15/07/2023

Title: WHISTLEBLOWING PROCEDURE

INDEX

1. PURPOSE

This procedure is adopted by Italfarmaco S.p.A., Chemi S.p.A. and Effik Italia S.p.A. (hereinafter the "Company") in compliance with the provisions of Legislative Decree No. 24 of 10 March 2023 (hereinafter the "Decree" or "D. Lgs. 24/2023") in force as of 30 March 2023, which implements Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, concerning the protection of persons who report breaches of national or European Union laws (c.d. *whistleblowing* directive) of which they become aware in the context of their work, detrimental to the public interest or the integrity of the public administration or private entity.

The term *whistleblower* refers to a person, an employee of an entity or administration, who reports breaches or irregularities committed to the detriment of the public interest and the entity to which he or she belongs to the bodies empowered to intervene.

All employees of the Company have an obligation to promote and guarantee the integrity of the actions performed by the Company. Therefore, in the event that an action or omission committed by an employee of the Company in the performance of his or her work duties may constitute a breach of national or European Union laws (as better specified in paragraph 4), it must be reported. To this end, the Company has activated and makes available to employees and third parties an easily accessible channel (Whistleblowing platform) for submitting and communicating the report of a breach.

This procedure is also subject to approval by the Board of Directors of each Company, together with the identification of the organisational roles involved in the process of handling whistleblowing reports and the related responsibilities.

In addition to what is regulated in this procedure, please refer to the Decree in attachment and to the channel activated by the Company and available on the appropriate web page of the institutional website respectively:

Italfarmaco S.p.a.: https://www.italfarmaco.it/it-it/Organizzazione

Effik Italia S.p.a. https://www.effik.it/Chi-siamo/Organizzazione

Chemi S.p.a. https://www.chemi.com

Employees will also have access to this procedure via the company intranet on the procedures page.

This procedure is part of the measures implemented by the Company to ensure compliance with regulatory provisions and guarantee compliance with the criteria set out in the Company's Code of Ethics.

2. SCOPE

This procedure applies to any report of information on breaches (as better specified in paragraph 4) acquired within the working context[1] , if detrimental to the public interest or the integrity of the public administration or the private entity, made through the appropriate reporting channels made available by the Company.

- Disputes, claims or demands of a personal nature that relate exclusively to individual employment relationships, i.e. employment relationships with hierarchically superior persons;
- national security breaches, as well as procurement relating to defence or national security aspects;
- violations mandatorily regulated by European Union or national acts[2] that already ensure appropriate reporting procedures.

are excluded from the scope of this procedure.

3. REFERENCES

- 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 196/2003 and ss.mm.ii.);
- Italian Anticorruption Authority guidelines on the protection of persons who report breaches of Union law and the protection of persons who report breaches of national laws - procedures for the submission and handling of external reports.

4. DEFINITIONS

- "**Reports**" means any written, oral or displayed communication in an interview, even in anonymous form, containing information on breaches;

- **"breaches"**: mean administrative, accounting, civil or criminal offences; conduct that is relevant under Leg. 231/2001, or breach of organisation and management models; offences falling within certain areas of EU law (public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection of privacy and protection of personal data and security of networks and information systems); acts or omissions detrimental to the financial interests of the European Union and the free movement of goods,

[1] To be understood as a subordinate employment relationship with the organisation or a professional/employment relationship, present or past.

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

persons, services and capital; acts or omissions detrimental to the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union specified in the relevant secondary legislation of the European Union;

