Whistleblowing Policy

Approved by the Board of Directors on 12 July 2023

Updated on 21 July 2026

Unieuro S.p.A.

Registered Office in Forlì (FO), Palazzo Hercolani, Via Piero Maroncelli, 10, 47122
VAT number: 00876320409

Revision history

Current revision:
3.0

Version	Reason for chance	Dates
1.0	Approval by the Board of Directors	15 March 2019
2.0	Update	12 July 2023
3.0	Update	21 July 2026

INDEX

Premise 4
1. Purpose and scope 5
2. Recipients 6
3. References 7
4. Definitions 7
4.1 Violation 7
4.2 Reporter 7
4.3 Internal Reporting 7
4.4 "Anonymous" reporting 8
4.5 Reporting in "bad faith" 9
4.6 Privacy Delegates 9
5. Liability 9
6. Internal Reporting Channels 10
7. Methods of transmission and investigation of reports 11
7.1 Transmission Mode 11
7.2 Pre-Check of the Alert 11
7.3 Investigation 12
7.4 Outcome of the investigation 12
7.5 Follow up 13
8. Periodic reporting 13
9. Protective measures envisaged 14
9.1 Whistleblower Protection 14
9.2 Rights of the Reported 15
10. Data protection and document storage 15
11. Approval and updating of the Policy 16

Premise

On December 29, 2017, Law n. 179, "Provisions for the protection of persons who report crimes or irregularities of which they have become aware in the context of a public or private employment relationship" came into force (published on the "*Gazzetta Ufficiale"*, General Series n. 291 of December 14, 2017). This law, aimed at encouraging the collaboration of workers to facilitate the disclosure of acts or phenomena contrary to ethical company rules within public and private entities, has undergone modifications following the publication of an additional legislative decree in the "*Gazzetta Ufficiale"*.

Specifically, Legislative Decree n. 24 of 2023[1], implementing Directive (EU) 2019/1937, amended the previous national regulations on Whistleblowing, enclosing in a single regulatory text the protection regime for subjects who report illegal conduct of which they have become aware in a work environment.

This regulatory framework aims to ensure full protection of the freedom of expression of the whistleblower's thoughts and the strengthening of legality and transparency within the Entities to prevent crimes.

While these protections were already established by the previous law of 2017, Legislative Decree n. 24 of 2023 involves a significant expansion of the scope of protection of whistleblowers in the private sector.

Legislative Decree n. 24 of 2023 amended art. 6 of Legislative Decree 231/2001[2] by providing in paragraph *2-bis* of the same that the Organization, Management and Control Models must guarantee a reporting system in order to highlight illegal conduct, guaranteeing internal reporting channels, as well as a reporting regime for the whistleblower, aimed at preventing retaliatory conduct by the employer and sanctioning violations of the legislation in question.

The most important changes concern: i) the expansion of reporting subjects; ii) the extension of the scope of violations that may be reported; iii) greater procedural of the internal activities of the entities (internal reporting channels) in order to ensure the confidentiality of the whistleblower and the of subjects involved in the report, as well as to ensure timely and efficient management of the same; iv) the introduction of an external channel entrusted to ANAC

[1] Published in the *Gazzetta Ufficiale*, General Series n. 63 of 15 March 2023.

[2] Legislative Decree n. 24 of 10 March 2023 amended the text of art. 6, paragraph 2-bis of Legislative Decree n. 231/2001 and repealed paragraphs 2-ter and 2-quarter of art. 6 of Legislative Decree n. 231/2001, previously governed by Law n. 179/2017.

(National Authority Anti-Corruption), also for the private sector[3]; v) the introduction of the possibility of making public disclosures of violations, subject to certain conditions[4]; vi) the strengthening of ANAC's role and sanctioning powers in relation to the proper implementation of the relevant regulations.

