Faba S.r.l.
VAT no.: 05284370268

Via G. Bortolan 28
Vascon di Carbonera
31050 Treviso Italy

T. +39 0422 44 76 00
F. + 39 0422 44 77 73

info@myfaba.com
www.myfaba.com

WHISTLEBLOWING POLICY

CORPORATE PROCEDURE
FOR THE MANAGEMENT OF REPORTS

Faba S.r.l.
VAT no.: 05284370268

Via G. Bortolan 44
Vascon di Carbonera
31050 Treviso Italy

T. +39 0422 44 76 00
F. + 39 0422 44 77 73

info@myfaba.com
www.myfaba.com

Contents

Faba S.r.l.
VAT no.: 05284370268

Via G. Bortolan 44
Vascon di Carbonera
31050 Treviso Italy

T. +39 0422 44 76 00
F. + 39 0422 44 77 73

info@myfaba.com
www.myfaba.com

Whistleblowing: I want to know more

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

Correct and effective management of reports (Whistleblowing) is extremely important to ensure compliance with the principles of legality and transparency defined by the Company (hereinafter also "Company" or "Organisation"), in compliance with current legislation and with the Company's rules of conduct.

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 evolved system documented through specific policies and training also allows actual protection of the Whistle-blower.

The Whistleblowing tool helps to identify and combat relevant illegal conduct pursuant to Legislative Decree 10 March 2023, no. 24 in implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, to protect the organisation from economic damage and damage to its image, to disseminate 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 ensure transparency and efficiency of the reporting channels applied;
- to promptly manage the reports made by the subjects as defined;

- to guarantee protection of the personal data of the reporting parties and possibly anonymity if they request it;
- to guarantee confidentiality of the information contained in the reports;
- to protect whistle-blowers from potential and possible retaliatory situations.

The purposes pursued are, therefore, to encourage and facilitate Reporting within the company and to reduce the risks of wrongdoing, 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 external service[1], in order to guarantee the protection of the whistle-blower's confidentiality. Its approach is that of the "service", that is, offering not only a channel through which to send reports, but an actual form of (professional) assistance and consultancy to the whistle-blower, who is free to use it even without documenting the report in complete confidentiality.
This is why it is essential that EthicPoint experts are contacted before each action, who will be able to provide all the necessary information.

1. Purpose and scope of application

This document defines the rules for correct and effective management of a report by a subject (Whistle-blower), also in

[1] Audit People S.r.l. – Benefit Company is ISO 9001-certified and adopts business best practices in line with the principles of the ISO 37002 and ISO 27001 standards.

order to identify and remove possible risk factors and to activate, if necessary, the competent authorities.
The objective of this document is to provide the whistle-blower and all parties involved with clear operational indications about the object, contents, recipients and methods of transmission and management of the reports and also with all the forms of protection that are offered, in accordance with 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 parties involved.
It applies to all activities performed by the Company[2].

Note 1: this procedure was adopted by the Administrative Body as an organisational act of the legal provisions and as a report[3] to the workers' representative bodies.
Note 2: The EthicPoint Whistleblowing service is the internal reporting channel pursuant to Legislative Decree 24 of 2023, which outsources certain 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

[2] Faba S.r.l. - VAT no.: IT 05284370268 - with headquarters in via G.Bortolan, 28 – 31050 Vascon di Carbonera (TV) - is an Italian company specialised in the production and distribution of innovative products designed to facilitate listening to fairy tales and educational content for boys and girls. The goal of FABA is to create a world of fun and educational games to grow up without the use of screens, stimulating imagination and learning.
[3] As required by article 51 of Legislative Decree 81 of 2015: *"... having consulted the representations or trade unions to acquire any observations ... (on)... procedures for receiving reports and for their management."*

down provisions for the protection of persons reporting breaches of national regulatory provisions"
- Legislative Decree no. 231/2001 - "Discipline of the administrative liability of legal persons, companies and associations even without legal personality, in accordance with 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 individuals 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)
- Operating Guide for private entities – Confindustria (applicable version)
- ISO 37002 - Guide for managing whistleblowing

See also Annex 1.

