WHISTLEBLOWING POLICY PINK FROGS COSMETICS Srl

PINK FROGS COSMETICS Srl
Registered Office in Rozzano (MI), Viale Toscana 46, CAP 20089

Premise and background

With Legislative Decree 24/2023, implementing EU Directive 2019/1937, the legislator approved regulations for the protection of persons who report violations of national or European Union rules that harm the public interest or the integrity of public or private entities, which they have become aware of in a public or private work context.

The aforementioned Decree, which provides specific regulations for the protection of whistleblowers, aims to encourage cooperation among workers and, in general, among the collaborators of entities (as better identified below) to promote, within public and private entities, the disclosure of acts or phenomena that are in conflict with European and national legislation.

The new regulations establish, on the one hand, the obligation for companies falling within its scope (e.g., those that have employed at least 50 employees during the last year) to set up an internal reporting channel that provides adequate guarantees of confidentiality and security and, on the other hand, the guarantee of protection for whistleblowers through the prohibition of retaliation and the imposition of specific penalties in the event of violation of the regulations.

In addition, the same protection is provided for those who, under certain conditions – which will be explained below – report violations through the external reporting channel established by the National Anti-Corruption Authority (ANAC) or for those who make public disclosures and reports to the judicial and accounting authorities.

1. Purpose of the Whistleblowing Policy

In accordance with the aforementioned legislation, Pink Frogs Cosmetics Srl (hereinafter also referred to as the "**Company**") has adopted its own internal reporting channel described in this procedure (hereinafter also referred to as the "**Policy**") which guarantees, including through encryption tools, the confidentiality of the identity of the reporting person, the person involved and any person mentioned in the report, as well as the content of the report and related documentation.

With this Policy, the Company, in accordance with the provisions of Article 5, paragraph 1, letter e) of Legislative Decree 24/2023, provides clear information on the aforementioned channel, on the procedures and requirements for making internal reports, as well as, in paragraphs 15 and 16 below, on the channel, procedures, and requirements for making external reports.

This Policy will be displayed on notice boards in the workplace and, in order to be easily visible, will be published in a specific section of the Company's website, so that it is also accessible to persons who, although not frequenting the workplace, fall within the categories of possible whistleblowers, summarized below.

With this Policy and the adoption of the internal reporting channel, the Company not only implements tools to prevent possible illegal conduct, but also intends to promote a corporate culture of combating illegality through the active and responsible participation of all employees and third parties.

2. Persons who can make reports

2.1. The Company encourages its employees and third parties to promptly report any behavior that constitutes or may constitute unlawful conduct and/or a violation of the law that damages the integrity of the Company, which they have become aware of in the context of their work.

In accordance and compliance with the provisions of Legislative Decree 24/2023, the following persons may make a report ("**Whistleblowers**")

- All Company personnel, including part-time, intermittent, fixed-term, temporary, or apprentice workers, or those who perform occasional services
- Self-employed workers who carry out their work at the Company
- Workers or collaborators who carry out their activities at the Company and who supply goods or services or perform work on behalf of third parties
- Holders of agency, commercial representation, and other collaborative relationships with the Company that result in the provision of continuous and coordinated work, mainly personal, even if not of a subordinate nature
- Freelancers and consultants who work for the Company
- Volunteers and interns, paid and unpaid, who work for the Company
- Shareholders and persons with administrative, management, control, supervisory, or representative functions within the Company, even if such functions are exercised on a de facto basis.

2.2. Reports may also concern known facts:

a) prior to the establishment of the employment relationship, during the selection process or in other pre-contractual phases;
b) during the probationary period;
c) after the termination of the legal relationship if the information on the violations was acquired during the relationship itself.

2.3. It should be noted that, in accordance with the provisions of Legislative Decree 24/2023, the protection provided for whistleblowers by this legislation, as described in letter b) of paragraph 13 below, also applies to the following persons:

i. facilitators, meaning natural persons who assist a Whistleblower in the reporting process, operating within the same working environment and whose assistance must be kept confidential
ii. persons in the same working environment as the Whistleblower and who are linked to them by a stable emotional bond or kinship within the fourth degree
iii. the Whistleblower's colleagues who work in the same work environment as the Whistleblower and who have a regular and ongoing relationship with that person
iv. the entities owned by the Whistleblower for which the Whistleblower works, as well as entities operating in the same work environment as the Whistleblower

3. Subject matter of the Reports

3.1. The protective measures provided for by law and described in letter b) of paragraph 13 of this Policy apply to Whistleblowers and the persons indicated in paragraph 2.3 of this Policy if, at the time of reporting, the Whistleblower had reasonable grounds to believe that the information on the reported violations was true and fell within the objective scope of the whistleblowing legislation referred to in this Policy in paragraph 3.

