

## WHISTLEBLOWING POLICY

### Foreword

The European Union, by Directive 2019/1937, has renewed the legislation concerning the protection of people reporting breaches of Union law, in order to create a minimum standard for the protection of whistleblowers' rights in all member states. Italy implemented the European Directive with Legislative Decree no. 24 of 10 March 2023 (hereinafter the "Decree").

By adopting this Policy, the company Slowear S.p.A. (hereinafter, the 'Company') has intended to comply with the aforementioned regulatory prescriptions, as well as with the guidelines provided this by ANAC in this regard.

The objective pursued is to provide the whistleblower, i.e. the person who reports violations, with clear operational indications on the subject, the contents, the recipients and the methods of transmission of the reports.

The reporting process shall ensure the confidentiality of the identity of the whistleblower from the receipt and in any subsequent contact. Pursuant to Article 5(1)(e) of the Decree this policy therefore provides information on the channels, procedures and prerequisites to make internal and external reports.

### 1. Reporting agents

Reports may be made by the following persons:

- a) employees, including workers performing:
  - part-time, intermittent, fixed-term, supply, apprenticeship, ancillary work (whose employment relationship is governed by Legislative Decree no.81/2015);
  - occasional services (pursuant to Article 54-bis of Decree-Law No. 50/2017, conv. by Law No. 96/2017);
- b) self employed workers
  - with a work contract (Article 2222 of the Civil Code.);
  - with a collaboration relationship (referred to in Article 409 of the Civil Code), such as agency, commercial representation and other collaboration relationships that take the form of the provision of continuous and coordinated work, mainly of a personal nature, even if not of a subordinate nature;
  - with collaborative relationships resulting in the performance of exclusively personal, continuous work, the manner of performance of which is organised by the principal;
- c) collaborators who perform their work for entities supplying goods or services or carry out works in favour of the Company;

- d) freelance professionals and consultants who work for the Company;
- e) volunteers and trainees, paid and unpaid, who work at the Company;
- f) the shareholder and persons with administrative, management, control, supervisory or representative functions, even if such functions are exercised de facto at the Company (e.g. members of the Board of Directors or Supervisory Body).

The protection of whistleblowers (Art. 6 of this Policy) also applies if the whistleblowing, the report to the judicial or accounting authorities or the public disclosure of information occurs in the following cases:

- a) when the legal relationship described above has not yet commenced, if information on violations has been acquired during the selection process or in other pre-contractual stages;
- b) during the trial period;
- c) after termination of the legal relationship if the information on the infringements was acquired in the course of the relationship.

## 2. Subject of the alert and alerts excluded

The following may be reported in the following table::

<i>Number of employees</i>	<i>With Organisational and Management Model Legislative Decree No. 231/01</i>	<i>Subject of the report</i>
50 or more	No	- European torts (Art. 3(2)(a), Legislative Decree No. 24/2023

More specifically, they may concern:

- a) breaches of national and European provisions consisting of offences in the following areas: public procurement; services, products and financial markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and security of networks and information systems;
- b) infringements of European provisions consisting of: (i) acts or omissions detrimental to the Union's financial interests; (ii) acts and omissions relating to the internal market; (iii) acts and behaviour that frustrate the object or purpose of the provisions of Union acts in the abovementioned areas;

## 3. Reporting channels: internal, external, public disclosure

The Company has set up an internal whistleblowing channel which guarantees the confidentiality of the identity of the person making the report, the person involved and the person mentioned in the report, as well as the content of the report and the relevant documentation.

It should be noted that whistleblowing must first be reported using the internal channel.

Whistleblowing through the external channel, set up and managed by ANAC, can only be reported under certain conditions, and public disclosure under even stricter conditions, without prejudice to the possibility of reporting to the judicial authorities.

#### 4. Content and method of submission of reports

**Whistleblowing** can be **reported** if the following conditions are met:

- when there is definite knowledge or reasonable and well-founded suspicion of a violation of national or European Union regulatory provisions that harm the public interest or the integrity of the Company,
- and
- learned in the work context.

Reports relating exclusively to:

- to disputes, claims or requests related to an interest of a personal nature of the reporter;
  - to the reporter's individual working or collaborative relationships with the Company, or with hierarchically subordinate figures;
  - to aspects of the reported person's private life, with no direct or indirect connection to the business and/or professional activity
- will not be taken into consideration.