3. Terms and Definitions: essential concepts to be aware of

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

- Reporting (internal): communication, verbal or written, of information on possible breaches or unlawful acts, submitted through the internal reporting channel.
- Whistle-blower: the natural person who makes the report (complaint or public disclosure) of information about breaches acquired within their work environment.

- Reported persons: those persons who are the subject of the Whistleblowing
- 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 breach is attributed or as the person in any case involved in the breach reported or publicly disclosed.
- Facilitator: natural person who assists a whistle-blower in the reporting process, operating within the same working context and whose assistance must be kept confidential.
- Work context: the work or professional activities, present or past, performed in the context of relationships with the Company through which, regardless of the nature of such activities, a person acquires information on breaches and in the context of which they could risk suffering retaliation in the event of notifying, public disclosure or reporting to the judicial or accounting authority.
- Follow-up: the action taken by the person entrusted with management of the reporting channel to assess the existence of the reported facts, the outcome of the investigations and any measures taken.
- Response: communication to the whistle-blower of information relating to the follow-up that is given or that is intended to be given to the report.
- Breach: conduct, actions or omissions that harm the public interest or the integrity of the public administration or private body.
- Retaliation: any behaviour, action or omission, even if only attempted or threatened, that occurs as a result of the reporting, of the complaint to the judicial or accounting authority or of the public disclosure and which causes or may cause the whistle-blower or the person who filed the complaint, directly or indirectly, unjust harm.

- Reporting in "bad faith": the Report made for the sole purpose of damaging or, in any case, harming the company, the Reported Person or third parties.
- Reporting: action by which a person brings to the attention of the competent authority (for example a judicial police officer) a prosecutable offence of which they have become aware.
- Public disclosure: making information about breaches publicly available through print or electronic media or otherwise using means of dissemination capable of reaching a large number of persons.

It is always advisable to consultAnnex 2 to clearly understand what can be reported and what are the reports that do not fall within the scope of Decree 24 of 2023 and therefore should not be made through whistleblowing reporting channels.

Important: for any uncertainty or clarifications, EthicPoint can be contacted through the references provided in this procedure.

4. The reporting channels

Internal reporting tools

In line with the provisions of the regulatory provisions on the protection of subjects who report offences or irregularities, the Company has established an independent and certified reporting channel with a specific address for the collection and management of reports.
The channel adopted makes it possible to report any breach provided for by Decree 24 of 2023 and by company procedures

by all potential whistle-blowers legitimised by the Decree, internal and external, ensuring effective and confidential communication.
This solution has the characteristic of protecting the whistle-blower's confidentiality as much as possible.
The reporting methods activated are as follows:

1	*Landing page*	Dedicated website - https://ethicpoint.eu/faba/ (including e-mail address instrumental to the operation of the service – faba@ethicpoint.eu)
2	*PO BOX*	PO BOX n. 301 c/o Centro MBE 0197 Post office box address (Via Cenisio 37, 20154 Milan): Audit People S.r.l. – Benefit Company – Indicating the name of the Organisation and if the double envelope procedure is envisaged.
3	*Free-phone number*	800 985 231 with voice messaging (only valid for Italy)

Pursuant to Article 4, paragraph 3 of Legislative Decree 24 of 2023, the Whistle-blower, through the channels described above, may request a face-to-face meeting to present their report verbally.

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 its working context activation of the internal channel is not envisaged as mandatory or, if envisaged, it has not been activated
- the internal report was not followed up on

- there are well-founded reasons to believe that the internal report would not be effectively followed up on
- the whistle-blower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest
- the person has reasonable grounds to believe that if they made the internal report, it would not be followed up on or that they would face retaliation

Public disclosure

The legislation also introduces the possibility for the whistle-blower to make a public disclosure benefiting from protection.
This is an extremely delicate development for businesses, due to the potential harm to the organisation 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 previously used, but there has been no response or the report has not been followed up on within the times envisaged by the decree;

• that the whistle-blower considers 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 breach be promptly disclosed with wide resonance to prevent its effects.

