Procedure for reports managment

ICAM S.p.A.

Date: 28th June 2024

Subject: Guidelines for the processing and management of Whistleblowing

Index

1 Document sheet

Document type	Procedure	
Year of first issue	2024	
Scope of application	ICAM S.p.A.	
Drafted by	External consultant	
Validated by	ICAM S.p.A. Legal Dept.	
Approved by	Board of Directors	
Issue (Publication)	28.06.2024	
Related documentation	Organization, management and control Model under Legislative Decree 231/2001 and Ethical Code	
Regulatory Sources	Law n.179/2017	
	Legislative Decree No. 24 of 2023, Implementation of Directive (EU) 2019/1937 on the protection of individuals reporting breaches of Union law, and containing provisions for the protection of individuals reporting breaches of national legal provisions	
	European Regulation 679/2016 on the protection of personal data (General Data Protection Regulation - "GDPR")	
Revision No.	**Main changes**	**Date**
1.0	Adaptation to the provisions of Legislative Decree 24 of March 10, 2023, "*Implementation of Directive (EU) 2019/1937*"	2024

2 Introduction

ICAM S.p.A. (hereinafter also referred to as "the Company") carries out its activities in compliance with external and internal laws, regulations and standards, including both national and international guidelines and *standards*.
The Company aims to promote the dissemination of a corporate culture based on legality, characterized by correct behavior and a strong system of *corporate governance*, thus defining appropriate tools aimed at preventing, detecting and communicating illegal conduct and/or conduct that violates ethical principles.
In particular, the Company has developed over time corporate protocols and control mechanisms aimed at eliminating or minimizing the risk of committing crimes and violations in the execution of activities that are potentially more exposed to the manifestation of unlawful behaviors.
In this context, in order to strengthen its organizational and governance system (as well as to comply with specific legal obligations in force), the Company has defined a process for receiving and managing reports regarding acts and/or facts that are potentially contrary to the law and internal company regulations, by anyone who, within the scope of the work activities carried out at the Company, becomes aware of them.

3 Objectives and general criteria

The purpose of this Procedure is to regulate the process for managing Reports that are brought to the Company's attention according to the methods described below, in relation to facts or circumstances that are useful for verifying potential violations.
Reports received and qualifying as "Whistleblowing Reports" will be processed in terms of receipt, analysis and processing in accordance with the legal provisions of Legislative Decree 24 of March 10, 2023 (hereinafter also referred to as the "Decree"), containing "*Implementation of the Directive (EU) 2019/1937 of the European Parliament and the Council dated October 23, 2019, on the protection of persons who report breaches of Union law and containing provisions on the protection of persons reporting breaches of national law provisions.*"
Reports that do not fall within the scope of "Whistleblowing Reports" in terms of objective or subjective matter, or reports on topics other than those specified in paragraph 5.2, or those received from individuals other than those indicated in paragraph 5.3 of this Procedure, will be classified as "Ordinary Reports." These reports do not fall within the scope of the obligations and protections outlined in the Decree; however, they will still be managed ensuring the confidentiality of the Whistleblower's identity, in compliance with the provisions of the 231 Model and this Procedure.

4 Definitions

For the purposes of this Procedure, in accordance with the provisions of the Decree, the following definitions are understood as follows:

a) "violation": behaviors, acts, or omissions that harm public interest or the integrity of the private entity;

b) "information on violations": information, including well-founded suspicions, related to breaches that have been committed or may, based on concrete elements, be committed within the organization with which the Whistleblower has a legal relationship, as per Article 3, paragraph 1 of the Decree, as well as information regarding conduct aimed at concealing such breaches;

c) "report": the written or oral communication of information on violations within the scope of this Procedure;

d) "internal report": the written or oral communication of information on violations submitted through the internal reporting channel referred to in Article 4 of the Decree;

e) "external report": the written or oral communication of information on violations submitted through the external reporting channel activated by the ANAC;

f) "public disclosure" or "disclose publicly": making information on violations publicly available through the press, electronic media, or other means of communication capable of reaching a large audience;