In addition:

- specious, defamatory, slanderous reporting or aimed solely at harming the reported person;
- reports related to violations that the whistleblower knows to be unfounded will not be allowed.

#### Contents of the report

The report, under **penalty of inadmissibility**, must contain:

1. the **identifying data** of the reporting person as well as an address to which subsequent updates can be communicated;
2. the **clear, complete and circumstantial description of the facts** being reported;
3. the **circumstances of time and place** in which the fact that is the subject of the report occurred and, therefore, a description of the facts that are the subject of the report, specifying the details relating to the circumstantial information and, where present, also the manner in which the facts that are the subject of the report came to light;

---

<sup>1</sup> Whistleblowers may directly make a **public disclosure** when:

- the reporting person has previously made an internal and external report, or has made an external report directly and no reply has been received within the prescribed time limits on the measures envisaged or taken to follow up the reports;
- the reporting person has justified reason to believe that the breach may constitute an imminent or obvious danger to the public interest;
- the reporting person has justified reason to believe that the external report may entail a risk of retaliation or may not be effectively followed up because of the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the recipient of the report may be in collusion with or involved in the perpetrator of the breach.

4. the **personal details** or other elements that enable the identification of the person(s) believed to be responsible for the reported facts;
5. an indication of **any other individuals who** may report on the facts being reported;
6. the indication of **any documents that** can confirm the substantiation of these facts;
7. **any other information** that may provide useful feedback about the existence of the reported facts.
8. the **express statement that they wish to benefit from whistleblowing protections**, e.g., by inserting the words "confidential to the reporting manager" in the case of using the analog channel (*see below*).

### Reporting method

**Whistleblowing reports** can be made in the following ways:



at the request of the reporter through a direct meeting with Ms Alessia Marchiori and/or Ms Sandra Levy.



by calling the number +39 041 8891332 and leaving a voice message.



by ordinary mail by registered letter with return receipt, putting the report in two sealed envelopes, including, in the first envelope, the identification data of the reporter, together with an identity document; in the second envelope, the subject of the report; both envelopes must then be placed in a third envelope with the wording "*reserved for the members of the whistleblowing committee*" on the outside and addressed to Ms. Alessia Marchiori and/or Ms. Sandra Levy.

### Anonymous reporting

Anonymous reports, i.e. reports from which the identity of the reporter cannot be established, will not be taken into account.

### Transmission of reports

Whistleblowing reports shall be sent to the members of the whistleblowing committee in the persons of Alessia Marchiori and/or Sandra Levy, in accordance with the reporting channel adopted. The one will replace the other in the event of the latter's prolonged absence, guaranteeing the handling of the report also in the event that one of the two is in a state of conflict of interest pursuant to point 6 of this policy.

Finally, it should be noted that the receipt of reports is suspended during the Company's closing period.

## **5. Report Management**

This procedure regulates the process of receiving, analysing and processing reports of unlawful conduct of which the reporting person has become aware in the context of his/her work.

In managing the internal reporting channel, the receiver operates in the following ways:

#### Receipt of Report

In the event that the report has been mistakenly transmitted/received to/from a person not appointed to receive it, and it is clear that it is a whistleblowing report, it shall be the latter's obligation to promptly acknowledge receipt thereof to the reporting manager, in any event within 7 (seven) days of such receipt, simultaneously notifying the reporting manager of such transmission to the reporting manager, without prejudice to all confidentiality obligations provided for by this policy also on the reporting manager (and consequently his liability in the event of breach thereof).

The receiver will issue the reporting person with an acknowledgement of receipt of the report within **seven days** from the date of receipt. The acknowledgement will be sent to the address indicated by the reporting person and, if not indicated, the report will be filed.

The Company shall proceed with the filing of reports received by ordinary mail by means of appropriate tools that guarantee confidentiality (e.g. within archives protected by security measures).

If the report is made orally, subject to the consent of the person making the report, it shall be documented by the person making the report either by recording it on a device suitable for storing and listening to it, or by means of a record.

If a recorded telephone line or other recorded messaging system is used as an internal channel for receiving reports, reports will be stored in devices suitable for storage and listening, or, alternatively, the report will be transcribed in full.