- **"Information on breaches"**: means all information, including reasonable suspicions, concerning breaches committed or likely to be committed in the organisation with which the reporting person or the person making the complaint to the judicial/accounting authority has a legal relationship and also information concerning conduct aimed at concealing such breaches;
- **"internal reporting"**: mean communication of "reports" through the established internal reporting channel;
- **"External reporting"** means the written or oral communication of information on breaches, submitted through the external reporting channel[3] ;
- **"public disclosure"** means making information about infringements publicly available through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people;
- **"Reporter (or whistleblower)":** means an individual who makes a report or public disclosure of information about breaches acquired in the context of his or her work;
- **"Facilitator":** means a natural person who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential;
- **"employment context"** means present or past work or professional activities through which, regardless of the nature of such activities, a person acquires information about breaches and in the context of which he or she could risk retaliation in the event of a public report or disclosure to the judicial or accounting authorities;
- **"Person involved"** means the natural or legal person mentioned in the report as the person to whom the breach is attributed or as a person otherwise implicated in the reported breach;
- **"IT channel manager":** means an external party identified by the Company responsible for the technical operation of the channel;
- **"channel manager**": means an internal person identified by the Company responsible for channel management and reporting with organisational and functional autonomy;
- **"Retaliation":** means any conduct, act or omission, even if only attempted or threatened, occurring as a result of the whistleblowing and closely related to the whistleblowing, the report to the judicial or accounting authorities or the public disclosure and which causes or may cause the whistleblower or the person who made the report, directly or indirectly, unjust damage;

[3] see Art. 7 of Legislative Decree 24/23

- **"Follow-up"** means the action(s) initiated by the entity entrusted with the management of the reporting channel;
- **"Acknowledgement":** means the communication to the person making the alert of information on the action taken or intended to be taken on the alert, including the measures envisaged or to be taken and the reasons for the choice made;
- **"platform":** means an internal reporting channel adopted by the Company (as further specified in paragraph 8) to transmit information on breaches;
- **"Supervisory Board ("SB")":** means Supervisory Board pursuant to Legislative Decree 231/2001 of Italfarmaco S.p.a., Effik Italia S.p.a. and Chemi S.p.a.;
- **"Model 231":** means Organisation, management and control model pursuant to Legislative Decree 231/2001 of Italfarmaco S.p.a., Effik Italia S.p.a. and Chemi S.p.a..

5. RESPONSIBILITIES

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

- makes available, also through this procedure and the information published on the platform, clear information on the channel, procedures and prerequisites for internal reporting;
- provides the reporting person with an acknowledgement of receipt of the report within the deadline;
- assesses the criteria for processability of the report;
- share the report with the internal interlocutors, as defined in this procedure, and the Supervisory Board (in the cases provided for), the initiation of any investigations, their outcome and the feedback to the reporter;
- sends feedback to the reporter on the closure of the handling of the report;
- maintains interlocutions with the reporting person and, where appropriate, manages the request for supplementary information and the performance of in-depth interviews with the reporting person, if requested;
- archives and stores the reporting documentation within the regulatory timeframe;
- coordinates and monitors the investigation phase with the internal functions/external teams in charge;
- share the report with the internal interlocutors, as defined in this procedure, and the Supervisory Board (in the cases provided for), the initiation of any investigations, their outcome and the feedback to the reporter;
- identifies improvement plans to avoid the recurrence of reportable events;
- manages the activities resulting from any public disclosures in the cases provided for;

- ensures respect for the principle of confidentiality.

The reporter:

- transmits reports in accordance with this procedure;
- is obliged to provide circumstantial information on the matter reported.

IT manager of the channel:

- guarantees the technical functioning of the channel.

The SB:

- in the case of relevant reports pursuant to Legislative Decree no. 231/01, coordinates and monitors the investigation phase with the internal functions/external teams in charge, assesses the outcome of the investigations and any consequent measures;
- ensures respect for the principle of confidentiality.

The legal representative:

- liaises with Italian Anticorruption Authority ("ANAC") in the event of any external reporting or activation of inspection activities by ANAC.

The Board of Directors:

- ensures that any measures are taken in accordance with the provisions of the sanctions system set out in the 231 Organisational Model;
- approves this procedure together with the associated organisational role structure;
- ensures compliance with the measures for the protection of the reporting person.

6. PERSONS WHO MAY REPORT INFORMATION ON BREACHES (SO-CALLED 'REPORTER')

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 (public and private);
- self-employed workers and collaborators working for public and private entities;
- freelancers;
- volunteers;
- consultants;
- shareholders;

- administrators;
- Providers of services for third parties in any capacity whatsoever (irrespective of the nature of such activities) even without consideration;
- even unpaid trainees;
- persons exercising functions of administration, management, control, supervision or representation, even if the relevant activities are performed in a de facto and not in a de jure capacity.

