WHISTLEBLOWING POLICY

Summary

1. PURPOSE AND SCOPE

1.1 PURPOSE

The term whistleblowing refers to the spontaneous disclosure by a reporting person (hereinafter, the "whistleblower*")* of an offence detrimental to the public interest or the integrity of the entity committed within the work context and witnessed by the whistleblower.

Legislative Decree No. 24 of 10 March 2023 (hereinafter, the "Decree"), which implements EU Directive 2019/1937, pursues the aim of strengthening the protection of whistleblowers and extending the scope of confidentiality protection to other persons than the whistleblower, who may nevertheless be recipients of retaliation, undertaken even indirectly, by reason of the role assumed in the whistleblowing process and/or the particular relationship that binds them to the whistleblower. The Decree also provides that anonymous reports may be made.

This policy governs the way in which Tessilform S.p.A. (hereinafter "the Company") implements the legislation on Whistleblowing and describes the process for handling reports, received through the internal channel by

anyone who becomes aware of acts and/or facts, even if only potentially, contrary to the law and the Company's internal regulations.

1.2 RECIPIENTS

The recipients of the safeguards and protection guaranteed by the law are:

- Employees;
- Self-employed persons working for the Company;
- Suppliers, subcontractors and employees of these;
- Freelancers and consultants;
- Volunteers and trainees, paid and unpaid;
- Shareholders and persons with functions of administration, management, control, supervision or representation, even if such functions are performed only in fact;
- Those who do not yet have a legal relationship with the Company (pre-contractual stage), as well as those whose relationship has ended or who are on trial period.

Due to the extension of the subjective scope of application of the relevant legislation, other recipients of the safeguards and protection guaranteed by the law are:

- Facilitator, a natural person who assists (advises or supports) the whistleblower in the reporting process, operating within the same work context;
- Persons in the same work environment as the whistleblower, who are related to him/her by a stable emotional or family relationship up to the fourth degree;
- Work colleagues, who work in the same work environment as the whistleblower and who have a regular and current relationship with this person;
- Entities owned by the whistleblower, exclusively or in majority partnership with third parties of the whistleblower;
- Entities where the whistleblower works;
- Entities operating in the same business environment as the whistleblower.

2. THE REPORTING OF BREACHES

Information on breaches of specific national and Union laws may be the subject of whistleblowing. There is no exhaustive list of offences or irregularities that may constitute the subject of whistleblowing; reports that concern conduct, risks or irregularities, whether committed or attempted, to the detriment of the public interest or the integrity of the entity are considered relevant.

It should be noted that, in accordance with the Decree, the protection and safeguards provided for in the law do not apply to reports concerning:

a) Disputes, claims or demands linked to an interest of a private nature of the whistleblower or which relate exclusively to his or her individual employment relationships;
b) Violations where already mandatorily regulated by EU or national acts (e.g. financial services, money laundering and terrorism, transport safety, environmental protection, consumer protection);
c) Infringements relating to national security, unless these aspects are covered by the relevant secondary legislation of the European Union.

Breaches will therefore be reportable that concern conduct, acts or omissions that harm the public interest or the integrity of the entity, consisting of:

1) Administrative offences;
2) Relevant offences under Legislative Decree 231/2001;
3) Offences falling within the scope of European Union or national acts (not already mandatorily regulated);
4) Acts or omissions detrimental to the financial interests of the European Union referred to in Article 325 TFEU (e.g. fraud and illegal activities);
5) Acts and omissions relating to the internal market, as referred to in Article 26(2) TFEU (e.g. EU budget fraud and corrupt activities);
6) Acts or conduct that frustrate the object or purpose of the provisions of the acts of the European Union in the fields indicated in numbers 3), 4) and 5).

Whistleblowers must ensure that the report is as circumstantial as possible and that the information regarding the person concerned as the potential perpetrator of the offence is such as to enable him/her to be identified and attributed the facts reported. Documents may be attached to the report to prove the truthfulness and substantiation of the facts reported.

In the case of a generic report, which does not contain sufficient information to initiate investigation activities, the Committee should ask the whistleblower - through the dedicated platform - to provide more details. If it is not possible to contact the whistleblower or the whistleblower does not provide further details within 15 working days of the request, the Committee will proceed to file the report.

3. REPORTING CHANNELS

Under the Decree, three reporting channels are made available to whistleblowers*:*

- The internal channel, activated by the Company;
- The external channel, set up by ANAC;
- Public disclosures, through the press or social media.

The legislation provides that, as a priority, whistleblowers use the internal channel and, only under certain conditions, may make an external report or public disclosure.

3.1 INTERNAL CHANNEL

The Company provides employees and external stakeholders with a reporting channel accessible via the link **in the "Whistleblowing" section on the Patrizia Pepe website**, which will lead directly to the online platform dedicated to receiving the reporting of breaches (hereinafter also referred to as "Platform").