Finally, the range of subjects protected by the legislation is expanded, also including the so-called facilitators, i.e. those who provide assistance to the whistleblower during the reporting process and whose activity must remain confidential, to third parties and legal entities connected to the whistleblower[5].

In order to comply with regulations, Unieuro (hereinafter also "the Company") has adopted this Policy to regulate the reporting of illicit behavior and/or violations of national and European provisions that involve misconduct in specific sectors and provides recipients with tools to make reports suitable for ensuring, by electronic instruments, the confidentiality of the identity of the whistleblower, the person involved and the person in any case mentioned in the report, as well as the content of the report and the related documentation.

1. Purpose and scope

This document (hereinafter referred to as the "Policy") is intended to:

- to set procedures through which to report illegal or illegitimate conduct or behavior, commission or omission, which constitute or may constitute a violation, or inducement to violate, the Group Code of Ethics, the Organization, Management and Control Model

[3] In addition to the so-called "internal" reports, the possibility of addressing reports to ANAC (so-called "external") is established, also for private entities, in certain cases: 1) when not provided, in the work context in which the whistleblower operates, the obligation to activate the internal reporting channel, or if, if mandatory, it has not been activated or, if present, is not compliant; 2) when an internal report has already been submitted that has not been processed or with a negative final measure; 3) when the whistleblower has reasonable grounds to believe that if he made the report he would run the risk of possible retaliation; 4) when the whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.
Guidelines will be issued by ANAC relating to the methods of presentation and concrete management of external reports.

[4] It also establishes the possibility of protecting the whistleblower through "public disclosures", provided that certain conditions are met (he has first reported internally and externally or directly externally, but has not taken appropriate action in response to the report within the three-month period, or has reasonable grounds to believe that there may be an imminent or obvious danger to the public interest or the prospects that the violation may be effectively addressed are scarce).

[5] Pursuant to art. 3 of Legislative Decree n. 24 of 10 March 2023, this includes, for example, work colleagues and/or family members or even legal entities related to the whistleblower.

pursuant to Legislative Decree 231/01 adopted by the Company or the policies and/or rules governing corporate processes, as well as violations of specific national and European provisions[6];

- to ensure a work environment in which employees and collaborators can peacefully report violations committed within the Company.

This Policy applies to Unieuro.

2. Recipients

The recipients of this Policy (hereinafter referred to as "Recipients" and/or "Whistleblowers") are:

- the top management and members of the corporate bodies of Unieuro;
- shareholders and persons with administrative, managerial, control, supervisory or representative functions, even if these functions are exercised in practice only;
- all employees, self-employed workers and internal collaborators of Unieuro;
- freelancers and consultants who work at Unieuro;
- workers or collaborators, who provide goods or services or who carry out works in favour of Unieuro;
- volunteers and interns, paid and unpaid, who work at Unieuro.

In addition, in accordance with the amendments to Legislative Decree n. 24 dated March 10, 2023, concerning Whistleblowing regulations, art. 2 and 3 of the Decree, it is also established

[6] According to art. 2 paragraph 1 letter a) number 5) of Legislative Decree n. 24 dated March 10, 2023, and the attachments to the Decree, means offences in the following sectors: public procurement; financial services, products and markets and the 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 and protection of personal data and network security, and of information systems. Infringements are also included: infringements of EU competition and State aid rules, as well as infringements concerning the internal market related to acts that infringe corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax rules.

that the protection of the whistleblower also applies: i) if the legal relationship has not begun; (ii) during the probationary period; iii) after the termination of the employment relationship.

3. References

- Organisation, Management and Control Model pursuant to Legislative Decree 231/01 (hereinafter also referred to as "Model 231");
- Code of Ethics of Unieuro S.p.A. (hereinafter also the "Code of Ethics");
- Legislative Decree no. 231 of 8 June 2001, as amended;
- Law n. 179 of 30 November 2017;
- Legislative Decree n. 24 of 10 March 2023;
- Company policies and procedures;
- Privacy Organizational Model (EU Regulation 679/2016);
- Anti-corruption policy.

