WHISTLEBLOWING
-
Whistleblowing Procedure

In the event of any discrepancy between the Italian and English versions, the Italian version shall prevail.

Target recipients:	• Any persons who may need to report a breach pursuant to Legislative Decree No. 24/23
Approved by	The Board of Directors

Revision

no.	Effective date	Description	Drafted by:
0	28-01-2021	First version of the document	-
1	15-11-2023	Second revision of the document	BoD
2	23-09-2026	Third revision of the document	BoD

TABLE OF CONTENTS

1. Definitions 4

2. Introduction 9

3. Purpose 9

4. The reports considered under this procedure 10

5. Scope of application 11

6. The report management process 12

6.1. Reporting channels 12

6.1.1. Internal reporting 12

6.1.2. External reporting 13

6.1.3. Public disclosure 14

6.2. Submitting a report 14

6.2.1. Internal reporting 14

6.3. Receipt and analysis of the report 15

7. Disciplinary and sanctions system 18

7.1. Initiation of the disciplinary and sanctions system 18

8. Whistleblower protection and the application of protection measures 20

8.1. Limitations of liability 22

9. Storage and archiving 22

10. Reporting 23

11. Special cases 23

ANNEX 1 – REPORT FORM 24

ANNEX 2 – PRIVACY POLICY – WHISTLEBLOWER 24

1. Definitions

This document contains the following terms and expressions which shall have the meanings described below:

- "***ANAC***": Autorità Nazionale Anti Corruzione (Italian National Anti-Corruption Authority), established by Law No. 190/2012, is an independent administrative authority whose purpose is to combat corruption in all areas of administrative activity in Italy.
- "***ANAC Guidelines***": guidance documents providing public and private entities with operational instructions for the management of whistleblowing reports;
- "***Offence risk activity***": a process, operation or act or series of operations and acts that may expose the Company to the risk of sanctions, pursuant to the Decree, as a result of an offence being committed.
- "***CCNL***": the National Collective Labour Agreement applicable to the Company's employees.
- "***Code of Ethics***": the document, which has been officially requested and approved by the Company's senior management, whose purpose is to function as an elucidation of corporate policy and which contains the general principles of conduct - i.e., recommendations, obligations and/or prohibitions - with which the Recipients are expected to comply and whose infringement may result in the application of sanctions.
- "***Working context***": the work or professional activities, present or past, conducted in the context of the relationships set forth in art. 3(3) or art. 3(4) of Legislative Decree No. 24/2023, through which, irrespective of the nature of such activities, a person acquires information relating to potential breaches and in relation to which they could be at risk of retaliation should such breaches be reported (internal and/or external), disclosed publicly or reported to the judicial or financial authorities;
- "***Legislative Decree No. 231***" or the "***Decree***": Legislative Decree No. 231 of 8 June 2001, containing the "*Regulations on the liability of legal persons, companies and associations with or without legal personality, pursuant to art. 11 of Law No. 300 of 29 September 2000*", published in the Official Journal No. 140 of 19 June 2001 and subsequent amendments and additions.
- "***Recipients***": Corporate bodies (Board of Directors and Board of Statutory Auditors), Employees, Suppliers and all those who conduct activities on behalf of the Company, with or without powers of representation, and irrespective of the nature and type of relationship they

have with the Company. Recipients are required to comply with the Model, the Code of Ethics and the preventive protocols.

- "***Employees***": all natural persons who have a contractual employment relationship with the Company.
- "***Public disclosure":*** making information relating to breaches publicly available through the press, electronic media or other methods of communication capable of reaching a wide audience.
- "***Facilitator***": a person who assists a whistleblower in the reporting process, who works within the same working context and whose assistance must be kept confidential.
- "***Information relating to breaches***": information, including reasonable suspicions, concerning any breaches committed or which, on the basis of concrete evidence, may be committed within the organisation with which the whistleblower, or the person submitting the report to the judicial or financial authorities, has a legal relationship as defined by art. 3(1) or art. 3(2) of Legislative Decree No. 24/2023 (i.e. public and private sector), as well as evidence pertaining to conduct aimed at concealing such breaches.
- "***Guidelines***": the Guidelines for the development of organisational, management and control models pursuant to Legislative Decree No. 231, published by trade associations, which were consulted for the purposes of preparing and adopting the Model.
- "***Organisational, Management and Control Model pursuant to Legislative Decree No. 231***" or the "***Model***": the Organisational, Management and Control Model considered by the Corporate Bodies to be suitable for preventing offences and which, therefore, has been adopted by the Company, pursuant to articles 6 and 7 of the Decree, for the purposes of preventing the commission of such offences by Senior Executives or Subordinates, as described in this document and its annexes.
- "***Corporate Bodies***": the Company's Board of Directors and/or the Board of Statutory Auditors, depending on the context of the sentence in question.
- "***Supervisory Body***" or "***SB***": the Body provided for by article 6 of the Decree whose role is to oversee the functioning of and compliance with the Organisational, Management and Control Model, as well as to update it when necessary.
- "***Personnel***": all natural persons who have a contractual employment relationship with the Company, including employees, temporary workers, collaborators, interns and freelance workers who have been recruited by the Company (for the purposes of the "whistleblowing"

legislation, any natural persons falling into the following categories are also considered personnel: where the employment or collaborative relationship has not yet commenced, if information pertaining to the breaches was acquired during the selection process or any other pre-contractual phase; during the probationary period; following the termination of the legal relationship if the information pertaining to the breaches was acquired during the course of the relationship).