In the event of a face-to-face meeting with the reporting person, a recording of the meeting will be made, or, if this is not done or the reporting person does not consent to the recording, minutes of the meeting will be drawn up and signed by both the manager and the reporting person, a copy of which will be provided to the latter.

#### Relations with the reporter and additions to the report

The receiver maintains contact with the reporter and may request additions if necessary.

In the case of minutes drawn up following a meeting with the reporting person, the latter may verify, rectify and confirm the minutes of the meeting by signing them.

#### Examination of the report

The receiver follows up on the reports received, assessing the existence of the reporter's legitimacy and that the report falls within the scope of the rule; this is followed by an assessment of the circumstances of time and place in which the event occurred.

At the outcome of the preliminary verification:

- if the prerequisites are not met, the alert is **closed**, by stating the reasons;
- if the prerequisites are met, the **investigation** is initiated.

## Investigation

The receiver guarantees the proper conduct of the investigation through:

- the collection of documents and information;
- the involvement of external parties (where the technical assistance of third-party professionals is required) or other corporate structures, which are obliged to cooperate with the reporting manager;
- the hearing of any other internal/external parties, where necessary.

The preliminary investigation is carried out in accordance with the following principles:

- the necessary measures are taken to prevent the identification of the reporter and the persons involved;
- audits are conducted by persons with the necessary training and activities are tracked and filed correctly;
- all those involved in the evaluation maintain the confidentiality of the information received, unless otherwise provided for by law;
- checks are carried out by ensuring that appropriate measures are taken for the collection, use, disclosure and storage of personal information and by ensuring that the needs of the investigation are balanced against the need to protect privacy;
- appropriate measures are ensured to manage possible conflicts of interest if the report concerns the recipient.

## Feedback to the reporter

**Within three months from the** date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within three months from the expiry of the seven-day time limit from the submission of the report, the receiver shall provide feedback on the report, alternatively notifying

- **filing** of the report, giving reasons for the decision, or
- the **merits of** the report and sending it to the competent internal bodies for follow-up, or
- the activity carried out and still to be carried out (in the case of alerts involving a more time-consuming verification activity) and any measures taken (measures taken or referral to the relevant Authority).

## **6. Conflict of interest**

Should one of the two members of the whistleblowing committee have a conflict of interest, e.g. as a whistleblower or as a reporter, the report will be handled by the other, without prejudice to the possibility of making an external report to the ANAC.

The reasons that led the person to report or publicly disclose are irrelevant to his or her protection.

## **7. Protection of the reporter and his responsibility**

Whistleblowers shall not suffer any form of retaliation. Indeed, the law provides that whistleblowers must not be sanctioned, demoted, dismissed, transferred or subjected to any other organisational measure that would directly or indirectly have a negative effect on their working conditions, or discriminate or retaliate against them.

In the context of judicial or administrative proceedings, or even out-of-court proceedings concerning the establishment of prohibited conduct vis-à-vis whistleblowers, it is presumed that such conduct was brought about as a result of the whistleblowing, public disclosure or complaint to the judicial or accounting authorities. The onus of proving that such conduct towards whistleblowers is motivated by reasons unrelated to the report, public disclosure or complaint remains on the person who has engaged in it.

Moreover, the alleged discriminatory or retaliatory measures suffered must be reported to Anac, which alone is entrusted with the task of ascertaining whether the retaliatory measure is consequent to the report of wrongdoing and applying, in the absence of proof by the Company that the measure taken is unrelated to the report, an administrative pecuniary sanction.

### Processing of personal data. Confidentiality

Any processing of personal data will be carried out in accordance with Regulation (EU) 2016/679 and Legislative Decree No. 196 of 30 June 2003; furthermore, failure to comply with confidentiality obligations may result in disciplinary liability, without prejudice to any further liability provided for by law.

The information on the processing of personal data following a whistleblowing report is available as an annex to the policy available on the Company's institutional website.

Internal and external reports and related documentation are kept for as long as necessary to process the report and in any case no longer than 5 years from the date of the communication of the final outcome of the reporting procedure, in compliance with the obligations of confidentiality and protection of personal data.

