Whistleblowing Procedure

CODE: ITF-PO-COM-007

Version 1.0

Publication date: 27/10/2026

Rev.	Description	Role	Name
1.0	Alignment with the new template and operational practices Update concerning Whistleblowing Channel Manager	**Responsible**	COM – G. Ravignani
		GM of Italfarmaco S.p.A.	M. Sangiovanni

Summary

1. DEFINITIONS 4

2. INTRODUCTION 6

2.1 OBJECTIVES OF THIS DOCUMENT 6

3. REFERENCES AND RELATED PROCEDURES 7

4. ROLES AND RESPONSIBILITIES 8

5. GENERAL PRINCIPLES 10

5.1 PERSONS ENTITLED TO MAKE A REPORT INFORMATION ON BREACHES (THE 'WHISTLEBLOWER') 10

5.2 INTERNAL REPORTING CHANNEL 11

5.2.1 Person responsible for the channel (the so-called 'channel manager') 12

5.2.2 Features of the internal reporting channel . IT administrator for the channel (IT Channel Manager) 12

5.2.3 Characteristics of reports and anonymous reports 13

5.2.4 Retention of documentation relating to internal reports 14

5.2.5 Information obligations 14

5.2.6 Confidentiality obligation 14

5.2.7 Protection of personal data 16

5.2.8 PROTECTION AND SUPPORT MEASURES 17

5.2.9 Prohibition of retaliation 17

5.2.10 Support measures 18

5.2.11 Limitation of liability for the whistleblower 18

5.2.12 Penalty regime 19

6. DESCRIPTION OF THE PROCESS 20

6.1 OPERATIONAL PROCEDURE FOR HANDLING REPORTS THROUGH THE INTERNAL CHANNEL 20

6.2. EXTERNAL REPORTING CHANNEL 22

6.3. PUBLIC DISCLOSURE 23

7. MONITORING OF THE PROCESS AND UPDATING OF THE PROCEDURE 23

8. ARCHIVING 23

9. TRAINING 24

10. ANNEX 24

1. DEFINITIONS

- **"reports"**: any written, oral or verbal communication, including anonymous reports, containing information on breaches;
- "**breaches**": any administrative, accounting, civil or criminal offence; any conduct constituting a violation under Legislative Decree No. 231/2001 or of the related organisational, management and control models; any infringement falling within the scope of European Union law, including public procurement, financial services, products and markets, anti-money laundering and counter-terrorist financing, product safety and compliance, transport safety, radiation and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, the protection of privacy and personal data, and the security of network and information systems; as well as any act or omission affecting the financial interests of the European Union pursuant to Article 325 of the Treaty on the Functioning of the European Union (TFEU), or undermining the proper functioning of the internal market, including breaches of EU rules concerning the free movement of goods, persons, services and capital;
- **"information on breaches"**: any information, including well-founded suspicions, concerning actual, attempted or potential breaches that have been committed, are being committed, or are reasonably likely to be committed within the organisation with which the whistleblower, or the person submitting a report to a judicial or supervisory authority, has or has had a legal or professional relationship. This also includes information relating to conduct intended to conceal such breaches;
- **"internal reporting"**: the submission of a reports through the designated internal reporting channels established by the Company in accordance with applicable whistleblowing regulations;
- **"external reporting"** any written or oral communication of information concerning actual or suspected breaches, submitted through the external reporting channel established by the competent authority in accordance with applicable whistleblowing legislation[1] ;

[1] see Article 7 of Legislative Decree 24/23

- **"public disclosure**": the act of making information on breaches available to the public through the press, electronic media, online platforms, or any other means of communication capable of reaching a wide audience;
- **"whistleblower":** a natural person who reports, through the designated reporting channels, or publicly discloses information concerning actual, attempted, or suspected breaches that came to their attention in a work-related context;
- **"facilitator":** a natural person who, in a work-related context, assists a whistleblower in making a report and is entitled to the same confidentiality protections afforded under applicable whistleblowing laws and regulations;
- **"employment context":** any current, past or prospective employment, professional, contractual or business relationship through which a person obtains information on breaches and in which they may be subject to retaliation for reporting such breaches, making a public disclosure, or submitting a complaint to the competent judicial or supervisory authorities;
- **"person involved":** a natural or legal person named in a report as being allegedly responsible for, involved in, or otherwise connected with the reported breach, and whose rights and interests must be safeguarded throughout the reporting process in accordance with applicable laws and regulations;
- **"IT channel manager":** the external party designated by the Company to manage and support the technical infrastructure of the reporting channel, ensuring its proper functioning, security, confidentiality and compliance with applicable legal and regulatory requirements;
- **"channel manager**": the internal function or individual appointed by the Company to receive, manage and follow up on reports submitted through the reporting channel, operating with the independence, impartiality, organisational autonomy and authority necessary to perform such duties effectively;
- **"retaliation":** any act or omission, including attempted or threatened actions, carried out in response to a report, public disclosure, or complaint submitted to a judicial or audit authority, and which results in, or may result in, direct or indirect unjustified harm, disadvantage, or adverse treatment to the reporting person or any individual entitled to protection under applicable whistleblowing legislation;