4. Definitions

4.1 Violation

Violation means any conduct, act or omission that harms the public interest or the integrity of the Company and that consists of a violation of the Code of Ethics, Model 231, the policies/procedures adopted by the Company and/or offenses that fall within the scope of the European Union or national acts indicated in the decree and in the annex to the decree.

4.2 Reporter

This means the natural person (internal or external to the Unieuro organisation) who reports or publicly disseminates information on violations acquired in the context of the professional or employment relationship with the Company.

4.3 Internal Reporting

For the purposes of this Policy, internal reporting means the communication, written or oral, made through the channels made available by the Company, by a whistleblower concerning information, including well-founded suspicions, concerning violations committed or which, on the basis of concrete elements, could be committed in Unieuro.

Reports must be made in good faith, based on precise and consistent facts and substantiated with specific information so as to be easily verified.

It is particularly important that the report includes, where these elements are known to the whistleblower:

- the indication of the company function / point of sale to which the report refers;
- the names and role of the persons involved (internal and/or external) or elements that may allow their identification;
- the names of any other persons who may report on the facts being reported;
- the date/time frame and place where the event occurred;
- the scope/object of the violation (Code of Ethics, Model 231, policies, national or European Union provisions, etc.);
- a detailed description of the facts that occurred and how they became known;
- indicate whether the facts have already been reported to other parties (supervisory authorities, internal or external parties, etc.);
- reference to any documents that can confirm the validity of the facts reported;
- the indication about the management of the whistleblower's personal data.

4.4 "Anonymous" reporting

Anonymous reporting means the reporting of violations or suspected violations received by the Company without indicating the identity of the whistleblower.

Next, the concept of "anonymous" is to be understood in the sense of "non-nominative". In terms of personal data protection legislation (General Data Protection Regulation 2016/679/EU – hereinafter "GDPR"), the report conveyed through the platform has a "pseudonymous" nature, in the sense that it is assigned an alphanumeric identification code and that Unieuro can interact with the whistleblower by giving feedback and carrying out the activities provided for by Legislative Decree 24/2023. Therefore, the whistleblower has full guarantee that his or her identity remains confidential, in accordance with Legislative Decree 24/2023 and the policy of protection of the whistleblower as a vulnerable subject pursued by Unieuro pursuant to the GDPR.

The report, even if "anonymous", must be documented and substantiated, to provide the useful and appropriate elements to allow an appropriate verification of the validity of the reported facts.

4.5 Reporting in "bad faith"

A report in "bad faith" means a report without foundation, libelous or defamatory, made with the aim of damaging or causing prejudice to employees, internal collaborators, members of corporate bodies or third parties (e.g. customers, suppliers, partners, consultants, collaborators) in a business relationship with Unieuro.

In the event that it is proven that the employee has made a report in bad faith, the Company may activate the disciplinary system provided for by its Model 231 and in line with the provisions of the whistleblowing regulations.

4.6 Privacy Delegates

Privacy Delegates means the Company Functions involved in the report, i.e. the subjects who have received specific privacy instructions from Unieuro regarding the management of Whistleblowing reports.

5. Liability

The verification of the validity of the reports and the decisions regarding their management are entrusted to the Internal Audit Director ("hereinafter also the "IA Director") of the Company.

In carrying out this activity, the AI Director, if he/she deems it appropriate, may share the subject of the report and be operationally supported by the Chief Legal & Risk Officer, Chief People & Culture Officer, RSPP and/or the DPO of the Company, maintaining and guaranteeing the confidentiality of the identity of the whistleblower, unless otherwise indicated by the whistleblower himself.

The AI Director, therefore:

- performs all preliminary activities (preliminary verification of the existence of the prerequisites, re-routing of non-relevant reports);
- evaluates the checks to be carried out, the functions to be involved in the analyses, the request for additional information or possible archiving;
- guarantees the confidentiality of the information received, including the identity of the whistleblower;
- prepares periodic reports regarding the reports received.

