Effective: 05/12/2023
Procedure - Document for external use

NOLOSTAND S.P.A - WHISTLEBLOWING MANAGEMENT PROCEDURE

L01.001 - first issue

REFERENCE PROCESS

Managing reports of breaches

RESPONSIBLE ORGANISATIONAL STRUCTURE/LEGAL ENTITY

Nolostand S.p.a

MAIN RECIPIENTS

All Nolostand staff including external staff; workers or external staff providing goods or services or carrying out works for third parties; freelancers; consultants; volunteers and trainees; shareholders and individuals with administrative, management, control, supervisory or representative functions.

OBJECTIVES

Nolostand S.p.a undertakes to protect from intimidation and retaliation individuals who have reported, in good faith, breaches of national or EU regulations that are detrimental to their interest or integrity, which they have become aware of in their own work-related context, as well as individuals other than the person making the report, who could be the recipients of retaliation, even indirect, due to their role in the reporting process and/or the particular relationship that connects them to the person making the report. As regards Reports made by persons who have declared their personal details and that are in bad faith and/or are proven to have a slanderous/defamatory content, the measures provided for in the corporate disciplinary system will be taken against the identified reporting person, and appropriate legal action will be evaluated.

MAIN CONTENTS

- Illustration of the mechanisms for protecting the reporting person, the reported person and confidentiality;
- Procedure for sending the report and report contents;
- Illustration of the process for handling reports, with information about the persons in charge and/or control bodies responsible for each activity;
- Description of activities to monitor corrective actions and the management of disciplinary measures.

MAIN NEW ASPECTS

This procedure incorporates the following new aspects:

- **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;
- **Legislative Decree 24/2023** (the "Whistleblowing Decree"), transposing Directive (EU) 2019/1937. The purpose of Legislative Decree 24/2023, in the wake of the European Directive, is to consolidate the legal protection of persons who report breaches of national or European regulatory provisions, which harm the interests and/or integrity of the public or private entity to which they belong, and of which they become aware in the course of their work. More generally, the decree aims to promote a culture of legality and compliance in organisational contexts, through the harmonisation of whistleblowing regulations in relation to indications of European Union institutions and international best practices.

Effective: 05/12/2023
Procedure - Document for external use

NOLOSTAND S.P.A - WHISTLEBLOWING MANAGEMENT PROCEDURE

L01.001 - first issue

APPROVAL LEVELS

Approved by the Board of Directors of Nolostand S.p.a on 5 December 2023

SCOPE

This document applies to the company Nolostand S.p.A.

TABLE OF CONTENTS

1. REFERENCE PRINCIPLES ***3***
1.1 LEGAL FRAMEWORK ***3***
2. REFERENCES ***4***
3. DEFINITIONS AND ABBREVIATIONS ***4***
4.PROCESS DESCRIPTION ***5***
4.1 REPORTING COVERED BY THIS PROCEDURE 5
4.2 RECIPIENTS 6
4.3 INTERNAL AND EXTERNAL REPORTING CHANNELS 6
4.4 CONTENT OF THE REPORT 8
4.5 PROTECTION OF CONFIDENTIALITY AND PROCESSING OF PERSONAL DATA 8
4.6 PROTECTIVE MEASURES FOR THE REPORTING PERSON 9
5. MANAGEMENT OF THE INTERNAL REPORTING CHANNEL 11
5.1 Management Body 11
5.2 Preliminary Verification 12
5. 3 Investigation 12
5.4 Special cases 13
5.5 Reporting 14
5.6 Filing, logging and storage 14
6. MONITORING OF CORRECTIVE ACTIONS ***15***
7. SANCTION SYSTEM ***15***
8.REGISTRATION, DISSEMINATION AND FILING ***17***
9.ANNEXES ***17***
DATA PROCESSING FOR PRIVACY PURPOSES ***17***

1. REFERENCE PRINCIPLES

1.1 LEGAL FRAMEWORK

The Legislator approved **Law no. 179 of 30 November 2017**, containing 'Provisions for the protection of persons reporting crimes or irregularities of which they have become aware in the context of a public or private employment relationship' (the '**Whistleblowing Law**'). This Law defines:

- the aspects protecting the reporting employee;
- the obligations of Entities and Companies in terms of the non-discrimination of reporting persons and the protection of their confidentiality;
- the need for the presence of one or more channels (in computerised form) enabling reporting persons to submit reports while guaranteeing the confidentiality of their identity;
- the ban on retaliatory or discriminatory acts against the reporting person for reasons related to the report;
- the need to have - in the disciplinary system - sanctions against individuals who violate the measures to protect the reporting person, and against individuals who make reports with wilful misconduct or gross negligence that turn out to be unfounded.

The law also reiterates that reports of unlawful conduct relevant under Decree no. 231/2001 or of breaches of the Company's organisation and management model, made by employees that have become aware of said, due to the functions they perform, must be described in detail and based on precise and consistent facts, which they have become aware of, due to the functions they perform.

Moreover, **the European Whistleblowing Directive (2019/1937)** requires all Member States to adopt specific regulatory provisions concerning the protection of individuals who report infringements and/or breaches of EU legislation (regulations, and EU directives implemented in the Member States). In addition, the aforementioned Directive provides for the adoption of new standards of protection for persons reporting wrongdoings they become aware of, through (i) the introduction of effective, confidential and secure reporting channels, (ii) the effective protection of reporting persons.

The law aims, among other things, to incentivise the cooperation of workers in order to encourage the emergence of corrupt phenomena within public and private entities, including through the provision of systems enabling workers to safely report any wrongdoing of which they become aware.