g) "whistleblower": the individual who makes a report or publicly discloses information about violations acquired in the context of their work environment;

h) "facilitator": an individual who assists a Whistleblower in the reporting process, working within the same work environment, and whose assistance must remain confidential;

i) "work environment": the current or past work or professional activities carried out as part of relationships referred to in Article 3, paragraphs 3 or 4 of the Decree, through which, regardless of the nature of such activities, an individual acquires information about violations and in which they could risk retaliation in case of reporting, public disclosure, or reporting to judicial or accounting authorities;

l) "involved person": the natural or legal person mentioned in the internal or external report or public disclosure as the person to whom the violation is attributed, or as a person otherwise implicated in the reported or publicly disclosed breach;

m) "retaliation": any behavior, act, or omission, even if attempted or threatened, carried out due to the report, the complaint to judicial or accounting authorities, or public disclosure, that causes or could cause unfair harm, either directly or indirectly, to the Whistleblower or the individual who made the complaint;

n) "follow-up": the action taken by the person responsible for managing the reporting channel to assess the existence of the reported facts, the outcome of the investigations, and any measures taken;

o) "feedback": communication to the Whistleblower regarding the follow-up actions being taken or intended to be taken in response to the report.

5 General principles, objective and subjective scope of application

5.1 Objective scope of application

For the purposes of this Procedure, "Whistleblowing Reports" are considered to be reports relating to violations that harm the public interest or the integrity of the private entity, and consist of:

1. unlawful conduct relevant under Legislative Decree No. 231 of June 8, 2001, or breaches of the organizational and management models provided therein, which do not fall under items 3), 4), 5), and 6), or breaches of the Ethical Code;
2. unlawful activities that fall within the scope of EU or national acts specified in the annex to Legislative Decree No. 24/2023, or national acts implementing EU acts listed in the annex to Directive (EU) 2019/1937, even if not specified in the annex to Legislative Decree No. 24/2023, relating to the following areas: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiological protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy protection and personal data protection; and security of networks and information systems;
3. acts or omissions that harm the financial interests of the Union under Article 325 of the Treaty on the Functioning of the European Union, as specified in the relevant secondary law of the European Union;
4. acts or omissions concerning the internal market, under Article 26, paragraph 2, of the Treaty on the Functioning of the European Union, including breaches of EU competition and state aid rules, as well as breaches related to the internal market connected to acts breaching rules on corporate tax or mechanisms whose purpose is to obtain a tax advantage that undermines the object or purpose of the applicable corporate tax legislation;
5. acts or behaviors that undermine the object or purpose of provisions in the EU acts in the sectors mentioned in the previous items 2), 3), and 4).

On the other hand, "Ordinary Reports" are considered all other reports, as specified in paragraph 3.

The Whistleblower must have well-founded reason to believe that the reported breach, or the information related to it, is true.

Reports cannot consist of claims, disputes,or personal requests from the Whistleblower relating exclusively to their individual employment relations, or their employment relations with superiors.

In any case, please note that any report submitted through the reporting channels defined in this Procedure will be considered within the limits of its relevance and verifiability.

5.2 Subjective scope of application

This Procedure is addressed to all individuals who hold representative, administrative or management functions, or who exercise, even de facto, the management and control of business activities, to all employees regardless of their contractual classification, to those who cooperate and collaborate with the Company - on whatever basis - in

pursuing its objectives, and more generally, to anyone with ties to the Company, even by virtue of different legal relationships (e.g., suppliers, consultants, collaborators, partners, candidates, former employees, etc.).

The following individuals are also included:

1. volunteers and interns, both paid and unpaid, who carry out their activities within the Company;
2. shareholders and individuals with functions of administration, management, control, supervisory or representation, even if these functions are exercised de facto, within the Company.