Also included in this category are all those persons who, for whatever reason, become aware of offences in the context of the Company's working environment, i.e:

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

7 . INTERNAL REPORTING CHANNEL

Company activated an internal reporting channel (Whistleblowing platform) to be used by the reporter to transmit information on breaches. The use of this channel enables more effective prevention and detection of breaches. This choice responds to the principle of fostering a culture of good communication and corporate social responsibility as well as improving its organisation.

The internal reporting channel provides for written or oral reporting through the platform accessible via the link available on the relevant page of the company website respectively:

Italfarmaco S.p.a.: https://www.italfarmaco.com/it-it/Organizzazione

Effik Italia S.p.a. https://www.effik.it/Chi-siamo/Organizzazione

Chemi S.p.a. https://www.chemi.com

By accessing the platform, the reporter, via a voice-recorded messaging system, can also request a direct meeting with the person responsible for handling the report.

The internal reporting channel guarantees the confidentiality of the identity of the whistleblower, the facilitator (if any), the persons involved and in any case mentioned in the report as well as the content of the report and of the documentation submitted, which can also be supplemented at a later stage.

7.1 Person in charge of the channel (so-called 'channel manager')

The management of the internal channel is entrusted to a collegiate body consisting of:

- Legal Affairs Director of Italfarmaco S.p.a. (Giulia Ferrarotti)
- DPO (Gaia Ravignani de' Piacentini)
- compliance consultant (Cristina Grossi)

whose members meet the requirements of autonomy, independence and are specifically trained.

The person in charge of channel management and reporting acts exclusively with regard to the activities indicated in Article 5 of this procedure.

7.2 Characteristics of the internal reporting channel. IT manager of the channel

The Company's internal reporting channel is supported by the '@Whistleblowing' platform, is web-based and accessible from all devices (PC, Tablet, Smartphone).

IT management of the channel is entrusted to:

- BDO Advisory Services Srl.

Data entered into the platform are segregated in the logical partition dedicated to the company and subjected to a scripting algorithm before being stored. Security in transport is guaranteed by secure communication protocols.

At the end of the entry of the report (regardless of whether it is anonymous or not), the platform provides a 12-character alphanumeric code, randomly and automatically generated by the IT platform, which cannot be reproduced and with which the reporter can at any time view the processing status of his/her report and interact with the person responsible through a messaging tool.

In the case of non-anonymous reporting, the data of the reporter ('user data') are not accessible to the channel manager. The channel manager, at his or her discretion, will only be able to view these fields ('plain text fields') following justification, appropriately traced, within the platform.

The report can only be viewed and managed by authorised persons. The person responsible has unique credentials for access, expiring every 3 months. The password policy adheres to international best practices.

Data Retention is governed by predefined deadlines with automatic reminders to the channel manager who will, on expiry, delete the data.

The company BDO, which owns the platform, is ISO27001 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 et seq. Company, as data controller, through the internal reporting channel is required to carry out a prior analysis of the organisational design including the fundamental assessment of the possible impact on data protection (Art. 35 of the GDPR) and appointed BDO Advisory Services srl as data processor pursuant to Art. 28 of the GDPR.

7.3 Report characteristics and anonymous reports

It is necessary that the report be as detailed as possible in order to allow the analysis of the facts by the persons competent to receive and handle reports. In particular, it must be clear:

- the circumstances of time and place in which the reported event occurred;
- description of the fact;
- personal details or other elements enabling identification of the person to whom the reported facts can be attributed.

Information on reported breaches must be truthful. Mere suppositions, unreliable indiscretions (so-called rumours), as well as news in the public domain, incorrect information (with the exception of genuine error), manifestly unfounded or misleading, or if merely damaging or offensive, shall not be considered. On the other hand, it is not necessary for the reporter to be certain of the actual occurrence of the reported facts and the identity of the author thereof.

It is also useful for the whistleblower to provide documents that may provide evidence of the facts being reported, as well as an indication of other persons potentially aware of the facts.

