DELTA PREG S.P.A.

Località Tei, 10 – 55011 Altopascio (LU) VAT no. 01723910467

WHISTLEBLOWING PROCEDURE

Document Code	WB - proc
Version	7.0
Issue	29 October 2026
Revision	Board of Directors Meeting dated 29/10/2026
Owner of data processing	**DELTA PREG S.P.A.**
Web Platform	https://deltapreg.comunicazioneilleciti.it
Manager of Whistleblowing reports	External consultant, formally appointed
Responsible for this document	Company management or persona specifically designated for this purpose
Level of confidentiality	Reports, the identity of the persons involved, and all related documentation shall be treated as strictly confidential and shall be accessible exclusively to the **Reports Manager** and any other persons specifically authorised to access them.
Level of dissemination	Maximum, with access to reports restricted to authorised personnel only.
Attachments	- Attachment 1 – Whistleblowing report form - Attachment 2 – Privacy Notice on the Processing of Personal Data in the Context of Whistleblowing Reports

1. Purpose, Scope and Principles of the Procedure

This procedure governs the methods for the submission, receipt, assessment and management of reports of violations made within the work-related context of **Delta Preg S.p.A. – Località Tei, 10 – 55011 Altopascio (LU), Italy – VAT No. 01723910467** (hereinafter also referred to as the "Company"), pursuant to Legislative Decree No. 24 of 10 March 2023.

The Company has established various reporting channels, including, in particular, an internal reporting channel through the online platform accessible at:

https://deltapreg.comunicazioneilleciti.it

The receipt and management of reports are entrusted to an external professional, appointed through a separate engagement agreement, who acts as the External Whistleblowing Reports Manager in a sole-member capacity, operating with autonomy, independence, impartiality and adequate professional expertise.

The purpose of this procedure is to promote the disclosure of violations that may harm the public interest or the integrity of the Company, ensure the timely and confidential handling of reports, protect the reporting person and other protected individuals, and prevent any form of retaliation.

The Company guarantees the confidentiality of the identity of the reporting person, the facilitator, the person concerned, any individuals mentioned in the report, as well as the content of the report and the related documentation.

This procedure applies exclusively to reports that fall within the subjective and material scope of **Legislative Decree No. 24/2023**. Communications that do not meet these requirements may be handled as ordinary reports, without the automatic application of the specific protection measures provided for by the Decree.

This procedure is aligned with the Company's organisational framework and documentation relating to personal data protection, information security, employment relationship management and internal control systems.

2. Applicable Legislation

This procedure is adopted in implementation of and in compliance with the following legislation:

- **Legislative Decree No. 24 of 10 March 2023**, implementing **Directive (EU) 2019/1937**;
- **Directive (EU) 2019/1937** on the protection of persons who report breaches of Union law;
- **Legislative Decree No. 211 of 30 December 2025**, concerning amendments to the regulations governing reports of breaches of European Union restrictive

measures;

- **Regulation (EU) 2016/679 (GDPR)** and **Legislative Decree No. 196 of 30 June 2003**, as amended by **Legislative Decree No. 101 of 10 August 2018**;
- **ANAC Guidelines No. 1/2025** on internal reporting channels, approved by Resolution No. 478 of 26 November 2025;
- **ANAC Guidelines** on external reporting, approved by Resolution No. 311 of 12 July 2023 and updated by Resolution No. 479 of 26 November 2025;
- Applicable **national and European Union provisions** relating to the violations that may be reported.

3. Subjective Scope of Application

DELTA PREG S.p.A. has established internal reporting channels in accordance with Legislative Decree No. 24/2023 and the requirements applicable to private-sector entities.

Reports may be submitted by natural persons who have obtained information concerning violations within the context of their work-related relationship with the Company, including, in particular: employees, self-employed workers, collaborators, freelancers and consultants, employees and collaborators of suppliers, volunteers and trainees, whether paid or unpaid, shareholders, persons performing administrative, management, control, supervisory or representative functions.

Reports may also be submitted by job applicants, individuals undergoing a probationary period, and persons whose relationship with the Company has ended, provided that the information was acquired during the recruitment process, the probationary period, or the previous employment or professional relationship.

4. Subject Matter of the Report

Pursuant to Legislative Decree No. 24/2023, reports, complaints or public disclosures may concern information regarding breaches of national or European Union legal provisions that harm the public interest or the integrity of the Company and of which the reporting person became aware within the work-related context.