In the event that the subject of the report involves the AI Director, the whistleblower may transmit the report directly and exclusively (through the tools made available to the Company) to the Chief Legal & Risk Officer. In this case, the latter will proceed independently in carrying out the investigations deemed necessary.

6. Internal Reporting Channels

In compliance with Whistleblowing regulations, the Company provides internal reporting channels.

Internal reports are collected through the following channels:

- **in written form**, through the use of the **Whistleblowing Portal** made available by the Company on its institutional website and which provides a guided path for the whistleblower.
  Access to the Whistleblowing Portal is subject to the "no-log" policy in order to prevent the identification of the whistleblower who intends to keep his or her identity confidential: this means that, if access is made from a device not connected to the company network, Unieuro's IT systems are not able to identify the access point to the portal (IP address); where access to the Whistleblowing Portal is made through a device connected to the company network, Unieuro implements technical and organisational solutions to prevent the user making the report from being traced. For each report entered, the Portal assigns a unique identification code that allows each whistleblower to check the progress of the report, in a completely confidential manner. Similarly, in the event that a report is not adequately substantiated, the AI Director or the Chief Legal & Risk Officer[7], using the Portal and its tools, will have the right to request further details from the whistleblower, always and only through this code and within the platform, for the purpose of an in-depth analysis of the reported case.
- **orally**, through the use of the Whistleblowing Portal made available by the Company on its institutional website by recording a voice message or by requesting a direct meeting with the manager of the reporting channel. In the case of a face-to-face meeting, the whistleblower shall ensure that the meeting takes place within a reasonable time.

[7] The report is forwarded to the Chief Legal & Risk Officer, who will proceed independently in carrying out the investigations deemed necessary, in the event that the subject of the report involves the Internal Audit Director

7. Methods of transmission and investigation of reports

7.1 Transmission Mode

With reference to the internal reporting channel, it is designed to ensure confidentiality on the identity of the whistleblower, the reported person or the persons involved, as well as on the content of the report and the documentation relating to it.

Recipients can send reports, according to the methods set out below, as soon as they become aware of the events that generated them.

Reports - as highlighted in chapter 6 "Internal Reporting Channels" - can be made in writing or orally form (by voice messaging or request for a meeting with the AI Director), through the use of the online Portal made available by Unieuro and which provides a guided path for the whistleblower.

For more details regarding the correct use of the Whistleblowing Portal and the compilation of the relevant fields relating to reporting, please refer to the dedicated FAQs on the Unieuro institutional website.

7.2 Pre-Check of the Alert

All reports received are managed by the AI Director who carries out a preliminary check in order to verify that the report falls within the scope of this Policy and that useful data and information have been provided to allow an initial assessment.

In this phase, the subject of the report may be shared and the support of other functions (Chief Legal & Risk Officer, Chief People & Culture Officer, RSPP, DPO) may be requested in order to assess the presence of suitable conditions to proceed with the investigation phase, always maintaining and guaranteeing the confidentiality of the identity of the whistleblower.

In any case, at the end of the report process, the whistleblower receives an identification code that enables him to check the progress of his report on the Portal and constitutes notice of receipt of the report on the Portal itself.

The whistleblower may also be contacted, in the manner previously described (through the platform's internal messaging), by the AI Director or the Chief Legal & Risk Officer[8] to request further information that may be necessary.

7.3 Investigation

The AI Director, in compliance with the terms provided for by the regulations:

- may reject the report because it is not considered admissible and/or not eligible for investigation;
- may request additional information to investigate the report before deciding whether to take charge of the report;
- it may initiate specific analyses, making use of the competent structures, as well as involving the corporate functions involved in the report (Privacy Delegates);
- ensures that the investigation is thorough, that it has a reasonable duration and that it respects the confidentiality of the whistleblower and the persons involved, including any person reported;
- provides, within the Whistleblowing Portal, for the drafting of a summary of the subject of the report, used for the population of the reports intended for the Supervisory Body.

