the presence of the aforementioned justification, in the following cases:

- disclosure and use of official secrets (Art. 326 of the Criminal Code);
- disclosure of professional secrecy (Art. 622 of the Criminal Code);
- disclosure of scientific and industrial secrets (Art. 623 of the Criminal Code);
- breach of the duty of loyalty and fidelity (Art. 2105 of the Civil Code);
- breach of the provisions relating to the protection of copyright;
- breach of the provisions relating to the protection of personal data;
- disclosure or dissemination of information about breaches that damages the reputation of the person concerned.

To benefit from the exclusion of liability, two specific requirements must be met at the same time:

- 1) well-founded reasons, at the time of collection or dissemination of the information, to believe that such disclosure or dissemination is necessary to reveal the breach;
- 2) the report/disclosure/complaint must have been made in compliance with the conditions of Legislative Decree 24/2023 (well-founded reason to believe that the information underlying the reports is true, use of the internal or external channel, public disclosure carried out in the manner prescribed by law).

(i) USE OF THE INTERNAL CHANNEL

The reporting person may send their report, together with any supporting documents, to the following addresses:

- **registered post**: Supervisory Body c/o MARMOLES MAN SRL, Viale Domenico Zaccagna no.
- 38, 54033 Carrara (MS). It is recommended that the report be sent in two sealed envelopes: the first containing the identifying details of the reporting person, an address and a telephone number at which they can be contacted, together with a photocopy of an identity document; the second containing the subject and description of the report, so as to separate the reporting person's identifying details from the report. Both
- must then be placed in a third sealed envelope bearing on the outside the words “confidential – for the attention of the Supervisory Body”);
- in **oral form** through a meeting requested by sending registered post (as above); with the reporting person's consent, the report is documented by the designated staff member in the form of minutes. The reporting person may check, correct and confirm the minutes of the meeting by signing them.

The Supervisory Body keeps a written record of all reports received, by maintaining a dedicated Register of Reports. Completeness checks are carried out periodically to verify that all reports received have been handled and entered in the Register of Reports. Once a report is received, a preliminary check of its admissibility and well-foundedness will be carried out. Personal data that are manifestly not useful for processing the report will not be collected or, if collected accidentally, will be immediately deleted. If the preliminary check is positive, appropriate follow-up will be given to the report, maintaining, where appropriate, dialogue with the whistleblower and requesting from them further clarifications, documents and information through the dedicated channel, or also through in-person meetings if they consent. Where necessary, documents and records will be obtained and third persons involved through hearings or other kinds of requests. The internal reporting system adopted guarantees the

reporting person appropriate confidentiality as to their identity, the content of the report and the documentation provided. Protection extends not only to the name of the reporting person but also to all elements of the report from which their identification could be derived, even indirectly. Information on the breaches provided by the whistleblower will be used by the Supervisory Body solely and exclusively for the purpose of following up the report and will not be used or disclosed in any other way. Where, at the request of the reporting person, the report is made orally during a meeting with the staff in charge, it is documented by the staff in charge, with the reporting person's consent, either by recording on a device suitable for storage and listening, or by minutes. In the case of minutes, the reporting person may check, correct and confirm the minutes of the meeting by signing them. Within three months of the date of the acknowledgement of receipt, or alternatively within three months of the expiry of the seven-day period from the submission of the report, feedback must be provided on the report.

(ii) USE OF THE EXTERNAL CHANNEL

It should be recalled that the new Legislative Decree no. 24/2023 has also introduced an "external" reporting channel, the **External Channel**, managed by ANAC (the Italian National Anti-Corruption Authority) and accessible at the following link: https://www.anticorruzione.it/-/whistleblowing. The **External Channel must be used under certain conditions**:

i. i. if the internal reporting channel is not present, since it is not mandatory, or is present but not active, or active but not compliant with Legislative Decree no. 24/2023;
ii. ii. if the reporting person has well-founded reasons to believe that, in the case of an internal report, due follow-up would not be given to it, or that they would be exposed to a risk of retaliation;
iii. iii. if the reporting person has already made an internal report to which no follow-up has been given;
iv. iv. if the reporting person has well-founded reasons to believe that the breach may constitute an imminent or manifest danger to the public interest.