The recipients of this Procedure may also include individuals to whom the protective measures for Whistleblowers may apply, specifically:

a. facilitators;

b. people within the same work environment of the Whistleblower, the person who made a report to judicial or accounting authorities, or the person who made a public disclosure, and who have a stable emotional or family relationship with them, up to the fourth degree of kinship;

c. co-workers of the Whistleblower, the person who made a report to judicial or accounting authorities, or the person who made a public disclosure, working in the same work environment and having a habitual and ongoing relationship with the aforementioned person;

d. entities owned by the Whistleblower or the person who made a report to judicial or accounting authorities, or the person who made a public disclosure, or for which such individuals work, as well as entities operating within the same work environment as the above-mentioned persons.

This Procedure is also published on the website https://www.icamcioccolato.com/it/. Therefore, the Procedure is made available to all potential stakeholders who become aware of the breaches described above.

6 Reporting channels

The recipients of this Procedure may make internal, external, public disclosures, and reports to judicial or accounting authorities regarding information on violations.

6.1 Internal reporting channels

Considering the above mentioned, the Company has activated a Platform accessible at the link https://icamcioccolato.whistleblowing.it/, through which it will possible to do:

- **written reports,** filling in the questionnaire and following the instructions available on the platform. This tool provides the highest level of confidentiality for the Whistleblower;
- **oral reports**, by requesting an in-person or telephone interview.

It is always possible to report unlawful conduct, not falling under the categories of paragraph 5.1, to the email address of the Supervisory Body, as indicated in the Company's Organization, Management, and Control Model.

6.2 External reporting channels

The National Anti-Corruption Authority (ANAC) has activated an external reporting channel that ensures, including through the use of encryption tools, the confidentiality of the Whistleblower's identity, the involved person, and the person mentioned in the Report, as well as the content of the Report and its related documentation.

The same privacy is guaranteed even when the Report is made through channels other than those indicated or reaches personnel other than those assigned to process Reports, to whom it will nonetheless be transmitted without delay.

The Whistleblower can submit an external report through the channel activated by ANAC **exclusively** for violations related to unlawful acts falling within the scope of EU or national acts mentioned in paragraphs 5.2, items 2), 3), 4), and 5).

External reports are made in writing via the online platform or orally through telephone lines or voice messaging systems, or, at the request of the Whistleblower, via a direct meeting scheduled within a reasonable timeframe.

An external report submitted to an entity other than ANAC is forwarded to ANAC within seven days of its receipt, and the Whistleblower is promptly notified of the transmission.

However, it should be noted that the Whistleblower can make an external report only if, at the time of submission, one of the following conditions applies:

I. there is no mandatory internal reporting channel activated within the Whistleblower's work context, or this channel, even if mandatory, is inactive, or, if activated, is not compliant with the requirements of Legislative Decree No. 24/2023;

II. the Whistleblower has already made an internal report and it has not been followed up;

III. the Whistleblower has valid reasons to believe that if an internal report were made, it would not be effectively followed up, or that making the report may result in retaliation;

IV. the Whistleblower has valid reasons to believe that the breach may represent an imminent or obvious danger to public interest.

ANAC publishes on its website, in a dedicated and easily accessible section (https://www.anticorruzione.it/-/whistleblowing) the necessary information for submitting reports (e.g., instructions for using the channel). ANAC also adopts its procedures for submitting and managing reports, which it updates periodically, as well as related guidelines, which should be consulted on the Authority's website in the most current version and in force *pro tempore*.

6.3 Public disclosure

For the same violations for which external reporting is allowed, public disclosure is also possible. This expression refers to making information about breaches publicly available through the press, electronic media, or any other means of dissemination capable of reaching a large number of people.

A person making a public disclosure, as defined above, benefits from protection under Legislative Decree No. 24/2023 if one of the following conditions is met:

I. the whistleblower has previously made both an internal and external report, or has directly made an external report, under the conditions and in the manner provided by this procedure, and no response has been given within the terms provided by the regulations regarding the measures that should have been taken or adopted in response to the reports;

II. the whistleblower has reasonable grounds to believe that the violation may constitute an imminent or apparent danger to the public interest;

III. the whistleblower has reasonable grounds to believe that the external report may cause a retaliation risk or may not have effective follow-up due to the specific circumstances of the case, such as situations where evidence may be concealed or destroyed, or where there is a well-founded fear that the person who received the report may be colluding with the infringer or involved in the breach itself.