Lastly, **Legislative Decree 24/2023** implementing 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 and on provisions concerning the protection of persons who report breaches of national laws (the **"Whistleblowing Decree")** regulates the protection of persons who report breaches of national or European Union law that harm the public interest or the integrity of the public administration or a private entity, with the main objective of transposing into a single law provisions on the protection of reporting persons, by coordinating (and repealing) existing regulations, aligning with the Directive. The Decree, with particular reference to the private sector, provides for the following, among others:

- the extension of reports that must be included in the scope in question (previously limited to breaches concerning Legislative Decree 231/2001);
- the extension of private-law entities required to put in place a reporting management system (including, for example: private entities that employed an average of at least 50 employees in the previous year; private entities in particular sectors and entities in the scope of Legislative Decree 231/2001, even if they do not reach an average of at least 50 workers);

- the possibility for reporting persons to use external reporting channels when special conditions are met;
- the possibility for the reporting person to publicly disclose (through the press or through electronic or other means of dissemination) the report under special circumstances;
- the application of sanctions in the event of non-compliance with the provisions of the Decree.

2. REFERENCES

- Code of Ethics;
- Organisation, Management and Control Model pursuant to Legislative Decree 231/01;
- Organisational Chart, Function Chart and Service Orders;
- **Law 179/2017** - Provisions for the protection of persons reporting crimes or irregularities they have become aware of in the context of a public or private employment relationship;
- **Directive (EU) 2019/1937** - Protection of persons who report breaches of Union law;
- **Legislative Decree 231/2001** - Administrative Liability of Companies and Entities;
- Regulation (EU) 2016/679 (GDPR) and Legislative Decree 196/03 - Data Protection Code, as amended by Legislative Decree 101/2018;
- **Legislative Decree 24/2023** implementing 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 and on provisions concerning the protection of persons who report breaches of national laws;
- **ANAC Guidelines**, Guidelines on the protection of people who report violations of Union law and the protection of people who report violations of national regulatory provisions. Procedures for the presentation and management of external reports.

3. DEFINITIONS AND ABBREVIATIONS

Model 231: Organisation, Management and Control Model pursuant to Legislative Decree 231/01.

Reporting Committee: cross-functional body formed by the following heads of the parent company Fiera Milano S.p.A.: (i) Director of Group Internal Audit, (ii) Director of Group Security (iii) Director of Legal (iv) Head of Compliance.

FM or Fiera Milano: Fiera Milano S.p.A.

SB: Supervisory Board of Nolostand with autonomous powers of initiative and control, tasked with supervising the operation of and compliance with Model 231 and ensuring it is updated. For the purposes of compliance with the Code of Ethics, the Supervisory Board is referred to as the "Authority for the Application of the Code".

Personnel: permanent and non-permanent employees (trainees, office workers, middle managers and executives), members of corporate boards and external staff working on a permanent basis for Nolostand S.p.a.

Third parties: external parties in a relationship of interest with Nolostand (suppliers, customers, consultants, auditing firms, business partners, associates, external staff, etc.).

Whistleblowing/Reporting: means any communication made, through the channels identified, submitted to protect the integrity of the Company, of violations of national or European regulatory provisions, of illegal conduct relevant to Legislative Decree 231 or the principles of the Code of Ethics, of the Organisational Model 231 and of the internal procedures

adopted by the company, based on precise and consistent facts, of which the recipients have become aware because of the functions performed

4.PROCESS DESCRIPTION

4.1 REPORTING COVERED BY THIS PROCEDURE

This Procedure covers the following types of Reporting (also referred to as 'whistleblowing'):

- unlawful conduct, relevant under Legislative Decree 231/01; and breaches or suspected breaches of the Model, the Code of Ethics or Preventive Protocols from which a sanction risk may arise for the Company pursuant to the Decree;
- corporate or business transactions for which it is suspected that a sanction risk may arise for the Company pursuant to the Decree;
- breaches of national or European Union law that are detrimental to the public interest of the private entity, which they have become aware of in the course of their work, and in particular:
  -administrative, accounting, civil or criminal offences; offences falling within the scope of European Union or national law indicated in the annex to Legislative Decree 24/2023 or national law implementing European Union law indicated in the annex to Directive (EU) 2019/1937, even if not indicated in the annex to this decree, relating to the following sectors: public procurement; financial services, products and markets and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and security of networks and information systems;
  acts or omissions affecting the financial interests of the Union (as referred to in Article 325[1] of the Treaty on the Functioning of the European Union, the fight against fraud and illegal activities detrimental to the financial interests of the EU) specified in relevant secondary legislation of the European Union;
  acts or omissions relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;
- suspicions about actual breaches or breaches which, on the basis of concrete elements, could be committed in the organisation in which the reporting person or the person making the complaint to the judicial or accounting authorities has a legal relationship of employment or self-employment, public or private, as well as elements concerning attempts to conceal such breaches.

Reported conduct:

- may qualify as the **commission** of a specific breach or even as merely an **omission** of expected conduct;
- may concern a request to commit a breach or inducement to commit a breach;
- is likely to cause damage or harm to the Company, whether economic, financial or even just reputational.

The following cannot be reported:

[1] For example fraud, corruption and any other illegal activity related to EU expenditure

a) challenges, claims or demands linked to a personal interest of the reporting person or of the person filing a complaint with the judicial or accounting authorities that relate exclusively to his or her individual work or public employment relationship, or to his or her work or public employment relationship with his or her superiors;
b) breaches of national security, and of contracts relating to defence or national security aspects, unless those aspects are covered by relevant secondary law of the European Union.

