WHISTLEBLOWING POLICY

ai sensi del Decreto Legislativo 10 marzo 2023, n. 24, riguardante la protezione delle persone che segnalano violazioni del diritto dell'UE e delle disposizioni normative nazionali ("Decreto 24/2023")

Indice

WHISTLEBLOWING POLICY

ai sensi del Decreto Legislativo 10 marzo 2023, n. 24, riguardante la protezione delle persone che segnalano violazioni del diritto dell'UE e delle disposizioni normative nazionali ("Decreto 24/2023")

1. Scope

Lomopress S.r.l. (hereinafter also referred to as the 'Company') is committed to promoting a corporate culture characterized by correct behavior and a good system of governance, and for this reason it recognizes the importance of having an internal regulation governing the reporting (hereinafter referred to as 'Reporting') of illegitimate behavior by personnel working for the Company and third parties.
This document (hereinafter referred to as the "Whistleblowing Policy" or even just the "Policy") defines the communication channels suitable for the receipt, analysis and management of Reports - also in anonymous form - of unlawful conduct (hereinafter referred to as "Unlawful Conduct") within the Company and is aimed at ensuring the widest dissemination of the culture of ethics and transparency.

The purpose of this Policy is to ensure a working environment in which staff and/or third parties can report Illegal Conduct occurring within the Company and to provide said staff and/or third parties (hereinafter also referred to as 'Whistleblowers') with operational guidance on how to make a Report.

2. Legal references

Law No. 179/ 2017 'Provisions for the protection of the authors of Reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship' ('Whistleblowing Law') came into force on 29th December 2017. The Whistleblowing Law introduced a 'binary' system, providing protection both for workers belonging to the public sector and for workers belonging to the private sector, where the relevant regulation is the one set out in Legislative Decree No. 231 of June 8th 2001 ('Decree 231'). It requires both public and private entities to activate internally alternative channels for reporting violations, at least one of which must be computer-based, the creation of specific procedures enabling the reporting of offences safeguarding the confidentiality of the whistleblower's identity.
With specific regard to private employment relations, Article 2 of Law No. 179/ 2017, by amending Article 6 of Legislative Decree No. 231/2001 on "Administrative Responsibility of Entities", extends to the private sector the protection of the employee or collaborator who reports offences or violations relating to the organization and management model of the entity of which he/she has become aware by reason of his/her office. With specific regard to the world of "supervised subjects", the changes made by Law 179/2017 are in addition to what is already provided for by other regulations indicated below. The recent Directive (EU) 2019/1937 of October 23rd 2019 published in the Official Journal of the Union on 26 November 2019 (L 305/17) concerning the protection of persons who report breaches of Union law ('Directive') provides further guidance; the Directive clarifies that the ones affected by the new legislation will no longer be only entities that have adopted the MOG, but, for example, also all companies with at least 50 employees (regardless of whether they have adopted the MOG), all companies operating in high-risk sectors (financial or vulnerable to money laundering or terrorist financing) regardless of the number of employees will be required to comply.
The Directive expressly provides that these entities will have to set up internal channels and procedures for Reports. These channels will have to be managed by a responsible person or department, designated to receive and process the Report, who will have to give feedback to the Whistleblower within a maximum period of 3 months. In addition, measures are provided for (reinstatement in the workplace, compensation for damages) to avoid retaliation by the employer against the employee, which are accompanied by sanctions if the Whistleblowing employee suffers discriminatory acts.
When transposing the Directive, Italy issued Legislative Decree No. 24 of March 10th, 2023, on protection of persons who report breaches of EU law and national regulatory provisions ("Decree 24/2023") and the "Guidelines on the protection of persons who report breaches of EU law and of national regulatory provisions

- procedures for the submission and management of external reports", approved by ANAC with Resolution No. 311 of July 12th 2023.

3. Recipients

The scope of this Policy is to regulate the process of receipt, analysis and processing of Reports sent or transmitted, even anonymously, within the Company.
The addressees of this Policy are:
- The personnel of the Company;
- directors and members of corporate bodies.
- third parties (e.g. third-party suppliers of products and/or services).

Recipients, who become aware of facts that are potentially the subject of a Report, are invited to make the Report promptly by means of the procedures described below, refraining from undertaking autonomous initiatives of analysis and/or investigation.

4. Roles and responsibilities

For the reporting system to be effective, the Company has entrusted to Sara Tagliaferri, as Internal Channel Manager (hereinafter 'SGCI'), the task of examining any reports received and assessing them.
The ICSG will report annually to the Board of Directors regarding the proper functioning of the Whistleblowing system and provide information about the activity carried out. If failures are found to be serious, she will request an extraordinary meeting of the Board of Directors to discuss appropriate action.