Note: the external reporting channel and public disclosure cannot be activated in the case of unlawful conduct relevant under Legislative Decree No. 231/2001 or breaches of the Organization and Management Model or the Company's Code of Ethics.

7 Management of internal reports

7.1 Committee for reports management

The Committee responsible for managing the internal reporting channels (hereinafter also referred to as the "Manager") is identified by the members of the Supervisory Body of ICAM S.p.A.

The members of the Report Management Committee receive a formal appointment as the individuals responsible for managing the internal channels, which also includes the designation letter for authorization under Articles 29 of EU Regulation 679/2016 (also "GDPR") and 2-quaterdecies of Legislative Decree No. 196/2003 (also "Privacy Code"). The letter provides specific instructions for the proper process of personal data related to the report, for which the Company is the Data Controller under Article 4, paragraph 1, point 7) GDPR.

If reports are received regarding one of the members of the Supervisory Body, these reports will be managed by excluding the involved member from the review process related to the content of the report.

7.2 Submission of the report

The whistleblower submits the report as soon as they become aware of the facts they wish to report.

When submitting the report through the platform, the whistleblower is required to complete a guided questionnaire with both open and closed questions, which will allow the Report Management Committee to investigate the subject of the report, thereby minimizing the need for direct contact between the Manager and the whistleblower. The platform also allows the whistleblower to *upload* any documentation they deem relevant to support their report. In any case, the platform ensures that the whistleblower can access the portal while safeguarding the privacy of their identifying data.

The report must be detailed and based on precise and consistent facts, and should preferably contain the following elements:

- the personal details of the Whistleblower — unless it is an anonymous report — including any relevant role within the company or the organization where they work, as well as the consent — or lack thereof — to use their identity immediately or at a later stage during the verification process and to disclose their identity to parties other than the members of the report management committee;
- the personal details of the person who carried out the actions being reported;
- a clear and complete description of the facts being reported;
- the time and place in which the reported actions took place;
- the identification of any beneficiaries and victims of the unlawful act or irregularity;
- the identification of any other individuals who may provide information regarding the reported facts;
- the submission of any documents that may confirm the validity of the reported facts;
- any other information that could provide useful feedback regarding the existence of the reported facts.

In this regard, it is advisable that the reports provide as many factual details as possible to enable the manager to conduct the necessary investigations.

The adopted reporting platform, equipped with appropriate technical security measures as required by Article 32 of the GDPR, hosted on a third-party *server*, ensures confidential registration and the use of encryption. The platform provider has signed a data protection agreement pursuant to Article 28 of the GDPR, committing to comply with the instructions provided by the Data Controller, even in the case of subcontracting.

The platform allows the storage of reports and attached documentation in an encrypted electronic format, in accordance with applicable data protection laws. The data and documents related to the report are stored in compliance with legal requirements.

At the end of the reporting procedure, the platform provides the whistleblower with a sixteen-digit code allowing him/her to access the system and his/her report to:

- monitor the progress of the report;
- add further factual elements or additional documentation to the report;
- request direct contact or a meeting with the Report Management Committee, and initiate an exchange of requests and information.

The platform enables the Report Management Committee to continue confidential communication with the whistleblower and request additional details if the report is not sufficiently detailed.

If the whistleblower chooses to use the internal reporting channel in oral form, he/she must access the platform and, under the "Choice of Reporting Channel" section, opt to request an interview for an oral report.

The whistleblower is not required to disclose their name but must provide a contact email or phone number to be reached.

7.3 Investigation and verification of the report

a. Receipt of the report

The Report Management Committee, upon receiving the report, issues an acknowledgment of receipt to the Whistleblower within seven days from the receipt date, using the same channel through which the Report was

submitted. In the case of an oral report, the receipt of the report coincides with the phone call/email to arrange the oral appointment.