4.2 RECIPIENTS

This procedure is valid for all Nolostand S.p.A. personnel, including external staff; workers or external staff providing goods or services or carrying out works for third parties; freelancers; consultants; volunteers and trainees; shareholders and individuals with administrative, management, control, supervisory or representative functions.
In particular, the recipients of this document are:

- the top management and members of the corporate bodies of Nolostand S.p.a;
- individuals who hold representative, administrative or managerial positions in the entity or in one of its organisational units with financial and functional autonomy, as well as individuals who manage and control said, also on a de facto basis;
- individuals managed or supervised by one of the above-mentioned persons (so-called subordinates);
- employees of Nolostand S.p.a;
- partners, customers, suppliers, consultants, external staff, trainees, associates and, more generally, anyone who is in a relationship of interest with Nolostand S.p.A ("Third Parties"), whether paid or unpaid.

4.3 INTERNAL AND EXTERNAL REPORTING CHANNELS

Reports can be made through various channels:

- in **writing:** (i) by computerised means, using dedicated reporting software suitable for guaranteeing, with encryption tools, the confidentiality of the reporting person's identity, of the reported person's identity and of the person(s) mentioned in the report, if any, as well as the content of the report and of the relevant documentation. The platform is accessible through a dedicated *link* on the Company's institutional website. Access to the Software is suitably configured for authorised company users; (ii) by ordinary mail, and only if the aforementioned portal is unavailable, to the address: Whistleblowing Committee c/o Fiera Milano S.p.A. Strada Statale Sempione, 28, 20017 Rho, (MI).
- **orally:** at the request of the reporting person, in a face-to-face meeting with the Reporting Committee, set within a reasonable time limit.

The management of the reporting channel is entrusted to FM's Group Security Department, through FM's Security Intelligence Function. It monitors the proper computerised operation of procedures for managing and filing the Reports received on the dedicated software, in order to ensure the traceability of all Reports received and of the documents annexed to them, in relation to their assessment and verification.
When, at the request of the reporting person, the report is made orally during a meeting with the staff member in charge, it shall, subject to the consent of the reporting person, be documented by the staff member in charge, in a recording on a device suitable for storage and listening, or in minutes. In the case of minutes, the reporting person may verify, rectify and confirm the minutes of the meeting by signing them.

The Reporting Committee, through the Security Intelligence Function, in the context of managing the internal reporting channel, carries out the following activities:

- issues the reporting person with an acknowledgement of receipt of the report **within seven days** of its receipt;
- liaises with the reporting person and may request additions from the latter if necessary;
- '**diligently follows up**' reports received (this action is overseen by the person entrusted to manage the report to assess the existence of the facts reported, the outcome of investigations and any measures taken. In meeting obligations concerning the exercise of a professional activity, diligence must be assessed as regards the nature of the activity exercised);
- provides feedback on the report **within three months** of the date of the acknowledgement of receipt or, in the absence of such a notice, within three months of the expiry of the seven-day period from the submission of the report;
- provides clear information on the channel, procedures and requirements for making internal reports, as well as on the channel, procedures and requirements for making external reports. The above information is displayed and made easily visible in the workplace, and is also readily accessible on the company website.

An internal report mistakenly submitted to a person other than the persons indicated shall be forwarded immediately, and in any case within seven days of its receipt, to the competent person, giving notice of its transmission, at the same time, to the reporting person. The person who has received the report in error is prohibited from keeping a copy of it.

An **anonymous report** is a report without elements that make it possible to identify the sender of the message.
That said, for the purposes of this procedure, it should be noted that anonymous reports will only be taken into account if they are substantiated and adequately documented.
In particular, they must contain a detailed statement of the essential elements of the fact and, where possible, the particulars of the person to whom the fact is attributed, of the people who are in a position to report on circumstances relevant to the reconstruction of the facts, and also indicate or, where possible, attach documentation supporting what has been alleged.
All aspects that do not meet the above criteria and that are merely general, approximate or are mere grievances, will be excluded from the reporting process.

The reporting person may also make an **external report** through the channels activated by the National Anti-Corruption Authority (ANAC) if, at the time of submission, one of the following conditions is met:

- the internal reporting channel is not active or, even if activated, does not comply with regulations;
- an internal report has already been made, and the report has not been followed up;
- the reporting person has reasonable grounds to believe that, if he or she were to make an internal report, the report would not be effectively followed up or the report might give rise to the risk of retaliation;
- the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

Lastly, it is possible for the reporting person to make a **public disclosure,** benefiting from the protection provided for internal/external reporting if, at the time of the public disclosure, one of the following conditions is met: (a) the reporting person has previously made an internal and external report, or has made an external report directly, under the conditions and in the manner laid down in regulations, and no reply has been received within the prescribed time limits regarding the measures envisaged or taken to follow up reports; b) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest; (c) the reporting person has reasonable grounds to believe that the external report may entail a risk of retaliation or may not be effectively followed up because

of 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 has received the report may be colluding with the perpetrator of the breach or involved in the breach itself.

4.4 CONTENT OF THE REPORT

Reports should be as detailed and comprehensive as possible.

Where possible, the reporting person is required to provide all available and useful information to enable the competent persons to carry out appropriate, due controls and checks to verify the validity of the reported facts, such as:

- a clear and complete description of the facts that are being reported;
- the circumstances of the time and place when and where the reported facts were committed;
- personal details or other elements identifying the person(s) who committed the reported facts (e.g. job title, place of employment);
- any documents supporting the report;
- an indication of any other persons who may report on the facts being reported;
- any other information that may provide useful feedback on the existence of the reported facts;
- any private interests linked to the report.