Therefore, mere assumptions or rumors, as well as information in the public domain, are not sufficient.

The information on violations to be reported may concern both violations that have been committed, including well-founded suspicions, and those that have not yet been committed but which the Whistleblower

reasonably believes could be committed on the basis of concrete evidence. Elements concerning conduct aimed at concealing violations may also be reported.

It should also be noted that reportable violations must be capable of damaging the integrity of the Company and must be learned by the Whistleblower in the context of their work, understood in a broad sense and therefore also including the subjects indicated in paragraph 2.1 above.

3.2. The Company must be notified of any violations of specific national and European Union regulations identified by Legislative Decree 24/2023 and summarized below.
In particular, within the Company, taking into account its organizational and governance structure and in line with the guidelines contained in the Operational Guide adopted by Confindustria, the following violations may be reported (hereinafter, "Reporting"):

a) Offenses committed in violation of the EU regulations indicated in Annex 1 to Legislative Decree No. 24/2023 and all national provisions implementing them (even if the latter are not expressly listed in the aforementioned annex). In particular, these are offenses relating to the following sectors:
   i. public contracts;
   ii. financial services, products, and markets, and the prevention of money laundering and terrorist financing;
   iii. product safety and compliance;
   iv. transport safety;
   v. environmental protection;
   vi. radiation protection and nuclear safety;
   vii. food and feed safety, and animal health and welfare;
   viii. public health;
   ix. consumer protection;
   x. protection of privacy and personal data and security of networks and information systems.
b) Acts or omissions affecting the financial interests of the European Union (Article 325 TFEU combating fraud and illegal activities affecting the EU's financial interests) as identified in EU regulations, directives, decisions, recommendations, and opinions.
c) Acts or omissions relating to the internal market, which undermine the free movement of goods, persons, services, and capital (Article 26(2) TFEU). This includes violations of EU rules on competition and state aid, corporate tax, and mechanisms designed to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax legislation.
d) Acts or conduct that defeat the object or purpose of EU provisions in the areas indicated in the previous points;
e) Conduct that violates the requirements of the Code of Ethics and Code of Conduct for Pink Frogs Cosmetics suppliers.

4. Facts that CANNOT be reported

The following circumstances are excluded from the scope of this Policy and therefore CANNOT be reported:

a) complaints, claims, or requests related to the personal interests of the whistleblower that pertain exclusively to their individual employment relationships, or that relate to their working relationships with their superiors, or that concern data processing carried out in the context of an individual employment relationship without harming the integrity of the Company. Therefore, reports concerning labor disputes, discrimination among colleagues, interpersonal conflicts between the reporting person and another worker are excluded.
b) reports of violations that are already subject to mandatory specific regulations indicated by Legislative Decree 24/2023 and which therefore do not fall within the scope of application of the latter decree (e.g., the banking and financial intermediation sector)
c) reports of violations relating to national security, as well as contracts relating to aspects of defense or national security.

5. Elements to be included in the Report

The Company invites Whistleblowers to make Reports that are as detailed as possible so as to provide useful and appropriate information to enable an appropriate investigation into the validity of the facts reported. It is particularly important that the report includes, where such information is known to the Whistleblower:

- the circumstances of time and place in which the event reported occurred
- a description of the event
- the personal details or other information that allows the person to whom the reported facts are attributed to be identified.

These elements are also relevant for the purposes of assessing the admissibility of the Report, as explained in paragraph 10 of this Policy.

It is also useful to attach documents that can provide evidence of the validity of the facts reported, as well as the names of other persons who may be aware of the facts.

6. Channels for submitting reports

Reports can be filed in various ways, as described in the following paragraphs of this Policy and briefly summarized below:

a) electronically, through a dedicated portal provided by the Company and accessible at the following link https://pinkfrogs.it/whistleblowing/

b) verbally, by calling the following dedicated telephone line 028257820 ext. 113;

c) through a direct meeting with the Managers (as identified below), at the request of the Whistleblower.