The information may concern:

- violations that have already occurred;
- violations that have not yet occurred but which, based on concrete elements, the reporting person reasonably believes are likely to occur;
- conduct intended to conceal violations.

4.1 Relevant Violations

This procedure applies to information concerning conduct, acts or omissions that harm the public interest or the integrity of the Company and which consist of:

- breaches falling within the scope of European Union acts or national provisions implementing them, in the areas of public procurement, financial services, products and markets, anti-money laundering and counter-terrorist financing, product safety and compliance, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, privacy and personal data protection, and the security of network and information systems;
- acts or omissions affecting the financial interests of the European Union;
- acts or omissions relating to the internal market, including infringements of European Union rules on competition, State aid and corporate taxation;
- acts or conduct that defeat the object or purpose of European Union provisions in the sectors referred to above;
- breaches of European Union restrictive measures falling within the scope of the applicable legislation

4.2 Exclusions

The following do not fall within the scope of this procedure:

- disputes, claims or requests relating to a personal interest of the reporting person and concerning exclusively their individual employment relationship;
- reports that are mandatorily governed by specific European Union or national regulations providing dedicated reporting channels;
- reports concerning national security matters or procurement involving defence or national security aspects, except as otherwise provided by European Union law.

4.3 General Principles

A report must be based on information acquired within the work-related context and on reasonable grounds to believe that the reported facts are true and fall within the scope of **Legislative Decree No. 24/2023**.

Absolute certainty regarding the reported facts is not required. The personal reasons that prompted the reporting person to submit a report are irrelevant for the application of the protection measures, provided that the conditions established by law are met.

The reporting person must present the information known to them accurately and in sufficient detail, without knowingly altering the facts or the supporting

documentation submitted.

5. Elements and Characteristics of Reports

Reports must be sufficiently detailed and based on specific and consistent factual elements in order to allow the Reports Manager to adequately assess and handle them.

In particular, where known, a report should contain:

- the time and place in which the reported event occurred;
- a clear and complete description of the facts;
- the identity, or other elements enabling the identification, of the person or persons allegedly involved in the reported conduct;
- details of any other persons who may provide information regarding the facts;
- any supporting documentation.

The Reports Manager may dismiss, with appropriate justification, reports that are clearly outside the scope of this procedure, excessively generic, lacking concrete elements, or not reasonably verifiable.

Before dismissing a report, whenever possible, the Reports Manager shall request clarifications or additional information from the reporting person through the confidential communication channel made available by the platform.

Failure to establish that a violation occurred does not, in itself, render a report manifestly unfounded. The reporting person remains entitled to the protection measures provided that, at the time of reporting, they had reasonable grounds to believe that the information reported was true and that all other conditions laid down by **Legislative Decree No. 24/2023** were satisfied.

6. Anonymous Reports

An anonymous report is a report that contains no information allowing the identification of the reporting person. The reporting platform allows reports to be submitted without disclosing personal details.

Anonymous reports shall be considered when they are sufficiently detailed and contain elements enabling verification of the reported facts. Such reports shall be recorded, managed and retained according to confidentiality and security standards equivalent to those applicable to identified reports, to the extent permitted by the impossibility of identifying the reporting person.

A person submitting an anonymous report must carefully retain the identification code issued by the platform, which is necessary to access the report, view communications from the Reports Manager, provide additional information and monitor the

progress of the report.

Where a person who initially submitted an anonymous report is subsequently identified and has suffered retaliation, they may benefit from the protection measures provided by **Legislative Decree No. 24/2023**, provided that the conditions established by law are met.

Anonymous reports that are clearly outside the scope of this procedure, excessively generic, or lacking useful elements to allow reasonable verification may be dismissed by the Reports Manager with appropriate justification. Whenever possible, before dismissing such reports, the Reports Manager may request clarifications or additional information through the confidential channel available on the platform.

7. Internal Reporting Channel

The Company has established an internal reporting channel pursuant to Article 4 of **Legislative Decree No. 24/2023**, formalised through a specific resolution of the Board of Directors.

The company trade union representatives or the trade union organisations referred to in Article 51 of **Legislative Decree No. 81/2015** were consulted regarding the establishment of the reporting channel.