In order for a report to be substantiated, these requirements do not necessarily have to be met at the same time, seeing that the reporting person may not have all the required information.

More specifically, through the IT channel and thus through the software, the reporting person is guided during each stage of the report and has the chance to compile a number of mandatory fields that meet the requested requirements, in order to best provide details.

It is essential that the elements indicated are known directly by the reporting person and that they are not reported or referred to by others.

4.5 PROTECTION OF CONFIDENTIALITY AND PROCESSING OF PERSONAL DATA

The identity of the reporting person and any other information from which this identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the reporting person, to persons other than those competent to receive or follow up the reports and expressly authorised to process such data.

Personnel of the company who receive a report and/or are involved, in any capacity whatsoever, in the management of the report, are required to guarantee the utmost confidentiality of the persons (reporting and reported persons) and the facts reported, except in the cases indicated below:

- the Reporting person incurs criminal liability on the grounds of slander or defamation under the provisions of the Italian Criminal Code;
- the Reporting person incurs non-contractual civil liability pursuant to Article 2043 of the Italian Civil Code;
- knowledge of the identity of the Reporting person is indispensable for the assessment of the Report;
- in the event of any investigations or proceedings initiated by the judicial authorities.

In the case of criminal proceedings, the identity of the reporting person is covered by secrecy in the manner and to the extent provided for in Article 329 of the Italian Code of Criminal Procedure.

In the case of proceedings before the Court of Auditors, the identity of the reporting person cannot be disclosed until the investigation phase is closed.

In the case of disciplinary proceedings, the identity of the reporting person may not be disclosed, where the objection to the disciplinary charge is based on investigations that are separate and additional to the report, even if consequent to it. If the objection is based, in whole or in part, on the report, and knowledge of the identity of the person making the report is indispensable for the defence of the accused person, the report may be used for the purposes of disciplinary proceedings only if the person making the report expressly consents to the disclosure of his or her identity. The reporting person shall be notified in writing of the reasons for the disclosure of the confidential data, where disclosure of the identity of the reporting person and of the information is also indispensable for the defence of the person concerned.

Breach of the duty of confidentiality, apart from the exceptions listed, is a source of disciplinary liability, without prejudice to any further liability provided for by law.

Personal data that are clearly not useful for processing a specific report are not collected or, if accidentally collected, are deleted immediately.

Reports and related documentation are kept for as long as necessary to process the report and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure, subject to confidentiality obligations.

The Controller for the processing of personal data in the management of the Reports is the legal entity, Nolostand S.p.A, that is the owner of the relationship to which the data refer.

The annex to section 11 of this Procedure contains the text of the privacy notice for the processing of personal data related to Reports.

4.6 PROTECTIVE MEASURES FOR THE REPORTING PERSON

Nolostand S.p.A. guarantees people who make reports in good faith against any retaliatory action or direct or indirect conduct as a result of the report, which causes or may directly or indirectly cause unjust harm to the reporting person.

Protection against retaliatory acts is extended to all individuals connected in a broad sense with the reporting organisation and/or person:

- self-employed workers, external staff, freelancers and consultants;
- volunteers and trainees, paid and unpaid;
- shareholders and persons with administrative, management, control, supervisory or representative functions, even if such functions are exercised on a de facto basis;
- so-called **facilitators** (people who assist the worker in the reporting process, operating in the same work-related context and whose assistance must be kept confidential);
- people in the same work-related context as the reporting person or the person who has filed a complaint with the judicial or accounting authorities or made a public disclosure and who are linked to them by a stable emotional relationship or relationship of kinship up to the fourth degree;
- co-workers of the reporting person or of the person who has filed a complaint with the judicial or accounting authorities or made a public disclosure, who work in the same work-related context as the reporting person and who have a regular and current relationship with that person;

- entities owned by the reporting person or the person who has filed a complaint with the judicial or accounting authorities or made a public disclosure, or for whom those persons work, as well as entities operating in the same work-related context as those persons.

The protection of reporting persons also applies if the report takes place in the following cases: (i) when the legal relationship has not yet begun, if information on breaches has been acquired during the selection process or at other pre-contractual stages; (ii) during the probationary period; (iii) after termination of the legal relationship if the information on breaches was acquired in the course of that relationship.

Persons making reports in good faith are also protected in the event that, at the time of making the report, they had reasonable grounds to believe that the information on the breaches was true and fell within the scope of the Procedure.

Protection also applies if, after anonymous reporting, the reporting person is identified and suffers retaliation.

The reasons that led the person to make a report or public disclosure are irrelevant to his or her protection.

The protective measures consist of:

- **A ban on and protection from retaliation**: the person making a report may not be subject to retaliation. Reporting persons may inform ANAC of the retaliation[2] they believe they have suffered and the Authority is obliged to inform the National Labour Inspectorate, for measures within its remit. The judicial authority shall take all measures, including provisional measures, necessary to ensure the protection of the subjective legal situation asserted, such as: compensation for damages, reinstatement in the workplace, an order to cease the retaliatory conduct engaged in, a declaration of the invalidity of the acts adopted as an act of retaliation1.

- **Support measures**: support measures are in place for reporting persons, provided by companies, such as: information, assistance, advice free of charge on how to report and on protection from retaliation, on the rights of the person concerned, as well as on the terms and conditions of access to legal aid. ANAC keeps a list of Third Sector entities that provide reporting persons with support measures. The list, published by ANAC on its website, contains the Third Sector entities that have entered into an agreement with ANAC.