- **"follow-up":** any activity carried out by the Channel Manager following the receipt of a report in order to assess its admissibility and merits, maintain contact with the reporting person where necessary, investigate the reported facts, and identify or implement any appropriate corrective, remedial or disciplinary measures;
- **"feedback":** a communication addressed to the whistleblower providing information on the receipt, assessment and handling of the report, including any investigative, corrective, remedial or disciplinary measures taken or envisaged, as well as the rationale underlying the decisions adopted;
- **"platform":** the internal reporting platform established by the Company, as further specified in Section 8, to enable the confidential and secure submission, receipt, processing and follow-up of reports relating to actual or suspected breaches in compliance with applicable whistleblowing legislation;
- **"Supervisory Body ("SB")":** the corporate body established pursuant to Legislative Decree No. 231/2001 and appointed by Company. to oversee the effectiveness, implementation, observance and updating of the Organisation, Management and Control Model adopted by Company;
- **"Model 231":** the Organisation, Management and Control Model adopted by Company pursuant to Legislative Decree No. 231/2001, designed to prevent the commission of offences giving rise to the administrative liability of legal entities and to promote a culture of compliance and ethical business conduct.

2. INTRODUCTION

2.1 Objectives of this document

This Procedure has been adopted by Italfarmaco S.p.A. (the "Company") in compliance with Legislative Decree No. 24 of 10 March 2023 (the "Decree" or "Legislative Decree 24/2023"), which transposes 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 (the "Whistleblowing Directive"). The Decree provides a framework for the protection of individuals who, in a work-related context, report, publicly disclose, or otherwise communicate information concerning actual or suspected breaches of national or European Union law that may prejudice the public interest or the integrity of public or private organisations.

The term *'whistleblower'* refers to a person, employed by an organisation or public administration, who reports to the authorised bodies violations or irregularities committed to the detriment of the public interest and the administration to which they belong.

The Company is committed to conducting its business with integrity, transparency and accountability. All employees are therefore expected to uphold these principles and contribute to maintaining the highest standards of ethical and compliant conduct. Any act or omission that may constitute a breach of applicable national or European Union law, as further described in Section 4 of this Procedure, should be reported through the designated reporting channels. To this end, the Company has established and made available to employees and eligible third parties a dedicated and easily accessible internal reporting channel (the "Whistleblowing Platform") for the submission and management of reports concerning actual or suspected breaches.

This Procedure is approved by the Board of Directors of each Company, which is also responsible for defining the organisational governance framework for whistleblowing management, including the identification of the functions involved and the allocation of the related roles, responsibilities and authorities.

In addition to the provisions set out in this Procedure, reference should be made to Legislative Decree No. 24/2023 and to the Company's whistleblowing reporting channel, accessible through the dedicated section of the corporate website at https://www.italfarmaco.it

Employees shall have continuous access to this Procedure through the Company intranet, where it is published in the section dedicated to corporate policies and procedures.

This Procedure forms part of the Company's broader compliance and ethics framework, supporting the prevention, identification and reporting of misconduct, while ensuring adherence to applicable legal requirements and the principles embodied in the Company's Code of Ethics and Model 231.

3. REFERENCES and related procedures

- Legislative Decree No. 24 of 10 March 2023;
- Directive (EU) 2019/1937;
- Organisation, Management and Control Model pursuant to Legislative Decree 231/01;

- European Regulation 2016/679 (GDPR);
- Privacy Code (Legislative Decree No. 196/2003, as amended and supplemented);
- ANAC guidelines on the protection of persons reporting breaches of Union law and the protection of persons reporting breaches of national regulatory provisions – procedures for the submission and handling of external reports.

