Whistleblowing Policy

Company Procedure for Managing Reports
Revision 01

Headquarters, software development and primary production unit (C1)
–Libra Division LAT237
HEMINA SPA
Hemina is under direction and coordination of ISOIL Industria SpA

Via Piemonte 2, 35044 Montagnana PD
Tax Code / VAT Number IT03317100281
Repertoire of economic and management PD 302565
Capital: euro 413,000.00
Tel. 0429/804424 r.a. Fax. 0429/807329
E mail : info@hemina.net

Secondary Production Unit (C2)
HEMINA SPA

Via Veneto, 5
35044 Montagnana PD
Tel. 0429/804424 r.a.
Fax. 0429/807329
E mail : info@hemina.net

HEMINA SPA

Summary

Whistleblowing: I want to know more

CSR (Corporate Social Responsibility) tool, essential for managing risks and protecting workers

Correct and effective management of reports (Whistleblowing) is extremely important to ensure compliance with the principles of legality and transparency defined by HEMINA S.p.A. (hereinafter also "Company" or "Organization"), in compliance with the current legislative provisions and the rules of conduct of the Company itself.

The purpose of the Whistleblowing system is to allow the Company to become aware of situations of risk or damage and to address the reported problem as promptly as possible. An advanced and formalized system through specific policies and training also allows real protection of the Reporter.

The Whistleblowing tool helps to identify and combat relevant illicit conduct pursuant to Legislative Decree 10 March 2023, n. 24 in implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, to protect the organization from economic and image damage, to spread the culture of ethics, legality and transparency within the company and to strengthen the system of internal controls and risk management.

The objectives of the Company through this procedure are therefore:
• to guarantee transparency and efficiency of the reporting channels applied;
• to promptly manage the reports made by the subjects as defined;
• to guarantee the protection of the personal data of the reporting subjects and, where applicable, anonymity if they request it;
• to guarantee the confidentiality of the information contained in the reports;
• to protect the reporting subjects from potential and possible situations of retaliation.

The objectives pursued are, therefore, to encourage and facilitate Reporting within the **company** and to reduce the risks of illicit conduct, building and strengthening the relationship of **trust** with **stakeholders** and promoting and increasing a corporate culture based on factors of transparency, integrity, good governance and corporate compliance.

The EthicPoint system

EthicPoint is an independent and certified[1] external service, in order to guarantee the protection of the confidentiality of the whistleblower. Its approach is that of a "service", that is, offering not only a channel to send reports, but a real form of assistance and (professional) advice to the whistleblower, who is free to use it even without formalizing the report in complete confidentiality.
For this reason, it is essential that before any action, the EthicPoint experts are contacted, who can provide all the necessary information.

1. Audit People Srl – Società Benefit is ISO 9001 certified and adopts corporate best practices in line with the principles of ISO 37002 and ISO 27001.

1. Purpose and application

This document defines the rules for the correct and effective management of a report by a subject (Reporter), also in order to identify and remove possible risk factors and activate, if necessary, the competent authorities.
The objective of this document is to provide the reporting person and all the subjects involved with clear operational instructions regarding the subject, content, recipients and methods of transmission and management of reports, as well as all forms of protection that are offered, pursuant to the law and internal procedures.

This procedure has also been defined as a guide for the preparation of circulars or information and training documents for the subjects involved.

It applies to all activities carried out by the Company.[2]

***Note 1*:** this procedure has been adopted by the Administrative Body as an organizational act of the provisions of law and as a **report**[3] to workers representative bodies.

Note 2: The EthicPoint Whistleblowing service is the internal reporting channel pursuant to Legislative Decree 24 of 2023, which outsources some reporting activities through a certified company, which is qualified through a specific service contract and appointed responsible for the processing of personal data for the purposes of the correct application of the GDPR.

2. Regulatory references

• Legislative Decree 24 of 10 March 2023 - "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law and laying down provisions concerning the protection of persons reporting breaches of national legislative provisions"
• Legislative Decree no. 231/2001 - "Regulation of the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of 29 September 2000" and subsequent amendments and additions
• Regulation (EU) 679/2016 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
• ANAC Guidelines (applicable version)
• Operational Guide for Private Entities – Confindustria (applicable version)
• ISO 37002 - Guide for the management of whistleblowing

See also Annex 1

---

[2] HEMINA SpA manufactures, markets, researches and develops mechanical, electromechanical and electronic instruments for industrial control and measurement. Furthermore, it offers calibration services for flow meters on behalf of third parties.

