METINVEST

REGULATORY AND METHODOLOGICAL DOCUMENTATION

EUROPEAN RE-ROLLING BUSINESS UNIT

BP CODE LEG-003, VERSION 1.0

METINVEST WESTERN EUROPE

WHISTLEBLOWING POLICY

Procedure for reporting misconducts and irregularities

GENOA
2023

Foreword

DEVELOPED BY: ERBU Legal Department

ADOPTED AND MADE EFFECTIVE: based on new law in force

INTRODUCED: first time

KEYWORDS: whistleblowing, reporting person, breaches, internal reporting, communication channel, investigation

CHANGE REGISTER:

Version	Approval date	Effective from
1.0	12.07.2023	15.07.2023

Version	Approval date	Effective from

Content

Whistleblowing Policy

Procedure for reporting misconducts and irregularities

Effective from 15-07-2023

---

1. Applicable whistleblowing law

1.1 In Italy several laws are used to discipline the so called "whistleblowing" in different areas, such as, for example, in the financial products and markets sector, for anti-money laundering or terrorism prevention purposes, in relation to transport safety or environmental protection. These regulations have recently been supplemented or superseded by the Legislative Decree 24/2023 (the "**Decree**") transposing the Directive (EU) 2019/1937 regarding the protection of persons who report actual or potential violations of Union and national law (the "**Directive**"; together with the national legislation transposing it and the sectoral regulations governing or, in any case, concerning whistleblowing, the "**Whistleblowing Law**").

1.2 Metinvest Trametal S.p.A. and Ferriera Valsider S.p.A. (hereinafter, the "**Companies**"), implement this procedure (the "**Whistleblowing Policy**"), in order to regulate the process of sending, receiving and investigating reports on breaches. The Whistleblowing Policy is regularly updated in order to integrate any amendments to the applicable Whistleblowing Law and it is made available to its recipients by means of publication on the Companies' sharepoint, which can be easily accessed by the link transmitted by the Companies to their employees via a specific email. The Whistleblowing Policy will also be published on the Companies' website at the following links: https://trametal.metinvestholding.com/it; https://valsider.metinvestholding.com/it.

1.3 The Companies inform that the adoption of the Whistleblowing Policy is known by the competent trade unions.

2. Definitions

2.1 By transposing the Directive, the Decree has defined the meaning of certain terms, including but not limited to the following:

a) "**Breach(es)**" means acts or omissions that (i) are unlawful and related to the Union acts and areas falling within the material scope of the Whistleblowing Law referred to in paragraph 7 of the Whistleblowing Policy; or (ii) defeat the object or the purpose of the rules in the Union acts and areas falling within the material scope of the Whistleblowing Laws referred to in paragraph 7 of the Whistleblowing Policy;

b) "**Report(s)**" means oral or written communication of information on Breaches;

c) "**Internal Reporting**" means oral or written communication of information on Breaches, submitted by means of the communication channels adopted by the Companies, as referred

to in paragraph 5 of the Whistleblowing Policy;

d) "**External Reporting**" means oral or written communication of information on Breaches to the competent authority as referred to in paragraph 5.4 of the Whistleblowing Policy;

e) "**Public Disclosure**" means making of information on Breaches available in the public domain;

f) "**Reporting Person(s)**" means a natural person who reports or publicly discloses information on Breaches acquired in the context of his/her work-related activities;

g) "**Person Concerned**" means a natural or legal person who is referred to in the Report or Public Disclosure as a person to whom the Breach is attributed or with whom that person is associated;

2.2 This Whistleblowing Policy uses the terms in the same meaning attributed to them in that context and it is to be considered an integral part of the Organisation, Management and Control Model of the Companies (hereinafter, the "**231 Model**"), where adopted, pursuant to the Legislative Decree No. 231/2001 (the "**231 Decree**").

3 General principles

3.1 The Companies are committed to promoting and maintaining – where applicable in accordance with the 231 Model – an adequate internal control system, to be understood as the set of all tools useful and necessary to direct, manage, and verify business activities, with the objective of ensuring compliance with the laws and the internal policies, protecting corporate assets, managing activities, and providing accurate and complete accounting and financial data.

