



WHISTLEBLOWING POLICY

Adopted by the Board of Directors on January 26th 2024

Version	Date	Approved by	Description of the updates
01	26/01/2024	IPI Srl BoD	First version

TABLE OF CONTENTS

1. INTRODUCTION.....	3
2. REFERENCES	3
3. DEFINITIONS	4
4. WHISTLEBLOWERS.....	6
5. THE PURPOSE OF THE REPORT	7
6. GOOD-FAITH OR BAD-FAITH REPORTS.....	7
6.1 Good-faith reports	7
6.2 Bad-faith reports	8
7. REPORTING METHOD	8
7.1 Internal report.....	8
7.2 External report and Public disclosure.....	8
7.3 Anonymous report	9
8. REPORT CONTENTS.....	9
9. REPORT MANAGEMENT PROCEDURES	10
10. WHISTLEBLOWER PROTECTION	13
11. REPORTED PARTY PROTECTION	15
12. SANCTIONING MEASURES	16
13. UPDATING.....	16
14. DISSEMINATION, INSTRUCTION AND TRAINING	17

1. INTRODUCTION

On March 30th, 2023, **Legislative Decree 24/2023** (hereinafter also referred to as the “**Whistleblowing Decree**” or just the “**Decree**”) came into force, implementing EU Directive 2019/1937, concerning the protection of persons who report breaches of European Union law and containing provisions regarding the protection of whistleblowers.

“Whistleblowing”, in particular, means the reporting of conduct, acts or omissions in breach of the Organisational, Management and Control Model pursuant to Legislative Decree 231/2001 and the Code of Ethics or of national or European Union regulations that affect the public interest or the integrity of the public administration or private entity, carried out by a person who has become aware of it as part of his or her public or private working context.

In the light of the above, this document (hereinafter referred to as the “**Whistleblowing Policy**” or “**Policy**”) aims to describe the tools that can be used, within the corporate context, to report unlawful conduct. Therefore, the purpose of the Policy is to:

- identify the persons who may make reports;
- delimit the scope of conduct, events or actions that may be reported;
- identify the channels through which reports can be made;
- represent the operational procedures for the submission and handling of reports, as well as for any subsequent investigation activities;
- inform the reporter and the reported party of the protection forms that are granted and guaranteed.

2. REFERENCES

Below are the main references relevant to this Policy:

- Directive (EU) 2019/1937 of the European Parliament and the Council of October 23rd, 2019 concerning the protection of persons who report breaches of Union law;
- EU Data Protection Regulation 2016/679;
- Legislative Decree 24 of March 10th, 2023 “Implementation of Directive (EU) 2019/1937 of the European Parliament and the Council of October 23rd, 2019 on the protection of

persons who report breaches of Union law and provisions concerning the protection of persons who report breaches of national laws”;

- Italian Anti-Corruption Authority (ANAC) Guidelines on the Protection of Persons Reporting Violations of Union Law and the Protection of Persons Reporting Violations of National Law;
- Confindustria Operational Guidelines for Private Entities;
- Legislative Decree 231/2001, “Regulations on the administrative liability of legal persons, companies and associations, including those without legal status”;
- Organisation, management and control model adopted pursuant to Legislative Decree 231 of June 8th 2001 adopted by the Company;
- Code of Ethics adopted by the Company.

3. DEFINITIONS

For the purposes of this Policy, the terms listed shall have the meaning specified below:

Recipients	Company employees on permanent and fixed-term contracts (executives, middle management, white-collar and blue-collar workers), directors, members of corporate and supervisory bodies, as well as anyone who, for whatever reason, has employment, collaboration or business relations with the Company, including collaborators, trainees, temporary workers, consultants, agents, suppliers and business partners, even before the legal relationship with the Company began or after it was terminated.
Public disclosure	Placing information about breaches in the public domain through the press or electronic media or other means of dissemination capable of reaching a large number of people.
Enabler	Person assisting the whistleblower with the reporting process, who operates in the same work environment and the assistance of whom is kept confidential.
231 model	Organisational, Management and Control Model adopted by the Company, which defines a structured and organic system of principles, internal rules, operating procedures and control activities, adopted for the purpose of preventing conduct liable

