Whistleblowing Policy

Corporate procedure for Handling Reports

Revision 01

Revision number	01
Update data	11.12.2023
Approval date	17.12.2023 BoD and 25.01.2024 SB and Privacy Advisor
Person responsible for drafting the document	CEO
Approval	BoD
Replaces	Non-applicable - First issue
Changes compared to previous revision	First issue
Confidentiality level	Confidential for internal use
Copyright or CC licence	Copyright of the Company
Notes	-
Contact person and contacts for information on the document	Patrizia Bolognesi – pbolognesi@mpi.it
File	MPI_WhistleblowingPolicy_R01_

Sommario

Whistleblowing: I want to know more

CSR (Corporate Social Responsibility) tool, essential to manage risks and protect workers

A correct and efficient handling of reports (Whistleblowing) is very important to guarantee compliance with the principles of legality and transparency defined by the Company (hereinafter also referred to as 'Company' or 'Organisation'), in accordance with the rules of conduct of the Company itself.

The purpose of the whistleblowing system is that of allowing the Company to be informed about situations of risk or harm and to deal with the issue reported in the timeliest manner. A system that is developed and finalised through specific policies and training also allows to provide real protection to the Whistleblower.

The whistleblowing tool contributes to identifying and dealing with illicit conduct relevant to that which is provided for in Legislative Decree no. 24 of 10 March 2023, in implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, for the protection of members from financial losses and reputational damage, to disseminate the culture of ethics, legality and transparency within the company and to strengthen the internal control system and the management of risks.

Therefore, the goals of the Company through this procedure are to:

guarantee transparency and efficiency in the reporting channels; handle the reports made by the whistleblowers in a timely manner; guarantee the protection of personal data of the whistleblowers and their identity in the event that an anonymous whistleblower was to request it;

protect the whistleblowers from any possible and potential situations of retaliation.

Therefore, the aims pursued are to encourage and facilitate the Reports within the **Company** and to reduce the risk of offences, by building and strengthening the relationship of **trust** with the **stakeholders** and fostering and enhancing a corporate culture based on factors of transparency, integrity, good governance and corporate compliance.

The EthicPoint System

EthicPoint is a certified, external service in terms of protecting the privacy of the whistleblower. Its approach is that of "service", that is to not offer only a channel to send reports, but to offer the whistleblower actual assistance and consultancy (professional), so that he/she is free to use it also without necessarily having to make the report anonymously. For this reason, it is essential that before any action is taken, the EthicPoint experts, who can provide all the necessary information, are contacted.

Purpose and field of application

This document defines the rules for a correct and effective handling of a report by a subject (Whistleblower), also for the purpose of identifying and eliminating the possible risk factors and to involve, if necessary, the competent authorities.

The goal of this document is that of providing the whistleblower and all those involved with clear operational instructions regarding the subject, contents, recipients and procedures for reporting and handling reports, as well as all the forms of protection that are offered, pursuant to law and internal procedures.

This procedure was defined also as a guide for the drafting of circulars or information and training documents for the subjects involved.

It applies to all activities carried out by the Company[1].

Note 1: this procedure was adopted by the Board of Directors as organisational measures of the provisions of law and for **reporting**[1] to workers' representative bodies.

Note 2: the EthicPoint Whistleblowing service is the internal reporting channel in accordance with Legislative Decree 24 of 2023, which externalizes some of the reporting activities

[1] MPI is an established business organisation known internationally as a supplier of the most varied types of magnetic materials in all industrial sectors. MPI guarantees experience, technical expertise and professionalism, global service and respect for the environment. It is above all for these important characteristics that the company has distinguished itself to date compared to other organisations in the market.

[1] As provided for by article 51 of Legislative Decree 81 of 2015: *"... having consulted with the representatives and labour unions to acquire any observations ... (on the) ... procedures for receiving reports and their handling."*

through a certified company, qualified through a specific service agreement and which appoints a personal data processor for the proper application of the GDPR.

Regulatory references

- Legislative Decree no. 24 of 10 March 2023
- ANAC (Italian National Anti-Corruption Authority) guidelines (applicable version)
- Operational Guide for private entities – Confindustria, the Italian Manufacturers' Association, (applicable version) • ISO 37002 - Guidelines for the management of whistleblowing

See also Annex 1.

Terms and definitions: essential concepts to be aware of

Before reading this procedure on handling reports, the definitions attributed to some of the terms within this Policy must be defined.