Anonymous reports, where substantiated, are equated with ordinary reports and in that case considered within the scope of this procedure also with regard to the protection of the reporter, if subsequently identified, and to record-keeping obligations.

7.4 Operational procedure for handling the report via the internal channel

The reporter transmits the alert via the dedicated internal channel.

The reporter activates the report through the above link in written mode, by filling in a guided form, or in oral mode through the voice messaging system on the platform.

If the whistleblower makes the report orally by means of a fixed meeting with the staff member in charge, the report, subject to the consent of the whistleblower himself/herself, is documented by the channel manager either by recording it on a device suitable for storage and voice playback or by drawing up a minute. In the latter case, the reporter may verify, rectify and/or confirm the minutes of the meeting by signing them.

Receipt of the report by the channel manager initiates the report handling process. The channel manager proceeds to its 'processing' according to a predefined process flow chart.

Upon receipt of the report, the responsible party shall notify the reporting party within 7 days of receipt of the report and acknowledgement of the report.

The channel manager proceeds with an initial verification of the correctness of the procedure followed by the reporting party and of the content of the report, both with reference to the scope defined by this procedure (so-called inherent nature of the content of the report) and to its verifiability on the basis of the information provided. At this stage, if the channel manager deems it necessary (e.g. in the event of any doubts), he will involve the Supervisory Board in order to assess the relevance under Legislative Decree 231/01 of the report. If the report is not inherent to the subject matter of this procedure, the channel manager formalises the outcome of the check and communicates it to the reporter within a reasonable time (no more than 3 months) and files the report.

If additional information is needed, the channel manager will contact the reporter via the platform. If the reporter does not provide any additional information within 3 months of the request for supplementation, the channel manager will proceed with the filing of the report, notifying the reporter and informing the Supervisory Board if it was involved in the assessment of the report.

If it is not necessary to acquire additional information, the channel manager will assess, on a case-by-case basis, with the Company whether and which company function should be appropriately involved for the relevant analysis and any consequent measures, always in compliance with the principle of confidentiality, and how to initiate the investigation phase.

In the case of information of relevant breaches pursuant to Legislative Decree 231/01, the channel manager, having verified the relevance of the report and having acquired all the elements, informs, in compliance with the principle of confidentiality, the Supervisory Board in order to assess how to initiate the investigation phase, without prejudice to compliance with the principle of autonomy and independence of the Supervisory Board with respect to the way in which the report is handled for the purposes and to the effects of Legislative Decree 231/01.

The channel manager, upon completion of the investigation, prepares a final report in order to proceed with the feedback to the reporter. Acknowledgement of receipt must be sent to the reporter within 3 months from the date of acknowledgement of receipt or from the expiry of the 7-day deadline from the submission of the report. Only in exceptional cases, should the complexity of the report require it, or in view of the reporting party's response time, the channel manager, having promptly informed the reporting party before the deadline, with appropriate justification, may continue the investigation phase for as long as necessary and giving the reporting party periodic updates.

In the event of relevant breaches pursuant to Legislative Decree 231/01, the channel manager shall notify the Supervisory Board of the results of the investigation. The Supervisory Board, within the scope of its operational autonomy, assesses the outcome received and, if the report is well-founded, any consequent measures and adopts any measures deemed necessary for the purposes of adapting the Model, taking the necessary communications for the application of any sanctions. Any consequent measures are applied in accordance with the provisions of the sanctions system set out in the 231 Organisational Model.

In the event of defamation or slander, ascertained by a conviction even at first instance, the Company shall proceed with a sanctioning procedure against the whistleblower.

It is specified that, from the receipt of the report until its closure, any person in a situation of conflict of interest must refrain from taking decisions in order to ensure compliance with the principle of impartiality.

7. 5 Retention of internal reporting documentation

Internal reports and all associated or supplemented documentation are retained, with an appropriate digital chain of custody, for as long as the report itself is processed.

In any case, the documentation shall only be kept for a time period of up to 5 years from the date of the communication of the final outcome of the alert procedure.