3.2 The responsibility for implementing an effective internal control system is shared to each level of the Companies organisational structure. Accordingly, the Companies' personnel and the internal functions and bodies, within the scope of functions and responsibilities assigned to them, are committed to establishing and actively participating in the proper functioning of the internal control system.

3.3 The Companies expect its personnel to cooperate in maintaining a climate of mutual respect for the dignity, honour and reputation of each individual in the Companies. The latter will take action to prevent insulting, discriminatory or defamatory interpersonal attitudes. The Companies therefore guarantee adequate protection against Reports made in bad faith or made with malice or gross negligence, censuring such conducts and applying, in accordance with the law, the provisions of the disciplinary system adopted by the Companies in this regard.

4 Subjective scope of the Whistleblowing Policy

4.1 The recipients of the protective measures set out in the Whistleblowing Policy are the persons who report the Breaches internally or to the competent judicial, administrative or accounting authority (the "**Authority**") and/or those who make a Public Disclosure of the information regarding the Breach. In particular the categories of recipients include:

a) workers employed by the Companies or by the Companies' contractors or suppliers, under any type of contract;

b) temporary employees;

c) candidates for job positions at the Companies, for information on alleged Breaches acquired in the recruitment process or in other pre-contractual negotiations;

d) self-employed workers and/or consultants and/or suppliers and/or collaborators who work for the Companies, including agents and brokers;

e) volunteers and/or trainees at the Companies;

f) shareholders and persons belonging to the administrative, management, supervisory or representative body at the Companies; and

g) former employees of the Companies, if the information regarding the alleged Breaches was acquired in a work-based relationship which has ended; and

h) all the functions, personnel, collaborators, and/or suppliers of the Companies, however involved in the legal, technical and/or organizational management of the Whistleblowing Policy.

4.2 The measures of protection set out in the Whistleblowing Policy for the aforementioned categories of Reporting Persons shall also apply to:

a) "facilitators", meaning a natural person who assist a Reporting Person in the reporting process in the work-related context, and whose assistance shall be confidential;

b) persons linked to the Reporting Person or to the person who reports the Breach to the Authority or to the person who publicly discloses information regarding the Breach, by a stable emotional or family relationship up to the fourth degree of kinship and who operates in the same work-related context;

c) colleagues of the Reporting Person and/or of the person who has reported the Breach to the Authority and/or has publicly disclosed the information regarding the Breach, who operate in the same work-related context as the Reporting Person and who has habitual and current relationship with the latter;

d) legal entities that the Reporting Person and/or of the person who has reported the Breach to the Authority and/or has publicly disclosed the information regarding the Breach owns, works for or is otherwise connected with in a work-related context.

All the aforementioned categories of recipients are the "**Recipients**" of the Whistleblowing Policy.

4.3 Everyone is bound to guarantee the absolute confidentiality of the identity of the Reporting Person, the Person Concerned and/or mentioned in the Report by using the criteria and methods of communication of Internal Reporting adopted by the Companies and better described in the following paragraphs, suitable to protect the reputation of the Reporting Person and of the persons involved in the Reports. The obligation to maintain the confidentiality applies to the entire whistleblowing procedure, including the documents and any further information collected by or provided to the Reporting Person and/or any other person mentioned in the report, in the context of the investigation.

4.4 Persons who breach the rules set out in the Whistleblowing Policy will be subject to the sanctions set out by the disciplinary system adopted by the Companies, as provided by law. The disciplinary system, the Code of Ethics, the 231 Model, as well as the internal procedures, policies and

regulations implemented by the Companies are published in the Companies' sharepoint; furthermore, the aforementioned documentation will also be published – where deemed necessary or appropriate from time to time – on the Companies' website: https://trametal.metinvestholding.com/it; https://valsider.metinvestholding.com/it.