7. The Channel in electronic form: The Whistleblowing Portal

7.1. The Company has adopted its own internal reporting channel, primarily by providing an online platform for the electronic submission of whistleblowing reports (hereinafter referred to as the "Portal"), which guarantees, including through encryption tools, the confidentiality of the identity of the whistleblower, the person involved, and any other person mentioned in the report, as well as the content of the report and related documentation.

The Portal can always be accessed via the following link https://pinkfrogs.it/whistleblowing/, which is also published on the Company's website, in the section dedicated to whistleblowing reports.

In any case, the Policy and the link to access the Portal for submitting Reports will always be available in the dedicated section of the Company's website at the following link: https://pinkfrogs.it/whistleblowing/

7.2. The Whistleblower may submit Reports using the features available on the Portal and described below, which, in compliance with the prescribed confidentiality requirements, allow Reports to be submitted electronically via the Portal itself.

Access to the Portal is subject to a "no-log" policy in order to prevent the identification of Whistleblowers who wish to remain anonymous. This means that the Portal's architecture does not allow tracking through access logs to the application, in order to protect the confidentiality of Whistleblowers' identities even when using the company network.

The Company recommends sending a Report by providing your contact details in order to allow the Report Managers (as identified below) to obtain any further information and thus carry out the investigation in a productive manner.
In any case, anonymous reports, if deemed admissible, will be handled by the Company in the same way as whistleblowing reports in accordance with the procedure described in this Policy, as far as compatible. Anonymous whistleblowers, therefore, if subsequently identified, will be guaranteed the protection and safeguards provided for by whistleblowing legislation and referred to in this Policy.

7.3. In order to file a Report through the Portal, the Whistleblower, subject to disclosure pursuant to Article 13 GDPR, must register with the Portal and create his or her own personal area. The Reporter is assigned a unique user profile with confidential authentication credentials (User ID and password) according to security standards in accordance with industry best practices. In any case, the architecture of the Portal does not allow direct access to registration data by management functions.

On his or her personal page, the Whistleblower will be able to view the status of the reports submitted, depending on the progress of the report management process. In order to create a new Report, the Reporter will be able to click on the appropriate "Create Report" button and, through the Portal, will be guided through each step of the Report creation process and will be asked, in order to better circumstantiate the Report, a series of fields to be filled in respecting the requirements.

Specifically, the first page of the reporting process will open, which requires the whistleblower's information to be provided. The latter may choose to remain anonymous by checking the appropriate box. On subsequent screens, the Whistleblower will be asked to better substantiate the facts by filling in certain fields, such as: the company where the event occurred (e.g., at a supplier), the date, place and author of the facts, and the company function to which the facts refer. The Whistleblower must also provide a brief description of the reported facts, may attach documents and indicate from a drop-down menu the type of violation to which the Report refers. Finally, prior to sending the Report, the Whistleblower will be asked to indicate an email to receive notifications on the status of their Report. These notifications will not contain any data related to the Report but will inform the Whistleblower of the progress of the Report. To view the contents of the progress, the Whistleblower will need to access the Portal.

The Company requests that the company e-mail address not be used for such notifications, although the e-mail address indicated on the Portal by the Whistleblower is not visible to Managers anyway.

The Portal also allows for the establishment of a secure communication between Whistleblower and recipient ensuring, at the Whistleblower's will, anonymity.

8. Channel in oral form

a) telephone line

Whistleblowings may be submitted by telephone by calling the following dedicated telephone line:

02 8257820 int 113

Managers (as identified below) are obliged to document the oral Whistleblowing Report by means of a detailed written account of the conversation bearing the date of the conversation and their own signature.

The Whistleblower, at the beginning of the meeting, will be referred to the privacy policy always available as an attachment to the Whistleblowing Policy.

b) face-to-face meeting

When, at the request of the Whistleblower, the Report is made orally in the course of a meeting with the Managers (as identified below), it shall, with the consent of the Whistleblower, be documented by the Managers themselves by means of a transcript that the Whistleblower may verify, rectify, and confirm by signing. The minutes will also be signed by the Managers. The Whistleblower will be given the privacy notice at the beginning of the meeting. The notice is in any case always available as an attachment to the Whistleblowing Policy.

9. Reporting Managers

The Company has adopted the following method of handling Reports, taking into account the articulation of the corporate organization.

9.1. Reports sent through the Portal are received exclusively by a Manager designated within the organization and specifically trained by the Company, both on whistleblowing and with regard to the related privacy implications, and authorized by the Company itself to manage the channel and the Reports. The Company ensures that this person (hereinafter "Manager") operates autonomously and with guarantees of independence in the performance of these duties.