• that the whistle-blower considers there are well-founded reasons to believe that the external report may involve a risk of retaliation or may not have effective follow-up because, for example,
there may be a danger of destruction of evidence or collusion between the authority responsible for receiving the report

and the perpetrator of the breach. In other words, these should be particularly serious situations of negligence or wilful misconduct within the institution.

Communication, information, training and awareness-raising

The Reporting Management System and the content of this procedure are subject to communication, information, training[4] and awareness-raising among all recipients.
This procedure is available to possible whistle-blowers and in particular it is available through:

1	Publication on the company website
2	E-mail sharing to staff

5. Report management

The parties involved (potential whistle-blowers)

It is necessary firstly to identify and define, clearly and exhaustively, the subjects affected by this policy, that is who can make a report.

The Company identifies as potential whistle-blowers both internal and external stakeholders. By way of example, the following are cited:

- employees of public administrations, employees of public economic bodies, bodies governed by private law subject to

[4] See specific program depending on the roles.

public control, in-house companies, bodies governed by public law or public service concessionaires;
- employees of private sector entities;
- self-employed workers, freelancers and consultants who work for public or private sector entities;
- volunteers and trainees, paid and unpaid, who work for entities in the public or private sector;
- shareholders and persons with administrative, management, control, supervisory or representative functions;
- facilitators;
- persons of the same working context as the whistle-blower and who are linked to them by a stable emotional bond or kinship within the fourth degree;
- work colleagues of the whistle-blower who work in the same working context as the same and who have a habitual and current relationship with said person.

Even when:

- the legal relationship has not yet started, if the information on the breaches was acquired during the selection process or at other pre-contractual stages;
- during the probationary period;
- after dissolution of the legal relationship if the information on the breaches was acquired during the course of the relationship.

Obligation of confidentiality

The objective of this procedure is to ensure the protection of the Whistle-blower, keeping their identity confidential, only in the case of reports from identifiable and recognisable subjects. Anonymous reports, where they are adequately detailed and provided with a wealth of details, that is, where they are able to reveal facts and situations relating them to specific contexts,

are considered equivalent to ordinary reports. Anonymous reports and their processing in any case take place through the same tools provided for confidential ones, even if the dialogue with the anonymous reporter is not possible after the report itself.
Anonymous reports are also subject to this procedure, as far as is applicable.
The identity of the whistle-blower and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed without the express consent of the same whistle-blower, to persons other than those competent to receive or follow up on reports, expressly authorised to process such data.
In the context of criminal proceedings, the identity of the whistle-blower is covered by secrecy in the manner and within the limits provided for in article 329 of the Code of Criminal Procedure[5].
In the context of disciplinary proceedings, the identity of the reporting person cannot be revealed where the contestation of the disciplinary charge is based on investigations that are separate and additional to the report, even if consequent to the same. If the complaint is based, in whole or in part, on the reporting and knowledge of the identity of the whistle-blower is essential for defence of the accused, the report will only be usable for the purposes of the disciplinary procedure in the presence of the express consent of the whistle-blower to the disclosure of their identity.

[5] Article 329 of the Code of Criminal Procedure in fact establishes that the acts of investigation performed by the public prosecutor and by the judicial police are covered by secrecy until the accused (or the suspect) becomes aware of them and, in any case, no later than 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.[6]
In particular, in consideration of the provisions of the relevant regulations, the report may concern actions or omissions, committed or attempted, concerning:

- administrative, accounting, civil or criminal offences;
- relevant unlawful conduct pursuant to Legislative Decree no. 231 of 8 June 2001, or breaches of the organisation and management models envisaged 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 that constitute implementation of the European Union acts indicated in the annex to Directive (EU) 2019/1937, although 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; privacy protection and protection of personal data and security of networks and information systems;
- acts or omissions affecting the financial interests of the Union 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;

[6] For further information, see ISO 37002 and ANAC Guidelines section "Objective scope" (in the applicable version).