5 Communication Channel of Internal Reporting

5.1 In order to facilitate the receipt of the Internal Reporting, the Companies identify the following internal communication channels (the "**Reporting Channels**")

(a) Email address:

The Reporting Person shall make the Internal Reporting, by writing to the email address **whistleblowing@metinvestholding.com** which the Companies have set in this regard. The maintenance of the aforementioned whistleblowing channel is ensured by the Companies' Supervisory Body and the Compliance Officer of the Group to which the Companies belong as the function responsible for (and specifically trained for) the receipt of the Internal Reporting (hereinafter, the "**Reporting Body**").

The Companies recommend that the Reporting Person who wishes to keep his or her identity confidential sends the Internal Reporting from a private email address managed by the Reporting Person himself or herself.

In case the Reporting Person wishes to report the Breach on anonymous basis, the Companies recommend (a) to not use an email account revealing, directly or indirectly, the sender's identity; (b) to not sign, mark, or anyhow personalize the Internal Reporting in a way that makes it referable to the Reporting Person and (c) to not specify any further detail that may reveal the identity of the Reporting Person throughout the procedure.

(b) Oral channel

In addition to the abovementioned reporting channel, the Reporting Person may also orally make Internal Reporting in a face to face meeting and/or via tele/videoconference, provided that all participants can be identified and are allowed to follow the discussion and intervene in real time on the discussion of the topics, to be arranged with the members of the Reporting Body within a reasonable period of time, at the request of the Reporting Person.

If the Internal Reporting is made orally, the Report is documented, with the consent of the Reporting Person, either by recording it on a device suitable for storage and listening or by minutes. In the case of minutes, the Reporting Person may verify, rectify and confirm the minutes of the meeting by signing them.

Regardless of the Reporting Channels chosen by the Reporting Person, the Companies must be impartial and guarantee, also by means of the use of encryption tools, the confidentiality of the identity of the Reporting Person, the Person Concerned and any other person mentioned in the Internal Reporting, as well as the content of the Internal Reporting and of the related documentation.

5.2 The Reporting Body (or the Compliance Officer of the Group to which the Companies belong, see paragraph 6 below for the case of conflict of interest) must also be sent any documentation on the reported events, as well as the results of any investigations already carried out on the matter,

for the assessment of the reported Breach.

5.3 All the information relating to the Reporting Channels, procedures and the requirements for making Reports shall be made easily visible in the workplace and available on the Companies' website

5.4 In addition to the above, the Reporting Person may also make an External Reporting by means of the channel activated and set up, through a specific internet platform, by the National Anti-Corruption Authority (ANAC), if one of the following conditions occurs:

a) the Reporting Person has already made an Internal Reporting and he/she has not been followed up;

b) the Reporting Person has reasonable grounds to believe that, if he/she were to make the Internal Reporting, it would not be effectively followed up, or that the Report might give rise to a risk of retaliation;

c) the Reporting Person has reasonable grounds to believe that the Breach may constitute an imminent or obvious danger to the public interest.

More details on the modalities of communication, reception and management of the Reports, transmitted by means of the external reporting channel, are available on the ANAC's website, at the following link https://www.anticorruzione.it/-/whistleblowing.

6 Conflict of interests

6.1 In the event that the Report concerns one or more of the Supervisory Body's members, **the Reporting Person shall not use the email channel of the Reporting Body**.

6.2 In such cases, the Breach shall be reported by using exclusively the following email address **angelina.chachuna@metinvestholding.com**, so as to route the handling of the Report directly to the the Compliance Officer of the Group to which the Companies belong.

6.3 Anyone who receives an Internal Reporting outside the Reporting Channels shall ensure that it is forwarded to the Reporting Body (or the Compliance Officer of the Group to which the Companies belong in the case of reports concerning the Supervisory Body) within three days of its receipt. The Reporting Body (or the Compliance Officer of the Group to which the Companies belong) shall give notice of the transmission to the Reporting Person within the seventh day from the date of receipt of the Internal Reporting. However, the management of the Report outside the Reporting Channels must be carried out in the utmost confidentiality, suitable to protect the reputation of the Reporting Person, the Person Concerned or any other person mentioned in the Report and the effectiveness of the investigations.