5. Reporting an unlawful conduct

If the personnel and/or a third party have a reasonable suspicion that Unlawful Conduct has occurred or may occur, they are required to make a Report, following the procedures described below.
In case personnel and/or third parties have doubts regarding how to classify a way of conduct as legitimate or not, they can talk with the ICSG unofficially in order that the case can be evaluated.
Whistleblowing channels guarantee the confidentiality of the Whistleblower's identity, unless the Whistleblower authorizes the disclosure.

6. Content of the report

Reports (which may relate to actions or omissions) must be made in good faith and must be substantiated with precise information and useful indications to allow due and proper verification and to ascertain the validity of the facts reported.
To this end, Reports should preferably contain the following elements:
- the personal details of the Reporting Party making the Report, with an indication of the position/assignment and the activity performed within the Company.
- a clear and complete description of the facts that are the subject of the Report
- if known, the circumstances of time and place in which the facts reported were committed.
- if known, the personal details or other elements enabling identification of the person who carried out the reported facts (e.g. the sphere in which the activity is carried out, the position held, the role played by the person in the event)
- an indication of any other persons who may report on the facts that are the subject of the Report;
- any documents that may confirm the truthfulness of the facts reported;
- any other information that may provide useful feedback on the existence of the facts reported.

7. Report procedure

To guarantee impartiality and independence of judgement, the Company provides two different alternative channels through which Reports can be made.

Specifically, Reports can be made as follows:

- in written form, by computerized means, through the SaaS platform "Whistlesblow.it
- orally, through a telephone line or voice messaging systems (WhatsApp) and, by request of the whistleblower, through a face-to-face meeting with the SGCI, which must be scheduled within a reasonable time.

8. Process- Investigations

All Reports, whether oral or written, made by every means, are handled by the SGCI, which must acknowledge to the complainant of the Report to the Reporting Party within and no later than seven days after receipt.

The management and the verification of the validity of the circumstances represented in the Report are entrusted to the ICSJ, which provides for it in compliance with the principles of impartiality and confidentiality, carrying out any activity deemed appropriate, including the hearing of the Whistleblower and any persons who may report on the facts reported.

The reports are subject to the following investigation process:

A. PRELIMINARY ANALYSIS

All the received Reports will be subject to a preliminary check by the ICS, aimed at verifying the presence of data and information useful for assessing their validity. Reports that do not fall within the scope defined in this Policy will be redirected to the competent functions without any prior assessment of merit. The Complainant will be provided with initial feedback as soon as possible and in any case within three months.

In carrying out the analysis phase, the ICS, for specific aspects dealt with the Reports and if deemed necessary, may:

-avail itself of the support of other corporate functions, to the extent of their respective competences, and of external professionals.

-request further information and/or additional documentation from the Whistleblower.

If, at the end of the preliminary phase, it emerges that there are no sufficiently circumstantiated elements or that the facts referred to are unfounded, the Report will be filed with the relevant reasons. Where, on the other hand, emerge or can be deduced useful and sufficient elements to assess the Report as well-founded, it will follow a second phase with specific investigations

B. SPECIFIC INSIGHTS

The SGCI will:

1) initiate the specific analyses by availing itself, if deemed appropriate, of the Company's competent structures or appointed external experts (if, for example, the competent function of the Company cannot be covered because it is involved in the Report)

2) request, if possible, the initiation of disciplinary proceedings against the Whistleblower, in case of a Report in relation to which the bad faith of the same and/or the merely defamatory intent are ascertained, possibly also confirmed by the groundlessness of the Report itself.

9. Results of investigations

At the end of in-depth investigations carried out, the ICSG will:

1) terminate the investigation at any time if, in the course thereof, it is established that the Report is unfounded.

2) Inform directly, if necessary, one or more of the following people, where present (unless they are the subject of the Report), for support and expertise based on the Report

- the Chief Executive Officer.
- the Head of Internal Audit;
- the Safety Manager ("RSPP");
- the Data Protection Officer ("DPO");
- the members of the Board of Statutory Auditors.

3) agree with the corporate bodies and functions on any initiatives to be taken before the closure of the report.

The activities described above are not necessarily carried out in a sequential manner.

10. Anonymous reports

The Company investigates, ascertains and verifies the reported facts regardless of the knowledge of the identity of the Whistleblower, who has the option of not indicating his or her personal details. However, the anonymous Whistleblower must be aware that the Report:

- carried out anonymously, it can only be taken into consideration in specific cases (i.e. if adequately substantiated and provided in great details, useful for verifying and ascertaining the validity of the reported facts);

- even if sent anonymously in the first instance, it may subsequently be supplemented with the whistleblower's personal details.