	to give rise to the types of offences and offences provided for in Legislative Decree 231/2001.
Code of Ethics	A document with which the Company affirms, in implementation of the values of legality, loyalty, honesty and professionalism, the principles and rules of conduct that its employees, the members of its administration and control bodies, suppliers, consultants, partners and those who have relations, directly or indirectly, permanently or temporarily with it, are required to comply with when carrying out their activities on its behalf
Supervisory Board ("SB")	The Supervisory Board of the Company appointed pursuant to Legislative Decree 231/01
Whistleblower	A natural person who makes an internal or external report or public disclosure of information on violations acquired in the context of his or her work context.
Reported Party	Person mentioned in the internal or external report, or in the Public Disclosure, understood as the person who is alleged to have committed the breach or as a person otherwise involved in the reported or publicly disclosed breach.
Report	Written or oral communication about breaches, including reasonable suspicions concerning breaches committed or likely to be committed by the Company, as well as elements concerning conduct aimed at concealing such breaches.
Anonymous reports	Reports lacking elements enabling their author to be identified.
External report	Written or oral disclosure of breaches, submitted through the external reporting channel referred to in section 7.2.
Bad-faith report	Any communication received by the company that proves to be unfounded according to objective elements and that proves, again according to objective elements, to have been made with the aim of causing damage.
Internal report	Written or oral disclosure of breaches, submitted through the internal reporting channel referred to in section 7.1.
Irrelevant report	Any communication received by the company concerning conduct that does not constitute a breach. All communications received by the company which, on the basis of the vagueness of their contents, do not allow adequate verification.
Breaches	Conduct, acts or omissions detrimental to the public interest or the integrity of the company and consisting of the conduct referred to in section 5.

4. WHISTLEBLOWERS

In accordance with the provisions of Article 3 of the Whistleblowing Decree, the following persons, i.e. the Whistleblowers, may submit a report:

- the company's employees, including part-time workers and collaborators, casual workers;
- self-employed workers and holders of a collaboration relationship who work for the company;
- company workers or collaborators, who supply goods or services or carry out works for third parties;
- the company's freelancers and consultants;
- volunteers and trainees, paid and unpaid;
- shareholders and persons with administrative, management, control, supervisory or representative functions in the company, even if such functions are exercised on a de facto basis;
- terminated employees, when information on breaches was acquired during the period they were working for the company;
- subjects who acquired information on violations during the trial period;
- persons not yet employed, when information on violations was acquired during the pre-contractual stages or in the selection process.

In accordance with Article 3, paragraph 5 of the Whistleblowing Decree, the company ensures the protection and safeguarding not only of the whistleblowers, as mentioned above, but also of individuals assisting the whistleblower throughout the whistleblowing process, such as Enablers, the identity of whom remain confidential. Additionally, the company guarantees protection for individuals associated with the whistleblower, such as colleagues or family members. This includes individuals within the same work context who are connected to the whistleblower by a stable emotional or family relationship up to the fourth degree, or individuals who maintain regular and ongoing relations with the whistleblower.







The company also guarantees protection to entities owned by the whistleblower or for which the whistleblower performs work, as well as to entities operating in the same work environment as the whistleblower.

5. THE PURPOSE OF THE REPORT

Pursuant to Article 2, paragraph 1, letter a) of the Whistleblowing Decree, reporting may concern:

- conduct or a situation contrary to the 231 Model, the Code of Ethics or the regulations, directives, policies and internal procedures adopted by the company and relevant under Legislative Decree 231/2001;
- breaches of European Union laws.

Irrelevant reports are considered non-executable and, therefore, will be archived. In particular, the following are considered irrelevant reports:

	reports relating to situations of a personal nature involving claims or grievances concerning relations with colleagues;
	having insulting tones or containing personal offences or moral judgments and aimed at offending or harming the personal and/or professional honour and/or decorum of the person or persons to whom the reported facts refer;
	reports based on mere suspicions or rumours concerning personal facts not constituting an offence;
	reports made for purely defamatory or slanderous purposes;
	reports of a discriminatory nature, in that they refer to sexual, religious or political orientation or to the racial or ethnic origin of the reported party;
	reports relating to information already in the public domain.