[3] As provided for in Article 51 of Legislative Decree 81 of 2015: "*... having heard the representatives or trade union organizations to acquire any observations ... (on) ... procedures for receiving reports and for their management.*"

3. Terms and definitions: essential concepts to know

Before proceeding with the reading of this procedure relating to the management of reports, it is necessary to clarify the meaning attributed to certain terms within this Policy.

- **Reporting (internal)**: communication, oral or written, of information on possible violations or misconduct, submitted through the internal reporting channel.
- **Reporter**: the natural person who reports (denunciates or publicly discloses) information on violations acquired in the context of his/her work.
- **Reported:** those who are the subject of a Report
- **Person involved**: the natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the violation is attributed or as a person otherwise implicated in the reported or publicly disclosed violation.
- **Facilitator**: a natural person who assists a whistleblower in the reporting process, operating within the same work context and whose assistance must be maintained reserved.
- **Work context**: the work or professional activities, present or past, carried out in the context of relationships with the Company through which, regardless of the nature of such activities, a person acquires information on violations and in the context of which he or she could risk suffering retaliation in the event of reporting, public disclosure or reporting to the judicial or accounting authority.
- **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 adopted.
- **Feedback**: communication to the reporting person of information relating to the follow-up that is being given or intended to be given to the report.
- **Violation**: behaviors, acts or omissions that harm the public interest or integrity of the public administration or private entity.
- **Retaliation**: any behavior, act or omission, even if only attempted or threatened, carried out as a result of the report, the complaint to the judicial or accounting authority or the public disclosure and which causes or may cause the reporting person or the person who filed the complaint, directly or indirectly, unjust damage.
- **Reporting in "bad faith"**: the Report made with the sole purpose of damaging or, in any case, cause harm to the company, the reported individual or third parties.
- **Report**: act by which a person brings to the attention of the competent authority (for example a judicial police officer) a prosecutable crime of which he has become aware.
- **Public disclosure**: making information about violations publicly available through print or electronic media or otherwise using means of dissemination capable of reaching a large number of people.

It is always recommended to consult Annex 2 to clearly understand what can be reported and which reports do not fall within the scope of Decree 24 of 2023 and therefore must not be made through whistleblowing reporting channels.

Important: for any doubts or clarifications, you can contact EthicPoint using the references provided in this procedure.

4. Reporting channels

Internal reporting tools

In line with the provisions of the regulations regarding the protection of individuals who report illicit activities or irregularities, the Company has established an independent and certified reporting channel by providing a specific address for the collection and management of reports.
The channel adopted allows any violation provided for by Decree 24 of 2023 and by company procedures to be reported by all potential whistleblowers authorised by the Decree, both internal and external, ensuring effective and confidential communication.
This solution has the characteristic of protecting the confidentiality of the whistleblower to the maximum.

The reporting modes activated are the following:

1.	***Landing page***	Dedicated web page (including email address instrumental to the functioning of the service4) PO
2.	***PO BOX***	PO BOX n. 301 c/o Mail Boxes Etc. - MBE Center 0197 Postal box address (Via Cenisio 37, 20154 Milan): Audit People Srl – Benefit Society – Indicating the name of the Organization and, if applicable, the double envelope procedure.
3.	***Toll-free number***	800 985 231 with voice messaging (valid for Italy only)

Pursuant to Article 4, paragraph 3 of Legislative Decree 24 of 2023, the Reporting Person, through the channels described above, may request a face-to-face meeting to orally present his/her report.

External reporting channels

ANAC

In order to use the reporting channel established by **ANAC**, certain **conditions** must be met, pursuant to art. 6 of the Decree, in particular:

- in your work context the activation of the internal channel is not foreseen as mandatory or, if provided, has not been activated,
- the internal report was not followed up,
- there are reasonable grounds to believe that internal reporting would not be given effective follow-up,
- the reporting person has reasonable grounds to believe that the violation may constitute a imminent or manifest danger to the public interest,
- the person has reasonable grounds to believe that if he or she made the internal report, it would not be followed up or that he or she would face retaliation.