7.1 Confidentiality Safeguards

The internal channel, including through encryption tools or other appropriate technical solutions, guarantees:

- the confidentiality of the reporting person's identity;
- the confidentiality of the facilitator;
- the confidentiality of the person concerned and any other persons mentioned in the report;
- the confidentiality of the report’s content and related documentation.

The identity of the reporting person may not be disclosed without their express consent, except where required by law.

7.2 Methods for Submitting a Report

A report may be submitted in two forms: **written** or **oral**.

a) Written Report

a.1 Paper Report – Anonymous: by completing the appropriate form attached to this procedure and sending it by post to the *Reports Manager* at the Company's address indicated above.

The paper form must be placed in a sealed envelope bearing only the wording:

"Strictly Confidential - Whistleblowing - For the Attention of the Reports Manager."

Where an anonymous report is submitted without a confidential contact address or any means of communication with the reporting person, the Reports Manager may be unable to acknowledge receipt, request further information and/or provide the feedback required by law.

To permit adequate assessment, an anonymous report must be sufficiently detailed and contain elements enabling verification of the reported facts.

a.2 Paper Report – Signed: by completing the appropriate form attached to this procedure and sending it by post to the Reports Manager at the Company's address, or by delivering it personally to the Reports Manager. Personal delivery must take place directly to the Reports Manager or according to the instructions provided by them, avoiding delivery to unauthorised persons. For this type of report, the double-envelope system must be used in order to ensure separation between the reporting person's identifying data and the content of the report. The reporting person shall place their personal details, contact information and a copy of an identity document in a first sealed envelope marked "Reporting Person's Identification Details". The completed reporting form shall be placed in a second sealed envelope marked: "Report". Both envelopes shall then be placed inside a third outer envelope for transmission to the person responsible for handling reports.

a.3 Through the Dedicated Reporting Platform

Accessible via the Company intranet and Company's website at:
https://deltapreg.comunicazioneilleciti.it

a.4 Through the Toray Group Global Reporting System

(Only for significant compliance violations; accepted languages: Japanese and English) sending an E-mail to: compliance.teu.mb@mail.toray

a.5 Through the Toray Group Independent Compliance Hotline in Europe

- E-mail: toray.hotline@aplaw.de
- Mail: **Atsumi & Sakai Europe GmbH Rechtsanwälte und Steuerberater, Barckhausstrasse 1, 8th Floor, 60325 Frankfurt am Main, Germany**

b) Oral Report

A report may be submitted:

- through a direct meeting with the Reports Manager, requested via the platform or through the confidential contact details provided in the information documentation, and arranged within a reasonable period;
- through the voice messaging system integrated into the reporting platform;
- through a direct meeting requested from the Supervisory Body at the corporate e-mail address: odv-dp.delta.mb@delta.toray;

- by calling the Toray Global Reporting System operated by Atsumi & Sakai Europe GmbH at: 00800 200 200 2.

Where the report is made during a face-to-face meeting, it shall be documented, subject to the reporting person's consent, either by means of an audio recording on a device suitable for storage and playback or by written minutes.

The reporting person may review, correct and confirm the minutes by signing them.

Features of the Dedicated Reporting Platform:

- ensures the confidentiality of both the report and the reporting person, proper data management, and the most effective and secure interaction;
- guarantees **encryption of data** and report content during transmission and storage;
- ensures the **logical separation of identifying information** from the report content;
- allows reports to be submitted **anonymously**;
- provides a **secure and confidential communication channel** between the Reports Manager and the reporting person, including in cases of anonymity;
- prevents unauthorised access to report contents and includes access-tracking systems;
- is available 24 hours a day through the Company website and/or corporate intranet.

Personal data are processed in compliance with applicable data protection legislation, including the GDPR, and retained for the period strictly necessary to manage the report and, in any event, no longer than the retention periods established by Legislative Decree No. 24/2023.

7.3 Management of Reports

Management of the reporting channel is entrusted to the **Reports Manager**, appointed by the Company as an external professional possessing autonomy, independence and appropriate expertise.

The external professional acts as a Data Processor pursuant to Article 28 of Regulation (EU) 2016/679, on the basis of a specific agreement containing the Company's documented instructions.

7.4 Reports Received by Unauthorized Persons

Where a report is submitted to a person other than the designated **Reports Manager**, it must be forwarded to the latter within seven (7) days of receipt, and the reporting person must be informed accordingly.