4. ROLES AND RESPONSIBILITIES

The channel manager, including through the use of the platform:

- provides, including through this procedure and the information published on the platform, clear information on the channel, the procedures and the conditions for making internal reports;
- provides the whistleblower with an acknowledgement of receipt of the report within the prescribed time limits;
- assesses the criteria for determining whether the report is admissible;
- shares the report with the internal contacts, as defined in this procedure, and the Supervisory Body (where applicable), and informs them of the initiation of any investigations, their outcome and the response to the whistleblower;
- provides the whistleblower with confirmation that the process of handling the report has been completed;
- maintains contact with the person making the report and, where appropriate, handles requests for further information and arranges any follow-up interviews with the person making the report, if requested;
- files and retains documentation relating to the report in accordance with the timeframes laid down by law;
- coordinates and monitors the investigation phase with the relevant internal departments or external teams;

- shares the report with the internal contacts, as defined in this procedure, and the Supervisory Board (where applicable), the initiation of any investigations, their outcome and the feedback to the whistleblower;
- identifies improvement plans to prevent the recurrence of the events reported;
- manages the activities arising from any public disclosure in the cases provided for;
- ensures compliance with the principle of confidentiality.

The whistleblower:

- submits reports in accordance with this procedure;
- is required to provide detailed information regarding the subject of the report.

IT channel manager:

- ensures the technical operation of the channel.

The Supervisory Body:

- in the case of reports deemed significant under Legislative Decree 231/01, coordinates and monitors the investigation phase with the relevant internal departments or external teams, assesses the outcome of the investigations and any resulting measures;
- ensures compliance with the principle of confidentiality.

The legal representative:

- liaises with ANAC in the event of any external report or the initiation of inspections by ANAC.

The Board of Directors:

- ensures that any necessary measures are adopted in accordance with the provisions of the sanctions system set out in the 231 Organisational Model;
- approves this procedure together with the structure of the related organisational roles;
- ensures compliance with measures for the protection of the whistleblower.

5. GENERAL PRINCIPLES

5.1 PERSONS ENTITLED TO MAKE A REPORT INFORMATION ON BREACHES (THE 'WHISTLEBLOWER')

This procedure shall apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context including, at least, the following:

- employees (in the public and private sectors);
- self-employed persons and contractors carrying out their work for public and private organisations;
- freelancers;
- volunteers;
- consultants;
- shareholders;
- directors;
- those providing services to third parties in any capacity (regardless of the nature of such activities), even where no remuneration is received;
- trainees, including unpaid ones;
- persons exercising administrative, managerial, control, supervisory or representative functions, even if the relevant activities are carried out de facto rather than de jure.

This category also includes all those persons who, in any capacity, become aware of unlawful acts within the Company's working environment, namely:

- when the employment relationship has not yet commenced;
- during the probationary period;
- upon termination of the employment relationship.

5.2 INTERNAL REPORTING CHANNEL

This procedure applies to any report of information regarding breaches (as further specified in paragraph 4) discovered within the employment context[2], where such breaches are detrimental to the public interest or the integrity of the public administration or the private organisation, and which is made via the dedicated reporting channels provided by the Company.

The following are excluded from the scope of this procedure:

- complaints, claims or requests relating to a personal interest that pertain exclusively to individual employment relationships, or to employment relationships with superiors;
- breaches relating to national security, as well as contracts concerning defence or national security matters;
- breaches that are mandatorily governed by European Union or national legislation[3], which already provide for specific reporting procedures.

The Company has set up an internal reporting channel (Whistleblowing platform) which the whistleblower must use to submit information on breaches. The use of this channel enables more effective prevention and investigation of breaches. This approach is in line with the principle of fostering a culture of good communication and corporate social responsibility, as well as improving the organisation itself.

The internal reporting channel allows for written or verbal submissions via the platform accessible via the link provided on the relevant page of the company website: https://www.italfarmaco.it

Upon accessing the platform, the whistleblower may also, via a voice-recording messaging system, request a face-to-face meeting with the person responsible for handling the report.

The internal reporting channel guarantees the confidentiality of the identity of the whistleblower, the facilitator (where applicable), the persons involved or otherwise mentioned in the report, as well as

[2] This refers to an employment relationship with the organisation or the provision of professional or work-related services, whether current or past.