[4] A dedicated email address has been activated for the Company: hemina@ethicpoint.eu

Public disclosure

The legislation also introduces the possibility for the whistleblower to make a public disclosure while benefiting from protection.
This is an extremely delicate development for businesses, due to the potential damage to the organization of a complaint made in the absence of justified reasons or well-founded evidence.

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

- that the internal and/or external channel has been used previously, but there has been no response or has not been followed up within the time limits set by the decree;
- that the whistleblower believes that there are well-founded reasons for an "imminent and obvious danger to the public interest", considered as an emergency situation or risk of irreversible damage, including to the physical safety of one or more persons, which requires that the violation be promptly disclosed with wide resonance to prevent its effects.
- that the whistleblower believes there are well-founded reasons to believe that the external report could entail a risk of retaliation or not have an effective follow-up because, for example,
- there could be a risk of destruction of evidence or collusion between the authority responsible for receiving the report and the perpetrator of the violation. In other words, there should be particularly serious situations of negligence or malicious behavior within the entity.

Communication, information, training and awareness

The Reporting Management System and the content of this procedure are the subject of communication, information, training[5] and awareness-raising among all recipients.
This procedure is available to potential whistleblowers, in particular it is available via:

1.	Sending via email to staff
2.	Publication on the company website (summary)
3.	Posting on company noticeboards

5. Reporting Management

The subjects involved (potential whistleblowers)

It is first necessary to identify and define, clearly and comprehensively, the subjects affected by this policy, or who can make a report. The Company identifies both internal and external stakeholders as potential whistleblowers. For example, the following are mentioned:

- employees of public administrations, employees of public economic bodies, private law bodies subject to public control, in-house companies, public law bodies or public service concessionaires;
- subordinate workers of private sector entities;

[5] See specific program depending on roles.

- self-employed workers, freelancers and consultants who work for public or private sector entities;
- volunteers and trainees, paid and unpaid, who carry out their work at public or private sector entities;
- shareholders and persons with administrative, management, control, supervisory or other functions representation;
- the facilitators;
- people in the same work context as the reporting person and who are linked to them by a stable emotional or kinship bond within the fourth degree;
- the reporting person's work colleagues who work in the same work context as the reporting person and who have a habitual and ongoing relationship with the reporting person.

Even when:

- the legal relationship has not yet begun, if information on violations has been acquired during the selection process or in other pre-contractual phases;
- during the probationary period;
- after the termination of the legal relationship if the information on the violations were acquired during the relationship itself.

Duty of confidentiality

The objective of this procedure is to ensure the protection of the Reporter, maintaining confidentiality of his identity, only in the case of reports coming from identifiable and recognizable subjects.
Anonymous reports , where they are adequately detailed and provided with a wealth of details, that is, where they are able to bring out facts and situations by relating them to specific contexts, are considered equivalent to ordinary reports. Anonymous reports and their processing takes place in any case through the same tools provided for confidential data, even if communication with the anonymous whistleblower is not possible after the report itself. Anonymous reports are also subject to this procedure, where applicable. The identity of the reporting person and any other information from which such identity may be deduced, directly or indirectly, may not be revealed, without the express consent of the reporting person, to persons other than those competent to receive or follow up on the reports, expressly authorised to process such data.

In the context of criminal proceedings, the identity of the reporting person is covered by secrecy in the manner and within the limits set out in Article 329 of the Code of Criminal Procedure.[6]
In the context of the disciplinary proceedings, the identity of the reporting person may not be revealed, where the challenge of the disciplinary charge is based on investigations that are separate and additional to the report, even if consequent to the same. Where the challenge is based, in whole or in part, on the report and knowledge of the identity of the reporting person is indispensable for the defense of the accused, the report may be used for the purposes of the disciplinary proceedings only in the presence of the express consent of the reporting person to the disclosure of his or her identity.

---

6 Article 329 of the Code of Criminal Procedure establishes, in fact, that the investigative acts carried out by the public prosecutor and the judicial police are covered by secrecy until the defendant (or the person under investigation) can have knowledge of them and, in any case, no later than the closure of the preliminary investigations.