8. External Reporting Channel - ANAC

The reporting person may submit an external report to the **National Anti-Corruption Authority (ANAC)** in the cases provided for by Article 6 of **Legislative Decree No. 24/2023**, particularly when:

- the internal reporting channel is not active or does not comply with the legal requirements;
- the reporting person has already submitted an internal report and no follow-up has been provided within the prescribed time limits;
- the reporting person has reasonable grounds to believe that the internal report would not be effectively addressed or that it could expose them to a risk of retaliation;
- the reporting person has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest.

The management of the external reporting channel falls exclusively within the competence of **ANAC**.

External reports may be submitted:

- in writing, through the IT platform made available by ANAC;
- orally, through dedicated telephone lines or voice messaging systems;
- through a direct meeting, upon request by the reporting person, scheduled within a reasonable timeframe.

The external channel guarantees:

- the confidentiality of the reporting person's identity;
- the confidentiality of the person concerned and any other individuals mentioned in the report;
- protection of the content of the report and the related documentation;
- the use of encryption tools and appropriate technical measures to safeguard personal data.

8.1 ANAC Obligations

ANAC:

- issues an acknowledgment of receipt of the report within seven (7) days, unless expressly requested otherwise by the reporting person or where such acknowledgment could jeopardise confidentiality;
- maintains communications with the reporting person and may request

supplementary information;

- carries out the necessary assessments and investigations;
- provides feedback within three (3) months of the acknowledgment of receipt, or within six (6) months where justified reasons exist;
- communicates the final outcome of the report, which may include dismissal or referral to the competent authorities.

Where the report does not fall within ANAC's jurisdiction, ANAC shall forward it to the competent administrative or judicial authority and shall inform the reporting person accordingly.

9. Public Disclosure

Pursuant to Article 15 of **Legislative Decree No. 24/2023**, a reporting person may make a public disclosure by placing information relating to violations in the public domain through the press, electronic media or other means capable of reaching a large number of people.

The reporting person shall benefit from the protection measures provided by the Decree if, at the time of the public disclosure, at least one of the following conditions is met:

1. they have previously submitted an internal report and an external report, or have submitted an external report directly, and no response has been provided within the statutory time limits;
2. they have reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest;
3. they have reasonable grounds to believe that the external report may expose them to retaliation or may not be effectively addressed due to the specific circumstances of the case, including, by way of example, the risk of evidence being concealed or destroyed, or a well-founded concern of collusion between the recipient of the report and the perpetrator of the violation.

Outside the circumstances described above, a public disclosure does not give rise to the protection measures provided by **Legislative Decree No. 24/2023**.

10. Reporting to Judicial Authorities

The reporting person retains the right to report unlawful conduct directly to the judicial authorities where they become aware of such conduct within the work-related context.

Where the legal requirements are met, a person who submits a report to the judicial authorities shall benefit from the protection measures provided by **Legislative**

Decree No. 24/2023.

Where facts emerge from the report or from the investigations carried out that must be notified to the judicial authorities, ANAC or other competent authorities, such communication shall be made by the Company or the Reports Manager within the limits of their respective duties and obligations.

Such communication shall be restricted to information that is relevant and necessary and shall be carried out in compliance with confidentiality obligations and the applicable provisions safeguarding the identity of the reporting person.

11. Protection of Confidentiality

11.1 Confidentiality of the Reporting Person's Identity and of the Report

The identity of the reporting person, and any other information from which such identity may be directly or indirectly inferred, may not be disclosed, without the reporting person's express consent, to persons other than those authorised to receive or follow up on reports, except where expressly required by law.

Confidentiality is also guaranteed with respect to:

- the facilitator;
- the person concerned;
- individuals mentioned in the report;
- the content of the report;
- the related documentation.

Information contained in a report may not be used for purposes other than those necessary to ensure appropriate follow-up.

Where a report is received by a person other than the Reports Manager, the recipient must forward it to the Reports Manager within seven (7) days, without retaining a copy, ensuring the confidentiality of the information and, where possible, informing the reporting person accordingly.

11.2 Confidentiality in Disciplinary and Judicial Proceedings

In disciplinary proceedings, the identity of the reporting person shall not be disclosed where the disciplinary charges are based on findings that are separate from and additional to the report itself.

Where the disciplinary charges are based, wholly or partly, on the report and knowledge of the reporting person's identity is essential for the defence of the accused person, such identity may be disclosed only with the reporting person's express consent.

The reporting person shall receive prior written notice, including the reasons justifying the disclosure.