(iii) USE OF PUBLIC DISCLOSURE OR COMPLAINT TO THE JUDICIAL AUTHORITY

Lastly, Legislative Decree 24/2023 has provided for the **Public Disclosure** channel, which consists of making information on breaches publicly known through the press, electronic media or, more generally, by using means of dissemination capable of reaching a large number of people (e.g. TV, radio, social networks), or by reporting the matter to the judicial authority. This last channel is to be used as a residual option, that is, when:

i. i. reports made through the other channels have not been followed up;
ii. ii. use of the other channels would expose the reporting person to a risk of retaliation (e.g. where there is a well-founded fear that the person to whom the report was made is colluding with the author of the breach, or is even personally involved);
iii. iii. the breach constitutes an imminent or manifest danger to the public interest.

2. Frequency

As necessary.

3. Equipment, products and software used

Not applicable.

4. Activities

Flowchart

Protocol

- LEVEL I LEVEL II LEVEL III
- PROCEDURAL SAFEGUARD SUBSTANTIVE SAFEGUARD
- CHECKS
- Input Output Phase owner Traceability: controls, records
- and reports
- Information to the Ethics Committee

USE OF THE INTERNAL CHANNEL

Breach and any active or omissive conduct, actual

- or suspected, capable of constituting a breach of the provisions contained in Decree 231:

• of the provisions contained in the Model

- Report of an attempted breach and of any active or omissive conduct, actual or suspected, capable of constituting a breach, to the SB through the internal channel.
- Whistleblower
- In writing, by registered post, or orally, at the express request of the reporting person, through a direct meeting to be held within a reasonable time.
- Where, at the request of the reporting person, the report is made orally during a meeting, it is documented, with the reporting person's consent, by
- The SB becomes aware of the report
- 231 of the Company, including the control protocols and procedures forming an integral part of it

• of the Company's Code of Ethics.

- recording on a device suitable for storage and listening, or by minutes. In the case of minutes, the reporting person may check, correct and confirm the minutes of the meeting by signing them.

Receipt of the report

- The report is taken in charge and, where possible, an acknowledgement of receipt is issued to the whistleblower within 7 days of receipt.
- If anonymous, verification is made of the attachment of serious and concordant evidence in support of the report.
- SB In the case of an oral report, and with the reporting person's consent, it is documented by recording on a device suitable for storage and listening, or by full transcription. The reporting person has the right to check, correct or confirm the

content of the transcription.

- The SB becomes aware of the report

Except in complex cases, the report is assessed within the following 10 days: it is decided whether it is well founded or not, whether the reporting person is among the qualified persons, and whether the case or conduct reported represents a

- If not well founded, the file is closed.
- If well founded, a request for clarification is sent to the author of the breach or attempted breach.
- SB Internal communications
- Analysis of relevant company documents and of assigned devices
- Hearing of persons able to provide information as evidence
- Management of the report – preliminary investigation

breach, or even merely a potential threat, to the Model 231

- or in exoneration of the reported breach
- Guarantee of anonymity Entry in the Register of Reports

The author of the breach or attempted breach must respond within the time limit granted by the SB.

- Receipt of justifications.
- SB Entry in the Register of Reports
- Management of the report – preliminary investigation.
- Assessment on the merits of the justifications given.