Subject and content of the report

Reports are considered relevant if they involve reasonable and sincere suspicions about an employee with reference to possible fraud, dangers or other serious risks that could threaten customers, colleagues, stakeholders, the general public or the reputation of the Company.[7]

In particular, also taking into account the provisions of the relevant legislation, the report may concern actions or omissions, committed or attempted, which concern:

- administrative, accounting, civil or criminal offences;
- unlawful conduct relevant pursuant to Legislative Decree 8 June 2001, n. 231, or violations of the organizational and management models provided for therein;
- offences falling within the scope of the European Union or national acts indicated in the Annex to Decree 24 of 2023 or of the national acts implementing the European Union acts indicated in the Annex to Directive (EU) 2019/1937, even if not indicated in the Annex to the Decree, relating to the following sectors: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and security of networks and information systems;
- acts or omissions which harm the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union specified in the relevant secondary legislation of the European Union;
- acts or omissions relating to the internal market, as referred to in Article 26, paragraph 2, of the Treaty on the Functioning of the European Union, including infringements of European Union rules on competition and State aid, as well as infringements concerning the internal market related to acts which infringe corporate tax rules or arrangements the purpose of which is to obtain a tax advantage which defeats the object or purpose of the applicable corporate tax law;
- acts or behaviors that frustrate the object or purpose of the provisions set out in the acts of the Union in the sectors indicated above.

The report cannot, however, concern personal complaints of the Reporting Person or requests that pertain to the rules of the employment relationship or to relations with the superior. hierarchical or colleagues, for which you should refer to the personnel office.[8]
The following essential elements must be clear in the report, also for the purposes of assessing admissibility:

1. the identifying data of the reporting person, as well as an address to which updates should be communicated;
2. the circumstances of time and place in which the event occurred and a detailed description of the event of the same;
3. the personal details or other elements that allow the identification of the subject to whom the data are to be attributed reported facts.

The report should preferably contain the following elements:

1. the indication of any other subjects who can report on the facts being investigated report;

---

7 For further information, see ISO 37002 and ANAC Guidelines, “Objective scope” section (in the version applicable).

8 For other cases of exclusion from the application of the Decree, please refer to the provisions of art. 1 of the Decree 24 of 2023.

2. the indication of any documents that can confirm the validity of such facts;
3 any other information that may provide useful evidence regarding the existence of the facts reported.

In summary, reports, to be taken into consideration, must be adequately detailed and based on precise and consistent factual elements.

The recipients of the report

The provision of internal reporting channels that guarantee maximum confidentiality of the identity of the Reporter must be in compliance with Legislative Decree 24 of 2023.
The management of the internal reporting channel (outsourced service) is also entrusted to dedicated internal functions and with personnel with moral requirements, specifically trained for the management of this activity and in matters of personal data protection and confidentiality.

In particular, the referents are:

1.	EthicPoint – External reporting channel management service for the protection of the whistleblower
2.	Labour consultant (external)
3.	HR Office (centralized at group level)

6. Procedure and duties of the person receiving the report

Verification of the validity of the report

EthicPoint takes charge of the report which is forwarded to the internal functions in charge, issuing to the reporting person a notice of receipt of the report within 7 days of the date of receipt.

The internal functions diligently follow up on the reports received by providing feedback within 3 months from the date of the acknowledgement of receipt of the same or, in the absence of such acknowledgement, within three months from the expiry of the seven-day period from the submission of the report, through the e-mail address indicated above or through the references that the reporter will eventually transmit in the reporting method chosen.

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

If necessary, internal functions request clarifications from the whistleblower or any other subjects involved in the report, adopting the necessary precautions. They also verify the validity of the circumstances represented in the report through any activity deemed appropriate, including the acquisition of documentation and the hearing of any other subjects who may report on the reported facts, in compliance with the principles of impartiality, confidentiality and protection of the identity of the Reporter.

The Company, based on an assessment of the facts reported, may decide, in the event of evident and manifest groundlessness, to archive the report.