- **Report (internal)**: communication, oral or written, of information on possible violations or offences, submitted through the internal reporting channel.
- **Whistleblower**: the individual who makes the report (the accusation or public disclosure) of information on violations acquired within the context of his/her work.
- **Reported person**: person who is the subject of a Report
- **Person involved:** the individual or legal entity mentioned in the internal or external report or in the public disclosure as the person to which the violation is attributed or as a person implicated in the reported violation or public disclosure.
- **Follow-up**: the action taken by the person entrusted with handling the reporting channel to assess the existence of the reported facts, the outcome of the investigations and any measures adopted.
- **Feedback**: communication to the whistleblower of information relative to the follow-up carried out or to be carried out in response to the report.
- **Violation**: behaviours, acts or omissions which cause damage to public interest or to a public administration or private institution.
- **Retaliation**: any behaviour, act or omission, including even tempted or threatened, implemented because of the report, the charge to the judicial or accounting authority or because of the public disclosure and that causes or may cause unjust damage, directly or indirectly, to the whistleblower or to the person making the accusation.
- **Report in bad faith**: the Report is made with the sole purpose of causing damage or, nonetheless, harm to the company, to the reported person or to third parties.
- **Accusation**: act with which a person is aware of a crime subject to prosecution by law and notifies the competent authorities (e.g., a police official).
- **Public disclosure**: disclosing information to the public on violations through print media or electronic means or nonetheless through means of dissemination capable of reaching a significant number of people.

It is **always recommended** to see Annex 2 to clearly understand what can be reported and what cannot be reported.

Important: for any question or doubt, contact EthicPoint through the contact information provided in this procedure.

Reporting channels

Internal reporting tools

In line with that which is provided for by regulatory provisions on the matter of protecting whistleblowers reporting violations or offences, the Company has established an independent and certified reporting channel with a specific address to receive and handle reports.

The channel adopted allows for reporting any violation as provided for in Decree 24 of 2023 and in the corporate procedures by all stakeholders, internal and external, guaranteeing effective and confidential communication.

The characteristic of this solution is to protect the confidentiality of the whistleblower as much as possible.

The reporting procedures are the following:

1	***Landing page***	Dedicated web page (including e-mail address instrumental to the operation of the service - mpi@ethicpoint.eu)
2	***PO BOX***	PO BOX no. 301 c/o Mail Boxes Etc. Post office box (Via Felice Bellotti 4, 20129 Milan): Audit People S.r.l – Benefit Corporation – Indicating the name of the Organisation and, if required, the double envelop procedure. IMPORTANT: Please be sure to notify your stakeholders to include the name of the company
3	***Free phone number***	800 985 231 with voice messaging (valid only for Italy)

Pursuant to Article 4, paragraph 3 of Legislative Decree no. 24 of 2023, the whistleblower, through the previously described channels, can request a face-to-face meeting to verbally present his/her report.

External reporting channels

ANAC

To be able to use the reporting channel set up by **ANAC**, certain **conditions** must be met, pursuant to Art. 6 of the Decree. In particular:

- in its work context, the activation of the internal channel as mandatory is provided or, if provided, has not been activated
- the internal reporting has not received follow up
- there are reasonable grounds to believe that the internal report would not receive efficient follow up
- the whistleblower has reasonable grounds to believe that the violation may constitute an imminent or clear danger for the public interest
- the whistleblower has reasonable grounds to believe that, if he/she were to make an internal report, the report would not receive follow up or he/she would meet with retaliation

Public disclosure

The regulation also introduces the possibility for the whistleblower to make a public disclosure benefiting from protection.

This is an extremely sensitive development for companies, because of the harmful potential for the institution for an accusation made without justified reasons or substantiated evidence.

To use this procedure, at least one of the following conditions must be met:

- the internal and/or external channel has been previously used, but no feedback was received or no follow up was carried out within the period provided for by the decree;
- the whistleblower believes there are well-founded reasons for an "imminent and clear danger to public interest", considered as an emergency situation or a situation of risk of irreversible harm, also to the physical safety of one or more people, requesting that the violation is disclosed in a timely manner with wide publicity to prevent its effects.
- the whistleblower believes that there are well-founded reasons to believe that the external report could lead to a risk of retaliation or not receive effective follow up because

there could be a risk of destruction of evidence or collusion between the authority responsible for receiving the report and the person committing the violation. In other words, these are particularly serious situations of negligence or malicious behaviour within the organisation.