In all the cases mentioned, the procedure for keeping internal reports and related documentation must comply with EU and national guarantees on the processing of personal data as well as with the measures on confidentiality.

7.6 Information Obligations

Information on the channel, procedures and prerequisites for making reports is displayed in the workplace (company notice boards) and on the company's intranet page through the publication of this procedure, and made known to persons who, although not frequenting the workplace, have a legal relationship with the Company through publication on the appropriate web page of the institutional website respectively:

Italfarmaco S.p.a.: https://www.italfarmaco.com/it-it/Organizzazione

Effik Italia S.p.a. https://www.effik.it/Chi-siamo/Organizzazione

Chemi S.p.a. https://www.chemi.com

The Company activates its internal reporting channel after hearing the representatives or trade union organisations.

8. EXTERNAL REPORTING CHANNEL

If the following conditions are met, the reporter may proceed with a report to ANAC through an external channel:

- if in the relevant working context, activation of the internal reporting channel is not mandatory or the channel itself has not been activated or does not comply with regulatory requirements;
- when the reporter has already submitted an internal report even though it has not been followed up;
- if the whistleblower has a well-founded reason to believe that by submitting an internal report, the report will not be effectively followed up or that the report, in itself, will lead to retaliation against him/her;
- where the reporter has a well-founded reason to believe that the reported breach may constitute an imminent or obvious danger to the public interest.

The external body entitled to receive external reports is ANAC according to the modalities and procedures duly adopted by the latter.

9. PUBLIC DISCLOSURE

On a residual and subordinate basis, the reporter may proceed with a public disclosure in the following cases:

- when it has already previously made an internal or external report, or has directly made an external report without having received a reply within the prescribed time limit;
- where it has reasonable grounds to believe that the breach constitutes an imminent or obvious danger to the public interest;
- where it has reasonable grounds to believe that the external report carries a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the recipient of the report may be colluding with or involved in the infringer.

10. DUTY OF CONFIDENTIALITY

All reports and their attachments shall not be used beyond the time required to follow them up.

It is provided that the identity of the reporter together with any other information from which such identity may be inferred, directly or indirectly, shall not be disclosed without the express consent of the person making the report to persons other than those competent to receive or follow up the reports, expressly authorised to process such data pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article *2-quaterdecies* of the Personal Data Protection Code pursuant to Legislative Decree no. 196 of 30 June 2003, as amended.

The Company shall protect the identity of the persons involved, the facilitators and the persons mentioned in the report until the conclusion of the proceedings initiated on account of the report, in compliance with the same guarantees provided for in favour of the reporter.

Mitigating circumstances for the protection of the right to privacy include:

- In the context of criminal proceedings, the identity of the reporter is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure: the obligation of secrecy is imposed on the acts of the preliminary investigation until such time as the suspect has the right to have knowledge of them and, in any case, no later than the closure of that phase;
- Within the framework of the proceedings established at the Court of Auditors, the identity of the reporter cannot be disclosed until the investigation phase is closed;
- within the framework of disciplinary proceedings, the identity of the whistleblower may not be disclosed where the allegation of the disciplinary charge is based on investigations that are separate from and additional to the report, even if consequent to it;

- where the accusation is based, in whole or in part, on the report and knowledge of the identity of the person making the report is indispensable for the accused's defence, the report will only be usable for the purposes of disciplinary proceedings if the person making the report expressly agrees to reveal his identity;
- in cases of disciplinary proceedings initiated against the alleged perpetrator of the reported conduct, written notice shall be given to the reporter of the reasons for disclosing confidential data when disclosure is also indispensable for the defence of the person concerned.

Subject to the mitigation measures listed above, the affected party, upon its request, is also heard through a cartel procedure by means of the acquisition of written observations and documents.

Confidentiality obligations include:

- the subtraction of the report and of the documentation attached thereto from the right of access to administrative acts provided for by Articles 22 et seq. of Law No. 241/1990 and to generalised civic access pursuant to Articles 5 et seq. of Legislative Decree No. 33/2013;
- The administrations and bodies involved in the handling of reports guarantee confidentiality during all stages of the reporting process, including the possible transfer of reports to other competent authorities.