The Company arranges for the direct archiving of reports in the following cases:

- manifest lack of interest in the integrity of the Company;
- manifestly unfounded due to the absence of factual elements suitable to justify investigations;
- manifest lack of legal requirements for the application of the sanction;
- clearly emulative purpose;
- ascertained generic content of the report or content that does not allow understanding of the facts, or report accompanied by inappropriate or irrelevant documentation;
- production of documentation only in the absence of reporting of illicit conduct or irregularity;

In the event that elements of non-manifest groundlessness of the fact are identified, the internal functions in charge forward the report, also for the adoption of the consequent measures, to the subjects competent, such as:

1.	Sole Director
2.	Board of Auditors
3.	Judicial authority for the profiles of their respective competence

In line with the legislation in force regarding the protection of personal data, in order to preserve the investigative purposes and in the cases provided for by law, the Reported Person may not be immediately made aware of the processing of his/her data by the owner, as long as there is a risk of compromising the possibility of effectively verifying the validity of the complaint or of collect the necessary evidence.

Personal data relating to reports and the related documentation are stored and maintained for the period necessary to complete the verification of the facts set out in the report and for the **subsequent 5 years from the closure of the report**, except for any proceedings arising from the management of the report (for example disciplinary, criminal, accounting) against the reported person or the reporting person (for example bad faith, false or defamatory statements). In this case, they will be stored for the entire duration of the proceedings and until the expiry of the terms for appealing the related provision. Personal data that are clearly not useful for the processing of a specific report are not collected or, if collected accidentally, are deleted immediately.

Verification of the validity of the anonymous report

The verification phase of the validity of the report by the Company is similar for both confidential and anonymous reports. However, for anonymous reports, the following indications will be taken into account:

- the need for a more in-depth analysis of the elements that exclude it direct archiving;
- the Company will contact the Reporting Part if technically possible.

7. Protection of the whistleblower

The Company formally declares that no form of discrimination or discrimination will be implemented
retaliation against the whistleblower; on the contrary, any behavior in this direction will be sanctioned. In particular, pursuant to Article 17 of Legislative Decree 24 of 2023, it is expressly established that whistleblowers cannot suffer any retaliation.
The protection does not apply in cases where the report contains false information made with malice or gross negligence.

In the event of suspected discrimination or retaliation against the Reporter, related to the report, or abuse of the reporting tool by the same, the Company may proceed with the imposition of disciplinary sanctions.

Support measures are foreseen for the reporting entity:

- information;
- free assistance and advice on reporting methods and protection from retaliation.

The protection does not apply in cases where the report contains false information provided with intent or gross negligence.

8. Responsibility of the whistleblower

This policy does not affect criminal, civil and disciplinary liability in the event of a slanderous or defamatory report, also pursuant to the Criminal Code and art. 2043 of the Civil Code.[9]

Any forms of abuse of this policy, such as manifestly opportunistic reports or reports made with the sole purpose of harming the person reported or other individuals and any other hypothesis of improper use or intentional exploitation of the Company which is the subject of this procedure, as well as unfounded reports made with intent or gross negligence, are also a source of liability in disciplinary proceedings and in other competent bodies.

9. The Sanctioning System

An effective whistleblowing system must provide for sanctions both against the Reporter, in the event of abuse of the reporting tool, and against the reported parties in the event of verification of the reported illicit acts in accordance with the provisions of the legislation in force, including the applicable collective bargaining agreement, and specifically by art. 21 of Legislative Decree 24 of 2023.

---

9 Article 2043 Civil Code: Any malicious or negligent act that causes unjust damage to another obliges the person who committed the act to compensate for the damage. The crime of slander consists essentially in accusing another person of having committed a crime, even though one knows that person is innocent (Article 368 of the Penal Code). Defamation: anyone who, outside the cases indicated in the previous article, by communicating with several people, offends the reputation of another (Article 595 of the Penal Code).

10. Further information and contacts

For any further information regarding the above procedure, please contact:

1.	Laura Cazzaniga – laura.cazzaniga@isoil.it
2.	Valentina Chiarelli – valentina.chiarelli@isoil.it

ANNEX 1: Legislative reference scenario

The protection of employees and collaborators reporting illicit conduct within the workplace, both in the public and private sectors, is already widely provided for in official documents of wide international scope, such as the international conventions of the UN, OECD, and the Council of Europe, all ratified by Italy as having binding content, and the Recommendations of the Parliamentary Assembly of the Council of Europe.