6. GOOD-FAITH OR BAD-FAITH REPORTS

6.1 GOOD-FAITH REPORTS

The Whistleblower is encouraged to make Reports that are as detailed as possible and provide as much information as possible, in order to allow due verification and adequate feedback. After

having made a Report, the Whistleblower who discovers any errors may immediately inform the same channel through which the Report was made.

6.2 BAD-FAITH REPORTS

Reports shall be deemed to have been made in bad faith if they turn out to be **deliberately** frivolous, false or unfounded, with defamatory content or in any case concerning **deliberately** erroneous or misleading information, for the sole purpose of damaging the company, the Reported Party or other people to whom the Report refers.

In this case, the company reserves the right to take appropriate action - including the adoption of appropriate disciplinary sanctions - against the Whistleblower.

7. REPORTING METHOD

7.1 INTERNAL REPORT

In accordance with the provisions of Article 4 of the Whistleblowing Decree, the Company has set up an internal whistleblowing channel consisting of a dedicated IT platform, freely accessible by whistleblowers, which can be accessed via a link [Whistleblowing – SignalACT \(signalact-inaz.it\)](https://signalact.inaz.it) published on IPI S.r.l.'s institutional website, which allows the submission of Reports in writing or orally (by leaving a voice message).

At the request of the Whistleblower, a direct meeting with the Reporting Manager may be arranged. To do this, the Whistleblower will have to send a request for a meeting through the same IT platform.

7.2 EXTERNAL REPORT AND PUBLIC DISCLOSURE

The Whistleblower may submit the Report to the ANAC (Italian Anti-Corruption Authority) through the external reporting channel made available by the same Authority if:

- the Whistleblower has already made an internal report but without any response;

- the Whistleblower has reasonable grounds to believe that, if it were to make an internal report, it would not be effectively followed up, or that the report might result in retaliation;
- the Whistleblower has well-founded reasons to believe that the breach may constitute an imminent or obvious danger to the public interest.

The Whistleblower may proceed by **Public Disclosure** if:

- the Whistleblower has already made an internal and external report but without any response;
- the Whistleblower has well-founded reasons to believe that, due to the specific circumstances of the case, the external report may entail a risk of retaliation or may not be effectively followed up.

7.3 ANONYMOUS REPORT

Anonymous reports will also be taken into account, provided **they are adequately substantiated and detailed**. Anonymous Reports limit the company's ability to investigate effectively, as it is impossible to establish a channel for asking the Whistleblower for information.

Among the factors relevant to assessing an anonymous Report, the company considers the importance of the reported Breach, the credibility of the facts represented and the possibility of verifying the truthfulness of the Breach from reliable sources.

8. REPORT CONTENTS

The Reports are, in any event and regardless of the procedure used, **detailed and based on precise and concise factual elements**, so as to enable the Reporting Manager to take the necessary measures and carry out the appropriate checks and investigations, also by carrying out investigations and issuing requests for clarifications to the Whistleblower, where identified. The Whistleblower may agree to be identified, giving contact details where he or she can be contacted (by way of example only: name and surname, e-mail address, telephone number).

What must the Report contain?

✓	clear and complete description of the facts being reported
✓	any information and any useful indication aimed at identifying the identity of the persons who committed the breach and to whom the Report relates
✓	the nature, background and any useful details to describe the subject of the Report
✓	circumstances of time and place, if known, relating to the subject of the Report
✓	any further information deemed useful for the investigation of the Report
✓	documentary or evidentiary allegations in support of the Report, including the indication of witnesses or persons who may be able to report on the facts that are the subject of the Report

Where available, appropriate documentation in support of the Report should be attached, including the indication of witnesses or persons who may be able to report on the facts that are the subject of the Report.

9. REPORT MANAGEMENT PROCEDURES

a. Receipt of the Report and Preliminary Verification

The company has set up a committee consisting of the HR Specialist and the Compliance Officer to handle Reports. If the purpose of the Report involves one or more members of the committee, the Whistleblower may forward the Report directly and exclusively (through the channels made available by the company) to a different contact person in the Human Resources Department, who will proceed to carry out the in-depth investigations deemed necessary. (In both cases, the “**Manager**”). To send the report to a party other than the Committee, the user must select from the platform's drop-down menu the option "Category" → "Reporting to third parties".The Manager has exclusive access to the channels dedicated to receiving Reports, which are managed securely and in such a way as to guarantee the confidentiality of the Whistleblower's identity as well as the protection of any third parties named in the Report, and to prevent access by unauthorised personnel.