- "***Senior Executives***": the persons defined by article 5(1)(a) of the Decree, i.e. the persons who hold a representative, administrative or management role within the Company; in particular, the members of the Board of Directors, the Chairman and any proxies and attorneys appointed by the Company.
- "***Subordinates***": the persons defined by article 5(1)(b) of the Decree, i.e. all personnel who operate under the direction or control of Senior Executives.
- "***Whistleblower":*** a natural person who reports or publicly discloses any information relating to breaches that they've acquired in their working context.
- "***Person involved***": the natural or legal person cited in the internal or external report or the public disclosure as the person who it is claimed has committed the breach or who it is claimed was otherwise involved in the reported or publicly disclosed breach.
- "***Public administrative body(ies)***" or "***PA***": The following are defined as public administrative bodies:
  - the Government (or State Administration);
  - Public Bodies; the Public Body must either be identified as such by law or is a Body that's subject to a system of public control, to oversight by the Government or other administrative body in relation to the appointment and dismissal of its directors, and to the administration of the Body itself. Furthermore, its management costs shall be funded, in part or fully, by the Government or another public administrative body; or the Government plays a role in setting its strategic direction; or is publicly financed; or has been established by another public administrative body. By way of a non-limiting example, and in the broadest possible sense, the following companies are considered public administrative bodies: Ferrovie dello Stato (Italian National Railways), Autostrade S.p.A. (Italian Motorway Agency), AEM Milano (the municipal utility organisation for Milan), etc.
  - Public Official: a person who performs "a public legislative, judicial or administrative function". Under criminal law, as set forth by article 357 of the Italian criminal code, "an

administrative function is considered public if it is governed by the rules of public law and so-called 'authoritative acts' and is characterised by the expression and manifestation, or the exercise, of the will of the public administrative body through authoritative or certifying powers";

- Public Service Officer: as set forth by article 358 of the Italian criminal code, a person who "performs a public service in one capacity or another. Where public service is understood to be an activity governed in the same manner as a public function, but which doesn't possess the powers that are typical of the latter, except for the authority to perform simple tasks and manual work." It should be noted that "in one capacity or another" is to be understood in the sense that a person performs a public function, even without having been formally or legally appointed (a "de facto" public service officer). The relationship between the PA and the person performing the service is irrelevant.

- "***Protocol***": the organisational, physical and/or logical measure provided for by the Model to prevent the risk of offences being committed.
- "***Offences***" or the "***Offence***": the series of offences, or the single offence, set forth by Legislative Decree No. 231 (including any potential subsequent amendments and additions).
- "***Retaliation***": any conduct, act or omission, even if only attempted or threatened, committed in response to the submission of a report (internal and/or external), the submission of a report to the judicial or financial authorities or its public disclosure which, directly or indirectly, causes or may cause harm to the whistleblower or the person who submitted the report.
- "***Report":*** the communication, in writing or orally, of information relating to a Breach or Breaches;
- ***"External report***": the communication, in writing or orally, of information relating to a breach, delivered via an external communication channel;
- ***"Internal report***": the communication, in writing or orally, of information relating to a breach, delivered via an internal communication channel;
- ***"Follow-up":*** the actions taken by the person responsible for managing the reporting channel to assess the veracity of the evidence or information reported, the outcome of the investigation and any measures taken;
- "***Disciplinary System***": the set of sanctions that may be applied in the event that a reported Breach is proven to be valid;
- "***Company***": Industrie Chimiche Forestali S.p.A.

- "***Breaches***": conduct, acts or omissions considered to be contrary to public interest or detrimental to the integrity of the public administrative body or private entity and which may be defined as follows:
  1. unlawful conduct as per the definitions established by Legislative Decree No. 231 of 8 June 2001, or breaches of the Organisational and Management Model provided for by the Decree and adopted by the Company, and which are not covered by paragraphs 2), 3), 4) and 5) below;
  2. offences falling within the scope of the European Union or national legislation indicated in the relevant annex to Legislative Decree No. 24/2023 or of the national legislation implementing the European Union legislation indicated in the annex to directive (EU) 2019/1937, even if not indicated in the relevant annex to Legislative Decree No. 24/2023 or, which relate to the following areas: public procurement; financial services, products and markets and prevention of money laundering and financing of terrorism; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and animal feed safety and animal health and welfare; public health; consumer protection; privacy and protection of personal data and security of networks and information systems;
  3. acts or omissions detrimental to the financial interests of the Union as per article 325 of the Treaty on the Functioning of the European Union as specified in the relevant secondary legislation of the European Union;
  4. acts or omissions affecting the internal market as per article 26(2) of the Treaty on the Functioning of the European Union, including breaches of European Union competition and state aid regulations, as well as breaches affecting the internal market in relation to conduct in breach of corporation tax regulations or mechanisms whose purpose is to obtain a tax benefit that undermines the objective or purpose of the applicable corporation tax regulation;
  5. conduct or behaviour that undermines the objective or purpose of the provisions of the European Union legislation in the areas indicated in paragraphs 2), 3) and 4) above.

2. Introduction

The Company has aligned its business policy with the principles of legality and correctness set forth by the Code of Ethics, thereby demonstrating its strong commitment to operating according to appropriate policies and to preventing any improper or illegal conduct. This policy is set out in the Organisational, Management and Control Model, it is aimed at preventing offence risks and has been adopted pursuant to articles 6 and 7 of Legislative Decree No. 231.

Any persons who become aware, within their working context, of any Breaches of national or European Union law considered to be contrary to public interest or detrimental to the integrity of the private entity, are obliged to submit a report in accordance with this procedure. Such reports must be as detailed as possible, made in good faith, and be based on reasonable grounds substantiated by clear and consistent facts and evidence.

This procedure constitutes the Company's internal implementation of the regulatory provisions relating to the protection of persons who report breaches as set forth by Legislative Decree No. 24/2023. This decree constitutes the primary reference for all the activities considered hereunder.

Furthermore, this procedure has been drawn up taking into account the ANAC Guidelines on Whistleblowing.

3. Purpose

The specific purpose of this procedure is to govern the process for managing reports of Breaches pursuant to Legislative Decree No. 24/2023, in a manner designed to ensure the confidentiality of the identity of the whistleblower, the person involved and any persons mentioned in the report, as well as the confidentiality of the contents of the report and the related documentation, in accordance with the "need to know" principle.