If the justifications are sufficient and well founded: | If the justifications are NOT sufficient and/or not well founded:

- closure of the file.
- The SB will provide a report to the Board of Directors within the following 7 days, so that it may take appropriate measures within the subsequent 15 days.
- The SB provides feedback to the whistleblower within three months from the date of receipt of the report, where possible.
- SB and Board of Directors Entry in the Register of Reports. Communications to the whistleblower.
- Monitoring by the SB that the procedure is successfully concluded, protecting the reporting person and the subject of the report.
- Report to the Administrative Body on the register of reports, in anonymous form, and on the outcome of the analyses carried out.
- Copy of the measure sent to the Board of Directors so that it may assess the adequacy of any company procedures.
- Copy of the report and of the measure sent to the Board of Statutory Auditors and to the Statutory Auditor.

USE OF THE EXTERNAL CHANNEL

Same inputs as the internal channel. Reporting persons may use the external channel (ANAC) when:

- Report of the attempted breach to ANAC through the use of the external channel.
- Whistleblower Through the dedicated web portal on the ANAC website, accessible at the link: anticorruzione.it/- /whistleblowing
- ANAC becomes aware of the report. Communication to the SB by the whistleblower of the use made of the external channel.

- within the working context, mandatory activation of the internal reporting channel is not provided for, or this channel, even if mandatory, is not active or, even if activated, does not comply with what the law requires;
- the reporting person has already made an internal report and it has not been followed up;
- the reporting person has well-founded reasons to believe that, if they made an internal report, it would not be effectively followed up, or that the report could entail a risk of retaliation;
- the reporting person has well-founded reason to believe that the breach may constitute an imminent or manifest danger to the public interest;
  - use of the external channel.

Receipt of the report

- The report is taken in charge. If anonymous, verification is made of the attachment of serious and concordant evidence in support of the report.
- The whistleblower is notified of receipt of the report within 7 days of receipt, unless the reporting person explicitly requests otherwise or unless ANAC considers that such notice would jeopardise the protection of the confidentiality of the reporting person's identity.
- ANAC ANAC opens the procedure for managing the report

Management of the report

- ANAC maintains dialogue with the reporting person and, where necessary, requests from them the appropriate supplementary information
- ANAC carries out the preliminary investigation necessary to follow up the report, including through hearings and acquisition of documents.
- The preliminary investigation is completed

Communication to the reporting person of the final outcome of the report

- ANAC gives feedback to the reporting person within 3 months or, where justified and reasoned grounds exist, 6 months from the date of the acknowledgement of receipt of the external report or, in the absence of such acknowledgement, from the expiry of 7 days from receipt.
- ANAC Conclusion of the reporting procedure.

USE OF PUBLIC DISCLOSURE OR COMPLAINT TO THE JUDICIAL AUTHORITY

Same inputs as the report through the internal and external channels. Reporting persons may make

  - The reporting person makes information on breaches publicly known through the press, electronic media or any other means of dissemination capable of reaching
  - Whistleblower The report has been made.
  - Communication to the Ethics Committee by the whistleblower

a public disclosure or complaint to the judicial authority when:

- the reporting person has previously made an internal and an external report, or has made an external report directly, and no feedback has been given within the set time limits on the measures envisaged or adopted to follow up the reports;
- the reporting person has well-founded reason to believe that the breach may constitute an imminent or manifest danger to the public interest;
- the reporting person has well-founded reason to believe that the external report may entail a risk of retaliation or may not be effectively followed up, given the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there is a well-founded fear that the person who received the report may be colluding with the author of the breach or involved in it.
  - reach a large number of people (e.g.
  - TV, radio, social networks, etc.). The reporting person files a complaint with the judicial authority.
  - Notice of the use of the public disclosure or of the filing of the complaint with the judicial authority.

5. Controls, records and reports

Preparation of appropriate reporting in the Register of Reports.