For each report, the IT platform [Whistleblowing – SignalACT \(signalact-inaz.it\)](https://signalact-inaz.it) immediately and automatically assigns its own protocol number, user name and password, which allows each Whistleblower to access the platform, check the progress of the Report and supplement useful documentation for the investigation.

The Manager makes an initial assessment of the plausibility and credibility of the conduct reported, carrying out an analysis to verify the existence of the legal and factual conditions, as well as the relevance and the presence of sufficient elements to further investigate the Report (also by requesting further information from the Whistleblower, if he/she has not remained anonymous). Following this analysis, the Managing Director decides whether to carry out further investigations with the formal start of the investigation, requesting, if necessary, additions from the Whistleblower through the chat provided by the platform, or to close and file the Report.

If the Reports concern facts that are relevant pursuant to Legislative Decree 231/2001, the Manager shall promptly inform the Supervisory Board appointed by the company and start the investigation with the support of the SB, jointly managing the various stages of the report.

b. The report sent to an unqualified subject

If the Report is submitted to a party other than the Manager, the receiving party shall, within seven days of its receipt, transmit the Report to the Manager, simultaneously notifying the Whistleblower that it has been sent.

c. Assessment and communication of outcome

The purpose of the assessment phase is to verify the validity of the Report received. The Manager carries out any activity deemed appropriate, including interviewing the whistleblower and any other person who may report circumstances useful for the purposes of ascertaining the facts reported, also in order to assess any remedial action.

The Manager may also rely on the support and cooperation of external consultants, appointed for the purpose, when, due to the nature and complexity of the assessment, their involvement is required. These persons are bound to the same obligations of protection of the whistleblower and of the reported party as provided above. The Committee has set aside an annual budget of €15,000 to meet any costs associated with the management of the report with the support of third parties (lawyers, experts, technicians); the Budget can be used autonomously without prior

authorisation from Management in order to guarantee the Committee's independence and autonomy in the management of reports.





If, during the investigation, objective elements emerge proving a “*lack of good faith*” on the part of the Whistleblower, the Manager will immediately notify the Board of Directors to assess the activation of any sanctioning procedures.

At the end of the investigative activity, after ascertaining the grounds of the Report, the Manager draws up a report summarising the assessments carried out and the resulting evidence, in order to share with the Board of Directors the adoption of sanctioning actions, or the preparation of any corrective actions. This report is also shared and managed with the Supervisory Body, if the Report concerns facts relevant to Legislative Decree 231/2001. In any case, the Manager shall periodically prepare a report summarising the investigations carried out during the period and the evidence that emerged, and share it with the Company's Supervisory Board.

c. Archiving

The decision to archive the Report is formalised in a **report** containing the reasons for the archiving. The report is shared with the Board of Directors and the Supervisory Board, if the Report concerns facts relevant to Legislative Decree 231/2001.

The Report is archived if:

	the Report is irrelevant;
	the Report refers to facts of such general content that they cannot be verified;
	the Report was made in bad faith;
	the preliminary investigation proved its groundlessness.

d. Timing of the Reporting Process

Sending an acknowledgement of receipt of the Whistleblower	<ul style="list-style-type: none">immediately, but no later than 7 days after receipt of the Report
Responding to the Report	<ul style="list-style-type: none">within 3 months from the date of acknowledgement of receiptin the absence of an acknowledgement of receipt, within 3 months of the expiry of the 7-day period following the submission of the Report
Response to request for a face-to-face meeting	<ul style="list-style-type: none">no later than 7 days after receipt of the request for a face-to-face meeting
Setting the date of a face-to-face meeting	<ul style="list-style-type: none">no later than 10 days after receipt of the request for a face-to-face meetingin cases of proven urgency, within 5 days of receipt of the request for a face-to-face meeting

e. Storage

The entire reporting management process is tracked within the IT platform [Whistleblowing – SignalACT \(signalact-inaz.it\)](#). All documentation relating to the Report is archived and stored within the same platform for as long as necessary for the management of the Report and, in any case, no longer than five 5 years from the closure of the Reporting procedure.