[3] Please refer to the annexes to Directive 2019/1937 and Legislative Decree 24/23.

the content of the report itself and the related documentation submitted, which may also be supplemented at a later date.

5.2.1 Person responsible for the channel (the so-called 'channel manager')

Management of the internal reporting channel is entrusted to a collegial body comprising:

- a member of the Company's legal affairs function/department
- the Company's Data Protection Officer
- a compliance adviser or a member of the Company's compliance function/department

These individuals meet the requirements of autonomy and independence and are specifically trained and formally appointed.

The person responsible for managing the channel and handling reports acts exclusively in relation to the activities set out in Article 5 of this procedure.

5.2.2 Features of the internal reporting channel . IT administrator for the channel (IT Channel Manager)

The Company's internal reporting channel is hosted on the "@Whistleblowing" platform; it is web-based and accessible from all devices (PCs, tablets, smartphones).

IT management of the channel is entrusted to:

- BDO Advisory Services Srl.

Data entered into the platform is segregated within the logical partition dedicated to the Company and processed using a scripting algorithm prior to storage. Security during transmission is ensured by secure communication protocols.

Upon completion of the report (regardless of whether it is anonymous or not), the platform provides a 12-character alphanumeric code, generated randomly and automatically by the IT platform and which cannot be reproduced, with which the whistleblower may at any time view the processing status of their report and interact with the channel manager via a messaging tool.

In the case of a non-anonymous report, the reporter's details ('user data') are not accessible to the channel manager. The channel manager may, at their discretion, view these fields (so-called 'plain text fields') only following a duly documented justification within the platform.

The report can only be viewed and managed by authorised individuals. The channel manager has unique login credentials, which expire every 3 months. The password policy complies with international best practices.

Data retention is governed by predefined expiry dates, with automatic reminders sent to the channel manager, who will proceed to delete the data upon expiry.

BDO, the owner of the platform, is ISO 27001 certified.

The processing of personal data must always take into account and comply with the obligations set out in the GDPR and Legislative Decree 196/2003, as amended and supplemented. The Company, in its capacity as data controller via the internal reporting channel, is required to carry out a prior analysis of the organisational structure, including a fundamental assessment of the potential impact on data protection (Article 35 of the GDPR), and has appointed BDO Advisory Services srl as data processor pursuant to Article 28 of the GDPR.

5.2.3 Characteristics of reports and anonymous reports

The report must be as detailed as possible in order to enable the facts to be analysed by the persons authorised to receive and handle reports. In particular, the following must be clear:

- the time and place at which the incident reported took place;
- a description of the incident;
- the personal details or other information enabling the identification of the person to whom the reported facts relate.

Information regarding reported breaches must be truthful. Mere assumptions, unreliable rumours (so-called 'office gossip'), as well as information in the public domain, incorrect information (except where due to genuine error), information that is manifestly unfounded or misleading, or information

that is merely harmful or offensive, shall not be considered as such. However, it is not necessary for the whistleblower to be certain that the reported events actually took place or to know the identity of the person responsible for them.

It is also helpful for the whistleblower to provide documents that may substantiate the facts reported, as well as the names of other individuals who may be aware of the facts.

Anonymous reports, where detailed, are treated in the same way as ordinary reports and, in such cases, are considered within the scope of this procedure, including with regard to the protection of the whistleblower, should they subsequently be identified, and to data retention obligations.

5.2.4 Retention of documentation relating to internal reports

Internal reports and all related documentation, whether attached or incorporated, are retained, with a specific digital chain of custody, for the time necessary to process the report.

In any event, the documentation is retained only for a period not exceeding 5 years from the date of notification of the final outcome of the reporting procedure.

In all the cases mentioned, the procedure for retaining internal reports and the related documentation must comply with EU and national safeguards on the processing of personal data, as well as with the measures in place regarding the right to privacy.

5.2.5 Information obligations

Information on the reporting channel, procedures and the conditions for making reports is displayed in the employment context (company noticeboards) and on the dedicated company intranet page via the publication of this procedure, and is made available to persons who, whilst not physically present in the employment context, have a legal relationship with the Company through publication on the dedicated web page of the institutional website https://www.italfarmaco.it

The Company shall activate its internal reporting channel after consulting with employee representatives or trade unions.