7 Content of the Reports

7.1 Reports shall be based on precise and concordant factual elements and concern Breaches which have already taken place, Breaches which have not yet materialized, but are very likely to take place, acts or omissions which the Reporting Person has reasonable grounds to consider as Breaches, as well as attempts to conceal Breaches. According to the Whistleblowing Law, the following constitute reportable Breaches:

a) violations of Code of Ethics, 231 Model or internal regulations, procedures or policies referred to therein (including the Whistleblowing Policy). With particular regard to the 231 Decree, in case of Reports, the following conducts constitutes a disciplinary offense under the 231 Decree: (1) the commission of retaliatory or discriminatory acts against the Reporting Person, contrary to the law, (2) obstructing or attempting to obstruct the reporting in a manner contrary to the law, (3) the violation of confidentiality obligations under the Whistleblowing Law, (4) the failure to verify and analyse the Reports, but also, conversely, (5) the Report for which it is established, even by a judgment of first instance, the criminal liability of the Reporting Person for crimes of defamation or slander (or in any case for the same crimes committed with the Report to the judicial or accounting authority) or his civil liability, for the same title, in cases of malice or gross negligence;

b) offences falling within the scope of the Decree and or EU law, including but not limited to the following fields: public procurement; financial services, products and markets, prevention of money laundering and financing of terrorism; product safety and compliance; safety at work; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety, animal health and welfare; consumer protection; human rights protection (including discrimination, child exploitation, abuse and/or sexual harassment); public health; protection of privacy and personal data and security of networks and information systems; EU rules on the internal market, in particular with reference to the rules on competition, state aid, corporate taxes, as well as the protection of the financial interests of the State and/or the European Union.

7.2 All those who detect or become aware of Breaches potentially committed by individuals who have dealings with the Companies, are required to act in accordance with the Whistleblowing Policy, reporting without delay, and by means of the Reporting Channels, facts, events and circumstances that they believe, in good faith and based on reasonable evidence, to have resulted in such Breaches.

7.3 The Internal Reporting must make it possible to proceed to due and appropriate verifications regarding the grounds of the circumstances that are reported, responsibilities, as well as all further elements, including documentary evidence, which are in the possession of the Reporting Person. For this purpose, the Internal Reporting, in addition to being promptly sent, must be as complete and exhaustive as possible and shall include the following elements:

a) a clear and complete description of the conduct, including omission, that is the subject of the Report;

b) the circumstances of time and place in which the facts were committed or the conduct were omitted;

c) the name(s) or other elements (such as the qualification and relationship, contractual or otherwise, with the Companies) that make it possible to identify the person(s) who has/have carried out the reported facts or the omitted conducts;

d) an indication of any other persons who may report on the reported facts;

e) an indication of any documentation that may confirm the grounds of such facts;

f) the indication of the quantification of any damages, economic or non-economic (*e.g.*, reputational) suffered by the Companies or, if such damages are not exactly determinable in

their amount, the data on the basis of which the existence (or the risk of their occurrence) emerges, although their quantification is uncertain;

g) any other information that may provide useful evidence regarding the existence of the reported facts.

8 Management and verification of merits of the Internal Reporting

(a) Preliminary analysis

8.1 As part of the management of the Reporting Channels, the Reporting Body (or the Compliance Officer of the Group to which the Companies belong) issues the Reporting Person with a notice of receipt of the Internal Reporting made within seven days from the date of receipt.

8.2 All the Internal Reporting are subject to a preliminary analysis carried out by the Reporting Body (or the Compliance Officer of the Group to which the Companies belong) in order to verify the presence of useful data and information to enable an initial assessment of the merits of the Report.

8.3 In carrying out the aforementioned analysis and, in compliance with the law, including the applicable privacy laws, the Reporting Body (or the Compliance Officer of the Group to which the Companies belong) may avail itself of the support of the Companies' functions from time to time competent and, where deemed appropriate, of specialized external consultants ensuring, in any case, the confidentiality and, where possible, the anonymization of any personal data contained in the Internal Reporting.