Through this procedure, the Company defines its model for receiving and managing internal reports and its internal reporting channel, identifying technical and organisational measures appropriate to the risks, including segregation of access, traceability of operations, data protection (including

encryption where applicable), and retention and deletion rules, in accordance with Regulation (EU) 2016/679 and the applicable personal data protection legislation.

4. The reports considered under this procedure

This procedure concerns reports that are submitted in relation to the following Breaches, as set forth by article 2 of Legislative Decree No. 24 of 10 March 2023:

1. unlawful conduct as per the definitions established by Legislative Decree No. 231 of 8 June 2001, or breaches of the Organisational and Management Model provided for by the Decree and adopted by the Company, and which are not covered by paragraphs 2), 3), 4) and 5) below;
2. offences falling within the scope of the European Union or national legislation indicated in the relevant annex to Legislative Decree No. 24/2023 or of the national legislation implementing the European Union legislation indicated in the annex to directive (EU) 2019/1937, even if not indicated in the relevant annex to Legislative Decree No. 24/2023 or, which relate to the following areas: public procurement; financial services, products and markets and prevention of money laundering and financing of terrorism; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and animal feed safety and animal health and welfare; public health; consumer protection; privacy and protection of personal data and security of networks and information systems;
3. acts or omissions detrimental to the financial interests of the Union as per article 325 of the Treaty on the Functioning of the European Union as specified in the relevant secondary legislation of the European Union;
4. acts or omissions affecting the internal market as per article 26(2) of the Treaty on the Functioning of the European Union, including breaches of European Union competition and state aid regulations, as well as breaches affecting the internal market in relation to conduct in breach of corporation tax regulations or mechanisms whose purpose is to obtain a tax benefit that undermines the objective or purpose of the applicable corporation tax regulation;
5. conduct or behaviour that undermines the objective or purpose of the provisions of the European Union legislation in the areas indicated in paragraphs 2), 3) and 4) above.

The reports may relate to:

- information, including reasonable suspicions, concerning any Breaches committed;
- information, including reasonable suspicions, concerning Breaches that, on the basis of concrete evidence, may be committed;
- evidence pertaining to conduct aimed at concealing such breaches.

With specific reference to the conduct referred to in paragraph 1), purely by way of example, the following cases are cited:

- unlawful conduct, as per the definitions established by Legislative Decree 231;
- breaches of the Model, the Code of Ethics or the preventive protocols which, pursuant to the Decree, may result in the imposition of sanctions on the Company;
- suspected breaches of the Model, the Code of Ethics or the preventive protocols which, pursuant to the Decree, may result in the imposition of sanctions on the Company;
- corporate or business operations in relation to which, pursuant to the Decree, there is a potential risk that sanctions may be imposed on the Company.

Reports of Breaches in relation to number 1) above may only be submitted via the internal reporting channel (see section 6.1.1. "Internal reporting").

5. Scope of application

5.1 Corporate Scope

This document applies to those Recipients identified in chapter "*1. Definitions*" above.
The report management process outlined in this document does not relate to commercial communications or to information that's of a deliberately pernicious nature and which does not fall within the Breaches set forth by Legislative Decree No. 24/23.

This procedure also **does not apply** to disputes, claims or requests with a connection to the personal interests of the whistleblower, or the person submitting a report to the judicial or financial authorities, that relate exclusively to their individual working relationships, or that are inherent in their working relationships with their superiors.

Generally speaking, the Company encourages its employees to resolve any labour disputes, where possible, through dialogue, even informally, with their colleagues and/or their direct superior.

5.2. Involvement of trade union organisations

In accordance with whistleblowing legislation and the guidance issued by the Italian National Anti-Corruption Authority (ANAC), when adopting and/or updating this procedure the Company shall provide prior information to the company-level trade union representatives.

The information shall concern the arrangements for managing reports and shall include the transmission of the relevant documentation, including the sections of the Organisational, Management and Control Model pursuant to Legislative Decree No. 231/2001 relating to the internal reporting channel.

Where there are no company-level trade union representatives, the above information shall be provided to the local organisations of the most representative trade union associations at national level.

Appropriate evidence that this requirement has been fulfilled shall be retained on file (communication sent and related receipts, any responses and/or acknowledgement that the assigned period has elapsed).

6. The report management process

6.1. Reporting channels[1]

6.1.1. Internal reporting

Pursuant to current legislation, the Company has established its own internal reporting channel in accordance with Legislative Decree No. 24/2023, which guarantees that the identity of the whistleblower, the person involved and any persons cited in the report, as well as its contents and any relevant documentation, shall remain confidential.

It is the responsibility of the Supervisory Body to oversee and manage this reporting channel.

[1] Legislative Decree No. 24/23, in addition to the reporting or disclosure channels indicated in this procedure, also makes provisions for the person involved, should they feel the necessity, to submit a report to the judicial or financial authorities.

The members of the Supervisory Body have been duly authorised by the Company to process the personal data contained in internal reports and operate in accordance with the strict necessity ("need to know") principle, with selective access to information and documentation connected with reports, in order to ensure maximum confidentiality.

In the event of absence, impediment or a conflict of interest affecting one or more members of the Supervisory Body, or where a report concerns one of its members, the abstention and replacement rules set out in Chapter 11 "Special cases" shall apply, ensuring operational continuity of the reporting channel and traceability of the handling of the report.

Reports may be submitted in the following ways:

- in writing, via e-mail, to the following certified e-mail address: icfspaodv@legalmail.it;
- in writing, by ordinary post, to Via Kennedy, 75, 20010 Marcallo con Casone (Milan), addressing the letter as follows: "For the attention of the Supervisory Body – strictly confidential and personal". In this case, the documentation relating to the report must be placed in a sealed envelope which, together with a separate envelope containing the whistleblower's identification details, must be placed inside a third sealed envelope addressed to the Supervisory Body as indicated above;
- orally, by requesting a face-to-face meeting with the Supervisory Body that's scheduled to take place within a reasonable time period. In such cases, subject to the whistleblower's consent, the internal report may be recorded, by an authorised member of staff, via a recording device, for subsequent archiving and listening, or via the taking of minutes. Where minutes are taken, the whistleblower may verify and correct them, and subsequently sign them to confirm their accuracy.