Within criminal proceedings, the identity of the reporting person shall be protected in accordance with Article 329 of the Italian Code of Criminal Procedure and any other applicable legal provisions.

11.3 Obligations of the Reports Manager and Other Persons Involved

The Reports Manager and any other persons lawfully involved in handling or investigating reports are bound by a specific enhanced duty of confidentiality.
The involvement of additional persons must be limited to what is strictly necessary. Where disclosure of the reporting person's identity is not indispensable, the information shall be anonymised or otherwise rendered non-identifiable in advance.
Any breach of confidentiality obligations may result in the consequences provided by applicable laws, contracts and appointment instruments.

12. Conditions for the Protection of the Reporting Person

The protection measures provided for by **Legislative Decree No. 24/2023** apply where, at the time of the report, the report to the judicial or accounting authorities, or the public disclosure:

1. the reporting person had reasonable grounds to believe that the information concerning the violations was true and fell within the material scope of application of the Decree;
2. the report, complaint or public disclosure was made in accordance with the procedures established by the applicable legislation.

The personal reasons that prompted the reporting person to submit a report, complaint or public disclosure are irrelevant for the purposes of protection.
Protection also applies:

- in the case of anonymous reports or public disclosures where the reporting person is subsequently identified and has suffered retaliation;
- where reports are submitted to institutions, bodies or agencies of the European Union in accordance with the applicable legislation.

11.1 Limitations on Protection

Protection measures do not apply, and disciplinary sanctions may be imposed on the reporting person, where it is established, including by a first-instance court judgment, that:

- the reporting person has incurred criminal liability for defamation, slander, or other offences committed through a report to the judicial or accounting authorities;

- the reporting person has incurred civil liability for wilful misconduct or gross negligence in relation to the same conduct.

An incorrect assessment of the reported facts shall not result in the loss of protection where, at the time of the report, the reporting person had reasonable grounds to believe that the information disclosed was true and the other conditions established by law were met.

13. Protection Against Retaliation and Discrimination

A person who submits a report, complaint or public disclosure pursuant to **Legislative Decree No. 24/2023** may not be subjected, for that reason, to any form of direct or indirect retaliation.

Retaliation means:

"Any act, omission or behaviour, whether actual, attempted or threatened, carried out as a result of a report, a report to the judicial or accounting authorities, or a public disclosure, and which causes or may cause unjust harm, directly or indirectly, to the reporting person or the person who made the complaint."

Pursuant to Article 19 of Legislative Decree No. 24/2023:

- retaliatory acts are null and void;
- in the event of a dispute, the burden of proof rests on the employer to demonstrate that any measures taken against the reporting person were based on reasons unrelated to the report.

A causal link must exist between the report and the allegedly retaliatory measure.

13.1 Examples of Retaliation

By way of example, and without limitation, retaliation may include:

- dismissal, suspension or equivalent measures;
- demotion or failure to promote;
- changes in duties, transfer, reduction of remuneration or modification of working hours;
- suspension of training or restrictions on access to training;
- negative performance assessments or unfavourable references;
- disciplinary sanctions or other punitive measures, including financial penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination or unfavourable treatment;
- failure to convert a fixed-term contract where there was a legitimate expectation of conversion;

- non-renewal or early termination of a fixed-term contract;
- reputational damage or economic or financial loss;
- inclusion on improper blacklists affecting future employment opportunities;
- early termination or cancellation of supply contracts;
- revocation of licences or permits;
- unjustified requests to undergo psychiatric or medical examinations.

13.2 Conditions for the Application of Protection

Protection against retaliation applies where:

- the person submitted the report, complaint or public disclosure based on a reasonable belief in the truthfulness of the information;
- the report falls within the material scope of **Legislative Decree No. 24/2023**;
- the report was submitted in accordance with the procedures established by law;
- a causal relationship exists between the report and the retaliatory measure.

Mere suspicions or rumours unsupported by objective evidence are not sufficient.
Neither absolute certainty regarding the reported facts nor the personal reasons that prompted the report are relevant for the purposes of protection.
Where the above conditions are not met, the protective regime shall not apply.

14. Processing of Personal Data

The processing of personal data carried out in relation to the management of reports shall comply with:

- **Legislative Decree No. 24/2023**;
- **Regulation (EU) 2016/679 (GDPR)**;
- **Legislative Decree No. 196/2003**, as amended by **Legislative Decree No. 101/2018**.

