Whistleblowing Policy

Approved by the Board of Directors on 15 March 2019
Last updated by the Board of Directors on 12 July, 2023

Unieuro S.p.A.

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

Index

Premise

On December 29th, 2017, Law n° 179 "Provisions for the protection of individuals who report crimes or irregularities of which they have become aware in the context of a public or private employment relationship" (published on the "*Gazzetta Ufficiale",* General Series n° 291 of 14 December 2017) came into force. 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 legislation 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 guarantee full protection of the freedom of expression of the whistleblower's thoughts and the strengthening of legality and transparency within the Entities as a function of crime prevention.

If these protections were already established by the previous law of 2017, the 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 intervened by amending art. 6 of Legislative Decree n° 231/2001[2] providing in paragraph *2-bis* of the same Model 231, must guarantee a reporting system to highlight illegitimate behavior, guaranteeing internal reporting channels, as well as a whistleblower protection regime, aimed at preventing retaliatory conduct by the employer and sanctioning violations of the relevant regulation.

The most important changes concern: i) the expansion of reporting subjects; (ii) the extension of the scope of violation that may be reported; iii) more systematic procedures for the company (internal reporting channels) in order to ensure the confidentiality of the whistleblower and of

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

[2] Legislative Decree n° 24 of March 10, 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 Legislative Decree n° 231/2001, previously governed by Law no. 179/2017.

the subjects involved in the report, as well as to ensure its timely and efficient management; iv) the introduction of an external channel entrusted to ANAC (National Authority Anti-Corruption), including 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 regulation.

Finally, the range of subjects protected by the legislation is expanded to 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. The company provides recipients with tools to make reports ensuring the confidentiality of the whistleblower's identity, the individuals involved, any persons mentioned in the report, as well as the content of the report and its supporting documentation, through appropriate computerized methods.

1. Purpose and scope

This document (hereinafter "Policy") is aimed at:

- to set procedures through which to report illegal or illegitimate conduct or behavior, commission or omission, which constitutes or may constitute a violation, or inducement

[3] In addition to the so-called "internal" reports, the possibility for private individuals to submit reports to ANAC (referred to as "external" reports) is established in certain cases: 1) when there is no obligation, within the work context of the whistleblower, to activate the internal reporting channel, or if it is obligatory but has not been activated or, if present, is not in compliance; 2) when an internal report has already been submitted but has not been processed or has received a negative final decision; 3) when the whistleblower has reasonable grounds to believe that they would face the risk of possible retaliation if they were to make the report; 4) when the whistleblower has reasonable grounds to believe that the violation may constitute an imminent or evident danger to the public interest. ANAC will issue guidelines on the methods of submission and concrete management of external reports.

[4] The possibility of protecting the whistleblower through "public disclosures" is also established, provided that certain conditions are met (the whistleblower has previously reported internally and externally, or directly externally, but no appropriate action has been taken in response to the report within a period of three months, or the whistleblower has reasonable grounds to believe that there may be an imminent or evident danger to the public interest or that the prospects of effectively addressing the violation are poor).

[5] Pursuant to Article 3 of Legislative Decree n° 24 dated March 10, 2023, examples of individuals considered as colleagues at work and/or family members, or even legal entities connected to the whistleblower..

to violate the Group Code of Ethics, the Model 231 adopted by the Company or the policies and/or rules governing business processes, as well as violations that consist of administrative, accounting, civil or criminal offenses or violations of specific national and European provisions;[6]

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

This Policy applies to the Company.

2. Recipient

Recipients of this Policy (hereinafter "Recipients" and/or "Reporters") are:

- the top management and members of Unieuro's corporate bodies;
- shareholders and persons with administrative, management, control, supervisory or representation functions, even if such functions are exercised merely in a "*mero fatto*" way;
- all employees, self-employed workers and internal collaborators of the Company;
- freelancers and consultants who work at the Company;
- workers or collaborators, who provide goods or services for the benefit of the Company;
- volunteers and interns, paid and unpaid, who work at the Company.

Additionally, in accordance with the amendments to Legislative Decree n° 24 dated March 10, 2023, concerning Whistleblowing regulations, it is also established in Articles 2 and 3 of the

[6] According to Article 2, paragraph 1, letter a), number 5) of Legislative Decree n° 24 dated March 10, 2023, and the attachments to the Decree, the term "violations" refers to the following sectors: Procurement; financial services, products and markets and prevention of money laundering and terrorist financing; Security and Compliance dei products; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and network security, and
of information systems. This also includes violations: infringements of EU competition and State aid rules, as well as infringements concerning the internal market related to acts infringing corporate tax rules or mechanisms the purpose of which is to obtain a tax advantage which defeats the object or purpose of the applicable tax legislatione on companies.