8.4 If, at the conclusion of the preliminary analysis, it emerges that there are not sufficiently circumstantial elements but the case appears to be founded and/or particularly alarming, the Reporting Body (or the Compliance Officer of the Group to which the Companies belong) may ask the Reporting Person further information and/or extend the preliminary investigation phase for an appropriate time.

8.5 If, at the end of the preliminary analysis referred to by the preceding paragraph there are still not sufficiently circumstantial elements or the facts referred to in the Report are deemed unfounded, the Report is archived by the Reporting Body (or the Compliance Officer of the Group to which the Companies belong), with a motivation of such decision.

8.6 The Reporting Person shall be informed by the Reporting Body (or the Compliance Officer of the Group to which the Companies belong) of the outcome of the Report, including the archiving thereof, by no later than three months from the date of the notice of receipt or, in the absence of such notice, within three months from the expiration of the seven-day period from the submission of the Report.

(b) Specific investigations

8.7 Where, as a result of the preliminary analysis, useful and sufficient elements emerge or can otherwise be inferred for an assessment of the merits of the submitted Internal Reporting, without prejudice to the right of defence of the Person Concerned, the Reporting Body (or the Compliance Officer of the Group to which the Companies belong) shall:

a) initiate specific analyses and investigations, making use, where appropriate, of the corporate functions involved, in any case in compliance with the law, including the applicable privacy

laws;

b) conclude the investigation at any time if, in its course, it is ascertained that the Report is unfounded (in this case, the rules on archiving described above will apply);

c) make use, where necessary, of external experts and consultants (in accordance with the rules described above);

d) interact with the Reporting Person, and ask the latter for integrations, as necessary;

e) agree with the relevant Companies' top management, any corrective actions necessary for the removal of the detected control's weaknesses, also ensuring the monitoring of the latter's implementation;

f) provide acknowledgement of the Report within three months from the date of the notice of receipt or, in case of lack of such notice, within three months from the expiration of the seven-day period from the submission of the Report;

g) agree with the head of the internal function involved in the Report, any initiatives to be taken to protect the interests of the Companies (*e.g.*, legal action) to be proposed to the Companies' top management;

h) provide any useful element so that the head of the internal function, provided with the appropriate powers, can assess the initiation of disciplinary proceedings against the Reporting Person, in case of Reports in relation to which the bad faith of the Reporting Person and/or the merely defamatory intent are established, and possibly confirmed by the merits of the Report itself;

i) submit the results of in-depth investigations of the Report to the Companies' top management, if the Report refers to employees and it is found to be well founded, so that the most appropriate measures can be taken against the employees concerned.

(c) Conclusion of the investigation

8.8 Save what stated under paragraphs 8.5 and 8.6 above for the preliminary phase, the investigation on the Report shall be considered concluded when the Companies, having undertaken the specific investigative measures mentioned in paragraph 8.7, decide one of the following: (i) archive the case, for it being unfounded or not sufficiently proven; (ii) start a disciplinary procedure against the Person Concerned and/or mentioned in the Report; (iii) file a Report or a claim before any competent authority; (iv) undertake any other measure, including of contractual nature, as a result of the investigation following the Report.

8.9 A Report that had been archived can be resumed and the investigation reopened if new and substantial elements emerge afterwards on the same reported violation(s). Such new elements can be derived by additional information provided by the initial Reporting Person, or by a new Report made by a different Reporting Person, or by information anyhow collected by the Companies in the course of their activities. In such case, the Reporting Person(s) shall be informed of it within the timeframe and with the modalities set out by this Whistleblowing Policy.

9 Protection measures for the Reporting Person, the Person Concerned and/or mentioned in the report

(a) Confidentiality obligations on the identity of the Reporting Person

9.1 In the context of disciplinary proceedings, the identity of the Reporting Person may not be disclosed where the contestation of the disciplinary charge is based on investigations which are separate and additional to the Internal Reporting, even if resulting from it. Where the charge is based, wholly or partially, on the Internal Reporting and the knowledge of the identity of the Reporting Person is indispensable for the defence of the Person Concerned, the Internal Reporting can be used for the purposes of disciplinary proceedings only if the Reporting Person have given his/her explicit consent to the disclosure of his/her identity.