- if anonymous, it might make it more difficult for the Company to keep in touch with the anonymous Whistleblower and ask for his cooperation where necessary.

- if anonymous, it might not exclude the risk of possible retaliation by the Whistleblower.

For all Reports – made by every means - will be taken necessary measures to guarantee the confidentiality of the personal data of the persons involved, unless otherwise provided by law.

11. Protective measures taken

11.1 Protection of the whistleblower

The Company protects the Whistleblower against any form of retaliation, discrimination or penalization because of making a Report in good faith. Any act of retaliation or discrimination against the Whistleblower is prohibited and, if established, may lead to disciplinary proceedings against the person responsible. The Whistleblower has the right to request a transfer to another office where reasonably possible and relevant to the case.

The Company ensures the confidentiality of the personal data of the Whistleblower, the witness and the reporter (natural or legal people involved in the Report or notification, as a person to whom the irregularity is attributed or to whom is associated with the irregularity).

The coorporate guarantees the Whistleblower's anonymity, except in cases where:

- the Whistleblower gives his/her consent to disclosure.
- its disclosure is required by local legislation (for instance, if it is necessary to involve the police department or the authorities, or if it is indispensable for the whistleblower's defense);
- its disclosure is necessary to prevent or reduce serious threats to people's health or safety.

Unauthorized disclosure of the identity of the Whistleblower, or of information from which the identity of the Whistleblower may be inferred, is considered a violation of this Policy and is subject to significant disciplinary action. Any action aimed at unlawfully disclosing the identity of the Whistleblower may also be sanctioned by the competent authorities.

11.2 Protection of data collected and preservation of documentation

The documentation related to Reports is confidential. Such documentation shall be stored securely and in accordance with the applicable regulations by the GSCIC.

The preservation of the documentation and Reports by the SGCI is guaranteed for a period not exceeding that necessary for the purposes for which the data were collected or subsequently processed, and in any case in compliance with the applicable data protection legislation. Any personal data contained in the Report, those relating to the identity of the Whistleblower or other individuals, shall be processed in compliance with the data protection regulations and the GDPR Policy adopted by the Company.

12. Training

Training is a fundamental element for the implementation and enforcement of this Policy, and, to this end, the Company undertakes to provide and update mandatory training on whistleblowing for all personnel, to highlight the specific procedures to be followed and the possible consequences in the event of inappropriate conduct.

13. Controls and reporting

Annually, the ICSG prepares a summary report of the received reports containing the results of the analysis, including the adoption (or non-adoption) of the measure.

14. Policy updating

This Policy has been approved by the Board of Directors, which will validate any subsequent updates made by the SGCI.

15. Privacy controls and activities

On the privacy side, the following aspects are to be monitored:

- The usability or non-usability of the data in the in-depth reporting activities in case their processing is contrary to the provisions of the EU Regulation 2016/679.

- Compliance with the principles of data quality and proportionality. Personal data must be processed for specified, explicit, legitimate purposes and in a manner not incompatible with those purposes. In this way , the WP29 has specified that internal whistleblowing procedures must be designed so as not to encourage anonymous whistleblowing as an ordinary mean of reporting wrongdoing.

- The obligation of the data controller to provide clear and complete information on the procedure. The data controller must inform data subjects about the processing that will be carried out on their personal data, and the confidentiality of the complainant must be guaranteed throughout the procedure and that illegal use of the system may lead to action being taken against the abuser. A balance must be struck between the protection of personal data or the legitimate interest of the data controller as a private entity (as referred to in Article 6(1)(f)), especially in view of the safeguards for the prevention of money laundering and the financing of international terrorism (this legal basis is extended to all entities obliged to put in place the aforementioned safeguards, thus also to private entities such as banking and financial intermediaries to other financial operators and not least to professionals and gaming service providers);

- The whistleblower's rights. The data controller or the person in charge of the whistleblowing procedure (possibly delegated by the data controller) must inform the whistleblower as soon as possible after the data concerning him/her have been recorded. Under no circumstances may the whistleblower be allowed to use his right of access to obtain information on the identity of the whistleblower (Art. 2-undecies of the National Code, Limitations to the rights of the data subject), unless the whistleblower has made a false statement in bad faith (WP29).

- Security of treatments. Verification that the company or the responsible organization for the internal whistleblowing procedures has applied all reasonable and feasible technical and organizational precautions to protect the security of the data collected, disseminated or stored.

- Management of internal whistle-blowing procedures: verification that the internal management of the system is compliant especially for the collection of reports.