- **Limitations of liability**: persons will not be punished if, in making a report: (i) they disclose or disseminate information on breaches covered by the obligation of secrecy, relating to copyright protection or the protection of personal data; (ii) they disclose information about breaches that offend the reputation of the reported person; (iii) there are reasonable grounds to believe that the disclosure or dissemination of the same information was necessary to disclose the breach. Liability is, however, not excluded for

[2] Article 17 of the Decree identifies certain cases: *a) dismissal, suspension; b) downgrading or non-promotion; c) change of duties, change of the place of work, reduction of salary, change of working hours; d) suspension of training; e) negative merit notes; () the adoption of disciplinary measures or other sanctions, including fines; g) coercion, intimidation, harassment or ostracism; h) discrimination or otherwise unfavourable treatment; i) the failure to convert a fixed-term employment contract into an employment contract of indefinite duration where the employee had a legitimate expectation of such a conversion; l) non-renewal or early termination of a fixed-term employment contract; m) 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; n) improper listing on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future; o) early termination or cancellation of the contract for the supply of goods or services; p) cancellation of a licence or permit; q) the request to undergo psychiatric or medical examinations'.*

conduct, acts or omissions not related to the report or not strictly necessary to disclose the breach.

Protection is not guaranteed if the reporting person is proven to be criminally liable for offences of defamation or slander, even by a ruling of the first instance, or is proven to have civil liability, in cases of wilful misconduct or gross negligence (disciplinary sanctions are also applied to the reporting person).

5. MANAGEMENT OF THE INTERNAL REPORTING CHANNEL

5.1 Management Body

The FM Whistleblowing Committee is the body responsible for receiving, examining and assessing reports.
The Whistleblowing Committee, as part of the management of the internal reporting channel, carries out the following activities:

- issues the reporting person with an acknowledgement of receipt of the report **within seven days** of its receipt;
- liaises with the reporting person and may request additions from the latter if necessary;
- '**diligently follows up**' reports received (this action is overseen by the person entrusted to manage the report to assess the existence of the facts reported, the outcome of investigations and any measures taken. In meeting obligations concerning the exercise of a professional activity, diligence must be assessed as regards the nature of the activity exercised);
- provides feedback on the report **within three months** of the date of the acknowledgement of receipt or, in the absence of such a notice, within three months of the expiry of the seven-day period from the submission of the report;
- provides clear information on the channel, procedures and requirements for making internal reports, as well as on the channel, procedures and requirements for making external reports. The above information is displayed and made easily visible in the workplace, and is also readily accessible on the company website.

Furthermore, for all Reports received, it is responsible for:

- informing the SB of Nolostand, where the report has relevant profiles pursuant to Legislative Decree 231/2001;

- evaluating the Reports received, activating the assessment and audit activities deemed necessary, with the support of the Group Internal Audit Department of Fiera Milano S.p.a and possibly specialised external companies;

- formalising the assessments and decisions made in specific intermediate or final reports to complete the investigations carried out;

- filing, through authorised users, their reports and supporting documents;

- updating, through authorised users, the status of reports in the dedicated web platform.

5.2 Preliminary Verification

The Whistleblowing Committee meets whenever a report is received, in any form, and has the task of verifying the admissibility of the report received.

All internal reports received are subject to a preliminary check by the Whistleblowing Committee, which analyses the communication and any documentation received from the Reporting Person and carries out a preliminary examination of the existence of the conditions, necessary to initiate further investigations. In particular, the initial assessment takes into account the existence of a reasonable presumption of validity/reliability, at least with regard to the possibility of carrying out concrete verifications of the facts reported, excluding all cases in which the completely generic nature of the reports does not even allow for a verification directed towards concrete perspectives, in which case the conditions for filing are implicitly determined.

In preliminary verification activities, the Whistleblowing Committee may avail itself of the support of the Internal Audit Department of Fiera Milano or specialised consultants, based on the specific skills required in relation to the content of the Report being verified.

At the end of the preliminary verification, the Whistleblowing Committee files unsubstantiated internal reports or those which, based on the description of the facts and the information provided by the Reporting person, do not allow obtaining a sufficiently detailed picture to be able to initiate further investigations to ascertain their validity, as well as those that are manifestly unfounded.

5. 3 Investigation

If the preliminary verification has established that the Internal Report is adequately substantiated and accompanied by evidence whose authenticity could be verified, the Whistleblowing Committee carries out the following activities:

- classifies the type of report and in the case of a report relating to the potential commission of significant offences for the purposes of Legislative Decree 231/01, it provides information to the Supervisory Board, also giving evidence of the decisions taken;
- in the event that the existence of sufficiently detailed elements emerges or - in any case - that the facts reported are not unfounded, inform the Chairperson and the CEO of the Company on a monthly basis;
- informs the Board of Statutory Auditors in cases of alleged accounting irregularities and/or deficiencies in the company's accounting control system;
- inform the competent functions, in all other cases;
- evaluates the further appropriate investigative actions to be carried out (e.g. requesting management insights, starting an audit or fraud investigation), possibly making use of the Internal Audit Department of FM based on specific skills, or of external consultants, where necessary;
- if it does not consider it necessary to request FM's Group Internal Audit Department, or possibly specialised companies to carry out investigations/audits, decide if and what recommendations to make in writing to the management of the areas/processes concerned and if there are elements to sanction illegal or irregular behaviour of Nolostand Staff or third parties, thus filing the Report;
- interrupts the investigation activities if, as a result of them, it emerges that the Report is unfounded;

- suggests any initiatives to be undertaken to protect the interests of the company (e.g. legal action, suspension/cancellation of suppliers from the Fiera Milano Group's Supplier Register, contractual withdrawal).