The Platform allows you to make an anonymous report, without registering and without having to enter your personal data. In this regard, if the whistleblower wishes to preserve anonymity, please remove any reference to the identity of the whistleblower from the subject of the report and any attachments.

To ensure complete anonymity for the whistleblower, it is recommended to report from a personal device via a private, non-corporate, network.

At the end of the reporting procedure, the whistleblower is issued with a receipt number that identifies his or her report and which he or she must subsequently use to view the progress of his or her report within the Platform.

No more than one reporting shall be opened for the same fact. Any additions must be included within the same reporting.

3.1.1. MANAGEMENT COMMITTEE

The Management Committee (hereinafter also referred to as the "*Committee*") is the body responsible for receiving and handling reports. The Committee is composed of three members from within the Company, who are qualified to hold the position by reason of their professional skills and functions. In compliance with the principles of impartiality and confidentiality, the Committee carries out any activity deemed appropriate for the assessment of the report, including the hearing of the persons who may report on the facts reported.

3.1.2. PRE-TRIAL PHASE AND INTERNAL INVESTIGATIONS

The Committee receives reports through notification of the presence of a report via the Platform. The Committee issues an acknowledgement to the whistleblower within seven days of receipt. At the same time, a communication channel is established between the whistleblower and the Committee for any requests or additions. For this reason, the whistleblower must regularly access the Platform and monitor the status of the investigation by entering the receipt number issued upon completion of the report form.

The Committee, in a collegial composition and in compliance with the principles of impartiality and confidentiality, may decide, to diligently follow up on the reports, to involve Co-workers, who are also specifically trained and authorized, to verify:

- that the whistleblower is one of the persons qualified to make a report;
- that the violation is one of the reportable violations;
- the merits of the report, filing it if unfounded, proceeding with internal investigations if found to be well-founded.

The Committee will acknowledge the report 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 period from the submission of the report.

As part of internal investigations, in order to verify the validity of the reports and the truthfulness of the reported facts, the Committee may analyse databases to identify possible links between the person concerned and third parties; collect relevant company documents; analyse the devices assigned to the person concerned to verify the existence of evidence confirming the report, such as e-mails or messages, in accordance with the provisions of the company's Regulation on the use of IT devices; conduct interviews with persons who may report information relevant to proving the reported violations.

For the purposes of its verification activities, the Committee may mandate specialized offices and/or third parties to carry out in-depth investigations, taking care to:

- issue a formal mandate, defining the scope of action and specifying the information it intends to obtain from the in-depth study requested;
- omit any information that might, even indirectly, lead to the identity of the whistleblower;
- omit any information relating to the whistleblower where not strictly necessary for the proper performance of the assignment;

- reiterate to the person in charge the obligation of confidentiality of the data processed (in the case of persons external to the Company, this obligation must be formalised in the service contract on behalf of the Committee).

For complete transparency of the process, reports filed as non-significant are noted with the subject of the report and the reasons for not proceeding with the subsequent investigation.

3.2 OTHER REPORTING CHANNELS

It is possible, upon the occurrence of conditions set out in the Decree, to proceed with the use of other reporting channels, such as the external channel set up by ANAC and public disclosures and/or referral to the competent Authorities.

4. RECORD KEEPING

Any data and documentation attached to the report will be kept for as long as necessary for the management and assessment of the report, but no longer than five years from the date of the communication of the final outcome of the reporting procedure.

5. PROTECTION OF WHISTLEBLOWER

The identity of the whistleblower and of other persons to whom the whistleblowing legislation extends the scope of protection may not be disclosed to persons other than the members of the Committee responsible for receiving and handling reports unless specifically authorised.

The measures adopted to guarantee the confidentiality of the whistleblower are not limited to protecting his or her identification data, but also all the elements of the report from which his or her identity may be inferred, even indirectly. Any disclosure of the whistleblower's identity to persons other than those competent to receive or follow up reports or otherwise authorised shall be made with the whistleblower's explicit consent.

The Company undertakes to ensure protection against any act of retaliation, discrimination or penalisation, whether direct or indirect, against the whistleblower for reasons connected, directly or indirectly, to the report. All personnel involved, in any capacity whatsoever, in the various phases relating to the management of reports are required to guarantee the highest level of confidentiality on the contents of reports and on the persons involved in the report.

The protection of the whistleblower cannot be guaranteed if it is established that the report is unfounded and defamatory, thus constituting willful misconduct on the part of the whistleblower.

6. UNTRUTHFUL REPORTING AND THE PROTECTION OF PERSON CONCERNED

To protect the dignity, honor and reputation of everyone, the Company undertakes to offer maximum protection against defamatory reports.