6. Operating instructions and related documents

a) Operating instructions

The SB receives reports through the channels indicated above and, where possible, issues an acknowledgement of taking charge to the reporting person within seven days of receipt. At the same time, a communication channel is set up between the reporting person and the SB for any requests or supplementary information. The reporting person may monitor the status of the preliminary investigation by requesting information through the channels indicated above, quoting the receipt number issued with the acknowledgement of taking charge of the report. The SB will give feedback on the report within three months from the date of the acknowledgement of receipt or, if no such acknowledgement was issued, within three months from the expiry of the seven-day period from the submission of the report. As part of the internal investigations, and in order to verify the well-foundedness of the reports and the truth of the facts reported, the SB may collect relevant company documents; analyse the devices assigned to the reported person to verify the existence of evidence confirming the report, such as e-mails or messages, in accordance with the Company's regulation on the use of IT devices; and carry out interviews with persons who may provide relevant information to prove the reported breaches. For verification purposes, the SB may entrust further investigation to third parties, taking care to:

- grant a formal mandate, defining the scope of action and specifying the information it intends to obtain from the requested investigation;
- omit any information that could, even indirectly, lead back to the identity of the reporting person;
- omit any information concerning the reported person, where not strictly necessary for the proper performance of the assignment;
- remind the entrusted person of the obligation of confidentiality regarding the data processed (in the case of persons external to the Company, this obligation must be formalised);

For full transparency of the process, reports archived as not relevant are recorded, stating the subject of the report and the reasons why no further investigation was carried out. The data and documentation attached to the report will be retained for the time necessary to manage and evaluate the report, and in any case for no longer than five years from the date of communication of the final outcome of the reporting procedure. The identity of the reporting person and of the other persons to whom the whistleblowing legislation extends protection may not be disclosed to persons other than the members of the SB competent to receive and manage reports, unless specifically authorised. The measures adopted to guarantee the confidentiality of the reporting person do not merely protect identifying data, but also all elements of the report from which their identity may be inferred, even indirectly. The Company undertakes to protect the reporting person against any act of retaliation, discrimination or penalisation, whether direct or indirect, on grounds connected, directly or indirectly, with the report. All personnel involved in any capacity in the various stages of managing reports are required to guarantee the highest level of confidentiality as to their contents and as to the persons involved in the report. The protection of the reporting person cannot be guaranteed where the unfounded and defamatory nature of the report is established, thereby constituting wilful misconduct on the part of the reporting person. Where, from the checks carried out on reports in accordance with this document, unlawful conduct attributable to employees is found, the Company will act promptly and immediately, through appropriate and proportionate sanctioning measures and provisions, taking into account the seriousness and the criminal relevance of such conduct and the initiation of criminal proceedings where they constitute an offence under current national law. In this regard, reference is made to the provisions of the Sanctions System. Where the investigations reveal wilful or negligent conduct on the part of third parties who have had and/or currently have dealings with the Company, the Company will act promptly, taking all the measures identified as necessary to protect itself.

This applies where the person receiving the report may be colluding with the author of the breach or involved in the breach itself.

Any disclosure of the identity of the reporting person to persons other than those competent to receive or follow up reports, or otherwise authorised, will take place with the express consent of the reporting person.

b) Related documents

- 1. Notice of activation of the whistleblowing system.
- 2. Whistleblowing notice.
- 3. Information notice pursuant to Arts. 13 and 14 of EU Regulation 2016/679.

c) Regulatory references

- 1. **Legislative Decree no. 231 of 8 June 2001** ("Discipline of the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law no. 300 of 29 September 2000");
- 2. **Regulation (EU) no. 2016/679** (General Data Protection Regulation – GDPR);
- 3. **Legislative Decree no. 196 of 30 June 2003** (Personal Data Protection Code), as amended;
- 4. **EU Directive 2019/1937** on the protection of persons who report breaches of Union law (so-called Whistleblowing);
- 5. **Legislative Decree no. 24 of 10/03/2023**, published in the Official Gazette on 15/03/2023, transposing Directive (EU) 2019/1937;
- 6. **ANAC Resolution no. 311 of 12 July 2023** – Guidelines on the protection of persons who report breaches of Union law and of persons who report breaches of national legislative provisions. Procedures for the submission and management of external reports;
- 7. "**New Whistleblowing Rules – Operational Guide for Private Entities**" of October 2023 – Confindustria;
- Document no. 1
- Notice of activation of the whistleblowing system
- ....., on .....
- Dear
- Mr./Ms. ...