5.2.6 Confidentiality obligation

All reports and related attachments shall not be used for any longer than is necessary to follow them up.

It is stipulated that the identity of the whistleblower, together with any other information from which that identity may be inferred, directly or indirectly, shall not be disclosed without the whistleblower's express consent to persons other than those authorised to receive or follow up on reports, who are expressly authorised to process such data in accordance with Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article *2-quaterdecies* of the Code on the Protection of Personal Data referred to in Legislative Decree No. 196 of 30 June 2003, as amended and supplemented.

The Company protects the identity of the persons involved, the facilitators and the persons mentioned in the report until the conclusion of the proceedings initiated as a result of the report itself, in accordance with the same safeguards provided for the reporting person.

Circumstances in which the protection of the right to confidentiality may be limited include:

- in the context of criminal proceedings, the identity of the whistleblower is protected by confidentiality in the manner and within the limits set out in Article 329 of the Code of Criminal Procedure: there is an obligation to maintain the confidentiality of the documents relating to the preliminary investigation until such time as the suspect is entitled to be informed of them and, in any event, no later than the conclusion of that phase;
- in proceedings before the Court of Auditors, the identity of the whistleblower may not be disclosed until the conclusion of the preliminary investigation phase;
- in disciplinary proceedings, the identity of the whistleblower may not be disclosed where the disciplinary charge is based on findings that are distinct from and additional to the report, even if they arise from it;
- where the allegation is based, in whole or in part, on the report and knowledge of the whistleblower's identity is essential for the defence of the accused, the report may be used for the purposes of the disciplinary proceedings only with the whistleblower's express consent to disclose their identity;
- in cases where disciplinary proceedings are initiated against the alleged perpetrator of the reported conduct, the whistleblower shall be notified in writing of the reasons for the disclosure of confidential information where such disclosure is also essential for the defence of the person concerned.

Subject to the mitigating measures listed above, the person concerned may, at their request, be heard through written proceedings by means of the submission of written observations and documents.

Confidentiality obligations include:

- the exclusion of the report and the documentation attached to it from the right of access to administrative documents provided for in Articles 22 et seq. of Law No. 241/1990 and from the general right of public access referred to in Articles 5 et seq. of Legislative Decree No. 33/2013;
- the administrations and bodies involved in the handling of reports shall ensure confidentiality throughout all stages of the reporting procedure, including any transfer of reports to other competent authorities.

5.2.7 Protection of personal data

All processing of personal data, including communication between the competent authorities, is carried out in accordance with:

- Regulation (EU) 2016/679;
- Legislative Decree No. 196 of 30 June 2003, as amended and supplemented.

The communication of personal data by institutions, bodies or agencies of the European Union is carried out in accordance with Regulation (EU) 2018/1725.

The processing of personal data relating to the receipt and handling of reports is carried out by the data controller, in accordance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679, by first providing the necessary information to the whistleblowers and the persons involved, and by taking appropriate measures to safeguard the rights and freedoms of the data subjects.

The information notice for data subjects, which also summarises their rights and how to exercise them, can be found in the dedicated section of the Whistleblowing platform.

5.2.8 PROTECTION AND SUPPORT MEASURES

Appropriate measures are in place to protect whistleblowers from direct and indirect retaliation.

These protective measures apply if, at the time of making the report, the whistleblower had reasonable grounds to believe that the information regarding the reported breaches was true (see paragraph 7.3), fell within the scope of the report and the reporting procedure had been followed.

In the event of defamation or slander, established by a conviction even at first instance, such protection is not guaranteed.

Protective measures also apply:

a) to facilitators;

b) to persons in the same employment context as the whistleblower who are linked to them by a stable emotional bond or by kinship up to the fourth degree;

c) to the whistleblower's work colleagues who work in the same workplace as the whistleblower and who have a regular and ongoing relationship with that person;

d) to organisations owned by the person making the report or for which they work, as well as to organisations operating within the same workplace as the aforementioned persons.

5.2.9 Prohibition of retaliation

The persons listed in paragraph 5.1 must not be subjected to any form of retaliation. By way of example, and without limitation, the following are considered 'retaliation': dismissal, suspension or equivalent measures; demotion or failure to promote; or a change of duties.

Any actions taken in breach of the prohibition on retaliation are null and void.