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

3. References

- The Model 231;
- Group Code of Ethics (hereinafter also "Code of Ethics");
- Legislative Decree n° 231 of June 8, 2001 and subsequent amendments;
- 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 private entity concerning any a violation of the Code of Ethics, Model 231, the policies / procedures adopted by the Company, administrative, accounting, civil or criminal offenses and / or offenses that fall within the scope of application 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 organization) who reports or publicly disseminates information on violations known in the context of the professional or working relationship with the Company.

4.3 Reporting

For the purposes of this Policy, reporting means the communication, written or oral, of information on possible violations transmitted by a whistleblower to the functions responsible for its receipt, through the Whistleblowing Portal.

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

It is particularly important that it includes, where these elements are known by the Reporter:

- the indication of the company function/point of sale to which the report refers;
- the names and roles 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, policy, national or European Union provisions, etc.);
- a detailed description of the facts that have occurred and how they have been known;
- indicate whether the facts have already been reported to other parties (supervisory authorities, internal or external subjects, etc.);
- reference to any documents which may confirm the validity of the facts reported;
- the indication about the management of the personal data of the whistleblower.

4.4 "Anonymous" reporting

Next, the concept of "anonymous" is to be understood in the sense of "non-nominative". In terms of the legislation for the protection of personal data (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 the Company can interact with the whistleblower by giving him feedback and carrying out the activities provided for by Legislative Decree 24/2023. Therefore, the Whistleblower has full guarantee that his identity remains confidential, in accordance with Legislative Decree 24/2023 and the policy for the protection of the whistleblower as a vulnerable subject pursued by the Company according to the GDPR.

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

4.5 Reporting in "bad faith"

"Bad faith" report means the report without foundation, libelous or defamatory, made for the purpose of damaging or prejudicing employees, internal collaborators, members of corporate bodies or third parties (e.g. customers, suppliers, partners, consultants, collaborators) in business relations with the Company.

In the event that it is demonstrated 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 Departments concerned by the report, i.e. the subjects who have received specific privacy instructions from the Company concerning the management of Whistleblowing reports.

5. Liability

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

In carrying out this activity, the IA Director, if he deems it appropriate, may share the subject of the report and be operationally supported by the Legal, HR, RSPP and/or DPO functions, maintaining and guaranteeing the confidentiality of the identity of the Whistleblower, unless otherwise indicated by the Whistleblower.

The IA Director, therefore:

- performs all preliminary activities (preliminary verification of the existence of the conditions, re-routing of reports not relevant);
- assesses the checks to be carried out, the functions to be involved in the analyses, the request for additional information or the possible archiving;
- guarantees the confidentiality of the information received, including the identity of the whistleblower;
- prepares periodic reports on the reports received.

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

6. The Whistleblowing Portal

The Company provides an online platform with free access by reporting parties, specifically dedicated to reports (Whistleblowing Portal), accessible via links on the Company institutional website; access to the portal is also guaranteed through the company intranet for authorized Whistleblowers.

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 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); in cases where, on the other hand, access to the Whistleblowing portal takes place via a device connected to the company network, the Company implements technical and organizational 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 way. Likewise, in the event that a report is not adequately substantiated, the IA Director or Legal Counsel, using the portal and its instrumentation, will have the right to request from the whistleblower, always and only through this code and within the platform, further detailed elements, for the purpose of an in-depth analysis of the reported case. [7]

7. Methods of transmission and investigation of reports

7.1 Mode of transmission

The reporting channel is designed to ensure confidentiality about the identity of the whistleblower or persons involved, about the content of the report and concerning the documentation relating to it.

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

Reports can be written or spoken (by voice messaging or a request for a meeting with the AI Director), through the use of the online platform made available by the Company and which provides a guided path for the Whistleblower.

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

For more details regarding the correct use of the Whistleblowing portal and the compilation of the related fields relating to the report, please refer to the dedicated FAQ on the Company institutional website.

7.2 Preliminary verification of the Report

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

In this phase, the subject of the report may be shared and the support of other functions (Legal, HR, 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, the whistleblower receives an identification code that allows the whistleblower to check the progress status of his report on the Platform and constitutes an acknowledgement of receipt of the report on the Online Platform.

The whistleblower may also be contacted, according to the methods set out (through the internal messaging of the platform) above, by the IA Director or Legal Counsel request further information that may be necessary.[8]

7.3 Investigation

The IA Director:

- may reject the report because it is not considered relevant;
- may request additional information before deciding whether or not to take charge of the report;
- can initiate specific analyses, making use of the competent structures, as well as involving the company departments involved in the report (Privacy Delegates);

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

- ensure that the investigation is accurate, has a reasonable duration and respects the confidentiality of the whistleblower and the persons involved, including any person reported;
- prepares, within the tool, a draft of summary of the object of the report, used to generate reports intended for the Supervisory Body.

If the IA Director considers the report valid, he will then inform:

- the Supervisory Body in the event of a report concerning the violation of the Organisation, Management and The Model 231, 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 Legislative Decree 231/01, and also in the event of violations consisting of administrative, accounting, civil or criminal offenses or violations of specific national and European provisions.