10. WHISTLEBLOWER PROTECTION

The Whistleblower is guaranteed protection by the Company if the instructions provided in the Policy are complied with. Protection is not guaranteed to the Whistleblower if he/she participated in the commission of the unlawful conduct. The protections granted to the Whistleblower are also extended:

- to the Enabler;

- to people in the same work environment as the Whistleblower with a stable emotional or kinship link up to the fourth degree;
- to the Whistleblower 's work colleagues with whom they have a regular and current relationship;
- to entities owned by the Whistleblower or for which the Whistleblower works, as well as to entities operating in the same work environment.

a. Confidentiality

In preparing and implementing its internal whistleblowing channel, the Company guarantees that **the identity of the Whistleblower, the Whistleblower and of any other persons involved, as well as the content of the Whistleblowing and of the relevant documentation**, shall be kept confidential. Reports may not be used beyond what is necessary to adequately follow them up.

The Whistleblower's identity and any other information from which it can be inferred, directly or indirectly, cannot be disclosed, without the Whistleblower's express consent, to persons other than those authorised to receive or follow up the reports and expressly authorised to process such data..

b. The Prohibition of Retaliation and Protection Measures

The Company **shall not tolerate any kind of threat, retaliation, unjustified sanction or discrimination** against the Whistleblower, the Reported Party or any person who has cooperated in the activities of investigating the grounds of the Report. The adoption of discriminatory or retaliatory measures against the Whistleblower may result in disciplinary proceedings against the person responsible.

In light of the provisions of Article 19, paragraph 1 of the Whistleblowing Decree, the Whistleblower may report to ANAC (the Italian Anti-Corruption Authority), through the methods established on the website <https://www.anticorruzione.it/>, any retaliation that they feel they have suffered within their work context.

Examples of retaliatory conduct include, but are not limited to:

	dismissal, suspension or equivalent measures
	downgrading or non-promotion
	change of duties, change of workplace, reduction of salary, change of working hours
	suspension of training or any restriction of access to it
	demerits or bad references
	the adoption of disciplinary measures or other sanctions, including fines
	coercion, intimidation, harassment or ostracisation
	discrimination or otherwise unfavourable treatment
	failure to convert a fixed-term employment contract into a permanent employment contract if the employee had a legitimate expectation of such change
	non-renewal or early termination of a fixed-term employment contract
	damage to a person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and/or loss of income
	inclusion on improper lists, on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future
	early termination or cancellation of the contract for the supply of goods or services
	cancellation of a licence or permit
	the request to undergo psychiatric or medical examinations

11. REPORTED PARTY PROTECTION

Appropriate protective measures are also provided for the benefit of the Reported Party, to prevent any discrimination. The submission and receipt of a Report is not sufficient to initiate any disciplinary proceedings against the Reported Party.

Should the decision be taken to proceed with the investigation, the Reported Party may be contacted and given the opportunity to provide any necessary clarification.

12. SANCTIONING MEASURES

Effective, proportionate and dissuasive sanctions may be applied:

- against the Reported Party, if Reports are well-founded;
- against the Whistleblower, if Reports are made in bad faith;
- against the person responsible, if the protection provided for in the Policy has been violated or if Reports have been obstructed or attempts have been made to obstruct them.

Disciplinary proceedings against employees of the Company may be commenced according to the seriousness of the breach, in application of the principles of proportionality, as well as the criteria of correlation between the breach and the sanction and, in any case, in compliance with the procedures provided for by the laws in force and the disciplinary system outlined within the Company's Model 231. In order to ensure impartiality and avoid conflicts of interest, decisions on any disciplinary measures, complaints or other actions to be taken are taken by the relevant corporate organisational functions and, in any case, by persons other than the person who conducted the whistleblowing investigation.

13. UPDATING

It is the Manager's responsibility to periodically review this Whistleblowing Policy and the reporting channels provided herein in the light of its operations and experience and to ensure, in any event, its constant alignment with the relevant regulations.

14. DISSEMINATION, INSTRUCTION AND TRAINING

This Policy is disseminated by uploading it on the Company website, displaying it on company notice boards and any other tool deemed appropriate. The Company promotes dissemination, information and training activities regarding this Policy to ensure the widest knowledge and most effective application of the same.