9.2 The Reporting Person shall be informed in writing of the disclosure of their confidential data in the case referred to in paragraph 9.1 above.

9.3 The Companies guarantee adequate protection of the confidentiality of the identity of the Reporting Person by censuring any conduct that violates the measures provided for their protection by the application of the disciplinary system's provisions adopted by the Companies in this regard. In addition, the Companies ensure that the identity of the persons in any case mentioned in the Report is also protected until the conclusion of the relevant proceeding.

(b) Prohibition of discrimination against the Reporting Person

9.4 With respect to the Reporting Person (and the persons deemed to be equivalent to the Reporting Person, under the previous paragraphs), any form of retaliation or discriminatory measure, whether direct or indirect, affecting working conditions for any reason directly or indirectly related to the Report, is prohibited. Any act undertaken in breach of this prohibition is void.

The protection measures apply when one of the following conditions is met:

a) at the time of the Internal or External Reporting or Public Disclosure, the Reporting Person has reasonable grounds to believe that the information about the reported Breach is true and falls within the objective scope of this Whistleblowing Policy;

b) an External Reporting has been submitted where permitted by law;

c) the Report has been subject to Public Disclosure made only if the Reporting Person:

i. has previously submitted an Internal Reporting by means of the Reporting Channels set up by the Companies and/or by the external reporting channel referred to in the Whistleblowing Policy and the Reporting Person has not received response in such regard;

ii. has reasonable grounds to believe that the Breach constitute an imminent and/or obvious danger to the public interest;

iii. has valid reason to believe that the Internal or External Reporting may determine the risk of retaliation and/or may not be effectively followed up due to the specific circumstances of the concrete case, such as those circumstances where evidences may be concealed or destroyed or where there is well-founded fear that the person who received the Report may be colluding with the author of the Breach or to be

involved in the Breach itself.

d) the Report has been submitted by means of the Reporting Channels and/or has been subject to Public Disclosure on an anonymous basis, where the Reporting Person has subsequently been identified and retaliated against, as well as in cases where the Report has been submitted to the relevant institutions, bodies and organs of the European Union.

9.5 The adoption of discriminatory measures against the Reporting Person may be complained to ANAC, for measures within its competence.

(c) Exceptions to the protection and disciplinary violations

9.6 The protection measures are not guaranteed to the Reporting Persons to whom a disciplinary sanction is imposed, because they have been convicted for defamation or slander or for the same crimes connected with the reporting to the judicial or accounting authority or when their civil liability, for the same title has been established for malice or gross negligence, even with a judgment of first instance.

9.7 The Companies reserve the right to take the appropriate actions, set out in the disciplinary system, against anyone who carries out, or threatens to carry out, acts of retaliation against those who have submitted Reports in accordance with the Whistleblowing Policy.

9.8 In addition to the above two paragraphs and the one that follows, the following constitute disciplinary offenses: (1) Breach of the Whistleblowing Policy as well as (2) unlawfully obstructing or attempting to obstruct the Report, (3) the violation of confidentiality obligations, and (4) the failure to verify and analyse Reports.

9.9 It is understood that the Companies may take the most appropriate disciplinary and/or legal measures to protect their rights, assets and image against anyone who, in bad faith, has made false, unfounded or opportunistic Reports and/or for the sole purpose of slandering, defaming or causing harm to the Person Concerned or other persons mentioned in the Report. It also constitutes a source of liability, in disciplinary and other competent venues, any other hypothesis of improper use or intentional abuse of the Whistleblowing Policy.

(d) Protection of the Person Concerned and/or mentioned in the Report

9.10 The Person Concerned shall be informed, as soon as possible, of the charges against him or her, whether or not they are based on the Internal Reporting, in compliance with the principles of adversarial process and defence which are generally applicable to disciplinary and/or sanction proceedings. The Person Concerned may be heard, or, at his or her request, shall be heard, including by means of a written procedure through the acquisition of comments and documents.