If a Report is submitted to a third party using channels or forms other than those specified in this procedure, the third party is required to forward the report to the report management committee within seven days of receipt and notify the Whistleblower of the transmission. Upon receipt of the report, the manager proceeds to enter it into the platform.

b. Investigation

The Manager diligently follows up on the Report, conducting an investigative process to verify its validity with full access to any necessary information and documentation required for the task.

For the verification process, the Manager may assign further investigation to internal offices and/or third parties, ensuring to:

- provide a formal mandate, defining the scope of action and specifying the information to be obtained from the requested investigation;
- omit any information that could, even indirectly, lead to the identity of the whistleblower or the content of the Report;
- omit any information about the person involved, unless strictly necessary for the proper completion of the task assigned;
- remind the appointed party of the confidentiality obligation concerning the processed data (in the case of external parties, this obligation must be formalized).

In cases where, for investigative reasons, it becomes necessary to disclose the content of the report and/or any attached documentation to other parties, the Manager will ensure that the personal data of the Whistleblower, as well as the identities of other individuals whose information must remain confidential (such as the facilitator, the person involved or others mentioned in the report), are redacted.

Furthermore, during the investigation, the Report Manager must:

- maintain communication with the Whistleblower and request any necessary additional information;
- interview, if necessary, the person(s) directly involved or any witnesses and informed individuals, either orally or through written procedures, by obtaining written observations and documents;
- conclude the investigations by documenting the reasons in cases where the report is archived.

In any case, the identity of the Whistleblower and any other information that could directly or indirectly reveal their identity will not be disclosed by the Report manager without the Whistleblower's consent, in order to protect them from potential retaliation or discrimination.

Moreover, concerning the confidentiality of the whistleblower's identity, the following must be considered:

a) in criminal proceedings, the Whistleblower's identity is protected by secrecy under Article 329 of the Italian Criminal Code.

b) in proceedings before the Court of Auditors, the whistleblower's identity cannot be disclosed until the investigative phase is closed.

c) in disciplinary proceedings:

1. the identity cannot be disclosed if the disciplinary charge is based on findings distinct and separate from the report, even if arising from it;
2. if the notification is based wholly or partly on the Report and knowledge of the Whistleblower's identity is essential for the defense of the accused one, the report will be usable in the disciplinary process only if the whistleblower has expressly consented to the disclosure of their identity.

In any case, the Whistleblower will be notified in writing of the reasons for the disclosure of confidential data in the scenarios outlined in letter c), point 2, as well as in internal and external reporting procedures when the disclosure of the whistleblower’s identity is essential for the defense of the person involved.

The whistleblower has the right to request updates or feedback on his/her report using the information channels mentioned in the previous paragraph 6. A denial of such information must be justified.

The activities outlined above will also be conducted in cases where the submitted Report is anonymous, provided

that it is sufficiently detailed and precise to allow the Report Management Committee to carry out the investigation. Otherwise, the report will be archived.

c. Closing of the report

Within ninety days from the expiration of the seven-day period from the submission of the report, the Report Manager must provide feedback to the Whistleblower.

Following the investigation, the Report Management Committee assesses the adoption of one or more of the following actions:

- archiving the Report due to insufficient evidence;
- archiving the Report due to the irrelevance of the reported facts;
- proposal of the initiation of disciplinary or sanctioning proceedings - in accordance with the current disciplinary and sanctioning system - against the individuals involved, who have been found to have committed a violation, unlawful act, or irregularity;
- proposal of the initiation of disciplinary or sanctioning proceedings - in accordance with the current disciplinary and sanctioning system and this Procedure - against whistleblowers who have submitted unfounded reports, based on false factual circumstances, and made with intent or gross negligence.

In particular, the Report Management Committee, in compliance with applicable regulations, communicates the outcomes of the investigations conducted on the received reports to the relevant functions, where necessary. Purely by way of example: i) to the General Manager and the Human Resources Function, in case of actions to be taken against employees; ii) to the Board of Directors and the Board of Statutory Auditors, in case of actions to be taken against directors and auditors.

