Procedure for Reports Management

1. Objective

This document describes the mechanism through which Great Lengths Group intends to regulate the process of receiving and managing reports, in compliance with the protection and privacy of the whistleblower and in compliance with the methods and regulations in force.

2. Introduction

Legislative Decree no. 24 of March 10th, 2023, implementing Directive (EU) 2019/1937 (hereinafter, the "Whistleblowing Decree"), came into force on March 30th 2023. This Decree regulates the protection of persons who report violations of national or European Union legislation that are harmful to the public interest or the integrity of public administrations or private entities, which they become aware of in the context of their work.

Article 5 of the Whistleblowing Decree requires that, for the correct management of reports, clear information be made available:

- on the internal reporting channel adopted by the Company;
- on the external reporting channel;
- on the procedures and prerequisites for making internal and external reports.

In light of the above, this document (hereinafter, the "*Whistleblowing Procedure*" or "*Procedure*") defines the reporting management system adopted by **Great Lengths Group** (hereinafter, "*Great Lengths*" or the "*Company*"), subject to prior information being provided to the trade union representatives where applicable, in compliance with the provisions of the Whistleblowing Decree.

3. Definitions

For the purposes of this Procedure, the following terms have the meaning indicated:

ANAC: National Anti-Corruption Authority.

Code of Ethics: a document defining the ethical principles and values that guide the Company in carrying out its activities.

- Recipients: individuals who fall within the categories indicated by the Whistleblowing Decree and who may submit reports or be involved in their management, including (but not limited to): employees (permanent/fixed-term; managers, executives, clerks, workers; collaborators, interns, trainees), self-employed workers (e.g., agents and consultants), shareholders, directors, members of corporate and supervisory bodies, as well as third parties (business partners, suppliers, customers - including professional salons - and other individuals acting in the name and/or on behalf and/or in the interest of the Company or with whom the Company maintains professional or business relationships).
- Public disclosure / "publicly disclose": making information about violations publicly available through the press, electronic media, or other means of dissemination capable of reaching a large number of people.
- Facilitator: Person who assists the whistleblower in the reporting process, working in the same work context; such assistance must remain confidential.
- GDPR: Regulation (EU) 2016/679 on the protection of personal data.
- Model 231: Organization, Management, and Control Model adopted by the Company pursuant to Legislative Decree No. 231/2001 (where applicable).
- Supervisory Body (SB): Body established pursuant to Article 6, paragraph 1, letter b) of Legislative Decree No. 231/2001 (where applicable), which performs supervisory functions and receives specific information flows, including regarding reports.
- Person involved: Person mentioned in the report as being implicated in the reported violation.
- Platform: IT tool that can be adopted by the Company to submit and manage internal whistleblowing reports (hereinafter also "Platform").
- Whistleblowing Manager: Internal person/office or independent external entity, with adequately trained staff, appointed by the Company to manage internal reports through the implemented channel.
- Feedback: Communication to the reporting person regarding the follow-up given or intended to be given to the report.
- Retaliation: Any behavior, act, or omission (including attempted or threatened) adopted as a result of an internal/external report or public disclosure, which causes or may cause, directly or indirectly, unfair harm to the reporting person.
- Whistleblower: Natural person who makes an internal or external report, or a public disclosure, regarding violations learned in the workplace.
- Reported Person/Perpetrator of the Violation: Person to whom the violation is attributed in the report or public disclosure.
- Reporting: Written or oral communication of information about violations, including well-founded hypotheses and reasonable suspicions, as well as information about conduct intended to conceal violations.

- External reporting: Communication of information about violations submitted through the external reporting channel implemented by ANAC.
- Internal reporting: Communication of information about violations submitted through the internal channel implemented by the Company.
- Follow-up: Actions taken by the person responsible for managing the channel to assess the existence of the facts, the outcome of the investigations, and any measures taken.

4. Scope

This Procedure governs the process of managing internal reports submitted by Whistleblowers and defines the obligations and methods of:

- Receiving, collecting, managing, and archiving reports submitted through the internal channel;
- Identifying the conditions for using the external channel;
- Defining information flows between the Whistleblowing Manager and other potentially involved corporate bodies/functions, depending on the type of report.

The Procedure is adopted in full compliance with confidentiality obligations and personal data protection rules, as provided for, among other things, by Articles 12 and 13 of the Whistleblowing Decree.