For further details, please refer to paragraph 6.2.

6.1.2. External reporting

The whistleblower may also submit an external report[2] to ANAC (Italian National Anti-Corruption Authority) if at least one of the following conditions are met:

a) the internal report that they submitted in accordance with this procedure has not been acted upon or followed up;
b) if they were to submit an internal report, the whistleblower has reasonable and proven grounds to believe that it would not be effectively acted upon or followed up, or that they themselves may be at risk of retaliation;
c) the whistleblower has reasonable grounds to believe that the breach may constitute conduct that's imminently or clearly detrimental to the public interest.

The external channel for submitting reports established by ANAC guarantees, similarly to the aforementioned internal channel established by the Company, that the identity of the whistleblower, the person involved and any other persons potentially involved in the report, as well as the contents of the report, shall remain confidential.

External reports are to be submitted in writing via the platform set up on the ANAC website in the section dedicated to "Whistleblowing". The report may also be submitted orally via telephone or voice message or, at the request of the whistleblower, via a face-to-face meeting that's scheduled to take place within a reasonable time period; the ways of accessing such channels are outlined by ANAC on its website.

6.1.3. Public disclosure

Furthermore, the whistleblower is guaranteed the right, should they wish, to disclose the knowledge they have publicly,[3] as long as at least one of the following conditions is met:

a) the whistleblower has previously submitted an internal report without receiving feedback within the specified timeframes, and subsequently submitted an external report to ANAC

[2] This chapter does not apply to reports of breaches as per the definitions established by Legislative Decree No. 231 of 8 June 2001, or breaches of the Organisational, Management and Control Model provided for by the Decree and adopted by the Company, such breaches may only be submitted via the internal reporting channel (article 3(2)(b) of Legislative Decree No. 24/23).

[3] This chapter does not apply to reports of breaches as per the definitions established by Legislative Decree No. 231 of 8 June 2001, or breaches of the Organisational, Management and Control Model provided for by the Decree and adopted by the Company, such breaches may only be submitted via the internal reporting channel (article 3(2)(b) of Legislative Decree No. 24/23).

without receiving feedback within a reasonable timeframe; or directly submitted an external report to ANAC without receiving feedback within a reasonable timeframe;

b) the whistleblower has previously submitted an internal and/or external report and did not receive a reply within the time limits stipulated by this procedure[4] in relation to the measures provided for or adopted in response to the report;

c) the whistleblower has reasonable grounds to believe that the Breach may constitute conduct that's imminently or clearly detrimental to the public interest;

d) the whistleblower has reasonable grounds to believe that the submission of the external report may subject them to a possible risk of retaliation or that it may not be effectively acted upon or followed up due to the specific circumstances of the case, for example, where evidence may have been concealed or destroyed or where there are reasonable grounds to believe that the person receiving the report may be colluding with the alleged perpetrator of the Breach or is involved in the Breach themselves.

6.2. Submitting a report

6.2.1. Internal reporting

Any person wishing to submit an internal written report may do so using the dedicated form provided in Annex 1 to this document.

Through a series of questions and requests for supporting evidence, this form guides the whistleblower through the process of providing a report that provides a clear, accurate and evidence-based account of the situation.

The reports must be based on accurate, consistent facts. The whistleblower is requested to attach all relevant documentation that may serve as evidence, and must refrain from undertaking any independent analytical or investigative activities.

[4] In accordance with the provisions of articles 5 and 8 of Legislative Decree No. 24/2023 *"Implementation of directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, on the protection of persons who report breaches of Union law and containing provisions relating to the protection of persons who report breaches of national legislation."*

6.3. Receipt and analysis of the report

In the first instance, the reports are managed by the SB, doing so in a confidential manner, adopting appropriate methods of verification so as to protect the identity of the whistleblower and any persons involved.

Preliminary analysis

All reports received are subject to a preliminary check by the SB so as to ascertain whether it is accompanied by the necessary information to conduct a preliminary verification of its validity and to be able to initiate the subsequent investigation activities.

The SB undertakes to issue the whistleblower with an acknowledgement of receipt within 7 days of the internal report being received.

Where the report is incomplete or insufficiently detailed, the SB may request additional information from the whistleblower, assigning a reasonable deadline.

Without prejudice to the confidentiality of the information received, during this preliminary analysis phase, the SB may call upon the support of other Company departments or specialised consultants to provide any specific expertise that may be required, depending on the content of the report, to conduct such analysis.

Following the completion of the preliminary checks, the SB may register the internal report under one of the following categories:

- unsubstantiated;
- one which, on the basis of the description of the facts and the information provided by the whistleblower, does not make it possible to obtain a sufficiently detailed picture of the situation so as to undertake further investigations into whether it is well-founded;
- one that is manifestly unfounded.

During the preliminary analysis phase, the SB:

- shall guarantee that the internal report is analysed and assessed impartially, fairly and meticulously;
- shall ensure the confidentiality of the information gathered, as well as of the identity of the whistleblower, where provided;
- shall undertake not to use the internal report for any purposes other than is necessary to adequately investigate and act upon it. The SB may not disclose the identity of the

whistleblower and any other information which may be used to identify them, directly or indirectly, without the express consent of the whistleblower themselves, to persons other than those responsible for receiving or investigating such reports, and who are expressly authorised to process such data pursuant to articles 29 and 32(4) of Regulation (EU) 2016/679 and article 2-*quaterdecies* of the Italian Personal Data Protection Code as set forth by Legislative Decree No. 196/03.

Anonymous reports, where sufficiently detailed and containing information suitable to allow checks to be initiated, may be handled in accordance with the same procedures set out herein.