- acts or omissions concerning the internal market, as referred to in article 26, paragraph 2, of the Treaty on the Functioning of the European Union, including breaches of European Union competition and state aid rules, as well as breaches concerning the internal market connected with acts which infringe corporate tax rules or mechanisms, the purpose of which is to obtain a tax advantage which defeats the object or purpose of the applicable corporate tax legislation;
- acts or conduct that defeat the object or purpose of the provisions of the acts of the Union in the areas indicated above.

The report may not instead concern complaints of a personal nature of the Whistle-blower or requests that relate to the discipline of the employment relationship or relations with a hierarchical superior or colleagues, for which reference must be made to the H.R. Office[7].

The following essential elements must be clear in the report, also for the purposes of eligibility screening:

1. the identification data of the whistle-blower, as well as an address to which updates can be communicated;
2. the circumstances of the time at and place in which the event occurred and its detailed description;
3. the general information or other elements that allow identifying of the subject to whom the reported facts are attributed.

The report should preferably contain the following elements:

1. an indication of any other subjects who may report on the facts subject to reporting;

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

2. an indication of any documents that may confirm the substantiation of these facts;
3. any other information that may provide useful feedback on the existence of the reported facts.

In summary, the reports, in order to be taken into consideration, must be adequately substantiated and based on precise and concordant factual elements.

Report recipients

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

In particular, the contact persons are:

1	EthicPoint – External management service of the reporting channel to protect the whistle-blower
2	People & Culture Manager – Vanessa Vidali
3	Supervisory Body

6. Procedure and tasks of the person receiving the report

Verification of the validity of the report

EthicPoint receives the report that is sent to the designated internal functions, issuing the whistle-blower notice of receipt of the report within 7 days from the date of receipt.
The internal functions diligently follow up on the reports received, providing feedback within 3 months from the date of the notice of receipt of the same or, in the absence of such notice, within three months from the expiry of the seven-day period from submission of the report, through the afore-mentioned e-mail address or through the references that the whistle-blower will possibly transmit in the reporting method chosen.
All information will be handled in accordance with the provisions on whistle-blower protection.
If necessary, the internal functions request clarification from the whistle-blower or from any other parties 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 consultation with any other persons who may report on the communicated facts, in compliance with the principles of impartiality, confidentiality and protection of the identity of the Whistle-blower.
The Company, on the basis of an assessment of the facts covered by the report, may decide, in the event of evident and manifest unfoundedness, to archive the report.

The Company directly archives reports in cases of:

- the manifest absence of interest for the integrity of the Company;
- manifest unfoundedness due to the absence of factual elements suitable to justify investigations;
- manifest non-existence of the legal conditions for application of the penalty;

- manifestly emulative purposes;
- ascertained generic content of the report or content such as not to allow understanding of the facts, or report accompanied by inappropriate or irrelevant documentation;
- production of documentation only in the absence of the reporting of illegal conduct or irregularities;
- lack of data that constitute essential elements of the Report.

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

1	Board of Directors
2	the Judicial Authority for the profiles under their respective jurisdiction

In line with current legislation on 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 their data by the Data Controller, while there is a risk of compromising the possibility of effectively verifying the validity of the complaint or of collecting the necessary evidence.

The personal data relating to the reports and the related documentation are kept and retained for the period necessary to complete verification of the facts set out in the report and for 5 years after closure of the report, except for any proceedings resulting from management of the report (for example disciplinary, criminal, accounting-related) against the Reported Person or the whistle-blower (for example statements made in bad faith, false or defamatory). In this case, they will be kept for the entire duration of the procedure and until expiry of the

terms of appeal of the relative provision. Personal data that are manifestly not useful for the processing of a specific report are not collected or, if accidentally collected, are deleted immediately.

Verification of the anonymous report validity

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

- the need for greater depth when verifying the elements that exclude direct archiving;
- contacting by the Company of the Whistle-blower will take place if technically possible.