In particular, this Procedure is aimed at:

1. Define the scope of application;
2. Identify the individuals who can submit reports;
3. Define the reportable conduct/facts;
4. Indicate the internal reporting channel;
5. Describe the operating procedures for submitting and managing reports and the protections afforded to the reporting party and other protected individuals.

5. Regulatory and documentary references

In addition to the Whistleblowing Decree, the following constitute relevant references (where applicable):

- Model 231 adopted by the Company;
- Code of Ethics adopted by the Company;
- Legislative Decree No. 231 of June 6, 2001 (“Decree 231”);
- Regulation (EU) 2016/679 (“GDPR”);

● Legislative Decree No. 196 of June 30, 2003, as amended by Legislative Decree No. 101/2018 (“Privacy Code”);
● ANAC Resolution No. 311 of July 12, 2023 – “Guidelines on the protection of persons reporting violations of Union law and the protection of persons reporting violations of national regulations. Procedures for submitting and managing external reports”;
● Confindustria – “New Whistleblowing Regulations. Operational Guide for Private Entities” (October 27, 2023);
● ANAC Resolution No. 478 of November 26, 2025 – “Guidelines on Whistleblowing for Internal Reporting Channels.”
● Confindustria - “Whistleblowing Regulations. Operational Guide for Private Entities”

6. Recipients

This Procedure applies to all those who:

1. intend to report unlawful acts learned in the context of their work at the Company;
2. are involved in the report (facilitators, named persons, witnesses, etc.);
3. are identified as the perpetrators of the reported violation;
4. are involved in the management of internal reports (reception, response, investigation, follow-up, and archiving).

These subjects are hereinafter also referred to as “*Recipients*”.

7. Who can report

The following persons (“*Reporters*”) may submit a report:

- Company employees (including agency workers, apprentices, casual/occasional workers, fixed-term, part-time, or intermittent workers);
- Self-employed workers performing activities for the Company (e.g., holders of contracts for work/services or intellectual services);
- Holders of collaboration agreements performing activities for the Company (e.g., agency, commercial representation, continuous and coordinated collaboration);
- Freelance professionals and consultants working for the Company;
- Volunteers and interns, paid or unpaid, working for the Company;
- Shareholders who, in exercising their rights, become aware of violations;
- Persons with administrative, management, control, supervisory, or representative roles at the Company, even if de facto.

The protection also applies when information on violations has been acquired:

- during the probationary period;
- before the establishment of the employment/legal relationship;
- after the termination of the relationship.

8. What can be reported

"*Report*" means the communication of information (even in the form of well-founded suspicions) relating to violations of national or European Union laws that harm the public interest or the integrity of the public administration or the Company, committed within the context of the organization of the Company with which the Reporting Party has one of the relationships indicated in this Procedure.

By way of example, they may be subject to reporting:

- the commission, or attempted commission, of relevant crimes pursuant to Decree 231 (where applicable);
- violation of the Code of Ethics and/or Model 231 (where applicable), including the regulations, directives, policies, and procedures referred to therein;
- violations of European legislation and the acts listed in Annex 1 of the Whistleblowing Decree and national implementing provisions relating to sectors such as:
    - public contracts (e.g., violations of procedural rules for the awarding of public contracts and concessions);
    - services, products, and financial markets; prevention of money laundering and terrorist financing;
    - product safety and compliance (including products and materials distributed for professional use in salons);
    - transportation and logistics safety (e.g., distribution to salons, training centers, and points of sale/partners);
    - environmental protection;
    - radiation protection and nuclear safety;
    - Food and feed safety and animal health and welfare (where relevant);
    - Public health;
    - Consumer protection (including salons and, indirectly, salon customers);
    - Privacy and personal data protection and security of networks and information systems (e.g., data of employees, collaborators, salons, training/event participants, etc.).
- Acts or omissions that harm the financial interests of the European Union;
- Acts or omissions affecting the internal market that affect the free movement of goods, persons, services, and capital (including violations of competition, state aid, corporate tax, and schemes to obtain undue tax advantages);
- Conduct that defeats the object or purpose of EU provisions in the above-mentioned areas;
- Violations of EU restrictive measures

Reports may also concern violations that have not yet been committed and that, based on concrete evidence, the whistleblower reasonably believes may occur. Such evidence may also consist of irregularities or anomalies that the whistleblower considers indicative of potential violations.