Communication, information, training and awareness

The Management System of reports and the content of this procedure are the object of communication, information, training[2] and awareness for all recipients.

This procedure is available to possible whistleblowers, in particular, it is available through:

1	Communication via e-mail to personnel
2	Notice on company bulletin boards
3	Registration of document on network folder
4	Publication on the company website (summary)

Handling reports

Parties involved (potential whistleblowers)

It is necessary to first identify and define, in a clear and exhaustive manner, the subjects affected by this policy, that is those who can make a report.

Among internal and external stakeholders, the Company identifies the following as potential whistleblowers. For example:

- employees of public administrations, employees of public corporations, of private law entities under public control, of in-house companies, of public law bodies, of public service providers;
- employees of private sector companies;
- self-employed, freelance professionals and consultants who work for public or private sector companies;
- volunteers or interns, with or without salary, who work for public or private sector companies;
- shareholders and people with administrative, management, control, supervisory or representative functions;
- facilitators;
- people in the same workplace as the whistleblower and who are linked to the whistleblower by a stable emotional bond or kinship up to the fourth degree;

[2] See specific programme in function of roles.

- colleagues of the whistleblower who work in the same workplace as the whistleblower and have a habitual and current relationship with the whistleblower. Also:
- the legal relationship has not yet started, if the information on the violations has been acquired during the selection process or in other pre-contractual phases; • during the trial period;
- subsequent to the termination of the legal relationship, if the information on the violations has been acquired during the relationship itself.

Confidentiality obligation

The goal of this procedure is to ensure the protection of the whistleblower, keeping his/her identity private, only in the case of reports from identifiable and recognisable subjects.

Anonymous reports, when these are adequately substantiated and made providing very detailed descriptions, where they can reveal very detailed facts and situations relating them to specific contexts, are treated as standard reports. Anonymous reports and their processing take place, nonetheless, though the same tools provided for confidential reports, even when the dialogue with an anonymous whistleblower is no longer possible following the report itself.

Anonymous reports are also subject to this procedure, in as much as it is applicable.

The identity of the whistleblower and any additional information from which the identity can be inferred, directly or indirectly, cannot be revealed without explicit consent of the whistleblower himself/herself, to people other than those authorised to receive or follow up on reports, explicitly authorised to process such data.

Within the criminal procedure, the identity of the whistleblower is covered by confidentiality in the manner and limits provided for by Article 329 of the Italian Code of Criminal Procedure[3].

Specifically, within the framework of disciplinary proceedings, the identity of the whistleblower may not be disclosed, where the disciplinary charge is based on investigations that are separate and additional to the report, even if consequent to it. If, on the other hand, the charge is based, in whole or in part, on the report and knowledge of the identity of the whistleblower is indispensable for the accused's defence, the report will be usable for the purposes of disciplinary proceedings only if the whistleblower expressly consents to the disclosure of his/her identity.

[3] Article 329 of the Italian Code of Criminal Procedure establishes, in fact, that the investigative acts by the public prosecutor and the police are confidential until the defendant (or suspect) is not made aware of them and, nonetheless, not beyond the conclusion of the preliminary investigations.

Subject and content of the report

Reports concerning reasonable and sincere suspicion related to an employee with reference to possible fraud, dangers or other risks that may threaten customers, colleagues, stakeholders, the public in general or the reputation of the Company are considered relevant[4].

Also in consideration of that which is provided for in the regulation of reference, the report can regard actions and omissions, committed or attempted, that are:

- violations of national or European regulatory provisions that cause damage to public interest or the integrity of public administration or private institutions, which have become known in a public or private workplace;
- punishable by administrative or criminal sanctions or by other administrative measures, also regarding the company pursuant to Legislative Decree 231 of 2001;
- related to the abuse of power entrusted to an employee, for the purpose of obtaining private advantages;
- evidence of poor functioning in the Company due to use for private purposes of the attributed functions (e.g., waste, nepotism, repeated lack of compliance with procedural times, non-transparent hiring, bookkeeping offences, false statements, violation of environmental and work safety regulations);
- implemented in violation of the Code of Ethics, of the internal corporate rules, the Organisational, Management and Control Model (Legislative Decree 231 of 2001) or any other policy or procedure or corporate rule applicable;
- likely to cause damage to the corporate assets or image or to members or shareholders;
- likely to cause damage to employees or other subjects who carry out their activity at the Company.

The report must not concern, on the other hand, the whistleblower's personal grievances or requests pertaining to rules of the work relationship or to relationships with superiors or colleagues, for which he/she must refer to human resources.