Subject: Whistleblowing – Information notice to all Stakeholders.

Dear Sir/Madam,

- with Legislative Decree no. 24 of 10/03/2023, our Company too has had to adopt a Whistleblowing Procedure.
- Whistleblowing is the tool through which any wrongdoing of which one has become aware in the course of one's activity can be reported, **confidentially and in a protected manner**.
- By way of non-exhaustive example, the following conduct is deserving of reporting: civil, criminal, administrative and accounting offences, concerning public procurement, financial services, money laundering, terrorist financing, privacy, or conduct relevant under Legislative Decree 231/2001.

A report may be made through three channels to be used **progressively and subsidiarily (and NOT alternatively)**:

- Internal channel.
- External channel.
- Public disclosure or complaint to the judicial authority.

Please be advised that MARMOLES MAN, **for the management of reports through the internal channel, has appointed an external, autonomous and independent Ethics Committee**:

- **registered post**: Supervisory Body c/o MARMOLES MAN SRL, Viale Domenico Zaccagna no.
- 38, 54033 Carrara (MS). It is recommended that the report be sent in two sealed envelopes: the first containing the identifying details of the reporting person, an address and a telephone number at which they can be contacted, together with a photocopy of an identity document; the second containing the subject and description of the report, so as to separate the reporting person's identifying details from the report. Both must then be placed in a third sealed envelope bearing on the outside the words “confidential – for the attention of the Supervisory Body”);
- in **oral form** through a meeting requested by sending registered post (as above); with the reporting person's consent, the report is documented by the designated staff member in the form of minutes. The reporting person may check, correct and confirm the minutes of the meeting by signing them.

The SB will guarantee **the confidentiality of the identity of the reporting person, of any persons involved and/or mentioned, as well as of the content of the documentation provided**. If made anonymously, the report must necessarily be supported by serious and concordant evidence. Furthermore, please note that the National Anti-Corruption Authority (ANAC) has set up its own portal, which generally serves as an external reporting channel and is accessible at the link: https://www.anticorruzione.it/-/whistleblowing . **The external reporting channel may be used only**:

- if the internal reporting channel is not present, since it is not mandatory, or is present but not active, or active but not compliant with Legislative Decree no. 24/2023;
- if the reporting person has well-founded reasons to believe that, in the case of an internal report, due follow-up would not be given to it, or that they would be exposed to a risk of retaliation;
- if the reporting person has already made an internal report to which no follow-up has been given;
- if the reporting person has well-founded reasons to believe that the breach may constitute an imminent or manifest

danger to the public interest. As a further residual option, when neither the internal nor the external reporting channel can be used, the legislation allows the reporting person to make information on breaches publicly known independently, through the press, electronic media or other means of dissemination capable of reaching a large number of people (e.g. TV, radio, social networks, etc.), or to apply to the judicial authority. For any information or requests for clarification, MARMOLES MAN remains entirely at your disposal. Kind regards,

– MARMOLES MAN SRL

– *-*

– Document no. 2 – Whistleblowing Notice

WHISTLEBLOWING SYSTEM

Whistleblowing is a direct communication system between each member of staff of MARMOLES MAN SRL and the SB, through which it is possible to **report unlawful conduct** of which one has become aware by reason of one's employment relationship.

Through this system a monitoring and reporting system is implemented that enables the early identification of a solution to certain problems, as well as the prevention of others.

The purpose is to introduce, in addition to the system of ordinary controls, a direct communication channel between each employee and the Ethics Committee which, **by guaranteeing the anonymity of the reporting person**, can contribute to the goal of continuous improvement of the company's organisation.