Furthermore, if there are elements that do not clearly indicate the falsity of the facts, the Manager has the discretion to involve other third parties (e.g., the person in charge of the Function where the event occurred, Legal Department, the person in charge of the unit for managing the contractual relationship) who are competent for evaluating and possibly adopting further actions or subsequent measures.

Finally, the Whistleblowing Management Committee informs the Whistleblower regarding the outcome of their report, usually through the same channel through which it was submitted.

d. Conservation of the documentation

The report and related documentation (records, minutes, collected documents, etc.) will be retained for the time strictly necessary for their management on the platform where the report was made.

In any case, in accordance with the provisions of Legislative Decree No. 24/2023, the conservation will be carried out for a maximum of five years from the date of communication of the final outcome of the whistleblowing procedure (Article 14 of Legislative Decree No. 24/2023). Specifically, the platform automatically deletes reports after the established retention period.

8 Protection of the Whistblower

In all stages related to the investigation of the reported facts, the Company ensures the protection of the Whistleblower against any retaliatory action they may face or discriminatory behavior adopted as a result of the whistleblowing (e.g., dismissal, bullying, demotion, etc.).

Protection applies, as explicitly foreseen by law, when:

- at the time of the report or the complaint to judicial or accounting authorities or public disclosure, the Whistleblower had valid reason to believe that the information about the reported breaches, disclosed publicly or reported, was true;
- the report or public disclosure was made in compliance with the methods described in paragraph 6 of this Procedure.

The reasons leading the person to report, disclose, or make a public disclosure are irrelevant for their protection. Protection is extended not only to the Whistleblower but also to the facilitator, colleagues with a stable emotional bond, colleagues with an ongoing and habitual relationship with the Whistleblower, entities owned by the Whistleblower or for which they work, as well as entities operating in the same work context as the Whistleblower.

Whistleblower protection also applies in the following stages of the employment relationship:

a) when the legal relationship (e.g., employment, collaboration, consultancy, supply contract, etc.) has not yet started, if the information regarding breaches was obtained during the selection process or other pre-contractual phases;

b) during the trial period;

c) after the termination of the legal relationship if the information about breaches was obtained during the relationship itself.

Protection extends to cases of reporting or filing complaints to judicial or accounting authorities, external whistleblowing, or public disclosure, made anonymously, if the Whistleblower is subsequently identified.

Protection does not apply if the Whistleblower's criminal responsibility is determined, even by a first-degree judgment, for crimes such as defamation or slander or for similar crimes committed by reporting to judicial or accounting authorities, or for civil responsibility for the same reasons, in cases of willful misconduct or gross negligence. In such cases, a disciplinary sanction is imposed on the Whistleblower or complainant.

According to Article 17 of Legislative Decree No. 24/2023, the following actions constitute retaliation: a) dismissal, suspension or equivalent measures; b) demotion or failure to promote; c) change in duties, change of workplace, reduction in salary, modification of working hours; d) suspension of training or any restriction on access to it; e) negative performance reviews or negative references; f) adoption of disciplinary measures or other sanctions, including financial penalties; g) coercion, intimidation, harassment, or ostracism; h) discrimination or otherwise unfavorable treatment; i) failure to convert a fixed-term employment contract into an indefinite-term contract, where the employee had a legitimate expectation of such conversion; l) failure to renew or early termination of a fixed-term employment contract; m) damages, including reputational damage, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income; n) placement on improper lists based on formal or informal sector or industry agreements, which may result in the inability to find employment in the sector or industry in the future; o) early termination or cancellation of a goods or services supply contract; p) cancellation of a license or authorization; q) request for psychiatric or medical examinations.

In addition to those explicitly indicated in Legislative Decree No. 24/2023, retaliation may also include, for example, demanding impossible results to be achieved in the ways and times specified; deliberately negative performance evaluations; unjustified revocation of assignments; unjustified failure to assign tasks, while assigning them to another person; repeated rejection of requests (e.g., vacation, leave); unjustified suspension of patents, licenses, etc.