In this context, if, at the end of the verification phase of the report, it is ascertained that the report is unfounded and that the whistleblower is guilty of willful misconduct and/or gross negligence, the Company shall take appropriate steps to protect itself and its employees.

The Company adopts similar forms of protection to guarantee the privacy of the whistleblower also for the alleged perpetrator of the violation, without prejudice to applicable legal provisions.

7. MEASURES AND SANCTIONS

If the checks on the reports, conducted pursuant to this document, reveal unlawful conduct attributable to employees, the Company shall act promptly and immediately, through appropriate and proportionate measures and sanctions, considering the seriousness as well as the criminal relevance of such conduct and the initiation of criminal proceedings in cases where it constitutes an offence for the purposes of the applicable national legislation.

Should the investigations conducted reveal willful/intentional misconduct on the part of third parties who have had and/or have ongoing relations with the Company, the Company shall act promptly by taking all measures identified as necessary for its own protection.

8. PROTECTION OF PERSONAL DATA

Privacy policy pursuant to Articles 13 and 14 of EU Regulation 679/2016 (GDPR) on the processing of personal data

With this notice, Tessilform S.p.A. (hereinafter also "the Company") provides information on the processing of personal data of the data subject who report breaches of law (hereinafter, "whistleblower") and of the other data subjects, mentioned in or involved in the report itself, including the potential perpetrators of the offences reported (hereinafter, "person concerned"). The processing will be based on the principles of fairness, lawfulness, transparency and protection of confidentiality.

DATA CONTROLLER

The Data Controller is Tessilform S.p.A., in the person of its legal representative, with registered office in via Gobetti 7/9, 50013 Capalle, Campi Bisenzio (FI). E-mail: *privacy@patriziapepe.it*

DATA PROTECTION OFFICER (DPO)

The DPO can be contacted by e-mail at *dpo@patriziapepe.it*

ORIGIN OF DATA

Information can be provided:

- in the report, by the whistleblower;
- in the course of the necessary investigative activities (e.g. from public sources, third-party interviewees, etc.);
- during the process of handling reports;
- through traffic logs on connections to the reporting platform recorded on the Company's corporate systems.

In order to ensure complete anonymity for the whistleblower, it is recommended to report from a personal device via a private, non-corporate, network.

TYPE OF DATA

- If the whistleblower does not decide to remain anonymous, personal data referring to him/her may be processed, specifically:
  - identification data;
  - contact data;
  - any special data, pursuant to Article 9 GDPR, related to a general state of health *(absence due to illness, maternity, accident, etc.), suitability for carrying out specific tasks, membership of a trade union and/or political party, holding elected public office or religious beliefs;*
  - any so-called judicial data, pursuant to Article 10 GDPR, related to *criminal convictions and offences or security measures;*
  - any personal data contained in the subject of the report.

- Personal data relating to third parties (potential perpetrators of a breach or irregularity that falls within the scope of reportable offences or persons informed of the facts) may be processed as a result of the report, specifically:
    - identification data;
    - contact data;
    - any special data, pursuant to Article 9 GDPR, related to a general state of health *(absence due to illness, maternity, accident, etc.), suitability for carrying out specific tasks, membership of a trade union and/or political party, holding elected public office or religious beliefs;*
    - any so-called judicial data, pursuant to Article 10 GDPR, *related to criminal convictions and offences or security measures;*
    - any personal data contained in the subject of the report.

- Personal data that may emerge from subsequent investigative activities;
- Traffic logs concerning connections to the platform recorded on company systems *(in general, logs are files that record - and thus make it possible to reconstruct - the entire 'history' of operations carried out by a user or a machine. Logs, in fact, record all operations, in chronological order, carried out in the normal use of a software, an application or more simply a computer. The log also records all operations that a computer performs autonomously, without the need for human intervention. Log management at the corporate level makes it possible to monitor a series of activities, including accesses to the system carried out in a given time frame (including those outside working hours, those unsuccessful or those via VPN), failed transactions, possible anomalies (both software and hardware) and possible malware threats. This information is necessary to understand the state of the company's IT security: both in the case of normal machine operation but, above all, in the case of errors and problems, such as possible hacker attacks, thus enabling the IT function to investigate their causes and find a resolution, avoiding or blocking harmful situations in good time).*

Only personal data that are strictly necessary and pertinent to achieving the purposes set out below will be acquired, in compliance with the principle of minimisation set out in Article 5(1)(c) GDPR.