14.1 Purposes and Principles of Processing

Personal data shall be processed exclusively for the management and follow-up of reports, in accordance with the principles of:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality.

Personal data that are manifestly irrelevant to the handling of a report shall be deleted immediately.

14.2 Roles and Parties Involved in Processing

The Company acts as the Data Controller for the processing of personal data carried out in connection with the receipt and management of reports.

Where the management of reports is entrusted to a professional or other external party independent from the Company's bodies, such party shall act as a Data Processor pursuant to Article 28 of Regulation (EU) 2016/679, under a specific agreement containing the documented instructions of the Data Controller.

The provider of the reporting platform acts as a separate Data Processor for the technical activities relating to service provision, maintenance, security, storage and support.

Individuals acting under the authority of the Data Controller or Data Processors must be expressly authorised and instructed, appropriately trained and subject to specific confidentiality obligations.

Any involvement of consultants, lawyers, investigators or other professionals in investigative activities shall be permitted only where necessary, after determining their role in the processing activities and the information to which they may have access.

All persons who, in any capacity, access reports or related documentation are bound by an enhanced duty of confidentiality.

14.3 Data Subjects' Rights

Data subjects are entitled to exercise the rights provided for in Articles 15 to 22 of Regulation (EU) 2016/679, to the extent that such rights are applicable to the processing concerned.

The exercise of these rights may be restricted, delayed or excluded in the cases provided for by Article 2-undecies of Legislative Decree No. 196/2003, where exercising such rights could cause actual and concrete prejudice to the confidentiality of the reporting person's identity, the conduct of investigations or other interests protected by law.

Any restriction shall not apply automatically but shall be assessed in light of the specific circumstances of the case and must be necessary and proportionate.

In the cases provided for by Article 2-undecies of Legislative Decree No. 196/2003, rights may be exercised through the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) in accordance with Article 160 of the same Decree.

14.4 Retention and Deletion

Reports and related documentation shall be retained for the time necessary to manage the report and, in any event, for no longer than **five (5) years** from the date on which the final outcome of the reporting procedure is communicated.

Personal data that are clearly unnecessary for the processing of a specific report shall not be collected or, if acquired inadvertently, shall be promptly deleted.

Upon expiration of the retention period, the report and related documentation shall be securely deleted or irreversibly anonymised.

Documents that are necessary for separate judicial, disciplinary or administrative proceedings may be retained within the relevant files on the basis of the applicable legal grounds and for the retention period applicable to those proceedings, limited to the information strictly necessary.

14.5 Consequences of Breaches of Whistleblowing Regulations

ANAC exercises the sanctioning powers provided for by Article 21 of Legislative Decree No. 24/2023 in cases involving:

- failure to establish a reporting channel;
- adoption of non-compliant procedures;
- failure to carry out verification and assessment activities;
- obstruction or attempted obstruction of reporting;
- breach of confidentiality obligations;
- retaliatory conduct.

Any civil, criminal, administrative, disciplinary or contractual liability of the persons involved shall remain unaffected where the relevant legal requirements are met.

15. Publication, Updating and Entry into Force

15.1 Publication and Dissemination

This procedure, the privacy notice and the information necessary to use the internal reporting channel shall be made available to all recipients through:

- publication on the Company's corporate website, in a dedicated section (where available);
- publication on the corporate intranet (where available);
- internal communication to employees and collaborators;
- availability to workers and external parties maintaining relationships with the Company.

Information concerning the internal reporting channels, including access instructions for the reporting platform, shall be easily accessible and presented in a clear and

understandable manner.
The Company shall promote appropriate awareness and training initiatives concerning whistleblowing in order to ensure proper understanding of the procedure and the related protection measures.

15.2 Updating of the Procedure

This procedure shall be reviewed periodically and updated whenever necessary due to:

- legislative amendments;
- new guidance issued by competent authorities;
- changes to the reporting channel or reporting platform;
- replacement of the Reports Manager;
- significant organisational changes;
- issues or deficiencies identified during implementation.

Any update shall be approved by the competent corporate body and communicated to recipients prior to its implementation.

15.3 Entry into Force

This procedure shall enter into force on the date indicated on the cover page and shall replace any previous Company provisions concerning the same subject matter.

16. Prevailing language

In case of contrast, the Italian version of this document shall prevail.