At a national level, the concept of "whistleblowing" was introduced for the first time with Law 190 of 2012 - Provisions for the prevention and repression of corruption and illegality in public administration - which, limited to the public sector, with the provision of art. 1, co. 51, introduced art. 54-bis in Legislative Decree 165 of 2001 - General rules on the organization of work in public administrations - regulating a system of protection for public employees who decide to report illicit conduct of which became aware of by virtue of the employment relationship.

Subsequently, with Law 179 of 2017 - Provisions for the protection of authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship - the concept of reporting in the private sector was introduced, modifying art. 6 of Legislative Decree 231 of 2001 and making corrections to the reporting regulations in
public sector. With regard to the private sector, this provision establishes that the Organization, Management and Control Models referred to in the Decree must provide for

a. one or more channels that allow senior management or those under their control or supervision – to protect the integrity of the entity – to make detailed reports of unlawful conduct (relevant pursuant to "231" and based on precise and consistent factual elements) or violations of the Organization and Management Model, of which they have become aware by virtue of the functions performed. Furthermore, the same article provides that such reporting tools guarantee the confidentiality of the identity of the whistleblower in the activities of managing the report

b. at least one alternative reporting channel suitable for guaranteeing, through electronic means, the confidentiality of the identity of the whistleblower

c. the prohibition of retaliatory or discriminatory acts (direct or indirect) against the whistleblower, for reasons related (directly or indirectly) to the reporting

d. within the disciplinary system, sanctions against those who violate the measures to protect the whistleblower, as well as those who make reports with intent or gross negligence that prove to be unfounded.

Finally, Legislative Decree 24 of 2023 implemented the European Directive 1937 of 2019 on the subject, regarding the protection of persons who report violations. It aims to give full and effective implementation to the principles of transparency and responsibility in the management of reports, as they are considered an essential tool, not only in terms of risk management and general compliance, but also as a tool for relations with stakeholders according to the most modern governance rules.

In compliance with Directive 1937 of 2019 and, therefore, with the aforementioned decree, the subjects - in particular those indicated in article 3 of decree 24 of 2023 - are required to report any behavior or situations that may be considered incorrect or inconsistent with internal procedures and more generally with the provisions of the law in force. [10]

[10] Reporting must be possible according to procedures defined by the company and through specific internal reporting channels (as provided for in Article 4), in order to guarantee the confidentiality of the whistleblower and his protection from possible retaliation.

ANNEX 2 – Concrete examples of illicit acts or irregularities linked to Legislative Decree 231/2001 (not exhaustive) [11]

- harassment
- discrimination
- administrative irregularities and irregularities in accounting and tax compliance
- false statements, falsification or alteration of documents
- violation of environmental and workplace safety regulations
- theft of goods owned by the company or third parties
- misappropriation of money, assets, supplies belonging to the Company or to third parties
- destruction, concealment or inappropriate use of documents, archives, furniture, installations and equipment
- acceptance of money, goods, services or other benefits as incentives to favor suppliers or companies
- falsification of expense reports (for example, "inflated" reimbursements or for false trips)
- falsification of attendance at work
- disclosure of information which by its nature or by explicit indication of the law or Company provisions are confidential, whether they are proprietary information of the Company or belonging to third parties (e.g. competitors)
- use of the Company's resources and assets for personal use, without authorization
- irregularities in anti-money laundering matters
- computer fraud
- actions or omissions that result in harm or danger to human rights, the environment, health public, security and public interest
- the existence of relationships with subjects (natural or legal persons) adhering to criminal organisations of any nature or who participate in violation of the principles of legality
- violation of restrictive measures in economic and commercial relations or sanctions adopted at national, EU and international level
- public procurement
- incorrect communication about services or products or product safety and compliance placed on the internal market, risks of lack of consumer protection
- misuse of sensitive information
- financing of terrorism
- environmental protection or public health
- protection of personal data
- security of networks and information systems
- violations of European rules on competition and State aid
- violations concerning the internal market and in the field of corporate taxation

Examples of unreportable offences or irregularities (non-exhaustive) [12] [13]

- reports regarding labour disputes and pre-litigation phases
- discrimination between colleagues, interpersonal conflicts between the reporting person and another worker or with hierarchical superiors

---

11 Examples related to the application of Legislative Decree 231 of 2001.

12 ANAC guidelines, par. 2.1.1.

13 Incorrect reports may also provide for sanctions against the Whistleblower, including criminal or administrative sanctions, even after the first level of judgment, except those relating to the employment relationship (for example, CCNL) or contractual.