In the case of a report sent by registered post, please prepare two separate envelopes:

- **the first** containing the identifying details of the reporting person, address and telephone number at which they can be contacted, together with a copy of their identity document**;**
- **the second** containing the subject and description of the report, and the name of the company by which the reporting person is employed;
- Both envelopes must then be placed in a **third, outer envelope** bearing the words "CONFIDENTIAL – FOR THE ATTENTION OF THE SB";
  - The SB

The channels through which the above reports may be sent are:

- Registered post: Supervisory Body c/o MARMOLES MAN SRL, Viale Domenico Zaccagna no. 38, 54033 Carrara (MS)
- ATTENTION

Anonymous reports will be taken into consideration only if supported by serious and concordant evidence. Otherwise, anyone wishing to make a report must ALWAYS state their first and last name.

The Ethics Committee will take appropriate measures to guarantee the anonymity of the reporting person as regards their identity, the content of the report and the documentation provided. The full privacy notice is available on the company website.

- Document no. 3

Information notice pursuant to Arts. 13 and 14 of EU Regulation 2016/679

This notice is provided pursuant to and for the purposes of Art. 13 of EU Regulation 2016/679 (hereinafter simply the "Regulation" or "GDPR"), to inform you that your personal data may be collected and processed in the context of the reporting of unlawful conduct and suspicious behaviour of which you have become aware by reason of your employment relationship (hereinafter simply the "whistleblowing report") and which may constitute a breach of the rules governing the activities of MARMOLES MAN. This document supplements any other notices already provided to you (e.g. the notice to employees) and does not repeat their content.

1. DATA CONTROLLER

The Data Controller, meaning the party that determines the means and purposes of processing your personal data, is MARMOLES MAN, with registered office in CARRARA (MS), Viale Domenico Zaccagna no. 38. For any information relating to the processing of personal data by MARMOLES MAN, you may submit a request to the e-mail address privacy@marmolesman.it or by registered post to: MARMOLES MAN SRL, Viale Domenico Zaccagna no. 38, 54033 Carrara (MS);

2. SOURCE OF THE DATA PROCESSED

The information may be provided:

- in the report, by the Reporting Person;
- in the course of the necessary preliminary investigation activities (for example, from public sources, interviewed third parties, etc.);
- during the process of managing the report;

3. TYPES OF DATA PROCESSED

Where the Reporting Person does not choose to remain anonymous, personal data referring to them may be processed, specifically:

- personal details;
- contact details;
- any special categories of data pursuant to Art. 9 GDPR, insofar as they reveal a general state of health (absence for illness, maternity, injury, etc.), suitability for specific duties, membership of a trade union and/or political party, holding of elected public office, or religious beliefs;
- any so-called judicial data pursuant to Art. 10 GDPR, insofar as they relate to criminal convictions and offences or related security measures;
- any personal data contained in the subject matter of the report.

Following the report, personal data referring to third parties (potential authors of an offence or irregularity falling within the reportable matters, or persons informed of the facts) may be processed, specifically:

- personal details;
- contact details;
- any special categories of data pursuant to Art. 9 GDPR, insofar as they reveal a general state of health (absence for illness, maternity, injury, etc.), suitability for specific duties, membership of a trade union and/or political party, holding of elected public office, or religious beliefs;
- any so-called judicial data pursuant to Art. 10 GDPR, insofar as they relate to criminal convictions and offences or related security measures;
- any personal data contained in the subject matter of the report.
- personal data arising from subsequent preliminary investigation activities;

Only personal data strictly necessary and relevant to achieving the purposes set out below will be collected, in compliance with the data minimisation principle under Art. 5, para. 1, letter c), GDPR.

4. PURPOSES AND LEGAL BASES OF PROCESSING

The Controller will process the above personal data:

- 1. In order to manage and diligently follow up the reports received, including the verification activities and internal investigations linked to checking the conduct reported, and the initiation of proceedings, including disciplinary ones, within the limits required by applicable rules. In addition, personal data may be processed in order to respond to requests from the competent administrative or judicial authority and, more generally, from public bodies in compliance with legal formalities. The data will also be processed to effectively prevent and combat fraudulent conduct and unlawful or irregular conduct.