In the report, the following essential elements must be clearly pointed out, also for the purpose of assessing admissibility:

[4] For further information, please consult ISO 37002.

1. the whistleblower's identification details, as well as contact information for communicating updates;
2. the circumstances of time and place relative to when the event took place and its relative detailed description;
3. the details or other elements which make it possible to identify the subject to whom to attribute the reported facts.

The report must preferably include the following elements:

1. information regarding any other people who can provide information on the facts that are the object of the report;
2. information on any documents that can confirm the substantiation of such facts;
3. any other information that can provide useful feedback on the substantiation of the reported facts.

In summary, for reports to be considered, they must be properly substantiated and based on elements of precise and consistent facts.

The recipients of the report

The internal reporting channels provided which guarantee maximum confidentiality on the identity of the whistleblower must be compliant with Legislative Decree 24 of 2023.

The management of the internal reporting channel (externalised service) is also entrusted to specific internal functions with personnel with moral requirements, specifically trained to handle such activity and on the protection of personal data and confidentiality.

Specifically, the internal contact people are:

1	EthicPoint – Certified external service for the protection of the whistleblower
2	Supervisory Board internal member
3	Supervisory Board external member
4	Supervisory Board external member

Procedure and duties of the person receiving the report

Checking the validity of the report

EthicPoint takes charge of the report, which is sent to the responsible internal departments, issuing a notice of receipt to the whistleblower within seven days of receipt.

The internal departments take up the reports received with diligence and provide follow up within three months from the date of the notice of receipt, or in lack of notice, within three months of the deadline of the seven-day term from the date the report was made, via the e-mail address above or to the contact information provided by the whistleblower in the chosen reporting procedure.

All the information will be handled in accordance with the provisions of the protection of the whistleblower.

If required, the internal departments request the whistleblower or any other subjects involved in the report for additional information, adopting the necessary precautions.

Furthermore, they verify the validity of the events represented in the report through every activity considered appropriate, including obtaining documents and hearing any other subjects who may provide information on the events reported, in compliance with the principles of impartiality, confidentiality and protection of the confidentiality of the whistleblower.

The Company, on the basis of an assessment of the facts of the report, may decide, in the case of evident and obviously unfounded information, to close the report.

The Company directly closes reports in the case of:

- obvious lacking interest in the integrity of the Company;
- obvious unfounded information due to lack of factual elements appropriate to justify verification;
- obvious lack of legal requirement to apply sanction;
- clearly emulative objective;
- verified generic content of the report or such as to not allow comprehension of the facts, that is report accompanied by inappropriate or ineffective documentation;
- the provision of only documentation without a report of unlawful or irregular conduct;
- lack of information constituting essential elements of the report.

In the event that there are elements relative to the fact that are not clearly unfounded, the internal departments in charge (SB) forward the report, also for the purpose of adopting consequent measures, to the following authorised subjects:

1	Chairman of the Board of Directors
2	Employer delegate for safety
3	Sole Statutory Auditor

4	Judicial authorities for profiles within their respective remit

In line with current law on the matter of the protection of personal data, to preserve the investigative purposes and in the cases provided for by law, the person who has been reported may not be immediately be informed of the processing of his/her personal data by the Data Controller, for as long as there is a risk of compromising the possibility of effectively verifying the legitimacy of the accusation or collecting necessary evidence.

Personal data relative to the reports and the relative documentation are stored and kept for the period necessary to complete the verification of the facts set out in the report and for the **subsequent 5 years from the moment that the report is closed**, with the exception of any proceedings resulting from the handling of the report (e.g., disciplinary, criminal, accounting) against the person reported or the whistleblower (e.g., bad faith, false or defamatory statements). In that case, they will be stored for the entire duration of the procedure and until the terms of appeal of the relative measure have expired. The personal data that are clearly not useful to the processing of a specific report are not collected or, if they are accidentally collected, they are cancelled immediately.

Checking the validity of the anonymous report

The verification phase on the validity of the report by the Company is the same both for the confidential report and the anonymous report. However, the following information will be considered for the anonymous report:

- the need for more in-depth information in verifying the elements that excluded that the report is directly closed;
- the Company will contact the whistleblower if technically possible.

Protection of the whistleblower

The Company officially declares that no discriminatory action or retaliation against the whistleblower will be implemented; in fact, any behaviour of this type will be sanctioned. In particular, pursuant to Article 17 of Legislative Decree 24 of 2023, it is explicitly decreed that whistleblowers cannot be subjected to any retaliation. Protection will not apply in cases in which the report contains information that is false made with deliberate malice and gross negligence.