7.4 Outcome of the investigation

At the end of the investigation, the IA Director (or Legal Counsel) communicates the outcome of the investigations carried out to the Supervisory Body or to the Top Management, according to the relative scope. The whistleblower, who by entering the identification code, provided to him, on the online Platform can monitor the process of his report, must receive feedback on the follow-up to the report within three months from the date of notice of its receipt.

Periodically, the IA Director prepares a summary report of the investigations carried out and the evidence that emerged, sharing it with the Supervisory Body.

That report must therefore:

- summarise the course of the investigation and the evidence collected;
- set out the conclusions reached;
- provide recommendations and suggest actions to be taken to remedy the violations found and ensure that they do not occur in the future.

If the Supervisory Body or the Top Management based on the scope detects that sound facts emerged, the evidences are then shared with the Company Departments responsible from time to time (always only to Privacy Delegates), in order to define corrective 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, based on the scope, should detect the lack of sufficiently detailed elements or, in any case, the groundlessness of the facts referred, the report will be archived, together with the related reasons, by the IA Director.

The Company may take the most appropriate disciplinary and/or legal measures to protect its rights, assets 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 guarantee compliance with the obligations in this regard, a series of administrative pecuniary sanctions are envisaged that ANAC can apply to private subjects 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 action for the sole reason that he or she has reported a violation of his or her own or others, in accordance with this Policy. However, this circumstance may be taken into account in the assessment of the disciplinary measure to be taken.

7.5 Follow up

The IA 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. Protective measures envisaged

8.1 Protection of the whistleblower

The whistleblower will not suffer retaliatory or discriminatory conduct for having made the report and, for example, the employee has the right to request transfer to another office. The Company ensures, where reasonably possible, the fulfillment of such requests.

The Company guarantees the confidentiality of the identity of the whistleblower, unless the whistleblower explicitly made her/his contacts details available for the Company, in the cases provided for by art. 12 of Legislative Decree 24/2023, based on given whistleblower’s consent to disclose his 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 whistleblower is always protected against any form of retaliation, discrimination or penalization and in any case the confidentiality of the identity of the whistleblower is ensured, without prejudice to legal obligations;
- no information on the identity of the whistleblower is provided to the reporter, without prejudice to legal obligations;
- 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 should be transmitted, as far as necessary, only to the persons in charge of processing and competent to initiate the verification procedure or to take the necessary measures depending on the findings. In any case, the recipients of the information must ensure that the latter is always handled confidentially and that the necessary security measures are applied.

The same protection measures shall also apply to: (a) facilitators; (b) persons in the same employment context as the reporting person, the person who has lodged a complaint with the judicial or accounting authority or the person who has made a public disclosure and who is linked to them by a stable emotional or family relationship 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 environment as the reporting authority or who have a habitual and current relationship with that person; (d) institutions owned by the reporting person or by the person who has lodged a complaint with a judicial or accounting authority or who has made a public disclosure or for whom those persons work, as well as institutions operating in the same working environment as those persons.

8.2 Rights of the Reported

The reported person must be granted the same guarantees of confidentiality as the reporting person, until the conclusion of the proceedings initiated by reason of the report. [9]

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

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, will a procedure be initiated solely because of the report, in the absence of concrete feedback regarding its content. This could possibly be done on the basis of other evidence found and ascertained starting from the report itself.

In order to guarantee the right of defense of the reported, it is provided the right to consult them through a securitization procedure, through the acquisition of written observations and documents.

If, finally, the report should be unfounded or in bad faith, for the sole purpose of damaging the person of the reported, the imposition of disciplinary sanctions against the whistleblower, as well as his possible criminal and civil liability in case of defamatory or slanderous report, remains unchanged.

9. Periodic reporting

The IA Director prepares periodically (eg. at least every six months or on the occasion of the meetings of the Supervisory Body) a summary report of the reports received, of the possible outcome of the audits carried out and of those in progress and transmits it to the Supervisory Body of the Company.

If deemed appropriate in relation to the subject matter and/or seriousness of the report received, the Supervisory Body may request that the IA Director report immediately to Top Management. In this case, Top Management may provide recommendations, including whether disciplinary action is necessary.

10. Data protection and document archiving

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

In order to guarantee the confidentiality of the Reporter, the person who manages the reports has the obligation to use them only to follow them up, as well as the prohibition to reveal the

identity of the Reporter 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 the 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 filed with the IA Director and must be accessible only to authorized personnel.

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

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

11. Approval and updating of the Policy

The Company approves this Policy by resolution of the Board of Directors. This is subject to revision if the regulations, referred to as best practices, are subject to change or interpretation of case-law. In the event of substantial changes 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. organizational updates or updates relating to the Whistleblowing portal), the Legal Counsel takes care of updating and revising the Policy and undertakes to ensure that it is correctly disseminated and applied.