PURPOSE AND LEGAL BASIS OF PROCESSING

The Controller will process the above-mentioned personal data:

1. In order to manage and diligently follow up the reports received, including the activities of verification and internal investigations in relation to the area of reference and the institution of proceedings, including disciplinary proceedings, within the limits provided for by the legislation in force. In addition, personal data may be processed in order to comply with requests by the competent administrative or judicial authorities and, more generally, by public entities in compliance with the formalities required by law. The data will also be processed to effectively prevent and combat fraudulent and unlawful or irregular conduct.
   Therefore, the legal basis justifying the lawfulness of the processing is to fulfil legal obligations and to perform tasks of public interest to which the Data Controller is subject and provisions of Authorities legitimated by law (Art. 6(1)(c) and (e); Art. 9(2)(b) and (g); Art. 10 GDPR).
   Any disclosure of the identity of the whistleblower to persons other than those competent to receive or follow up reports or otherwise authorised will be made with the express consent of the whistleblower (Art. 6(1)(a) GDPR).

2. In order to: i) meet the Controller's needs for internal control and monitoring of business risks, as well as for the optimisation and streamlining of corporate and internal administrative management processes; ii) ascertain, exercise or defend a right or legitimate interest of the Controller in any competent forum to guarantee the exercise of the right of defence pursuant to Art. 24 of the Constitution; iii) managing IT security and protecting the assets and security of data, user assistance and maintenance of security systems and perimeter protection of traffic logs concerning connections to the Whistleblowing Platform recorded on company systems.
   Therefore, the legal basis justifying the lawfulness of the processing is the legitimate interest of the Controller (Art. 6(1)(f) GDPR).

METHODS OF PROCESSING

The information as identified above is processed by the members of the Committee, which is composed of specially appointed persons who are authorised and suitably trained for this purpose.
Data is collected electronically, through the dedicated Whistleblowing platform as defined in the Whistleblowing Policy, in order to guarantee the confidentiality of the whistleblowers and any other persons involved and the confidentiality of the information contained in the reports. The platform used for receiving reports is located on a company server.

DATA COMMUNICATION

The personal data collected may be disclosed to other subjects whose involvement is necessary to carry out the required investigative activities, aimed at verifying the grounds of the reported fact, as well as the adoption of any measures.
In particular, on the basis of the roles and work tasks performed, personal data will be processed by persons specifically instructed and authorised to carry out processing operations, such as, by way of example, external consultants, managers of the area in which the person concerned operates, the System Administrator. Please note that the information and data collected may be transmitted to the competent Authorities.

Any disclosure of the identity of the whistleblower to persons other than those competent to receive or follow up reports or otherwise authorised will be made with the express consent of the whistleblower.

The list of any third parties appointed as Data Processors for the provision of services outsourced by the Controller, such as the provision of IT infrastructure, communication services, etc., is available upon request.

PROVISION OF DATA

In order to make a report, the provision of personal data is optional; however, if provided, in certain cases it may be necessary for authorised personnel to use them to pursue the purposes already expressed. Failure to provide the data necessary to follow up the report will prevent the activities from being carried out.

DATA TRANSFER

The Data Controller does not transfer personal data to third countries. Should it become necessary to transfer data outside the EU, the Controller will verify that the suppliers provide adequate guarantees, as provided for in Article 44 et seq. of the GDPR.

DATA RETENTION

The personal data collected will be kept for the time strictly necessary to fulfil the purposes already indicated in the preceding paragraphs, and in any case for no longer than five years from the date of the communication of the final outcome of the report, unless further storage is required by law (e.g. in the event of legal or disciplinary proceedings, until the conclusion of such proceedings). After this period has expired, the Data Controller shall delete the personal data.

RIGHTS OF THE DATA SUBJECT

The Data Controller informs data subjects that, in general terms and subject to proof of identity, they may exercise their rights under Articles 15 et seq. of the GDPR, in particular: i) right of access; ii) right of rectification; iii) right to erasure; iv) right to restriction of processing; v) right to object; vi) right not to be subject to automated decision-making.

Rights may be exercised by contacting the Controller by sending a request to the e-mail address privacy@patriziapepe.it.
For any information in connection with this policy and in the event of a breach of data protection legislation, you can contact the DPO at *dpo@patriziapepe.it.*

In the present case, however, pursuant to the provisions of Articles 2-undecies and 2-duodecies of Legislative Decree No. 196/2003 "Privacy Code", the Data Controller reserves the right to limit or delay the exercise of such rights, within the limits set by the applicable provisions of law, in particular where there is a risk that an actual, concrete and not

otherwise justified prejudice to the confidentiality of the identity of the whistleblower may arise and that the ability to effectively verify the merits of the report or to gather the necessary evidence may be compromised.

In particular, the exercise of these rights:

- will be possible in accordance with the provisions of the law or regulations governing the sector (including Legislative Decree No. 231/2001, as amended);
- may be delayed, limited or excluded by reasoned communication without delay to the data subject, unless such communication would jeopardise the purposes of the limitation, for such time and to the extent that this constitutes a necessary and proportionate measure, having regard to the fundamental rights and legitimate interests of the data subject, in order to safeguard the confidentiality of the identity of the whistleblower.

Data subjects also have the right to lodge a complaint with the Data Protection Authority.