7. Protection of the whistle-blower

The Company formally declares that no form of discrimination or retaliation will be implemented against the whistle-blower; on the contrary, any behaviour in this direction will be sanctioned. In particular, pursuant to article 17 of Legislative Decree 24 of 2023, it is expressly stated that whistle-blowers may not suffer any retaliation. The protection does not apply in cases where the report contains false information made with intent or gross negligence.
In the event of suspected discrimination or retaliation against the Whistle-blower, related to the report, or abuse of the whistleblowing tool by the Whistle-blower, the Company may impose disciplinary sanctions.

Support measures are envisaged for the whistle-blower:

- information;

- free assistance and consultancy on reporting methods and protection from retaliation.

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

8. Whistle-blower responsibilities

This policy is without prejudice to criminal, civil and disciplinary liability in the event of slanderous or defamatory reporting, also pursuant to the Criminal Code and to art. 2043 of the Italian Civil Code[8].
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 areas.

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

[8] Article 2043 of the Italian Civil Code: Any intentional or negligent act, which causes unfair damage to others, obliges the person who committed the act to compensate for the damage. The crime of slander consists, essentially, of blaming another person for having committed a crime, despite knowing them to be innocent (Article 368 of the Italian Criminal Code). Defamation: anyone, except for the cases indicated in the previous article, communicating with more than one person, who offends the reputation of others (Article 595 of the Criminal Code).

collective bargaining agreement, and specifically with art. 21 of Legislative Decree 24 of 2023.

10. Further information and contacts

For any further information relating to the above procedure, please contact:

1	Veronica Balbi - veronica.balbi@maikii.com

11. ANNEX 1: Legislative Reference Scenario

The protection of the employee and collaborator, reporting illegal conduct within the working environment of both the public and private sectors, is already extensively provided for in official documents of wide international scope, such as the international Conventions of the UN, OECD, and Council of Europe, all ratified by Italy as binding content, and the Recommendations of the Parliamentary Assembly of the Council of Europe.
Nationally, 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, para. 51, introduced art. 54-bis in Legislative Decree 165 of 2001 - General rules on the organisation of work in public administrations - regulating a system of protections for public employees who decide to report illegal conduct of which they have become aware by reason 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 then introduced, amending art. 6 of Legislative Decree 231 of 2001 and making corrections to the regulation of reporting in the public sector. With regard to the private sector, this provision stipulates that the Organisation, Management and Control Models referred to in the Decree must provide for:

a. one or more channels that allow senior management figures 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 breaches of the Organisation and Management Model, of which they have become aware by virtue of the functions performed. In addition, the same article provides that such reporting tools guarantee the confidentiality of the identity of the whistle-blower in the reporting management activities
b. at least one alternative reporting channel suitable to guarantee, with IT methods, the confidentiality of the identity of the whistle-blower
c. the prohibition of retaliatory or discriminatory acts (direct or indirect) against the whistle-blower, for reasons related (directly or indirectly) to the reporting
d. within the disciplinary system, sanctions against those who breach the whistle-blower's protection measures, as well as those who make reports with intent or gross negligence that prove to be unfounded.

Finally, Legislative Decree 24 of 2023 transposed the European Directive 1937 of 2019 on the subject, concerning the protection of persons who report breaches. It seeks to fully and effectively

implement the principles of transparency and accountability 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 accordance with Directive 1937 of 2019 and, therefore, with the afore-mentioned decree, 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 incorrect or inconsistent with internal procedures and more generally with the provisions of the law in force[9].

[9] Reports must be possible as per 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 whistle-blower and their protection from any retaliation.

12. ANNEX 2 – Concrete examples of offences or irregularities connected to Legislative Decree 231/2001 (non-exhaustive) 10

- harassment
- discrimination
- administrative, accounting and tax compliance irregularities
- false declarations, falsification or alteration of documents
- breach of environmental and occupational safety regulations
- theft of property owned by the company or by third parties
- misappropriation of money, securities, 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 favour suppliers or companies
- falsification of expense reports (for example, "inflated" reimbursements or claiming for false trips)
- falsification of attendance at work
- disclosure of information that by its very nature or by explicit indication of the law or company provisions is confidential, whether it is information owned by the Company or belonging to third parties (for example competitors)
- use of the Company's resources and assets for personal use, without authorisation
- anti-money laundering irregularities
- cyber fraud

[10]Examples related to the application of Legislative Decree 231 of 2001.