9. How to send the report

9.1 Reporting mode

To send an internal report, it is necessary to use the Platform adopted by the Company, accessible from a PC or mobile device, via the link/address indicated by the Company in its internal information channels (whistleblowing@greatlengths.com) and/or on the company website (where applicable).

The report can be made:

a. in **written**, electronic, or electronic form:

b. **orally** through dedicated telephone lines or voice messaging systems and, upon request of the whistleblower, through a direct meeting with the report manager, which must be scheduled within a reasonable time.

In this regard, it is clarified that the choice of reporting method, whether written or oral, is up to the reporting person. For the company, however, it is mandatory to provide both written channels - analog and/or electronic - and oral channels, making both available to the reporting person.

Precautions in case of anonymous reporting

If the Reporter chooses to remain anonymous, he/she is required to adopt, as far as possible, adequate precautions to reduce the risk of identification, including:

1. Avoid sending from company devices;
2. Avoid using devices connected to the company network/intranet;
3. Access the Platform by manually typing the address/URL into your browser;
4. Avoid entering personal data or elements that could allow identification.

If the Reporter uses audio recording, they must not provide personal information or information that could be used to identify them. Where provided by the Platform, their voice may be automatically altered to make it unrecognizable.

Anonymous reports will be processed only if they are sufficiently detailed and suitable to allow for an analysis of the circumstances surrounding the time, place, and manner of the reported event.

It is understood that the principles of this Procedure do not prejudice or limit the reporting obligations to the competent authorities.

9.2 Content of the report

The report must concern facts known to the whistleblower in his/her work context and, where possible, clearly include:

- circumstances of time and place where the event occurred;

- description of the facts;
- personal details or other information useful for identifying the person to whom the events are attributed (if known);
- any other parties involved.

The Reporter may attach documents via the Platform's upload function to provide useful information for the assessment.

The Reporter is encouraged to submit reports only when they have acquired sufficiently complete information to establish a high probability that the event has occurred (or has occurred) and that it is attributable to the specific Reporter. In general, reports should be as detailed as possible to allow for appropriate verification.

If the report is generic or inadequately detailed, the Whistleblowing Manager may request additional information via the Platform's messaging system, in compliance with the protections provided by the Whistleblowing Decree and the option of anonymity.

In the event of frivolous, false, or unfounded reports, containing defamatory content, or made with intent or gross negligence (so-called "bad faith reports"), the Company reserves the right to adopt the resulting measures, including any disciplinary sanctions, in accordance with applicable law.

10. Recipients of the report (access to reports)

The Company ensures that access to the Platform and reports is reserved for the **Whistleblowing Manager**.

Depending on the content of the report, access may be extended:

- to the Supervisory Body (where applicable), in the event of reports impacting Decree 231, Model 231, and/or the Code of Ethics;
- to people expressly authorized by the Whistleblowing Manager, when strictly necessary for the investigation or for the exercise of powers not included in the role of the Whistleblowing Manager (e.g., initiation of disciplinary proceedings by the relevant function).

If an internal report is received from a person other than the Whistleblowing Manager (and therefore outside the Platform) and the Reporting Person expressly declares that they wish to benefit from whistleblowing protections, or this can be deduced from the content, the report must be forwarded within 7 days to the Whistleblowing Manager, simultaneously notifying the Reporting Person (if not anonymous).

11. Safeguards provided in the internal reporting channel

11.1 Confidentiality

The Company guarantees confidentiality:

- the identity of the Reporter;
- the identity of the Facilitator;
- the identity of the Person involved and any other individuals mentioned;
- the content of the report and any attached documentation.

The identity of the Reporter may not be disclosed, without express consent, to anyone other than those authorized to receive or follow up on the report and specifically authorized to process such information. The prohibition on disclosure also applies to any information or element from which the identity of the Reporter may be deduced, directly or indirectly.

Confidentiality is also ensured in the event of legal and disciplinary proceedings. Specifically:

a) Criminal proceedings: the obligation of confidentiality applies to preliminary investigation documents until the deadlines established by law;

b) Proceedings before the Court of Auditors: the obligation of confidentiality applies until the conclusion of the preliminary investigation phase;

c) Disciplinary proceedings: the identity of the Whistleblower cannot be revealed to the Reported Person if the disciplinary action is based on additional and separate investigations other than the report (even if consequential). If the action is based, in whole or in part, on the report and knowledge of the Whistleblower's identity is essential for the accused's defense, the report may be used for the purposes of the proceedings only with the consent of the Reporting Person; in this case, the Whistleblowing Manager shall communicate in writing the reasons for the need for disclosure.