9.11 Information regarding the proceedings initiated against the Person Concerned (or other persons otherwise mentioned in the report) may be delayed or excluded if there is a substantial risk that such disclosure would compromise the Companies' ability to effectively investigate the Person Concerned and/or to gather the necessary evidence, until such risks cease to exist, always in compliance with applicable law provisions.

10 Processing and protection of Personal Data

10.1 The Companies are the data controllers of personal data collected and processed in the context

referred in to the Whistleblowing Policy (the "**Data Controllers**"). The Data Controllers will process personal data of the data subjects involved in the report, in accordance with the principles set forth by the Regulation 2016/679 (the "**GDPR**"), providing them with all the necessary information, pursuant to Articles 13 and 14 of the GDPR, as well as by implementing appropriate measures to ensure the protection of data subjects' rights and freedoms.

10.2 In the context of managing the Report and the related procedure, the Data Controllers are supported by the Reporting Body (or by the Compliance Officer of the Group to which the Companies belong) and the auxiliary personnel in charge, duly authorized to process personal data pursuant to Article 29 of the GDPR and Article 2-*quaterdecies* of Legislative Decree 196/2003 (the "**Privacy Code**").

10.3 In addition to the above, the Data Controllers may be supported by external experts and consultants, duly authorized to process personal data under a specific data processing agreement (the "**DPA**"), in accordance with Article 28 of the GDPR.

10.4 The Data Controllers ensure that any third party, possibly involved in the management of the reporting procedure (*e.g.*, personnel assigned to the Companies' internal functions involved in the Report), processes personal data only if expressly authorized and under the instruction provided by the Data Controllers.

10.5 The exercise of the rights provided for in Articles 15-22 of the GDPR by the Person Concerned may be limited or precluded altogether, in accordance with the provisions set forth by Article 2-*undecies* of the Privacy Code, where their exercise may result in an actual and concrete prejudice to the protection of the confidentiality of the Reporting Person and persons considered equivalent to the latter, and/or to the progress of investigations or the exercise of the Companies' right in court. This is without prejudice to the possibility for the Person Concerned to exercise their rights by requesting the intervention of the Italian data protection authority (*Garante per la protezione dei dati personali*) according to the modalities set forth by Article 160 of the Privacy Code.

10.6 For further details on the above and on the modalities of the processing activities carried out by Data Controllers, please refer to the information notice addressed by the Companies in this regard, available on the Companies' sharepoint.

11 Detention and access to the Documentation

11.1 The Reporting Body (or the the Compliance Officer of the Group to which the Companies belong]), and all the functions that may be involved in the activities regulated by the Whistleblowing Policy, shall ensure, each to the extent of its competence and also by means of the information systems used, the traceability of the data and information and shall provide for the detention and filing of the documentation produced, on paper and/or electronically, so as to allow the proof of the different phases of the process itself.

11.2 The detention of the original documentation of the Reports, in appropriate paper/electronic archives with the highest standards of security/confidentiality is guaranteed.

11.3 The original paper and/or electronic documentation must be kept for as long as necessary for the processing of the Report and in any case for no longer than five years from the date of the communication of the final outcome of the reporting process, in compliance with the principles of confidentiality and minimization referred to in Article 5 of the GDPR.

11.4 The documentation related to each Report may be subject to longer retention periods (i) in execution of applicable legal obligations and provisions, (ii) for administrative purposes and/or (iii) to assert and/or defend the rights and/or legitimate interests of the Companies or third parties, including in case of complaints, litigation or pre-litigation.

11.5 The Reports done in bad faith shall be archived after deletion of the names and of any element that may allow the identification of the Reporting Person and any person involved in the Report.

11.6 The unfounded Reports, which are subject to archiving, are kept until the expiry date of the statute of limitations applicable to the reported conduct or to the right to compensation arising therefrom, whichever is longer, accompanied by an explanatory note of the reason for the deletion.

12 Final provisions

12.1 The procedure should be revised as the need arises.

12.2 Legal Department is responsible for regular revision of the procedure.