- actions or omissions that result in harm or danger to human rights, to the environment, to public health, to safety and to the public interest
- the existence of relationships with subjects (natural or legal persons) belonging to criminal organisations of any nature or who participate in breaching the principles of legality
- breach 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 safety and conformity of products placed on the internal market, risks of failure to protect consumers
- misuse of sensitive information
- terrorist financing
- environmental protection or public health
- personal data protection
- security of networks and computer systems
- breaches of European competition and state aid rules
- internal market and corporate tax breaches

Examples[11] of unlawful acts or irregularities that cannot be reported (not exhaustive)[12]

- reports concerning labour disputes and pre-litigation phases
- discrimination between colleagues, interpersonal conflicts between the whistle-blower and another worker or with hierarchical superiors

[11] ANAC guidelines, para. 2.1.1.

[12] Incorrect reports may also provide for sanctions against the Whistle-blower, including criminal or administrative sanctions, even after the first level of judgement, except those relating to the employment relationship (for example CCNL) or contractual relationship.

- reports relating to data processing performed 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 body
- reports of breaches where they are already compulsorily governed by the European Union or by national acts indicated in part II of the annex to the decree or by the national acts that constitute the implementation of the European Union acts indicated in part II of the annex to Directive (EU) 2019/1937, although not indicated in part II of the annex to the decree (Legislative Decree no. 24/2023)
- market abuse reporting under 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 whistle-blowers
- reports concerning credit institutions and investment firms referred to in Directive (EU) 2013/36 of the European Parliament and of the Council
- reports of breaches in the banking sector.

13. ANNEX 3 – Examples ofretaliation

- suspension
- unjustified elimination of advantages or benefits (including smartworking)
- demotion or non-promotion
- salary reduction
- change in working hours
- the suspension of training
- non-assignment of 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
- the non-renewal 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 opportunity and loss of income
- inclusion in so-called "black lists" on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in the sector or industry in the future
- dissolution of the contract for goods or services
- the cancellation of a licence or permit
- imposition of psychiatric or medical examinations

These actions are also prohibited with regard to the following subjects, in order to avoid "transversal" retaliatory conduct:

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

14. ANNEX 4 - Reporting management process diagram

Reporting management procedure

1. EthicPoint receives the report and conducts the first analysis with the company's management body
2. Initial communication to the whistle-blower (within 7 days, additional to the automatic notification 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 to start investigation and action activities regarding the passing of information (report classification)
4. Activity log
5. Second contact with the company management body (after 15 days) to check progress and initial assumptions and the possible need for support.
6. Activity log
7. Third contact with delegated subject (after 60 days) project progress and activities for feedback on the report.
8. Third contact recording
9. Response to whistle-blower (within 90 days)
10. Closing records.

Company website

The receiver receives the report, then conducting the first 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, conducts the first analysis with the company management body and proceeds with the standard transmission process (as described in the previous paragraph).

Vocalisation

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

Software

EthicPoint defines with the company management body the procedure for activating the repository of reports and activities.

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

Definitions

Management body: person(s) assigned to the investigation phase of the report

Investigation: analysis process in order to define the necessary actions to manage the event including the corrective and preventive actions to be implemented, any sanctions or possible reporting to the competent authorities.
It includes:

- Document analysis
- Collection of necessary information
- Interviews
- Involvement of external experts as required
- Hypothesis development and analysis
- Definition of useful tests
- Minutes of activity and decisions

Unique identified number: code that objectively identifies a report

Escalation: transfer of the report to the next (hierarchical) level of governance in the event that the delegated entity does not respond in a timely manner to the requests or is involved in the report itself.

Reference documents:

- EthicPoint service contract and activation letter
- EthicPoint service technical data sheet