- reports relating to data processing carried out in the context of the individual employment relationship in the absence of damage to the public interest or the integrity of the public administration or private entity
- reports of violations where they are already mandatorily regulated by the European Union or national acts indicated in Part II of the Annex to the Decree or by the national acts which constitute the implementation of the European Union acts indicated in Part II of the Annex to Directive (EU) 2019/1937, even if not indicated in Part II of the Annex to the Decree (Legislative Decree no. 24/2023)
- market abuse reports referred to in Regulation (EU) No 596/2014 of the European Parliament and of the Council and Commission Implementing Directive (EU) 2015/2392 adopted on the basis of that Regulation, which already contain detailed provisions on the protection of whistleblowers
- reports concerning credit institutions and investment firms referred to in the Directive (EU) 2013/36 of the European Parliament and of the Council
- reports of violations in the banking sector.

ATTACHMENT 3 – Examples of retaliation

- suspension
- unjustified elimination of advantages or benefits (including smart working)
- demotion or failure to promote
- salary reduction
- the change in working hours
- suspension of training
- failure to assign merit notes or negative references
- the imposition or administration of unjustified disciplinary measures
- coercion, intimidation, harassment or ostracism
- discrimination, disadvantageous or unfair treatment
- failure to convert a fixed-term employment contract into a permanent employment contract, where the worker had legitimate expectations of being offered permanent employment
- failure to renew or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media, or financial loss, including loss of economic opportunities and loss of income
- inclusion in so-called "black lists" on the basis of a sectoral or industrial agreement formal or informal, which may result in the person being unable to find employment in the sector or industry in the future
- the termination of the contract for goods or services
- the cancellation of a license or permit
- undergoing psychiatric or medical examinations

Such actions are also prohibited with respect to the following subjects, in order to avoid conduct of "transversal" retaliation:

- facilitators, i.e. those who assist the Reporter in the reporting process and whose assistance must be reserved
- third parties connected with the Reporters (for example colleagues or family members)
- legal entities connected to the Reporting Party

ATTACHMENT 4 - Report management process scheme

Report Management Procedure

1. EthicPoint receives the report and carries out the first analysis with the company management body
2. Initial notification to the reporter (within the expected 7 days, in addition to the automatic one generated by the platform)
3. First contact with the company management body (immediate and in any case within 3 days) to define the credibility and relevance of the report and start of investigation and action activities regarding the transfer of information (classification of the report)
4. Registration of the activity
5. Second contact with the company management body (after 15 days) to verify the status progress and initial hypotheses and if support is needed.
6. Activity registration
7. Third contact with delegated subject (after 60 days) project progress and activities for response to the report.
8. Third contact registration
9. Feedback to the reporter (within 90 days)
10. Closing records.

Company web page

The recipient receives the report by carrying out the initial analysis with the company management body and proceeds with the standard transmission process (as described in the previous paragraph).

PO BOX

EthicPoint receives the material, carries out the initial analysis with the company management body and proceeds with the standard transmission process (as described in the previous paragraph).

Voice

EthicPoint receives the report by activating the detection procedure (for example voice recording or verbalization) by carrying out the first analysis with the company management body and proceeds with the standard transmission process (as described in the previous paragraph).

Software

EthicPoint defines the procedure for activating the reporting and activity repository with the company management body.

Note: if the software is activated, the other channels described will not be available.

Definitions

Management body: person (people) in charge of the investigation phase of the report

Investigation: analysis process aimed at defining the necessary actions for managing the event, including corrective and preventive actions to be implemented, any sanctions or possible reporting to the competent authorities.

Includes:

- Document analysis
- Gathering of necessary information
- Interviews
- Involvement of external experts as needed
- Development of hypotheses and their analysis
- Definition of useful evidence
- Recording of activities and decisions

Unique Identified Number: code that objectively identifies a report

Escalation: passing the report to the next (hierarchical) governance level in the event that the delegated subject does not respond adequately to the requests or is involved in the report itself.

Reference documents:

- EthicPoint service activation contract and letter
- Technical data sheet of the EthicPoint service