Disciplinary sanctions for violations of the confidentiality obligation may be provided for in Model 231 (where present) and/or in internal policies.

11.2 Prohibition of retaliation and protective measures

It is forbidden any retaliation (even attempted or threatened) following a report, which causes or may cause unjust damage to the Reporter or other protected subjects.

In addition to the whistleblower, the following are protected:

- the Facilitator;
- the persons mentioned in the report;

- persons in the same work environment as the Reporter who have a stable emotional or family relationship within the fourth degree;
- co-workers with a regular and ongoing relationship with the Reporter;
- entities owned by the Reporter;
- entities where the Reporter works.

By way of example (not limited to), retaliatory conduct includes:

- Dismissal, suspension, or equivalent measures;
- Demotion or failure to promote;
- Change of duties, location, reduction in pay, or change in hours;
- Suspension of training or restrictions on access to it;
- Demerit notes or negative references;
- Disciplinary measures or sanctions, including financial ones;
- Coercion, intimidation, harassment, or ostracism;
- Discrimination or unfavorable treatment;
- Failure to convert to permanent employment when there is legitimate expectation;
- Failure to renew or early termination of fixed-term contracts;
- Reputational damage (including on social media) or economic or financial harm, including loss of opportunity or income;
- Inclusion on improper lists that hinder future job opportunities;
- Early termination or cancellation of contracts for the supply of goods or services;
- Cancellation of licenses or permits;
- Request for psychiatric or medical assessments.

Retaliation (even if only threatened) must be reported to ANAC, which is responsible for determining the consequences of the report. If the whistleblower claims to have suffered retaliation, it is up to the perpetrator of the alleged retaliation to demonstrate that it is not related to the report.

Protective measures do not apply if the whistleblower is found criminally liable for defamation or slander (or crimes committed with the report), even if the first instance ruling is not final, or if the whistleblower is found civilly liable for intentionally or negligently reporting false information. In such cases, disciplinary sanctions may apply.

The other protected subjects (other than the whistleblower) must demonstrate the link of consequence between retaliation and reporting.

12. How to manage the report

The Whistleblowing Manager:

- issues the reporting party with an acknowledgement of receipt within 7 days;
- maintains contact with the reporting party, where necessary;
- ensures proper follow-up on reports;
- provides feedback to the reporting party;
- ensures documentation of the activities performed and proper archiving.

12.1 Stages of the procedure

The process of managing reports is divided into four phases:

1. receipt of the report and preliminary verification;
2. investigation;
3. communication of the outcome;
4. archiving.

a) Receipt of the report and preliminary verification

After the report is submitted via the Platform, the system can notify the Whistleblowing Manager that it has been received. The Whistleblowing Manager can view the content (and possibly listen to the audio message) by accessing the Platform.

Within 7 days of receipt, the Whistleblowing Manager will send the Reporting Party (via Platform messaging) a receipt acknowledgement, informing them that they will proceed with the investigation.

Reports are subject to preliminary verification; the investigation is initiated only after any suspicion of fraud has been ruled out:

- manifestly unfounded;
- reports not falling within the scope of the Whistleblowing Decree.

If the report is manifestly unfounded or falls within those excluded from the scope of the Whistleblowing Decree, the Whistleblowing Manager will notify the reporting party in writing and archive the case.

If the report falls outside the scope of the Whistleblowing Decree, the Whistleblowing Manager may forward it to the relevant function (e.g., Legal Department/Unit or Compliance Department), which will handle it as an ordinary report and inform the reporting party. The Whistleblowing Manager may, however, decide to keep the reporting party's identity confidential, where this strengthens protection and is compatible with management.

Under no circumstances may the Whistleblowing Manager determine individual liability or carry out legitimacy/substantive checks on corporate actions and measures: his or her activity

is limited to verifying the validity of the reported facts and activating the required follow-up procedures.

b) Investigation

The investigation is aimed at verifying the validity of the report (unless it is manifestly unfounded). To obtain useful information and documents, the Whistleblowing Manager may:

- contact the Reporting Party via the Platform messaging service for clarifications and additions;
- request a hearing with the Reporting Party, the Reported Party, and/or other individuals who can provide useful information;
- seek the support of external consultants and/or competent company departments, when necessary due to the nature and complexity of the investigations. These individuals are bound by the same protection and confidentiality obligations set forth in this Procedure.