The aforementioned Manager has been identified as the Head of the Sustainability function.

In the event that situations, even if only potential, of conflict of interest should arise at the time of receipt of the Report by the Manager, the management of the Report will be the responsibility of another Manager identified in the Company Director, who is also specifically trained and authorized as of now by the Company to manage Reports in these specific cases.

Therefore, the Company, by this Policy, requires all possible Whistleblowers to direct the Report to the Administrator if they have a well-founded suspicion that there is a conflict of interest situation involving the Manager identified in the Sustainability Manager.

The same individuals indicated above are also responsible for receiving and handling Reports sent by voice message or by meeting in person.

In any case, the Internal Reporting submitted to a person other than those indicated above shall be transmitted, within seven days of its receipt, to the appropriate person, giving simultaneous notice of the transmission to the Whistleblower.

The Company, by this Policy, hereby requires all its personnel to immediately transmit to the aforementioned Manager and in strict confidentiality any Report they may erroneously receive.

All Company personnel shall also receive specific training in order to ensure compliance with this requirement.

9.2. In carrying out its management activities, each Manager:

(a) issues notice of receipt of the Whistleblower within seven days from the date of receipt;
(b) maintains contact with the Whistleblower and may request additions from the Whistleblower, if necessary;
(c) diligently follows up on the Reports received;
(d) provide acknowledgement of the Report within three months from the date of the notice of receipt or, in the absence of such notice, within three months from the expiration of the period of seven days from the submission of the Report.

The Managers are also responsible for providing information on the use of the Internal Whistleblowing channel, the procedures and prerequisites for making internal whistleblowing reports as described in this Policy, as well as, also by referring to the provisions of Sections 15 and 16 below, for providing information on the channel, procedures and prerequisites for making external whistleblowing reports.

It is also reiterated that any anonymous report, if deemed admissible, will be handled by the Company in the same way as a whistleblowing report according to the procedure described in this Policy, insofar as compatible. The anonymous Whistleblower, therefore, if subsequently identified, will be guaranteed the safeguards and protection measures provided by the whistleblowing regulations and referred to in this Policy.

10. Preliminary Examination of the Report

a) *verification of proceeding of the Report*

Upon receipt of the Report, the Manager, as identified above, preliminarily proceeds to verify the existence of the subjective and objective conditions for making an internal report. At the outcome of this preliminary screening, where none of the above conditions are met, the Manager shall dismiss the Report as unfeasible.

b) *verification of the admissibility of the Report*
Once it has been verified that the report has the subjective and objective requirements defined by the legislature and is therefore procedural, it is necessary to verify its admissibility as a whistleblowing report.
It should be noted that the Report must clearly indicate the circumstances of time and place in which the fact being reported occurred, a clear and circumstantiated description of the facts, personal details or other elements that make it possible to identify the person to whom the reported facts are attributed.

The Report is considered inadmissible and is dismissed for the following reasons:

a) generic content of the Report such that it does not allow understanding of the facts or report of wrongdoing accompanied by inappropriate or irrelevant documentation
b) lack of data constituting the essential elements of the report
c) manifest groundlessness of the facts constituting the essential elements of the report
d) production of only documentation in the absence of the Report of Illicit Conduct.

If what is reported is not adequately substantiated, the Manager may request additional elements from the Whistleblower through the Portal's secure communication system, or even in person if the Whistleblower has requested a face-to-face meeting.

At the outcome of this preliminary screening, if the Report is found to be inadmissible or inadmissible, the Manager will file the Report, ensuring the traceability of the supporting reasons.

11. Investigation and fact-finding

Once the admissibility of the Whistleblower has been assessed, the individuals entrusted with the management of the reporting channel will initiate the internal investigation of the reported facts or conduct to assess the existence thereof.

Investigation activities during the course of the inquiry will be carried out in compliance with the obligation of confidentiality of the identity of the Whistleblower and other protected persons and ensuring timeliness and compliance with the principles of objectivity, competence and professional diligence.

The Manager must ensure that the necessary verifications are carried out, always taking care that the confidentiality of the Whistleblower, the reported person, and other persons protected by the regulations (e.g., facilitators and persons mentioned in the report) is not compromised, by, for example:

- directly acquiring the information elements necessary for the assessments through the analysis of the documentation/information received;
- through the involvement of other company structures or even external specialized individuals (e.g., IT specialist) in view of the specific technical and professional skills required;
- hearing from any internal/external parties, etc.