In the context of judicial or administrative proceedings, or in the event of out-of-court disputes concerning the investigation of prohibited conduct, acts or omissions directed solely at whistleblowers, it is presumed that such conduct, acts or omissions were carried out as a result of the report. The burden of proving that such conduct or acts is motivated by reasons unrelated to the report lies with the person who carried out the retaliatory acts.

Whistleblowers may report to ANAC any retaliation they believe they have suffered, including attempted or threatened retaliation.

ANAC informs the National Labour Inspectorate so that it may take the measures falling within its remit.

5.2.10 Support measures

Whistleblowers may contact third-sector organisations listed on the ANAC website. These are organisations that carry out activities in the public interest for the non-profit pursuit of civic, solidarity-based and socially beneficial aims (*"promotion of a culture of legality, peace among peoples, non-violence and unarmed defence; promotion and protection of human, civil, social and political rights, as well as the rights of consumers and users of services of general interest; promotion of equal opportunities and mutual aid initiatives, including time banks and solidarity purchasing* groups") and which have entered into agreements with ANAC.

The support measures provided consist of free information, assistance and advice on how to make a report and on the protection against retaliation offered by national and European Union legislation, on the rights of the person involved, as well as on the terms and conditions for accessing legal aid.

5.2.11 Limitation of liability for the whistleblower

No liability (including civil or administrative liability) shall be incurred by anyone who discloses or disseminates information on breaches:

- covered by a duty of confidentiality,
- relating to copyright protection,
- provisions relating to the protection of personal data,
- which damage the reputation of the person involved or reported,

if, at the time of disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of such information was necessary to expose the breach and the report was made in accordance with the conditions for protection.

Furthermore, the following protection measures are highlighted:

- the right to make a report and the associated safeguards may not be restricted by contractual agreement;
- the exclusion of any other liability, including civil and administrative liability, for the acquisition of or access to information on breaches, except where the conduct constitutes a criminal offence;
- the exclusion of any other liability in respect of conduct, acts or omissions carried out where they are linked to the report and strictly necessary to disclose the breach or, in any event, not linked to the report.

5.2.12 Penalty regime

The disciplinary system adopted by the Company pursuant to Article 6(2)(e) of Legislative Decree 231/2001, and referred to in the General Section of the 231 Model, provides for sanctions to be imposed on those whom the Company determines to be responsible for offences relating to:

- the commission of, or proposal to carry out, acts of retaliation; the obstruction of reporting (including attempted obstruction); or the breach of confidentiality obligations;
- failure to establish reporting channels, failure to adopt procedures for managing such reports, or procedures that do not comply with the requirements of the decree, or failure to verify and analyse reports,
- civil liability of the reporting person, including where a judgment has been handed down at first instance, for defamation or slander in cases of wilful misconduct or gross negligence, unless that person has already been convicted, including at first instance, of the offences of defamation or slander;

as well as against anyone who breaches this procedure.

For the same offences, ANAC may impose administrative fines (ranging from €500 to €50,000) should such offences be established.

6. DESCRIPTION OF THE PROCESS

6.1 OPERATIONAL PROCEDURE FOR HANDLING REPORTS THROUGH THE INTERNAL CHANNEL

The whistleblower submits the report via the dedicated internal channel.

The whistleblower submits the report via the link provided above, either in writing by completing a guided form, or verbally via the voice messaging system on the platform.

If the whistleblower makes the report verbally during a scheduled meeting with designated staff, the report is, subject to the whistleblower's consent, documented by the channel manager by recording it on a device suitable for voice storage and playback or by drawing up a minutes of the meeting. In the latter case, the whistleblower may verify, correct and/or confirm the minutes of the meeting by signing them.

Receipt of the report by the person responsible for the channel initiates the report handling process.

The person responsible for the channel proceeds to 'process' it in accordance with a predefined process flowchart.

Upon receipt of the report, the person responsible shall send an acknowledgement of receipt to the reporter within 7 days of receiving the report and taking charge of it.

The person responsible for the channel carries out an initial check on the correctness of the procedure followed by the reporter and the content of the report, both in relation to the scope of application defined by this procedure (i.e. the relevance of the report's content) and its verifiability based on the information provided. At this stage, should the person responsible for the channel deem it necessary (e.g. in the event of any doubts), they will involve the Supervisory Body to assess the relevance of the report under Legislative Decree 231/01. If the report does not relate to the subject matter of this procedure, the channel manager shall formalise the outcome of the review and notify the whistleblower within a reasonable timeframe (no later than 3 months) and close the report.