Accordingly, the legal basis making the processing lawful is the necessity to comply with legal obligations and to carry out tasks of public interest to which the Controller is subject, and provisions of authorities empowered by law [Art. 6, para. 1, letters c) and e); Art. 9, para. 2, letters b) and g); Art. 10 GDPR]. Any disclosure of the identity of the reporting person to persons other than those competent to receive or follow up reports, or otherwise authorised, will take place with the express consent of the reporting person [Art. 6, para. 1, letter a) GDPR].

- 2. In order to: i) meet the Controller's internal control needs and business risk monitoring requirements, as well as optimise and improve internal business and administrative management processes; ii) establish, exercise or defend a right or legitimate interest of the Controller in any competent forum, in guarantee of the right of defence under Art. 24 of the Constitution; iii) manage IT security and protect data assets and security, user support, and the maintenance of security systems and perimeter protection, including traffic logs relating to connections to the whistleblowing Platform recorded on company systems.

Accordingly, the legal basis making the processing lawful is the need to pursue a legitimate interest of the Controller [Art. 6, para. 1, letter f) GDPR]. Failure to consent to the processing of data for the purposes indicated above does not allow the reporting person to submit whistleblowing reports. The provision of common data, such as personal or contact details, by the reporting person is to be regarded as voluntary, since the law recognises the possibility of making a report anonymously (see below).

5. ANONYMOUS REPORTING

Where you are required to submit a whistleblowing report, the provision of your personal data is entirely optional. If no data is provided, the report will be considered provided it is supported by circumstantiated and detailed elements; this means that reports made anonymously, meaning without any indication of the reporting person's identity, will also be accepted and assessed. With regard to the identity of the reported person, the provision of personal data is likewise optional but, in its absence, the report will be managed only where there are further elements enabling the identification of the author of the alleged act and the appropriate checks can continue. Should you decide to voluntarily disclose your identity in the whistleblowing report, your data will be processed only by personnel expressly authorised to carry out that activity and bound by strict confidentiality commitments, both as regards your identity and as regards the content of the report. In any case, sharing the content of the report with certain persons expressly identified by law remains subject to this (see below, point 6 – c).

- 6. **RECIPIENTS AND COMMUNICATION OF DATA** All personal data included in the report, including your personal data, and more generally the documentation produced in support of it, will not be disseminated, except where communication or dissemination is

required in accordance with the law by public bodies for purposes of defence, security or the prevention, detection or prosecution of offences.

In carrying out its activities and pursuing the purposes referred to in the preceding point 3, data may be shared, to the strictly necessary extent, with certain third parties, where investigative needs require that MARMOLES MAN makes them aware of the content of the report or of the documentation attached. All the persons in question, listed below, are formally authorised to process the data, have been appropriately instructed and trained, and are bound by a duty of secrecy as to all information of any kind learned in connection with whistleblowing reports. The persons in question are:

- a) The SB and any other person operating under its authority, duly authorised to process data pursuant to Art. 2-quaterdecies of Legislative Decree 196/2003;
- b) external suppliers and consultants, with whom MARMOLES MAN has entered into agreements pursuant to Art. 28 GDPR for the processing of data and who therefore act as data processors, supporting the Company in relation to the management of whistleblowing reports;
- c) persons, bodies or authorities to whom your personal data must be communicated by law or on the orders of authorities. These persons are all independent controllers.