In cases where discrimination or retaliation against the whistleblower is suspected, which can be correlated to the report, or abuse of the reporting tool by the whistleblower, the Company can implement disciplinary sanctions.

Measures of support are provided for the whistleblower:

- Information;

- Free assistance and advice on the reporting procedure and protection from retaliation.

Protection will not apply in cases in which the report contains information that is false made with deliberate malice and gross negligence.

Responsibility of the whistleblower

This policy is without prejudice to the criminal, civil and disciplinary liability in the event of a libellous or defamatory report under the Italian Criminal Code and Article 2043 of the Italian Civil Code[5].

Also included as sources of liability, in regulatory or other judicial courts, are any forms of abuse of this policy, such as obviously opportunistic reports or reports made exclusively to damage the person reported or other subjects and any other hypothesis of improper use or intentional exploitation of the Company subject to this procedure, as well as unsubstantiated reports made with deliberate malice and gross negligence.

The system of sanctions

An effective whistleblowing system must provide for sanctions both for the whistleblower, in the event of abuse of the reporting tool, and for the reported person in the case of the investigation of offences reported in accordance with that which is provided for in current regulations, including applicable collective bargaining, and specifically by Legislative Decree 24 of 2023 on the protection of people who report violations of laws of the Union and of national regulatory provisions.

Additional information and contacts

For any additional information relative to the procedure above, please contact:

1	Patrizia Bolognesi – pbolognesi@mpi.it

[5] Article 2043 of the Italian Civil Code: Any malicious or negligent act, which causes unjust damage to others, requires the person committing the act to compensate the damage. The crime of slander consists, essentially, in accusing another person of having committed a crime, while knowing that the person is innocent (Article 368 of the Italian Criminal Code). Defamation: anyone, excluding the cases in the previous article, who in communicating with several people, damages the reputation of other people (Article 595 of the Italian Criminal Code).

ANNEX 1: Legislative reference scenario

The protection of the employee and the collaborator, reporting illegal conduct within the work environment both in the public and private sector, is already widely provided for in official documents of wide international scope, such as UN, OECD international conventions and European Council, all ratified by Italy as binding content, and the Recommendations of the Parliamentary Assembly of the European Council.

On a national level, the concept of 'whistleblowing' was first introduced with Law 190 of 2012 - Provisions to prevent and repress acts of corruption and illegality in the public administration - which, solely for the public sector, with the provision of Art. 1, para. 51, introduced Art. 54-bis in Legislative Decree 165 of 2001 - General rules concerning employment in public administration - regulating a system of protection for the public employee who decides to report unlawful conduct of which he/she has become aware by reason of the employment relationship.

Subsequently, with Law 179 of 2017 - Provisions to protect people reporting crimes or irregularities they become aware of in the context of a public or private employment relationship - the concept of reporting in the private sector was introduced, amending, Art. 6 of Legislative Decree 231 of 2001 and bring about corrective action in the regulations for reporting in the public sector. Regarding the private sector, this measure rules that the Organisational, Management and Control Models provided for in the Decree, must provide for:

a. one or more channels that allow, for senior management or those under their control or their supervision – in protection of the integrity of the entity – for substantiated reports on unlawful conduct (material for the purposes of '231' and based on precise and consistent facts) or violations of the Organisational and Management Model, of which they may become aware in fulfilling their own duties. Furthermore, the same article provides that such reporting tools ensure the confidentiality of the identity of the whistleblower in the activity of handling of the report
b. at least one alternative reporting channel suitable to guarantee, with electronic means, the confidentiality of the identity of the whistleblower
c. the prohibition of acts of retaliation or discrimination (direct or indirect) against the whistleblower, for reasons connected (directly or indirectly) with the report
d. within the disciplinary system, sanctions against those violating the measures to protect the whistleblower, as well as against those who make reports which turn out to be made with deliberate malice or gross negligence.

Lastly, Legislative Decree 24 of 2023 transposed European directive 1937 of 2019 on the matter, regarding the protection of whistleblowers. Its intention is to give full and effective implementation of the principles of transparency and responsibility in handling reports, considered an essential tool, not only in terms of managing risks and general compliance,

but also as a tool for relations with stakeholders in accordance with the most recent rules of governance.