If the report concerns alleged violations relevant to Legislative Decree 231, Model 231, or the Code of Ethics (where applicable), the Whistleblowing Manager shall involve the Supervisory Body as provided in paragraph 11.2.

In any case, the Whistleblowing Manager shall provide feedback to the Reporting Party within 3 months from the date of the notification of receipt of the report or, in the absence of such notification, within 3 months from the expiry of the 7 days from the submission of the report.

The feedback may consist, for example, of communication:

- archiving;
- the progress of the investigation;
- the launch of an internal verification/investigation and the related findings;
- measures adopted or intended to be adopted to manage the issue.

The activities carried out and the results must be adequately documented.

c) Communication of the outcome

At the end of the investigation, the Whistleblowing Manager communicates the results in writing to the Reporting Person.

In the event of a well-founded report, the Whistleblowing Manager may forward the information to the competent function for the exercise of disciplinary power and/or for the adoption of corrective organizational measures, in compliance with the safeguards provided for by this Procedure.

d) Archiving

The Whistleblowing Manager proceeds with archiving, for example, in the event of:

- Generic report that fails to understand the facts or documentation that is irrelevant/unsuitable to clarify the content;

- Unfounded report;
- Report excluded from the scope of the Whistleblowing Decree;
- Production of documentation only in the absence of a structured report.

The archiving must be motivated and communicated in writing to the Reporting Person (if not anonymous).

12.2 Information flow to the Supervisory Body

In cases of reports regarding alleged violations of Decree 231, Model 231 and/or the Code of Ethics (where applicable), the Whistleblowing Manager promptly informs the Supervisory Body, so that it can evaluate the facts and arrange for the investigations deemed necessary, also with the support of the company control functions.

At the end of the assessments, the Supervisory Body communicates the decisions to the Whistleblowing Manager, who concludes the process by communicating the outcome to the Reporting Person.

12.3 Conflict of interest management

The Whistleblowing Manager, if in managing the report:

- is in a significant conflict of interest situation (typical or atypical);
- is the same as the Reporter;
- is the same as the Reported Person or another person affected by the facts (e.g., a witness);

must refrain from handling the report.

In such cases, the Reporting Person is required to report to the Supervisory Body (where present) by ordinary mail, following the "three envelopes" procedure:

1. Insert your identifying information into the first envelope (unless you wish to remain anonymous);
2. Insert the report into the second envelope (separating the identifying information from the contents);
3. Insert both into a third, sealed envelope, marked "CONFIDENTIAL" on the outside, addressed to the Supervisory Body, which will act as the Whistleblowing Manager’s deputy.

13. Sanctioning measures

In compliance with current legislation, applicable collective bargaining agreements and internal provisions, if reports of bad faith (slanderous/defamatory) or illicit/irregular behavior emerge, the Company may adopt disciplinary sanctions:

- against anyone who commits acts of retaliation or unlawful harm, directly or indirectly, against the Reporter or other protected individuals;
- against anyone who hinders or attempts to hinder the reporting;
- against anyone who violates confidentiality obligations;
- against the Reported Person, for proven liability;
- against anyone who violates the protections set forth in this Procedure;
- against anyone who makes unfounded reports with intent or gross negligence.

Disciplinary measures are proportionate to the severity of the conduct found. For further details (where applicable), please refer to the provisions of Model 231 and internal procedures.

ANAC sanctioning measures

ANAC can apply an administrative fine ranging from 10,000 to 50,000 euros when it ascertains:

- Failure to establish reporting channels;
- Failure to adopt procedures for submitting and managing reports;
- Procedures that do not comply with Articles 4 and 5 of the Whistleblowing Decree.

The Company's management body is jointly liable for the sanction with its individual members, without prejudice to the right of recourse against those responsible for the violation.

Sanctioning measures for whistleblowers

The "disciplinary system" envisaged in Model 231 must always provide for sanctions against those who, with intent or gross negligence, make reports that prove to be unfounded.

Article 21, paragraph 1, letter c) introduces a specific provision (the wording of which was described as "unclear" by Confindustria) according to which the ANAC would be entitled to impose a fine of €500 to €2,500 against the whistleblower if their civil liability, based on intent or gross negligence, for the offenses of defamation and slander is established (see p. 7 of the Confindustria commentary on the "Legislative Decree implementing Directive (EU) 2019/1937, concerning the protection of persons who report violations of Union law and national regulations").