The duty of proving that such actions or acts are motivated by reasons unrelated to the Report, public disclosure, or complaint lies with the person who carried them out.

In the event of suspected discrimination or retaliation against the person who made the report, related to the Report, or abuse of the reporting system by the same person, the Company will apply disciplinary sanctions.

Retaliation reports must be submitted exclusively to ANAC for the investigations entrusted to it by law and for the possible imposition of an administrative fine on the responsible person. ANAC, in turn, may make use of the National Labor Inspectorate and the Public Function Inspectorate, while retaining exclusive competence over the assessment of the collected elements and the imposition of sanctions.

If, by mistake, the Company receives a retaliation communication, it is required to ensure the confidentiality of the identity of the person who submitted it and to forward it to ANAC, providing the person who made the communication with notice of this transmission.

Individuals who have suffered retaliation have the right to be reinstated in their position.

9 Disciplinary measures and other initiatives

An effective *Whistleblowing* system must include certain sanctions for those involved when violations or unlawful acts are confirmed against them, as well as for the person making the report in case of abuse of the reporting system, for the Committee Managing the Reports in case of non-compliance with this Procedure, and for anyone who, in different ways, violates the confidentiality obligations and the retaliation prohibitions that protect the person making the report.

Therefore, in accordance with the provisions of the relevant national collective agreement, sanctions are foreseen for those responsible for the violations listed in Article 21, paragraph 1 of Legislative Decree No. 24/2023, including the following behaviors:

- failure to establish reporting channels;

- failure to adopt procedures for reporting and managing reports;
- adoption of procedures that are not compliant with Legislative Decree 24/2023;
- failure to carry out the verification and analysis activities of the report;
- commission of retaliatory actions;
- obstruction or attempted obstruction of the report;
- breach of confidentiality obligations.

The Company does not tolerate any detrimental consequences against the person making the report in disciplinary matters and protects them in case of adoption of "discriminatory measures, direct or indirect, affecting the working conditions for reasons directly or indirectly linked to the report."

However, this protection has a limit in the cases of:

- proven criminal liability of the person making the report, even with a first-degree sentence, in "cases of liability for slander or defamation or for the same reasons under Article 2043 of the Civil Code."
- civil liability of the person making the report, in cases of fraud or gross negligence, for the same crimes mentioned above.

Regarding the last two behaviors indicated, in fact, if the person involved believes that the person making the Report did so with the sole purpose of slandering or defaming them, he/she may file a complaint against persons unknown to him/her.

If the Judicial Authority decides to proceed against the person making the report, it may request the Company to provide the identity of the person who made the report. In this case, following the decisions of the Authority, disciplinary measures deemed appropriate will be applied to the person making the report.

However, the person making the report is not punishable, even for civil or administrative liability, if he/she reveal or disclose information about breaches covered by the secrecy obligation or related to the protection of copyright or personal data, or if he/she reveal or disclose information about breaches that harm the reputation of the person involved or reported, when, at the time of the disclosure, there were reasonable grounds to believe that the disclosure of such information was necessary to expose the breach and the report.

10 Processing of personal data

In the context of this process, the personal data processing of the individuals involved or mentioned in the Reports is protected, in accordance with the law in force and company procedures regarding personal data protection.

When the Report is entered into the IT platform for managing Reports, the person making the Report receives information regarding the processing of his/her personal data. In any case, this information is also published in the section of the website dedicated to reporting channels.

The Company ensures that the processing of personal data is carried out lawfully, fairly and in accordance with the specific rules set forth by applicable laws.

Furthermore, it is specified that the confidentiality of the Company employee who submits a Report is protected as pursuant to the provisions of Article 2-*undecies*, titled "*Limitation of the Rights of the Data Subject*" of Legislative Decree No. 101 of August 10, 2018, containing "*Provisions for the adaptation of national law to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation)*."