In compliance with Directive 1937 of 2019 and, therefore, the above decree, the subjects - in particular those indicated in Article 3 of decree 24 of 2023 - are required to report any conduct or situations that may be considered improper or inconsistent with internal procedures and more generally with the provisions of current law[6].

[6] The reports must be possible as per procedures defined by the company and through specific internal reporting channels (as provided for by Article 4), with the purpose of ensuring the confidentiality of the whistleblower and his/her protection from possible retaliation.

ANNEX 2 – Examples of offences or irregularities to be reported (non-exhaustive)

- harassment
- discrimination
- irregularities in administrative and accounting and tax commitments
- false statements, falsifying or altering documents
- violation of environmental and work safety regulations
- theft of property owned by the company or third parties
- misappropriation of funds, assets, supplies belonging to the company or third parties
- destruction, concealment or inappropriate use of documents, archives, furniture, installations and equipment
- acceptance of funds, goods, services or other benefits as incentives to favour suppliers or companies
- falsifying expense reports (e.g., 'inflated' refunds or for false travel)
- falsifying work attendance
- disclosing information that by nature or by explicit indication of law or corporate standards is confidential, or information that is owned by the company or third parties (e.g. competitors)
- using resources and assets of the Company for personal use, without authorisation
- anti-money laundering irregularities
- computer fraud
- actions or omissions that result in harm or danger to human rights, the environment, public health, public safety or public interest
- existence of relationships with subjects (natural or legal persons) belonging to criminal organizations of any type or who violate the principles of law
- violation of restrictive measures in economic and commercial relationships or in the sanctions adopted at a national, EU and international level
- public tenders
- incorrect communication on services or products or safety and compliance of products sold on the domestic market, risks in failing to provide consumer protection
- improper use of sensitive information

- terrorist financing
- environmental or public health protection
- personal data protection
- network and information systems security
- violations of European regulation on competition and state aids
- violations regarding the domestic market and corporate tax

Examples[7] of offences or irregularities that cannot be reported (non-exhaustive)[8]

- Reports regarding labour disputes and pre-litigation phases
- Discrimination among colleagues, interpersonal conflicts between the whistleblower and another worker or with supervisors
- Reports regarding processing of data carried out in the context of an individual work relationship in absence of damage to public interest or to the integrity of the public administration or private entity
- Reports of violations already compulsorily regulated by acts of the European Union or national ones indicated in part II of the annex to the decree, that is by national ones constituting implementation of the acts of the European Union indicated in part II of the annex to the directive (EU) 2019/1937, even if not indicated in part II of the annex to the decree (Leg. Decree no. 24/2023)
- Reports related to market abuse pursuant to Regulation (EU) no. 596/2014 of the European Parliament and the Council on the Commission Implementing Directive (EU) 2015/2392 adopted on the basis of the above regulation, already containing detailed provisions on the protection of whistleblowers
- Reports regarding credit institutions and investment firms pursuant to Directive (EU) 2013/36 of the European Parliament and Council
- Reports of violations in the banking sector.

[7] ANAC guidelines, para. 2.1.1.

[8] Improper reports may provide for sanctions also for the whistleblower that are also of a criminal or administrative nature also after first instance proceedings, with the exception of those related to work relationships (e.g. bargaining agreements) or contractual.

ANNEX 3 – Examples of retaliation

- suspension
- elimination of advantages or benefits without motive (including remote work)
- demotion or lack of promotion
- salary reduction
- change in working hours
- training suspended
- notes of merit not assigned or bad reference
- imposition or administering of unjustified disciplinary measures
- coercion, intimidation, harassment or ostracism
- discrimination, unfair or unequal treatment
- failure to convert a fixed term employment contract into a permanent contract, when the employee had legitimate expectations to believe he/she would be offered permanent employment
- failure to renew or early termination of a fixed term employment contract
- damages, also to the reputation of a person, in particular on social media, or financial losses, including loss of economic opportunities or loss of income
- 'black-listing' on the basis of a formal or informal sector or industrial agreement, that may lead to the impossibility for the person to find employment in the sector or industry in the future
- termination of a contract for goods or services
- cancellation of a leave or approval
- subjection to psychiatric or medical evaluations

Such actions are also prohibited from being committed against the following subjects, for the purpose of avoiding 'cross-retaliation':

- facilitators, that is those who assist the whistleblower in the reporting and whose assistance must be confidential
- third parties associated with whistleblowers (e.g., colleagues or family members) • legal persons associated with the whistleblower