If the IA Director deems the report to be proceeding and admissible, he will then inform:

- the Supervisory Body in the event of a report concerning the violation of the Organisation, Management and Control Model pursuant to Legislative Decree 231/01, the Code of Ethics, the Anti-Corruption Policy;
- Top Management if the report concerns the violation of company procedures or guidelines for activities that fall outside the scope of application of Legislative Decree 231/01, and also in the event of violations of specific national and European provisions.

7.4 Outcome of the investigation

At the end of the investigation, the AI Director (or the Chief Legal & Risk Officer) communicates the outcome of the investigations carried out to the Supervisory Body or to the Top Management, by competence. The whistleblower, who by entering the identification code provided to him, on the online Portal can monitor the process of his report, must receive feedback on the follow-up

[8] The report is transmitted to the Legal Department if the subject of the report involves the Internal Audit Director

that is intended to be given to the report within three months from the date of notice of its receipt.

If the Supervisory Body or the competent Top Management detects the validity of what has emerged, it is shared, based on the results, with the competent Company Functions from time to time (always in the person of the Privacy Delegates), in order to define any intervention plans to be implemented and the actions to be taken to protect the Company. Otherwise, if, at the end of the analysis, the Supervisory Body or the Top Management should detect the absence of sufficiently detailed elements or, in any case, the groundlessness of the facts referred to in the report, the latter will be archived, together with the related reasons, by the AI Director.

The Company may take the most appropriate disciplinary and/or legal measures to protect its rights, property and image, against the employee who has committed or has been involved in a violation; any disciplinary measures will be taken in agreement with the HR Department and in compliance with the relevant CCNL (National Labor Collective Agreement).

In addition, in compliance with the Whistleblowing Policy, to ensure compliance with the obligations in this regard, there are a series of administrative fines that ANAC can apply to private entities in case of violation of the rules established by the decree.

An Employee who has committed or has been involved in a violation will not be immune from disciplinary measures for the sole fact of having reported his or her own or others' violation, pursuant to this Policy. However, this circumstance may be taken into account in the assessment of the disciplinary measure to be adopted.

7.5 Follow up

The AI Director, on the recommendation of the Supervisory Body or Top Management, may provide for the execution of follow-up interventions to verify the effective resolution of critical issues or the progress of the related action plan, requesting information from the identified Managers.

8. Periodic reporting

The IA Director prepares, on an annual basis, a summary report of the reports received, the investigation activities carried out or still in progress and the evidence that has emerged,

including an analysis of the trend of the same compared to previous years, which is shared with the Supervisory Body and, where deemed appropriate, with the Top Management.

9. Protective measures envisaged

9.1 Whistleblower Protection

The whistleblower will not be subjected to retaliatory or discriminatory conduct for having made the report.

Retaliation means any behavior, act or omission, even if only attempted or threatened, that occurs in the work context and that causes, directly or indirectly, unjust damage to the protected person. Examples of retaliatory measures include, but are not limited to: i) dismissal, suspension or equivalent measures; ii) demotion in rank or non-promotion; (iii) changes in duties, changes in the place of work, reduction in salary, changes in working hours; (iv) suspension of training or any restriction of access to training; v) the request for psychiatric or medical examinations.

Unieuro guarantees the confidentiality of the identity of the whistleblower and of any other information, including any attached documentation, from which his/her identity can be directly or indirectly traced. This is without prejudice to the right for the whistleblower to make himself available to contacts freely provided by him or for Unieuro, in the cases provided for by art. 12 of Legislative Decree 24/2023, the possibility of asking the whistleblower for consent to the disclosure of his or her identity.