At all stages of the process, the Whistleblowing Committee:

- guarantees impartiality, autonomy and independence of judgment in the analysis and evaluation of internal reporting;
- ensures the confidentiality of the information collected and the confidentiality of the Reporting person's name, where provided;
- undertakes not to use internal reports beyond what is necessary to adequately follow up on them.

At the end of the preliminary phase by the Whistleblowing Committee, decisions may take the form of:

- corrective action recommendations;
- proposals for disciplinary measures for the parties involved in the reported facts (both internal and third parties);
- timely information to the Board of Directors and the Board of Statutory Auditors for the adoption of appropriate reporting actions to the judicial authority in the cases provided for by the relevant laws;
- filing, if the reports (i) do not fall within the definition set out in this Procedure by forwarding the same, if necessary, to other company Departments/Functions; (ii) are clearly unfounded or in bad faith or of such generic content that it does not allow any verification regarding the same or relating to facts already known and the subject

of appropriate evaluation and disciplinary actions provided for by this Procedure and by the relevant external regulations and provisions.

The reasons for the dismissal decision are formalised in writing and communicated to the Reporting person.

All parties involved will not be able to reveal the identity of the Reporting person and any other information from which such identity can be deduced, directly or indirectly, without the express consent of the Reporting person, to persons other than those competent to receive or follow up on the reports, expressly authorised to process such data pursuant to articles 29 and 32, paragraph 4, of Regulation (EU) 2016/679 and Article 2-quaterdecies of the code on the protection of personal data referred to in Legislative Decree 30 June 2003, No. 19.

5.4 Special cases

In order to guarantee the independence and impartiality of judgment of the body responsible for receiving, examining and evaluating, as well as the full collegiality of the Whistleblowing Committee, if the Report concerns one or more members of the Whistleblowing Committee, the same Committee proceeds to exclude the reported member(s) from specific investigation activities.

They may be informed - in writing - that a report has been received, with respect to which they have a conflict of interest. For this reason, they will not be informed of the content at first and will not be required to carry out any activity. In the further course of the investigation, it may instead be useful - and indeed necessary - to involve the reported persons in the investigation, for instance by means of a hearing with them. In such circumstances, and in order to ensure

the collegiality of the Committee, a substitute, identified in the person of the Risk & Compliance Director, steps in.

Where the Internal Reporting concerns, on the other hand, an internal component of the Supervisory Body, the standard procedure mentioned above is followed.

If the internal report containing serious, precise and concordant elements concerns more than one member of the Supervisory Board or the only external member, if any, it must be forwarded to the Board of Directors, by means of delivery to the Chairman of the Board of Directors of the document file.

The Board of Directors, having consulted the Board of Statutory Auditors, after having collectively assessed whether the internal report is accompanied by the information necessary to preliminarily verify its validity and be able to start subsequent in-depth activities, carries out the investigation making use of the company's expertise and, if necessary , of specialised consultants.

The investigation follows the process described in this Procedure.

The decision of the Board of Directors is formalised through a written resolution.

If the report concerns a member of the Board of Directors or a member of the Board of Statutory Auditors, it will be handled by the remaining members of the two corporate bodies.

The Whistleblowing Committee, after having collectively assessed that the internal Report is accompanied by the information necessary to verify its merits beforehand and to be able to initiate subsequent in-depth activities, will initiate the investigation using the competent company structures or specialised external consultants.

The final decision is formalised in a specific written resolution.

5.5 Reporting

Every month, the Security Intelligence Function, in the name and on behalf of the Whistleblowing Committee, sends communication of any reports received to the Supervisory Body, to the Control and Risks Committee of FM, to the Board of Statutory Auditors and to the Board of Directors.

The Whistleblowing Committee reports every six months on the proper functioning of the internal Reporting systems, reporting in a report the aggregated information on the results of the activity carried out and on the follow-up given to the Reports received; in drafting this report, the Committee is required to comply with the provisions of the regulations on the protection of personal data.

5.6 Filing, logging and storage

The Whistleblowing Committee assigns a specific alphanumeric ID to the report and proceeds to record the details of the report on a computer register, in particular:

- day and time;
- reporting person;
- subject of the report;
- notes;
- status of the report (to be filled in at each stage of the process, e.g. preliminary investigation, investigation and communication of the evidence that emerged, filing).

If the report arrives on an electronic platform, the software itself provides for complete and confidential logging in compliance with the relevant legislation.

Where the report is received via a different channel, the same logging procedure is carried out.

Internal Reports that do not pass the preliminary phase are filed and are taken into account in the periodic reporting.

In any case, the Group Security Department, through the Security Intelligence Function, is required to record the internal Report and the activities carried out following its receipt in the register of reports and investigations and to report them in the annual report to the Board of Directors, ensuring the confidentiality of the identity of the Reporting person and the parties reported.

The assessments and decisions of the Whistleblowing Committee, the information provided in the case of reports relating to relevant facts and the (possible) recommendations and proposals for the application of disciplinary measures are in all cases formalised in writing by the Whistleblowing Committee in a special report and are stored in protected network folders, in order to ensure traceability, confidentiality, conservation and availability of data throughout the procedure.