11. PROCESSING OF PERSONAL DATA

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

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

The disclosure of personal data by EU institutions, bodies or entities is made 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 compliance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679, by first providing appropriate information to the reporting subjects and the persons concerned and by taking appropriate measures to protect the rights and freedoms of the persons concerned.

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

1 2. PROTECTION AND SUPPORT MEASURES

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

Protection measures apply if at the time of the report the reporting person had reasonable grounds to believe that the information on the reported breaches was true (see Section 7.3), fell within the objective scope and the reporting procedure was followed.

In the case of defamation or slander, established by conviction even at first instance, protections are not guaranteed.

Protection measures also apply:

(a) to facilitators;

(b) persons in the same employment context as the reporting/reporting person who are linked to them by a stable emotional or family relationship up to the fourth degree;

(c) co-workers of the reporting/whistleblowing person who work in the same work environment as the reporting/whistleblowing person and who have a regular and current relationship with that person;

(d) entities owned by the reporting/whistleblowing person or for which those persons work, as well as entities operating in the same work environment as those persons.

1 2.1 Prohibition of retaliation

The persons listed in paragraph 5 shall not be subject to any retaliation. The following, by way of example but not limited to, are considered "retaliation": dismissal, suspension or equivalent measures; downgrading or non-promotion; change of function.

Acts taken in violation of the prohibition of retaliation are null and void.

In the context of judicial or administrative proceedings, or in the case of out-of-court disputes concerning the ascertainment of the prohibited conduct, acts or omissions against the reporting person alone, it is presumed that such conduct or acts were carried out as a result of the reporting. The burden of proving that such conduct or acts are motivated by reasons unrelated to the reporting is on the person who carried out the retaliatory acts.

Whistleblowers may inform ANAC of retaliation they believe they have suffered, whether attempted or contemplated.

ANAC informs the National Labour Inspectorate, for measures within its competence.

12.2 Measures of Support

The reporting party may turn to Third Sector entities on the list published on the ANAC website. These are bodies that carry out activities in the general interest for the pursuit, on a non-profit basis, of civic, solidarity and socially useful purposes ("*promotion of the culture of legality, peace among peoples, non-violence and non-armed defence promotion and protection of*

human, civil, social and political rights, as well as of the rights of consumers and users of general interest activities, 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 information, assistance and advice free of charge on how to report and on the protection from retaliation offered by national and EU legislation, on the rights of the person concerned, and on the terms and conditions of access to legal aid.

12.3 Limitation of liability of the reporter

There is no liability (including civil or administrative liability) for anyone who discloses or disseminates information on breaches:

- covered by the obligation of secrecy,
- related to copyright protection,
- of the provisions on the protection of personal data,
- which offend the reputation of the person involved or denounced,

whether, at the time of the disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of the same information was necessary to disclose the breach and the reporting was consistent with the conditions for protection.

In addition, protective measures include:

- The rights to make a report and the related protections cannot be restricted in a contractual manner;
- the exclusion of all other liability, including civil and administrative liability, for the acquisition of or access to information on breaches, unless the conduct constitutes a criminal offence;
- the exclusion of any other liability with regard to conduct, acts, omissions carried out if connected to the report and strictly necessary to disclose the breach or, in any case, not connected to the report.

13. Penalty regime

The disciplinary system adopted by the Company pursuant to Article 6, paragraph 2, letter e), of Legislative Decree 231/2001, and referred to in the General Section of the 231 Model, provides for sanctions to be applied against those whom the Company ascertains to be responsible for offences related to

- commission of retaliation or proposed adoption, obstruction of reporting (even attempted) or breach of confidentiality obligations,

- Failure to set up reporting channels, failure to adopt procedures for handling them, 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 for defamation or slander in cases of wilful misconduct or gross negligence, unless that person has already been convicted, also at first instance, of the offences of defamation or slander;

as well as against anyone who violates this procedure.

For the same offences, ANAC may intervene with the application of administrative pecuniary sanctions (from €500 up to €50,000) if the same offences are ascertained.

ATTACHMENTS

Legislative Decree No. 24 of 10 March 2023