Unauthorized disclosure of the identity of the whistleblower or information from which it can be inferred is considered a violation of this Policy.

In addition, it is necessary that:

- the same guarantee of confidentiality provided for the whistleblower is provided for the persons involved and/or mentioned in the report, as well as for the facilitators;
- the management of reports is kept separate from the management of other personal data. The information collected and processed in the context of the management of reports must be transmitted, as far as necessary, exclusively to the persons in charge of processing and competent to initiate the verification procedure or to adopt the necessary measures according to the results. In any case, the recipients of the information must

ensure that the information is always handled confidentially and that the appropriate security measures are applied.

The same protection measures also apply to: a) facilitators; b) persons in the same working context as the reporting person, the person who has filed a complaint with the judicial or accounting authority or the person who has made a public disclosure and who are linked to them by a stable emotional or family bond within the fourth degree; (c) work colleagues of the reporting person or of the person who has lodged a complaint with the judicial or accounting authority or made a public disclosure, who work in the same working context as the reporting person and who have a habitual and current relationship with that person; (d) entities owned by the reporting person or the person who has lodged a complaint with the judicial or accounting authority or who has made a public disclosure or for which the same persons work, as well as entities operating in the same working environment as those persons.

9.2 Rights of the Reported

The reported person must be granted the same guarantees of confidentiality as the reporting person, until the conclusion of the procedure initiated on the basis of the report[9].

During the verification and verification of possible non-compliance, the individuals subject to the reports may be involved or be notified of this activity but, in no case, a procedure will be initiated solely because of the report, in the absence of concrete evidence regarding its content. This could possibly happen on the basis of other evidence found and ascertained starting from the report itself.

In order to guarantee the right of defence of the reported persons, the right to question them by means of a paper-based procedure, through the acquisition of written observations and documents, is envisaged.

Finally, if the report is found to be unfounded or in bad faith, for the sole purpose of damaging the person reported, the imposition of disciplinary sanctions against the whistleblower remains unaffected, as well as his possible criminal and civil liability in the event of a defamatory or slanderous report.

10. Data protection and document storage

The information and any other personal data acquired are processed – also in the context of the Portal – in compliance with the GDPR and Legislative Decree n. 196/2003 (Personal Data

[9] Pursuant to art. 12 paragraph 7 of Legislative Decree n. 24 of 10 March 2023.

Protection Code) and subsequent amendments, as well as in compliance with the rulings of the EU and national data protection authorities.

In order to guarantee the confidentiality of the whistleblower, the person who manages the reports is obliged to use them only to follow up on them, as well as the prohibition to reveal the identity of the whistleblower or information from which it can be deduced, without his express consent, to persons other than those competent and authorized by law.

The documentation relating to reports must be stored securely and in compliance with the regulations in force within the Company on the classification and processing of information. This documentation must be stored with the IA Director and must only be accessible to authorized personnel.

This documentation shall include at least the name, identification code and structure/office of the whistleblower (where available), details of the whistleblower, statements, activities carried out, outcome of the investigation and actions taken.

In order to ensure the management and traceability of the reports and related activities, the IA Director takes care of the preparation and updating of all the information regarding the reports and ensures, using the Portal and its IT tools, the archiving of all the related supporting documentation for the time necessary for the processing of the same and in any case no later than a period of 5 years from the date of communication of the final outcome of the reporting procedure.

11. Approval and updating of the Policy

Unieuro approves this Policy by resolution of the Board of Directors. This is subject to revision if the regulations, referred to as best practice, are subject to changes or jurisprudential interpretations. In the event of substantial amendments and interventions (e.g. significant regulatory updates), the Policy is expected to be subject to further approval by the Chief Executive Officer; in the event of changes of a purely formal nature (e.g. organisational updates or updates relating to the Whistleblowing Portal), the Chief Legal & Risk Officer is responsible for updating and revising the Policy and undertakes to ensure that it is correctly disseminated and applied.