Anonymous reports lacking a minimum level of contextual detail and/or which are manifestly unfounded may be archived in accordance with the criteria set out in this procedure, with the outcome of the preliminary assessment duly recorded.

Anonymous reports received shall in any event be recorded in the Reports and Investigations Book (Reports Register) and retained in accordance with Chapter 9.

Reports that do not proceed beyond the preliminary analysis

Internal reports that do not proceed beyond the preliminary stage shall be archived by the SB in a dedicated and segregated logical area, protected by appropriate technical measures (including encryption), suitable for ensuring the confidentiality of the whistleblower's identity and of the contents of the report, and accessible exclusively to duly authorised members of the Supervisory Body; such reports shall be accounted for in the periodic reporting described below.

In any case, the SB shall record any internal reports submitted, together with the activities conducted following their receipt, in the Reports and Investigations Book, always guaranteeing the confidentiality of the identity of the whistleblower and any persons involved. The Reports and Investigations Book must be kept by the SB and shall only be accessible to persons whom the Company authorises to access it.

Reports that proceed beyond the preliminary analysis

In the event that the SB's preliminary analysis establishes that the internal report, having been adequately substantiated and accompanied by evidence that sufficiently corroborates it, details conduct that is liable to sanctions, even if only disciplinary, the Supervisory Body shall:

a) provide immediate and reasoned information to the functions/bodies responsible for the application of sanctions and the disciplinary system, hereinafter detailed in Chapter 7 "Disciplinary and sanctions system", so that they may independently determine the disciplinary action to be taken, and who must, where the persons involved are Company employees, also ensure compliance with the principles of specificity[5], immediacy[6] and immutability[7] of the incident[8]. When independently determining the appropriate disciplinary action to be taken, these functions/bodies may conduct further investigations and analysis, and in doing so may request the support of the SB which shall remain the only intermediary between them and the whistleblower so as to guarantee their anonymity. Where, following their further investigations and analysis, these functions/bodies:
   i. consider that the conduct should not be the subject of disciplinary action, they shall immediately inform the SB which shall file the report in the manner described hereinbefore (see para. *Reports that do not proceed beyond the preliminary analysis*) and inform the whistleblower regarding the status of the procedure;
   ii. decide to proceed with issuing a notification of the charges, together with this, the person involved must be sent the relevant privacy policy pursuant to article 14 of the GDPR or, in any case, within one month of the date on which the data processing commenced;

b) inform the management body, for the assessments falling within its remit, indicating the subject matter of the report, the outcome of the investigation, any activation of the disciplinary and sanctions system, and any corrective actions aimed at preventing similar situations in the future;

c) on completion of the investigative activities, draft a final report to be sent to the function/body responsible for implementing the disciplinary action and/or corrective actions aimed at avoiding the occurrence of similar situations in future (also pursuant to article 7(4) of Legislative Decree No. 231).

[5] See Court of Cassation Judgement No. 10662 of 14 May 2014.
[6] See Court of Cassation Judgement No. 12337 of 15 June 2015, Court of Cassation Judgement No. 30985 of 27 December 2017, Court of Cassation Judgement No. 19256 of 17 July 2019, Court of Cassation Judgement No. 24605 of 4 November 2020.
[7] See Court of Cassation Judgement No. 11868 of 9 June 2016.
[8] In such circumstances, the disciplinary measures shall be applied in compliance with the provisions of article 7 "*Disciplinary Sanctions*" of Law No. 300 of 1970 (Workers' Statute).

The SB undertakes to process internal reports received within a reasonable time and to provide feedback to the whistleblower, through the channel selected by the whistleblower (e.g. the designated internal platform/channel), subject to confidentiality requirements, within:

- three months of the date of acknowledgement of receipt,
  or, in the absence of such an acknowledgement,
- within three months of the conclusion of the seven-day period which commenced on the date the report was submitted.

7. Disciplinary and sanctions system

7.1. Initiation of the disciplinary and sanctions system

Where the investigations establish that the Breaches covered by the internal report are well-founded, the body/function responsible for activating the disciplinary and sanctions system shall determine the type of sanction to be imposed on the persons who committed them, in compliance with the applicable rules and the principles of proportionality and graduality.
In addition to the Breaches themselves, the following conduct may constitute autonomous sanctionable behavior, irrespective of whether the report is well-founded:

- adopting retaliatory or discriminatory measures, including attempted or threatened measures, against the whistleblower;
- obstructing or attempting to obstruct a report;
- breaching confidentiality obligations relating to the whistleblower, the person involved, and/or persons mentioned in the report, as well as the contents of the report and related documentation;
- failure by competent persons to perform, or negligent performance of, verification, analysis, management, and feedback activities relating to reports;
- failure to establish the internal reporting channel and/or failure to adopt or update the Whistleblowing Procedure, or adopting safeguards/procedures non-compliant with Legislative Decree No. 24/2023 and ANAC Guidelines, where attributable to competent persons.

Depending on the status of the Person involved and, where applicable, their employment-law classification, the Disciplinary System shall be activated by:

- the HR department / Operations Director / Chairman of the Board of Directors / CEO if the person involved is an employee;
- the Board of Directors if the person is manager;
- the Shareholders' Meeting if the person is a Statutory Auditor;
- the Shareholders' Meeting if the person is a Director;
- the Board of Directors if the person is member of the SB;
- the CEO if the persons a third party.

The sanction may be graduated in accordance with the severity of the breach, pursuant to the provisions of the applicable legislation for the particular case (e.g. labour laws in the case of Company employees).

In the event that the whistleblower is jointly responsible for the Breach, they shall be treated differently with respect to their co-offenders, however, their case will be handled in accordance with the Breach committed and the applicable protocols.

The identity of the whistleblower and any other information which may be used to identify them, directly or indirectly, may not be disclosed without their express consent. The whistleblower's free, specific, unequivocal and informed consent shall be received in writing and kept by the SB together with the other report related documentation.