Internal reports received shall be retained for as long as necessary for the processing of the report and, in any event, no longer than five years from the date of the communication of the final outcome of the reporting procedure in compliance with the confidentiality obligations set out in Article 12 of Legislative Decree 24/2023 and the principle set out in Article 5(1)(e) of Regulation (EU) 2016/679 and Article 3(1)(e) of Legislative Decree no. 51 of 2018. In the event of defence investigations by the Company (the controller) or investigations and inspections by the judicial authorities or judicial police, as well as in the event of litigation or proceedings, this deadline may be extended until the conclusion of such activities or proceedings.

6. MONITORING OF CORRECTIVE ACTIONS

It is the responsibility of the management of the areas/processes concerned to implement the recommendations received from the Whistleblowing Committee based on this Procedure and for the corrective actions (action plan) possibly indicated in the reports drawn up at the conclusion of the audits conducted by the Group Internal Audit/Group Security Department of FM, with the possible support of specialised companies.

The Whistleblowing Committee, with the support of FM's Group Security Directory/Group Internal Audit Department, monitors the implementation of recommendations and action plans, informing, for reports on relevant facts, the FM and Risks Control Committee, the Board of Statutory Auditors, senior management entities and the Supervisory Board (for issues of competence).

The Whistleblowing Committee, through authorised users, stores the information received regarding corrective actions in the dedicated database corresponding to the reference report.

7. SANCTION SYSTEM

Depending on the profile of the party to whom the internal report refers (reported person), the Whistleblowing Committee identifies the company function responsible for proceeding with any necessary measures/interventions, informing the SB and Board of Directors, whilst keeping the identity of the Reporting person secret, except in cases of law or authorisation for disclosure by the Reporting person themselves.

In particular, the Whistleblowing Committee, in compliance with the relevant legislation, indicates the need for measures:

- to the Human Resources & Organization Department of FM, in the case of disciplinary sanctions to be applied against employees and managers;
- to the Board of Directors and the Board of Statutory Auditors, in the case of measures to be taken against members of the Board of Directors or of the Board of Statutory Auditors, or of the Supervisory Board;
- to the Head of the Organisational Function that manages the contractual relationship;
- to the Chief Executive Officer, for information.

Without prejudice to the prerogatives of Nolostand's Board of Directors for violations of Model 231 and the Code of Ethics, the Whistleblowing Committee, throughout the reporting process, proposes the application of the measures considered most appropriate, in compliance with current legislation, individual National Collective Labour Agreements and internal regulations if reports of bad faith or illegal or irregular behaviour emerge.

In the case of criminally significant behaviour for which Nolostand is obliged to file a complaint or for which they could file a complaint, in compliance with the provisions of the relevant laws, the Whistleblowing Committee promptly informs the company's Board of Directors and Board of Statutory Auditors for the adoption of appropriate actions.

In the case of measures for significant events pursuant to Legislative Decree 231/01, the Whistleblowing Committee makes a proposal for measures in accordance with the SB and in compliance with Model 231, without prejudice to the skills and responsibilities of the SB in this area.

The body responsible for activating the sanctioning system decides which type of sanction to impose on subjects who have committed violations ascertained following internal reporting.

The sanction, which must be in line with the provisions of the applicable labour law, should be proportionate to the seriousness of the offence.

In the event that the Reporting person is jointly responsible for the violations, privileged treatment is provided for the latter compared to the other jointly responsible persons, compatibly with the violation committed and with the applicable regulations.

In the case of disciplinary proceedings, the identity of the reporting person may not be disclosed, where the objection to the disciplinary charge is based on investigations that are separate and additional to the report, even if consequent to it. If the objection is based, in whole or in part, on the report, and knowledge of the identity of the person making the report is indispensable for the defence of the accused person, the Internal Report may be used for the purposes of disciplinary proceedings only if the person making the report expressly consents to the disclosure of his or her identity. In case of refusal by the Reporting person, the Whistleblowing Committee will file the Internal Report without following up on it.

In this latter case, notice is given to the reporting person by means of written communication of the reasons for the disclosure of the confidential data. Notice of the disclosure of the identity of the reporting person and of the information is also given when it is also indispensable for the purposes of the defence of the person involved.

The person involved can be heard, or, upon their request, is heard, also through a paper procedure through the acquisition of written observations and documents.

This procedure is without prejudice to the criminal and disciplinary liability of the Reporting person in the event of a slanderous or defamatory report pursuant to the Italian Criminal Code and Article 2043 of the Italian Civil Code.

The behaviour of those who make reports that prove to be unfounded with intent or gross negligence is also sanctioned.

Any form of abuse of this procedure, such as internal reports that are manifestly opportunistic and/or made for the sole purpose of harming the complainant or other subjects, and any other suggestion of improper use or intentional exploitation of the institution that is the subject of this procedure.

Therefore, when the reporting person's criminal liability for offences of defamation or slander or, in any event, for the same offences committed with the report to the judicial or accounting authorities or his/her civil liability, for the same reason, in cases of wilful misconduct or gross negligence, is established, even by a judgment of first instance, the protections provided for in this procedure are not guaranteed and a disciplinary sanction is imposed on the reporting or whistleblowing person (including in cases of reporting or complaint to the judicial or accounting authorities or anonymous public disclosure, if the reporting person is subsequently identified and retaliated against).

8.REGISTRATION, DISSEMINATION AND FILING

This Procedure is published on:

- the Company's website;
- the intranet of the Fiera Milano Group.

Internal reports received shall be retained for as long as necessary for the processing of the report and, in any event, no longer than five years from the date of the communication of the final outcome of the reporting procedure in compliance with the confidentiality obligations set out in Article 12 of Legislative Decree 24/2023 and the principle set out in Article 5(1)(e) of Regulation (EU) 2016/679 and Article 3(1)(e) of Legislative Decree no. 51 of 2018.