Should it be necessary to obtain further information, the channel manager will contact the whistleblower via the platform. If the whistleblower fails to provide additional information within 3 months of the request for further details, the channel manager will proceed to close the report, notifying the whistleblower and informing the Supervisory Body if it was involved in the assessment of the report.

If no further information is required, the channel manager will assess, on a case-by-case basis, together with the Company, whether and which corporate function should be appropriately involved in the relevant analysis and any subsequent measures – always in accordance with the principle of confidentiality – as well as the procedure for initiating the investigation phase.

In the case of information concerning material breaches under Legislative Decree 231/01 , the channel manager, having verified the relevance of the report and gathered all the necessary information, shall inform the Supervisory Body, whilst respecting the principle of confidentiality, in order to assess how to initiate the investigation phase, subject to the principle of the Supervisory Body's autonomy and independence with regard to how the report is handled for the purposes and effects of Legislative Decree 231/01.

Upon completion of the investigation, the channel manager shall prepare a final report in order to provide feedback to the whistleblower. Feedback to the whistleblower must be provided within 3 months of the date of the acknowledgement of receipt or by the expiry of the 7-day period following the submission of the report. Only in exceptional cases, where the complexity of the report so requires, or in view of the time taken by the whistleblower to respond, may the channel manager – having promptly informed the whistleblower before the deadline and providing appropriate justification – continue the investigation for as long as necessary, whilst providing the whistleblower with regular updates.

In the event of significant breaches as defined by Legislative Decree 231/01, the channel manager shall report the findings of the investigation to the Supervisory Body. The Supervisory Body, within the scope of its operational autonomy, shall assess the findings received and, should the report be substantiated, shall consider any consequent measures and adopt such measures as may be deemed necessary to amend the Organisational Model, whilst initiating the necessary

communications for the application of any sanctions. Any consequent measures shall be applied in accordance with the provisions of the sanctions system set out in the 231 Organisational Model.
In the event of defamation or slander, established by a conviction even at first instance, the Company shall initiate disciplinary proceedings against the whistleblower.
It should be noted that, from the receipt of the report until its closure, any person found to be in a conflict of interest must refrain from making decisions in order to ensure compliance with the principle of impartiality.

6.2. EXTERNAL REPORTING CHANNEL

Where the following conditions apply, the whistleblower may submit a report to ANAC via an external channel:

- where, in the relevant employment context, the use of the internal reporting channel is not mandatory, or the channel itself has not been established, or does not comply with the statutory requirements;
- where the whistleblower has already submitted an internal report but no action has been taken on it;
- if the whistleblower has reasonable grounds to believe that, by submitting an internal report, it will not be effectively followed up or that it will, in itself, result in retaliation against them;
- where the whistleblower has reasonable grounds to believe that the reported breach may constitute an imminent or obvious danger to the public interest.

The external body authorised to receive external reports is ANAC, in accordance with the methods and procedures duly adopted by the latter.

6.3. PUBLIC DISCLOSURE

As a last resort and subject to the above, the whistleblower may proceed with public disclosure in the following cases:

- where they have already made an internal or external report, or have made an external report directly without receiving a response within the prescribed time limit;
- where the whistleblower has reasonable grounds to believe that the breach constitutes an imminent or obvious threat to the public interest;
- where the whistleblower has reasonable grounds to believe that the external report entails a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case in question, such as where evidence may be concealed or destroyed, or where there is a well-founded fear that the recipient of the report may be colluding with the perpetrator of the breach or involved in the breach itself.

7. MONITORING OF THE PROCESS AND UPDATING OF THE PROCEDURE

It is the responsibility of COM to ensure that the procedure is updated in a timely manner should any organisational and/or process changes occur.

This document remains valid for three years from the date of publication. COM and/or the departments involved in the process are required to review it as the expiry date approaches; should it be deemed valid at the end of the three-year period, the Compliance Officer shall simply confirm its content by issuing a new version and submitting it for approval.

8. ARCHIVING

The procedure is archived electronically in the company's document management system.

9. TRAINING

Regarding the training, the person responsible for the procedure is available to provide guidance and support in addressing any questions related to its application or interpretation, as well as to provide any additional information that may be required.

10. ANNEX

Legislative Decree No. 24 of 10 March 2023