During the disciplinary proceedings, the identity of the whistleblower, in the absence of their express consent, cannot be disclosed where the allegation for which the disciplinary proceedings have been initiated is based on investigations that are separate and additional to the report, even if they were conducted as a consequence of it.
If, however, the disciplinary proceedings are initiated partly or entirely on the basis of the report, and having knowledge of the whistleblower's identity is essential for the person involved to be able to build a case for their defence, the Supervisory Body, where it has not already obtained the whistleblower's consent, shall inform them, in writing, of the reasons for which it is necessary for their identity, or any other information from which it may potentially be inferred, to be disclosed, so as to ensure that the report can be fully followed up, or to enable the correct implementation of the disciplinary proceedings.

In the event that the whistleblower refuses to give their consent for their identity to be disclosed, the SB shall archive the internal report without any further action being taken.

This procedure is without prejudice to the whistleblower's criminal and disciplinary liability should the report be found to be libellous or defamatory pursuant to the Italian Criminal Code and article 2043 of the Italian Civil Code.
In the event that a report is considered to be unfounded and has been submitted maliciously or as a result of gross negligence, such conduct may result in the application of disciplinary sanctions.
The abuse of this procedure, in any form whatsoever, such as internal reports that are clearly opportunistic and/or have been submitted for the sole purpose of harming the person involved or any other persons, and any other potential improper use or intentional exploitation of the Company in relation to this procedure, may result in action being taken, either disciplinary or a referral to other competent authorities.

Therefore, in the event that the whistleblower is found to be criminally liable for the offences of defamation or slander, even through a judgement from the court of first instance, or to be civilly liable in cases of wilful misconduct or gross negligence, the protections set forth by this procedure are no longer guaranteed and a disciplinary sanction,[9] as set forth in this chapter, may be imposed on the said whistleblower.

8. Whistleblower protection and the application of protection measures

Any form of retaliation towards the whistleblower is strictly prohibited.
In accordance with legislation, the prohibition of any acts of retaliation and the measures established by law to protect whistleblowers also apply:

a) to facilitators;
b) to any persons operating within the same working context as the whistleblower or the person who submitted a report to the judicial or financial authorities or made a public disclosure and who have a connection to them through a stable emotional or family relationship up to the fourth degree of kinship;

[9] For further details in this regard, please refer to the provisions of art. 16 of the Legislative Decree No. 24/23 "*Conditions for the protection of whistleblowers*".

c) to any co-workers of the whistleblower or the person who submitted a report to the judicial or financial authorities or made a public disclosure, who work in the same working context as the whistleblower and have a regular and current relationship with that person;
d) to any entities owned by the whistleblower or the person who submitted a report to the judicial or financial authorities or made a public disclosure or for which these persons work, as well as any entities operating in the same working context as the aforementioned persons.

The protective measures apply when, at the time of the report's submission (internal and/or external), or its submission to the judicial or financial authorities or its public disclosure, the whistleblower:

- had reasonable grounds to believe that the information regarding the Breaches being reported was true and related to Breaches of national or European Union law considered to be detrimental to the interests or integrity of the Company, which they became aware of within the working context;
- submitted the report (internal and/or external) in accordance with the provisions of the applicable legislation pursuant to Legislative Decree No. 24/2023.

With regard to the protection measures afforded to whistleblowers, the reasons that prompted them to submit a report or make a public disclosure are irrelevant.
The conditions established for protecting whistleblowers also apply in cases of anonymous reporting (internal and/or external), an anonymous report submitted to the judicial or financial authorities or an anonymous public disclosure, if the whistleblower is subsequently identified and is subjected to retaliation, as well as in cases where reports are submitted to the competent institutions, bodies or boards of the European Union, in accordance with the conditions set forth in this procedure (as well as by article 6 of Legislative Decree No. 24/2023).

Any acts of discrimination against whistleblowers may be communicated to ANAC, which in turn will inform the National Labour Inspectorate for the measures falling within its competence.

Any actions taken that infringe the anti-retaliation regulations shall be considered null and void and, wherever a whistleblower has been dismissed as a result of submitting a report (internal and/or external) or making a public disclosure, the whistleblower shall be entitled to be reinstated to their job.

In the context of judicial, administrative or extrajudicial proceedings concerning the establishment of the prohibited conduct, acts or omissions towards the whistleblower, it is presumed that such conduct or acts were committed in connection with the report's submission (internal and/or external), public disclosure or its submission to the judicial or financial authorities. As required by law, the burden of proving that such conduct or acts are motivated by reasons unrelated to the report's submission (internal and/or external), public disclosure or its submission to the judicial or financial authorities lies with the entity that perpetrated them (e.g. the employer).
Moreover, in the event that the whistleblower submits a claim for damages to the judicial authorities, having shown that they submitted a report (internal and/or external), made a public disclosure or submitted a report to the judicial or financial authorities and suffered harm, it is presumed, unless proven otherwise, that the harm was as a direct consequence of that submission or disclosure.

8.1. Limitations of liability[10]

In accordance with legislation, a whistleblower shall not be punished for disclosing or disseminating information regarding Breaches covered by confidentiality obligations, other than that set forth by article 1(3) of Legislative Decree No. 24/2023, or which relates to the protection of copyright or the protection of personal data, or discloses or disseminates information regarding Breaches which damages the reputation of the person involved or reported, if, at the time of the disclosure or dissemination, there were reasonable grounds for believing that the disclosure or dissemination of that information was necessary to report the Breach, and the report (internal and/or external), public disclosure or submission to the judicial or financial authority was made pursuant to the provisions of Legislative Decree No. 24/2023.
In such cases, any further liability, including civil or administrative liability, is also excluded.

Unless it constitutes an offence, the Company or whistleblower shall not incur any liability, including civil or administrative liability, for acquiring or accessing the information relating to the Breaches.

In any case, criminal or any other liability, including civil or administrative, is not excluded for conduct, acts or omissions that are not related to the report's submission (internal and/or external), or its submission to the judicial or financial authorities or its public disclosure, or that are not strictly necessary for the purposes of reporting the Breach.