### Responsibility of the reporter

The Company guarantees the whistleblower the right to be informed (within a reasonable period of time) of any reports involving him/her, guaranteeing the right of defence where disciplinary measures are initiated against him/her.

This procedure is also without prejudice to the criminal and disciplinary liability of the whistleblower in the event of a libellous or defamatory report under the Criminal Code and Article 2043 of the Civil Code.

Any form of abuse of the whistleblowing reporting procedure, such as reports that are manifestly unfounded and/or made with the sole purpose of harming the reported person or other persons, and any other hypothesis of improper use or intentional exploitation of the procedure itself, shall also give rise to liability in disciplinary and other competent fora.

## **8. Entry into force and amendments**

This policy shall enter into force on December 17<sup>th</sup>, 2023. Upon its entry into force, all provisions previously adopted on the subject, in whatever form communicated, shall be deemed repealed, insofar as they are incompatible or dissimilar, since they are replaced by the present policy.

The Company will provide the necessary publicity and give a copy of the policy to each employee.

All employees may propose reasoned additions to this policy when deemed necessary; proposals will be examined by the Company's General Management.

This policy is, however, subject to periodic review.

Mira, Venezia, December 15<sup>th</sup>, 2023



## **POLICY STATEMENT ON THE PROCESSING OF PERSONAL DATA EX ART. 13-14 OF REGULATION (EU) 2016/679 UNDER THE WHISTLEBLOWING POLICY**

With this information notice, SLOWEAR S.p.A. (hereinafter the "Company") intends to provide the indications required by articles 13 and 14 of Regulation (EU) 2016/679 (or "*General Data Protection Regulation*" - "*GDPR*"), concerning the processing of personal data carried out by the Company within the scope of its "*Whistleblowing Policy*", adopted in compliance with Legislative Decree no. 24 dated 10 March 2023<sup>1</sup> and, in particular, of all activities and fulfilments connected to the operation of the Company's system for the management of *whistleblowing* reports.

The information below is provided to "reporting" persons and to all other persons potentially "concerned", such as, for example, persons indicated as potentially responsible for unlawful conduct, any "facilitators" (as defined by the reference legislation), and any other person involved in the "*Whistleblowing Policy*" in various ways.

### **1. Data controller and DPO – “Data Protection Officer”**

The Personal Data Controller is SLOWEAR S.p.A. with administrative headquarters in Mira (Venice), Via della Fornace 15-17.

### **2. Categories of personal data processed and purposes**

According to this Policy, personal data may be acquired by the Company insofar as they are contained in *whistleblowing* reports, that is to say in the acts and documents annexed thereto, received by it through the channels envisaged by the aforementioned Policy.

The receipt and handling of such reports may give rise to the processing of the following categories of personal data, depending on their content:

- a) common personal data referred to in Article 4(1) of the GDPR, including, for example, personal details (name, surname, date and place of birth), contact details (landline and/or mobile telephone number, postal/email address), job role/assignment;
- b) “special” personal data as defined in Article 9 of the GDPR, including, for example, information relating to health conditions, political opinions, religious or philosophical beliefs, sexual orientation or trade union membership;
- c) judicial' personal data under Article 10 of the GDPR, relating to criminal convictions and offences, or to related security measures.

With regard to the aforementioned categories of personal data, **we stress the importance that the reports forwarded should be free of information that is manifestly irrelevant for the purposes of the reference discipline**, inviting, in particular, the reporting parties to refrain from using personal

---

<sup>1</sup> Legislative Decree implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019.

data of a 'particular' and 'judicial' nature unless deemed **necessary and unavoidable** for the purposes of the reports, in compliance with Article 5 of the GDPR.

The aforesaid information shall be processed by the Company - the Data Controller - in accordance with the provisions laid down by Legislative Decree No. 24/2023 and, therefore, in general, **in order to carry out the necessary preliminary investigation activities aimed at verifying the grounds of the reported facts and the adoption of the consequent measures.**

In addition, the data may be used by the data controller for **purposes related to the need to defend or ascertain one's rights** in the context of judicial, administrative or extrajudicial proceedings and in the context of civil, administrative or criminal litigation arising in connection with the report made.