9.ANNEXES

DATA PROCESSING FOR PRIVACY PURPOSES

Privacy notice on the processing of personal data related to the operation of the whistleblowing system

Pursuant to Articles 13 and 14 of Regulation (EU) 679/2016 (hereinafter also the "GDPR"), provides some information regarding the processing of personal data related to the management of reports of unlawful conduct (so-called whistleblowing).

THE CONTROLLER

The controller of personal data (hereinafter referred to as the "Controller") is Nolostand S.p.a (hereinafter also referred to as the "Company"), that may be contacted in writing at:

- the registered office in Milan, Piazzale Carlo Magno 1
- At the email address: direzione@nolostand.it .

PLACE OF DATA PROCESSING

The processed personal data are not transferred to countries outside the EU or disseminated.

TYPES OF DATA PROCESSED AND PURPOSE OF THE PROCESSING

Through the reporting channels indicated in the Whistleblowing Management Procedure adopted by the Company, the following categories of personal data may be collected:

- personal and contact details of the reporting person, if the latter decides to communicate them, (unless the report is sent anonymously);
- personal data also referring to subjects other than the reporting person (such as the reported person, the facilitator and other people possibly involved in the reporting), contained in the reporting or in any case in possession of the Company and mainly relating to the relationship with the same Company (e.g. qualification , area/office to which they belong, etc.), and to the potential violations being reported (which could also concern criminally relevant conduct or the details of possible crimes).

The aforementioned personal data are processed by the Controller for purposes related to the receipt and management of the report, the carrying out of the necessary investigative activities to verify its validity and the adoption of any consequent measures provided for by the reference standards and described by the Whistleblowing Management Procedure adopted by the Company.

Where present in the report and necessary for the relevant investigation, personal data belonging to particular categories may also be acquired and processed (such as, for example, racial and ethnic origin, religious and philosophical beliefs, political opinions, membership of political parties or trade unions, as well as personal data revealing health status and sexual orientation).

It remains understood that, in accordance with the provisions of the relevant regulations, personal data which are manifestly not useful for the processing of a specific report are not collected or, if collected accidentally, are deleted immediately.

LEGAL BASIS FOR PROCESSING

For the purposes highlighted above, the processing of personal data is necessary for the fulfilment of the obligations established by the aforementioned regulations regarding Whistleblowing (Legislative Decree 24/2023 and Article 6 of Legislative Decree 231/2001, as amended by law 179/2017), to which the Controller is subject (Article 6 par. 1 letter c) GDPR) and for the pursuit of legitimate interests (Article 6 par. 1 letter f) GDPR) connected to technical management and the security of the reporting channels, as well as the fight against any unlawful conduct (for example in violation of the Company's Code of Ethics) and the possible assessment, exercise and defence of rights in court. Any processing of personal data relating to potential criminal offences reported is carried out on the basis of the provisions in Article 10 of the GDPR insofar as authorised by specific sector regulations as above, and also to protect or defend rights in judicial proceedings (see Article 2-octies, paragraph 2, letter e) of Legislative Decree 196/2003 - "Privacy Code"), while the processing of special data is carried out only where it is necessary for the management of the report based on the aforementioned regulations and for the purpose of ascertaining, exercising or defending a right in court (pursuant to Article 9 , paragraph 2, letters b), f) and g) of the GDPR).

RETENTION TIMES

To pursue the above purposes, the processed data are kept for a period of no less than five years from the date of closure of activities to manage reports, in such a way as to guarantee the confidentiality and protection of personal data, and to be able to reconstruct the entire dossier if required. In the event of defence investigations by the company (the controller) or investigations and inspections by the judicial authorities or judicial police, as well as in the event of litigation or proceedings, this deadline may be extended until the conclusion of such activities or proceedings. If, as a result of the aforementioned assessments, the report is not followed up, the data will be retained for one year after being collected.

RECIPIENTS OF DATA

Personal data are processed by authorised and instructed Company personnel and, where appropriate, by other corporate bodies (e.g. the Supervisory Board) or by external parties,

acting as processors, who support the Company in carrying out certain technical, organisational and consulting activities. In addition, where necessary, personal data may be disclosed to the judicial authorities, the police, or other public and/or private entities entitled to receive them in accordance with current legislation.

PROCESSING METHODS

Personal data are processed using mainly automated methods and with organisational and processing logics strictly related to the above-mentioned purposes and in any case in such a way as to guarantee the security, integrity and confidentiality of the data in compliance with the organisational, physical and logical measures provided for by provisions in force.

RIGHTS OF DATA SUBJECTS

Each data subject (the reporting person, the reported person etc.), has the right to obtain from the Company, in the cases provided for, access to the data concerning him/her and to obtain a copy of said data, to rectify or supplement them if they are inaccurate or incomplete, to erase them or to obtain the restriction of their processing if the conditions are met, and to object to their processing for reasons relating to his/her particular situation. As regards data subjects other than the reporting person, it should be noted that the exercise of the aforementioned rights may be restricted pursuant to Article 2-undecies(1)(f) of the Privacy Code, if the exercise of such rights may actually and concretely prejudice the confidentiality of the reporting person's identity.

Data subjects may contact the Data Protection Authority, also by filing a complaint where deemed necessary, to protect their personal data and rights.

CONTACTS

In order to exercise the aforementioned rights and for any further information concerning the processing of personal data, data subjects may contact the Controller at the addresses given in the first paragraph of this document.