[10] See art. 20 of Legislative Decree No. 24/2023.

9. Storage and archiving

The SB shall be informed of any sanctions imposed as a result of any internal or external reports. The relevant corporate functions (the Personnel Department) shall store and archive any documentation relating to the disciplinary and sanctions process.
The SB shall therefore archive the documentation relating to the internal report received through the electronic channel and to the related investigation in a dedicated and segregated logical area (including, where appropriate, within the Company's information systems), protected by technical and organisational measures appropriate to the risks, including encryption where applicable, access segregation, traceability of operations and retention/deletion rules.

Any paper documents, as well as the Reports and Investigations Book held by the SB, must be kept by the SB and shall only be accessible to persons whom the Company authorises to access them.
Pursuant to the confidentiality obligations set forth by article 12 of Legislative Decree No. 24/2023 and the principle set forth by article 5(1)(e) of Regulation (EU) 2016/679 and article 3(1)(e) of Legislative Decree No. 51 of 2018, any internal reports received shall be retained for as long as is necessary for them to be processed and, in any case, for a period not exceeding five years from the date that the final outcome of the subsequent procedure is communicated. Upon expiry of this retention period, the Company shall proceed with the deletion or anonymization of personal data, unless a different retention period is strictly necessary to protect the Company's rights in relation to pending proceedings or initiatives (e.g., disciplinary actions, litigation, transmission to authorities) originating from the report.

As part of the technical and organisational measures adopted, the Company shall, where applicable, ensure safeguards suitable to reduce the risk of tracing the whistleblower's identity when reports are submitted or accessed through web browsers or other electronic tools, consistently with the privacy risk assessment and the internal operating instructions.

The SB may maintain a Report Register, in which the personal details of the whistleblower, the persons involved, identified as those possibly responsible for the unlawful conduct, as well as any persons who, for whatever reason, are cited in the internal report must be anonymised[11], for the

[11] The storage of anonymised data does not breach the provisions of article 12 of Legislative Decree No. 24/23, which stipulate the time periods for retaining personal data, and complies with the provisions of article 5(1)(e) of Regulation (EU) 2016/679.

purposes of providing future evidence regarding the adequate management of the report pursuant to Legislative Decree No. 24/23, as a requirement for the effective implementation of the Model for preventing offence risks pursuant to article 6 of Legislative Decree No. 231, and for establishing the absence of any fault on the part of the organisation.

10. Reporting

The Supervisory Body shall report annually on the functioning of the internal whistleblowing systems, providing aggregated data on the results of any activities conducted as well as the follow-up work conducted in response to any reports submitted.
In producing this report, the SB is required to comply with the legislative provisions set forth in relation to protecting the whistleblower's identity and of the applicable legislation regarding the protection of personal data.

11. Special cases

Where a report concerns an internal member of the Supervisory Body, the standard procedure described above shall apply, but the member concerned shall abstain from participating in the activities and decisions relating to that report.

Where an internal report concerns more than one member of the SB, or where conflicts of interest arise that prevent the report from being handled impartially, the report shall be forwarded to the Board of Directors and, in particular, to the Chairman of the Board of Directors, together with any supporting documentation.

In such cases, the Board of Directors, having consulted the Board of Statutory Auditors, shall promptly identify the person entrusted with managing the report and conducting the investigation, ensuring that access to information is limited to authorised persons only; the confidentiality of the whistleblower's identity, the person involved, any persons mentioned, and the contents and documentation of the report is preserved; and the investigation follows, insofar as compatible, the process described in this procedure and is duly documented. The Board of Directors, having consulted the Board of Statutory Auditors, shall then collectively assess whether the report contains the information necessary to preliminarily verify its merits and initiate the subsequent activities, and shall proceed with the follow-up and investigation, where necessary with the support of other

Company functions or specialised consultants, in compliance with the confidentiality obligations laid down by applicable law and this procedure.

The investigation shall follow the process previously outlined in this procedure.

The decision of the Board of Directors shall be formalised by means of a written resolution.

ANNEX 1 – REPORT FORM

ANNEX 2 – PRIVACY POLICY – WHISTLEBLOWER

WHISTLEBLOWING REPORT FORM

Please attach or enclose any documentation that you feel may be relevant or that may be used as evidence to support this report; if the report is submitted verbally, please provide any such documentation directly.

WHISTLEBLOWER'S DETAILS

Name and Surname *(non mandatory)* _____

Department and job title *(non mandatory)* _____

Preferred contact details (e.g. private e-mail address, telephone number, etc.)

Does the whistleblower have any personal interests in relation to this report? ☐ Yes ☐ No

Please describe the nature of this personal interest

Is the whistleblower jointly responsible for the breaches being reported? ☐ Yes ☐ No

REPORTED OFFENCE

Period during/date on which the reported offence occurred

_____

Corporate area or department in which the reported offence occurred

_____

Persons involved:

Internal	External

Description of the reported offence

Other persons who may have relevant information concerning the reported offence

Internal	External

Has this report been sent to any other persons or entities? Yes ☐ No ☐

Please specify these other persons or entities and when it was sent

Date Signature *(non mandatory)* _____

PRIVACY POLICY - WHISTLEBLOWER
pursuant to art. 13 of Regulation (EU) 2016/679 regarding the processing of personal data in relation to the reporting of breaches in accordance with Legislative Decree No. 24/23

Pursuant to article 13 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, hereinafter the "GDPR") and the applicable personal data protection legislation - we inform you that the personal data you provide as a whistleblower (hereinafter also the "Data Subject") via this "Report Form" or provided by other means to internally report a breach pursuant to Legislative Decree No. 24/2023, shall be processed in accordance with the aforementioned regulations and with the principles of correctness, lawfulness and transparency by personnel authorised by INDUSTRIE CHIMICHE FORESTALI S.P.A. pursuant to article 29 of the GDPR and article 2-*quaterdecies* of the Italian Personal Data Protection Code as set forth by Legislative Decree No. 196 of 30 June 2003.