In the event that it is necessary to make use of the technical assistance of third-party professionals, as well as the support of personnel from other company functions/departments - in order to guarantee the confidentiality obligations required by the regulations - the Manager shall ensure that any type of data that could allow the identification of the Whistleblower or any other person involved (e.g., facilitator or additional persons mentioned within the report) is obscured.

Upon completion of the investigation, the Manager shall prepare a final report containing at least:

- the facts established;
- the evidence gathered;
- the causes and deficiencies that allowed the occurrence of the reported situation.

In the event that the Report is found to be well-founded, the Manager - always in compliance with the confidentiality obligations established in this policy - activates the relevant company managers to take the due and most appropriate mitigating and/or corrective actions.

In addition, in the event of a well-founded report, the Manager forwards the outcome of the investigation to the competent function for the possible initiation of disciplinary proceedings aimed at imposing, where appropriate, disciplinary sanctions in line with the provisions of the applicable regulations and the reference collective labor agreements, as well as to the company management for the appropriate evaluations regarding any further action to be taken also for the protection of the Company.

The stages of the investigation activity are properly tracked and archived depending on the type of reporting channel used (for example, if the Portal was used, the documentation will be archived within it according to the security measures adopted therein and, if the minutes of the hearing of the in-person meeting were drawn up, they will be archived within a folder accessible only to Managers).

In any case, in accordance with the provisions of Legislative Decree 24/2023, during the investigation and investigation phases of the Whistleblower, the identity of the Whistleblower, the reported person, and all persons involved and/or mentioned in the Whistleblowing is always protected.

12. Feedback to the Whistleblower

At the outcome of the preliminary investigation, and in any case within the aforementioned period of 3 (three) months, the Manager shall provide feedback to the Whistleblower regarding the action taken or intended to be taken on the Report, giving an account of the action taken to assess the existence of the facts reported, the outcome of the investigation and any measures taken or to be taken.

At the expiration of the aforementioned specified time limit, the feedback may be final if the investigation has been completed or of an interlocutory nature on the progress of the investigation, if the investigation, due to, for example, the complexity of the case, has not yet been completed.

Therefore, at the expiration of three months, the Manager may notify the Whistleblower:

- the fact that the report has been dismissed, giving reasons;
- the fact that the merits of the report have been ascertained and forwarded to the competent internal bodies;
- the activity carried out so far and/or the activity it intends to carry out if the investigation is not yet completed.

In the latter case, the Manager will in any case also inform the Whistleblower of the subsequent final outcome of the investigation of the Report (archiving or ascertainment of the merits of the report with transmission to the competent bodies).

13. Whistleblower Protection

The first protection placed by the legislator in favor of the Whistleblower is the obligation to ensure the confidentiality of the Whistleblower's identity from the moment the Report is received and at every stage thereafter.

In addition, the legislation prohibits any form of retaliation against the Whistleblower understood as any behavior, act or omission, even if only attempted or threatened, that occurs in the work context and that determines - directly or indirectly - an unfair damage to the protected subjects.

To this end, in accordance with current regulations, the Company has established a series of mechanisms aimed at the protection of the non-anonymous Whistleblower, providing:

a. the protection of the confidentiality of the Whistleblower's identity
b. the prohibition of retaliation against the Whistleblower

Finally, further protection granted by Legislative Decree 24/2023 to the Whistleblower is the limitation of his or her responsibility with respect to the disclosure and dissemination of certain categories of information, which would otherwise expose him or her to criminal, civil and administrative liability.

a) Duty of confidentiality

Confidentiality is guaranteed for every mode of reporting, therefore, whether it is through the Portal or via voice message or face-to-face meeting.

In fact, the Manager is specially instructed to maintain the confidentiality of both the identity of the Whistleblower, the content of the Report and related documentation, and the identity of the Whistleblower and any persons mentioned in the Report.

The Portal also ensures the confidentiality of the Whistleblower's identity through encryption tools, both in transit and at rest. Credentials assigned to users (both Whistleblowers and Managers) are unique and confidential and comply with the security requirements of industry best practices. Only the Manager can access the content of the Reporting person.