### **3. Legal bases of personal data processing**

The legal basis for the processing of personal data is mainly constituted by the **fulfilment of a legal obligation** to which the Data Controller is subject - Article 6(1)(c) of the GDPR - who, in particular, by virtue of the aforementioned legislation, is required to implement and manage information channels dedicated to receiving reports of unlawful conduct detrimental to the integrity of the Company and/or the public interest.

In the cases contemplated by the same rules, a **specific and free consent** may be requested **to the reporting person** - pursuant to Article 6(1)(a) of the GDPR - and, in particular, where there is a **need to disclose his identity**, or where the **recording of the reports collected orally**, that is to say through direct meetings with the Reporting Manager, is envisaged.

The processing of '**special**' personal data, which may be included in the reports, is based on the **fulfilment of obligations and the exercise of specific rights of the Data Controller and the data subject in the field of labour law**, pursuant to Article 9(2)(b) of the GDPR.

As for the purpose of establishing, exercising or defending a right in court, the relevant legal basis for the processing of personal data is the **legitimate interest of the Data Controller** in doing so, referred to in Article 6(1)(f) of the GDPR; for the same purpose, processing of personal data of a '**particular**' nature, if any, is based on Article 9(2)(f) of the GDPR.

### **4. Nature of personal data provision**

The provision of personal data is compulsory since anonymous reports, i.e. reports from which it is not possible to determine the identity of the person making the report, are not taken into account, in accordance with the Company's "*Whistleblowing Policy*". The personal data provided will be processed to manage the report within the limits and with the guarantees of confidentiality imposed by the relevant legislation.

### **5. Method of processing and period of retention of personal data**

The processing of personal data included in the reports forwarded in accordance with the "*Whistleblowing Policy*" shall be carried out by persons "authorised to do so" by the Company and shall be based on the principles of fairness, lawfulness and transparency, pursuant to Article 5 of the GDPR.

Personal data may be processed using analogue and/or computerised/telematic methods, functional for storing, managing and transmitting them, in any case in application of appropriate physical, technical and organisational measures to guarantee their **security and confidentiality at every stage of the procedure, including the filing of the report and of the related documents** - without prejudice to the provisions of Article 12 of Legislative Decree no. 24/2023 - with particular reference to the identity of the reporter, the persons involved and/or in any case mentioned in the reports, the content of the reports and related documentation.

The reports received by the Company, together with the attached deeds and documents, shall be retained for the time necessary for their management and, in any case, as provided for by the legislation, **for a period not exceeding five years from the date of the communications of the relevant final outcomes**. After this period, the reports will either be deleted from the system or stored in an anonymised form.

Consistent with the indications provided in paragraph 1, personal data included in alerts that are manifestly irrelevant to the purposes of the alerts will be immediately deleted.

## **6. Areas of communication and transfer of personal data**

In addition to the aforementioned internal figures specifically authorized by the Data Controller, the personal data collected may also be processed, as part of the "Whistleblowing Policy" and in pursuit of the purposes indicated, also by the following third parties.

If there are grounds for, personal data may be transmitted to the Judicial Authority and/or Police Bodies that request it in the context of judicial investigations.

Under no circumstances will personal data be disseminated.

## **7. Rights of the interested party**

Each interested party is empowered to exercise the rights referred to in articles 15 and seq. of the GDPR, in order to obtain access, for example, from the Data Controller to their personal data, the rectification or cancellation of the same or the limitation of the processing concerning them, without prejudice to the possibility to lodge a complaint with the Data Protection Authority, in the absence of a satisfactory feedback,.

In order to exercise these rights, it is necessary to submit a specific request in free form to the following address of the Data Controller: *privacy@slowear.com*, or to send to the same address the form available on the *website* of the Personal Data Protection Authority.

In this regard, please note that the aforesaid rights of data subjects to the processing of personal data may be restricted pursuant to and for the purposes of Article 2-*undecies* of Legislative Decree no. 196 of 30 June 2003 ("*Privacy Code*", as amended by Legislative Decree no. 101/2018), for the time and within the limits in which this constitutes a necessary and proportionate measure, where their exercise may result in concrete and effective prejudice to the confidentiality of the identity of the reporting parties.

In such cases, the interested parties will still have the right to refer the matter to the Guarantor Authority so that the latter may assess whether the conditions for taking action under Article 160 of Legislative Decree no. 196/2003 are met.