1. Controller

The data controller is INDUSTRIE CHIMICHE FORESTALI S.P.A. (hereinafter also the "Company" or "Controller"), represented by its pro tempore legal representative, with registered office at Via Kennedy, 75 Marcallo con Casone 20010 Milano, and contactable via the following e-mail address privacy@forestali.it.

2. Processing purpose and legal basis

Personal data are processed for the purpose of effectively managing internal reports of alleged breaches, i.e. of conduct, acts or omissions considered to be contrary to the public interest or detrimental to the integrity of the public administrative body or private entity, as defined by art. 2(1)(a) of Legislative Decree No. 24/23, which the whistleblower became aware of by virtue of their relationship with the Controller. The personal data processed are those relating to the whistleblower which are contained in the internal report, and/or in the records and documents associated with it.

The personal data may also be processed for the purpose of conducting the necessary investigations aimed at verifying the grounds for the reported breaches, as well as, where appropriate, for the adoption of suitable corrective measures and the imposition of appropriate disciplinary and/or judicial measures against the persons responsible for the breaches. The legal basis that legitimises the processing of personal data derives from the requirement on the Controller to fulfil its legal obligations (art. 6(1)(c) of the GDPR), as set forth by Legislative Decree No. 165/2001, Legislative Decree No. 231, Legislative Decree No. 179/2017 and Legislative Decree No. 24/2023; the processing may also concern special categories of personal data as well as data relating to criminal convictions and the offences detailed within the reports, pursuant to the provisions of articles 9(2)(b) and 10 of the GDPR.

3. Categories of personal data processed

To accomplish the aforementioned purposes, the Controller shall process the following categories of personal data:

- general personal data such as first name, surname, job position, etc. (art. 4(1) of the GDPR);
- special categories of personal data, as provided for by article 9 of the GDPR, processed, where applicable, in relation to the content of the reports and/or the records and documents accompanying to them;
- personal data relating to criminal convictions and offences (as per art. 10 of the GDPR) processed, where appropriate, in relation to the content of the reports and/or the records and documents accompanying to them.

4. Categories of data recipients

The personal data provided shall be processed by the members of the Supervisory Body (SB), as persons authorised to process such data by the Controller, for the purposes of managing the reporting channel and following up and responding to the reports received, in accordance with the provisions of Legislative Decree No. 24/2023 and the Organisational, Management and Control Model pursuant to article 6 of Legislative Decree No. 231.

The data shall not be communicated to any other parties, however, it may be transmitted to the judicial authorities, if necessary. The data collected shall not be communicated to third countries, defined as countries not belonging to the European Economic Area (EEA). If the report is submitted externally and is sent, as per articles 6 and 7 of Legislative Decree No. 24/2023, to ANAC (Italian National Anti-Corruption Authority), information relating to the processing of personal data shall be provided by the Authority itself through the appropriate channels.

5. Storage period criteria

Pursuant to the confidentiality obligations set forth by article 12 of Legislative Decree No. 24/2023 and the principle set forth by article 5(1)(e) of the GDPR and article 3(1)(e) of Legislative Decree No. 51 of 2018, any internal reports received shall be stored for as long as is necessary for them to be processed and, in any case, for a period not exceeding five years from the date that the final outcome of the subsequent procedure is communicated.

6. Data processing methods

The personal data shall only be processed by members of the SB, either electronically or manually, and only for the purpose in relation to which the data were collected so as to guarantee that the identity of the whistleblower, the report's contents and that of any relevant documentation remain confidential, adopting appropriate technical and organisational measures to safeguard the data against unauthorised or unlawful access, destruction, loss of integrity and confidentiality, even accidental. To guarantee that the identity of the whistleblower remains confidential throughout the entire duration of the report management process, their identity shall be known only to the members of the SB. The identity of the whistleblower shall always be protected following the submission of the report, however, the confidentiality of their identity is not guaranteed in cases where they are proven, in accordance with the provisions of the Italian Criminal Code or with article 2043 of the Italian Civil Code, to be liable for slander or defamation, or where knowledge of their identity is essential for the person involved to be able to build a case for their defence. Therefore, aside from the aforementioned exceptions, the identity of the whistleblower may not be disclosed without their express consent, and all those receiving the report, or who are involved in its management, are obliged to safeguard the confidentiality of that information.

7. Provision of data

The provision of personal data is entirely optional. However, failure to provide such information may undermine the investigation into the report: anonymous reports will only be considered and progressed if they are adequately substantiated and provided in sufficient detail to fully describe the facts and evidence of the case.

8. Rights of Data Subjects

The rights set forth in articles 15-22 of the GDPR may be exercised, within the limits of the provisions of article 2-*undecies*(3) of Legislative Decree No. 196/2003, by contacting the Controller via the aforementioned contact details. Pursuant to art. 2-*undecies*(3)(f) of Legislative Decree No. 196/2003, the aforementioned rights may not be exercised through a request to the Controller, or by lodging a complaint, pursuant to article 77 of the GDPR, with the Data Protection Authority, if exercising such rights may genuinely jeopardise the confidentiality of the whistleblower's identity. Exercising such rights may, in any case, be delayed, limited or excluded by means of an immediate notification from the Controller explaining the detailed reasons, unless such a notification may compromise the purpose of the limitation, for a period and to the extent that this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the whistleblower, the person involved or the other persons cited in the report. In such cases, pursuant to article 2-*undecies*(3) of Legislative Decree No. 196/2003, the Data Subject is entitled to exercise the aforementioned rights via the Data Protection Authority using the approach set forth by article 160 of the aforementioned Legislative Decree. In cases where it is considered that the processing of personal data infringes the provisions set forth by the GDPR, a complaint may be lodged with the Data Protection Authority, as provided for by art. 77 of the GDPR itself (with the exclusion of the limitations provided for in art. 2-*undecies*(3) of Legislative Decree No. 196/2003), or legal action may be initiated (art. 79 of the GDPR).