However, a whistleblower who reveals or disseminates information on violations covered by the obligation of confidentiality (with the exception of national or European Union provisions regarding classified information; legal and medical professional secrecy; and the confidentiality of judicial decisions) or relating to copyright or personal data protection, or who reveals or disseminates information on violations that harm the reputation of the person involved or reported, is not punishable when, at the time of disclosure or dissemination, there

were reasonable grounds to believe that disclosure or dissemination of the information was necessary to reveal the violation and the report was made pursuant to Article 16.

In such cases, any further liability, including civil or administrative liability, is also excluded.

Unless the act constitutes a crime, the whistleblower does not incur any liability, including civil or administrative liability, for the acquisition of information on violations or for access to such information.

In any case, criminal liability and any other liability, including civil or administrative liability, is not excluded for behaviors, acts or omissions not connected to the report or which are not strictly necessary to reveal the violation.

14. Processing of personal data

All processing of personal data related to the Platform and the management of reports is carried out in compliance with the GDPR, the Privacy Code, and any other applicable legislation.

The processing related to the receipt and management of reports is carried out by the Company as Data Controller, in compliance with the principles set forth in Articles 5 and 25 of the GDPR, providing appropriate information to the Reporting Party and the persons involved pursuant to Articles 13 and 14 of the GDPR, and adopting appropriate measures to protect the rights and freedoms of the data subjects.

Specific information on the processing of personal data related to the management of reports is made available within the Platform.

The Company, the Whistleblowing Manager, and any other parties involved guarantee that the data is processed lawfully, fairly, and transparently, and that only the data necessary for managing reports is collected.

Access to the data is permitted only to expressly authorized and adequately trained individuals, including those in data and information security.

The Company adopts appropriate technical and organizational measures to ensure a level of security appropriate to specific risks, including based on data protection impact assessments (DPIA), and protective measures against unauthorized or unlawful processing, as well as against accidental loss, destruction, or damage.

Personal data manifestly irrelevant to managing the report are not collected or, if accidentally collected, are deleted immediately.

15. Other reporting channels

15.1 External reporting to ANAC

In addition to the internal channel, the Reporting Party can make a report through the external channel established by ANAC, available at the link:

- https://whistleblowing.anticorruzione.it/#/

External reporting is permitted in the cases provided for by the Whistleblowing Decree.

The operating procedures for external reporting are defined and made available by ANAC in the dedicated section of its website.

15.2 Public disclosure

Public disclosure consists of making information about violations publicly available through the press, electronic media, or other channels capable of reaching a large number of people.

The Whistleblower may make public disclosure in the cases provided by the Whistleblowing Decree.

If the Whistleblower voluntarily reveals his or her identity, he or she will not be entitled to confidentiality protection (without prejudice to the other forms of protection provided for by the Decree). If the Whistleblower uses a pseudonym or nickname that does not permit identification, the public disclosure will be treated as an anonymous report.

15.3 Report to the Judicial Authority

The whistleblower may contact the competent judicial authorities to report any unlawful conduct in their workplace.

Even in such cases, the competent authorities are required to comply with the rules on protecting the confidentiality and content of reports set forth in the Whistleblowing Decree.

16. Retention of reports and documentation

The reports received are stored on the Platform for the time necessary for management and, in any case, no longer than 5 years from the date of communication of the final outcome of the activities carried out by the Whistleblowing Manager.

If, at the request of the Whistleblower, the report is made orally during a meeting, the same - with the prior consent of the Whistleblower - is documented by the Whistleblowing Manager (or authorized parties) through:

- recording on a device suitable for storage and listening; or
- meeting minute.

In the case of a report, the Reporting Person can verify, correct and confirm the content by signing.

17. Update

The competent function (e.g. Legal Affairs/Compliance Department) periodically reviews this Procedure, at least annually, and the reporting channels provided for therein, based on the operations and experience gained, in order to ensure its alignment with the relevant legislation.

18. Dissemination, information and training

This Procedure, adopted pursuant to the Whistleblowing Decree and an integral part of the Company's compliance system (and Model 231, where applicable), is made available through the Company's internal information channels and, where appropriate, also through publication on the company website and/or other appropriate means (e.g., company noticeboards).

The Company promotes communication, information, and training activities to ensure the widest possible awareness and most effective implementation.