7. PROCESSING METHODS

The information identified above is processed by the members of the SB, a body composed of persons specifically appointed as authorised persons and suitably trained for that purpose. Data is collected by IT and paper-based means, as defined in the Whistleblowing Protocol, so as to guarantee the confidentiality of reporting persons and of any other persons involved, and the confidentiality of the information contained in the reports. Personal data will be processed lawfully, fairly and transparently, in compliance with all applicable legislation and in a manner balanced with respect to the various interests involved. Data will be collected and recorded for specified, explicit and legitimate purposes, namely solely to manage and follow up the reports received; personal data manifestly not useful for processing the report will not be collected or, if collected accidentally, will be deleted without delay. The Controller ensures that data are accurate and, where necessary, updated; it also ensures that all reasonable measures are taken to promptly erase or rectify inaccurate data relating to the specific report to be managed. Data will be processed by IT and paper-based means and tools, in a manner and for periods strictly necessary to achieve the purposes for which it was collected. MARMOLES MAN employs appropriate organisational, technical and physical security measures suitable for protecting information against possible alteration, destruction, loss, theft, improper or unlawful use.

8. TRANSFER OF DATA ABROAD

The Data Controller does not transfer personal data to third countries. Should a transfer of data outside the EU become necessary, the Company will verify that the suppliers provide adequate safeguards, as provided for in Arts. 44 et seq. GDPR. The complete and up-to-date list of data recipients may be requested from the Controller at the contact details indicated above.

9. DATA RETENTION PERIODS

The personal data collected will be kept for the time strictly necessary to fulfil the purposes already indicated in the preceding paragraphs, and in any case for no longer than five years from the date of communication of the final outcome of the report, unless further retention becomes necessary by virtue of legal obligations (for example, where judicial or disciplinary proceedings are under way, until their conclusion). Once this period has elapsed, the Controller will proceed to erase the personal data.

RIGHTS OF THE DATA SUBJECT

Data subjects, in general terms and upon proof of their identity, have the right to request from the Controller, at any time:

- confirmation of whether or not data provided are being processed, the purposes, the categories of data processed, the recipients, the retention period and, where applicable, their source (Art. 15 GDPR). The person who is the subject of a whistleblowing report is not entitled to exercise this right;
- the rectification without undue delay of inaccurate personal data and the completion of incomplete data (Art. 16 GDPR);
- the erasure without undue delay of your data (Art. 17 GDPR);
- the restriction of processing of your data under Art. 18 GDPR where, for example, you consider that the processing carried out by MARMOLES MAN is unlawful and/or inappropriate;
- the portability of your data under Art. 20 GDPR, where applicable. Upon your express request, you will be provided with a list of the personal data concerning you in a structured, commonly used and machine-readable format (e.g. an Excel file);
- the withdrawal of any consent given for any purpose. This does not affect the lawfulness of processing based on consent carried out before the request;
- to object to the processing of your personal data pursuant to Art. 21 GDPR;

With particular reference to the last point, the right to object to processing carried out on the basis of the Company's legitimate interest may be exercised, in accordance with Art. 21, para. 1, GDPR, by setting out the specific reasons connected with your particular situation on which the objection is based; in such cases MARMOLES MAN will refrain from further processing your personal data unless there are compelling legitimate grounds for processing which override your interests, rights and freedoms, or for the establishment, exercise or defence of a legal claim. Your request will be dealt with within one month of receipt; that period may be extended by a further two months at most in cases of particular complexity. MARMOLES MAN states that, pursuant to Art. 2-undecies of Legislative Decree 196/2003, the rights listed above may not be exercised by request to the Controller or by complaint under Art. 77 GDPR where their exercise could result in an actual and concrete prejudice to the confidentiality of the identity of the person making a whistleblowing report. The prejudice will be assessed case by case in concrete terms. MARMOLES MAN declares that it will avail itself of the above restriction only where it is a necessary and proportionate measure and that, in such a case, you will be informed in writing without delay. In any case, if you consider that the processing of your personal data is contrary to the regulations in force, the data subject has:

- the right to apply to the competent courts pursuant to Art. 79 GDPR, subject to the limits set out in Art. 2-undecies of Legislative Decree 196/2003;
- in any case the right to lodge a complaint with the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali), as the competent supervisory authority. Further information on your rights regarding the protection of personal data can be found on the Garante's website at www.garanteprivacy.it.