The identity of the Whistleblower and any other information from which such identity may be inferred, directly or indirectly, will not be disclosed without the express consent of the Whistleblower himself/herself, to persons other than the Manager, competent to receive or follow up on the Reports, expressly authorized and instructed to process such data in accordance with Articles 29 and 32(4) of Regulation (EU) 2016/679 (GDPR) and Article 2-quaterdecies of the Code on the Protection of Personal Data under Legislative Decree No. 196 of June 30, 2003.

Within the scope of disciplinary proceedings, the identity of the Whistleblower person may not be disclosed, where the contestation of the disciplinary charge is based on separate findings additional to the Report, even if consequent to the Report.

If the charge is based, in whole or in part, on the Whistleblower and the knowledge of the identity of the Whistleblower is essential for the defense of the accused, the Whistleblower will be usable for the purposes of disciplinary proceedings only in the presence of the express consent of the Whistleblower to the disclosure of his/her identity.

Similarly, in the event that in internal reporting procedures the disclosure of the identity of the Whistleblower is also indispensable for the defense of the person implicated, the identity of the Whistleblower may be disclosed only upon obtaining the express consent of the Whistleblower.

In both of the aforementioned cases, in addition to the acquisition of the Whistleblower's consent, the Whistleblower will still be given notice in writing of the reasons for the disclosure of confidential data.

The Company shall protect the identity of the persons involved (the Whistleblowers) and the persons in any case mentioned in the report until the conclusion of the proceedings initiated because of the Report in compliance with the same guarantees provided in favor of the Whistleblower. This is without prejudice to the Company's right to report the facts before the Judicial Authority.

b) Prohibition of retaliation

The Company ensures the Whistleblower protection against any act of harassment, retaliation, or discrimination for reasons related, directly or indirectly, to the Report made in good faith. Any act of

retaliation or discrimination against both the Whistleblower and the persons indicated in Section 2.3. of this Policy above (e.g., facilitators) is prohibited.

Retaliation is defined as any conduct, act or omission, even if only attempted or threatened, carried out by reason of the report, and which causes or may cause the Whistleblower, directly or indirectly, unfair harm.

Acts of retaliation resulting from a Report are in any case null and void.

The protection provided by the regulations and reported in this paragraph also applies to anonymous Whistleblowers, if the Whistleblower is subsequently identified and retaliated against.

If the Whistleblower's criminal liability for the offenses of defamation or slander or his civil liability, for the same title, in cases of malicious intent or gross negligence, is established, even by a judgment of first instance, the protections set forth in this letter b) are not guaranteed and a disciplinary sanction is imposed on the Whistleblower.

Whistleblowers and persons indicated in Section 2.3. above of this Policy may notify ANAC of retaliation they believe they have suffered.

Therefore, a person who believes that he or she has suffered retaliation, even attempted or threatened retaliation, as a result of a report may communicate this to ANAC, which will have to ascertain the causal link between the retaliation and the report and, therefore, take the consequent measures.

In particular, if the Authority considers the communication inadmissible, it will archive it; if, on the other hand, it should ascertain its validity and the causal link between reporting and retaliation it will initiate the sanctioning procedure.

The ANAC will inform the National Labor Inspectorate for measures within its jurisdiction.

There are cases in which the Whistleblower loses protection: i) if the Whistleblower's criminal liability for the offenses of defamation or slander is established, even by a judgment of first instance, or if such offenses are committed by reporting to the judicial or accounting authorities; ii) in case of civil liability for the same title due to malice or gross negligence. In both cases a disciplinary sanction will be imposed on the Whistleblower or whistleblower.

c) Limitation of liability for the Whistleblower

Pursuant to Legislative Decree 24/2023, the Whistleblower will not be held criminally, civilly or administratively liable for the following cases:

- disclosure of information on violations covered by secrecy other than forensic and medical professional secrecy and other types of secrecy provided for in Article 1, paragraph 3 of Legislative Decree 24/2023;
- Violation of the provisions on copyright protection;
- violation of the provisions on the protection of personal data;
- disclosure or dissemination of information on violations that offend the reputation of the person involved.

However, Legislative Decree 24/2023 places two conditions on the operation of the above limitations of liability:

1) that at the time of the disclosure or dissemination there are reasonable grounds to believe that the information is necessary to disclose the reported violation;

2) that the report is made in compliance with the conditions provided by Legislative Decree 24/2023 to benefit from the protection against retaliation (reasonable grounds to believe that the reported facts are true, the violation is among those that can be reported and the terms and conditions of access to the report are complied with).

I in any case, it should be considered that liability is not excluded for conduct that:

- are not related to the reporting;
- are not strictly necessary to disclose the violation;
- configure an unlawful acquisition of information or access to documents

Where the acquisition takes the form of a crime (think of abusive access to a computer system or an act of hacking), the criminal liability and any other civil, administrative and disciplinary liability of the Whistleblower remains unaffected.

Conversely, it will be non-punishable, for example, the extraction (for copying, photography, removal) of documents to which one had lawful access.

14. Data Processing and Storage of Reports

The processing of the personal data of the persons concerned (Whistleblowers, persons mentioned in paragraph 2.3 of this Policy above, person involved, persons mentioned in the Whistleblowing) for the purpose of managing the Whistleblowing is carried out by the Company, as Data Controller, in accordance with Regulation 679/2016 (GDPR) and for the sole purpose of managing and following up the Whistleblowing.

The processing is necessary in order to implement the legal obligations provided for by the whistleblowing regulations set out in Legislative Decree 24/2023, compliance with which is a condition for the lawfulness of the processing pursuant to Articles 6(1)(c) and (2) and (3), 9(2)(b) and Articles 10 and 88 of the GDPR.

The processing will be conducted in accordance with the principle of minimisation and, therefore, personal data that are manifestly not useful for the processing of a specific Report are not collected or, if accidentally collected, are deleted immediately.

The processing of personal data relating to the receipt and management of Reports will be carried out, pursuant to Article 4 of Legislative Decree 24/2023, exclusively by the Committee of Managers, as parties expressly authorised and instructed by the Data Controller for the management of the reporting channel pursuant to Article 29 of the GDPR, in compliance with the principles set out in Articles 5 and 25 of the GDPR.

The Company has also carried out a data protection impact assessment with reference to the processing operations connected to the management of the Reports, and has therefore identified technical and organisational measures suitable to guarantee a level of security appropriate to the specific risks arising from the processing carried out in this context.

Furthermore, the Company has regulated the relationship with the provider of the IT portal pursuant to Article 28 of the GDPR.

The Reports and the related documentation are kept for the time necessary for the processing of the Report and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure, in compliance with the aforementioned confidentiality obligations and the principle set out in Article 5(1)(e) of Regulation (EU) 2016/679.

For further details regarding the processing of data, please refer to the full privacy policy, published for all data subjects (including the reported person) on the Portal and available as an annex to this Policy and then disseminated to the recipients together with this Policy.

In any case, the privacy policy is always available on the Portal, as well as provided to the Whistleblower, on the Portal itself, at the time of registration and at the end of the process for sending each Report.

15. Information on the external reporting channel established at ANAC

ANAC has activated an external reporting channel that guarantees, through the use of encryption tools, the confidentiality of the identity of the reporter, the person involved and the person mentioned in the report, as well as the content of the report and the related documentation.
External Reports must be transmitted only to ANAC as the only body competent to handle them. The IT platform for sending external Reports to ANAC is available at the following link https://www.anticorruzione.it/-/whistleblowing.

16. Conditions for External Reporting

The Whistleblower may make an External Report if, at the time of its submission, one of the following conditions is met

a. the mandatory activation of the internal reporting channel is not envisaged within his/her work context, or this channel, even if mandatory, is not active or, even if activated, does not comply with the legislation;
b. the Whistleblower has already made an internal report in the manner set out in this Policy, and the report has not been followed up;
c. the Whistleblower has well-founded reasons to believe that, if he/she were to make an internal report, it would not be effectively followed up, or that the same report could give rise to the risk of retaliation
d. the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

17. Training and Communication

Training and communication are fundamental elements for the effective implementation and application of the Policy. In this regard, the Company undertakes to ensure that the Whistleblower is made aware of the provisions included in the Policy and to provide its staff with training programmes concerning the whistleblowing legislation, confidentiality obligations and this Policy, including the procedures and operating methods adopted by the Company to manage the internal whistleblowing channel for all employees.

This Policy shall in any event be published on the Company's website and available at the following link https://pinkfrogs.it/whistleblowing/.

18. Policy Update

The Policy and the Portal will be periodically updated in order to ensure constant alignment with regulations and due to the evolution of the company's operations and organisation.

Pieve Emanuele, 26/05/2025

Matteo Locatelli – Legal Representative

Attachment:

- Privacy policy pursuant to Articles 13 and 14 of EU Regulation 679/2016 (GDPR)