TESSILFORM S.p.A.

POLICY WHISTLEBLOWING

Version	Date
v. 1.0.	10.07.2023
v. 1.1.	17.05.2024
v. 1.2.	03.02.2025

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*"), implementing EU Directive 2019/1937, pursues the aim of strengthening the protection of reporting persons and extending the scope of confidentiality protection to other subjects, other than the Whistleblower, who, however, may be the recipients of retaliation, even indirectly, due to the role assumed in the reporting process and/or the particular relationship that leads to the binds to the Whistleblower. The Decree also provides for the possibility of anonymous reporting.

This policy regulates the ways in which Tessilform S.p.A. (hereinafter "the Company") implements the legislation on Whistleblowing and describes the process of managing reports, received through the internal channel by anyone who is aware of acts and/or facts, even if only potentially, contrary to the law and internal company regulations.

1.2 RECIPIENTS

The following are the recipients of the safeguards and protection guaranteed by the legislation:

- Employees;
- Self-employed persons working for the Company;
- Suppliers, subcontractors and their employees;
- Freelancers and consultants;
- Volunteers and trainees, whether they receive a reimbursement of expenses or not;
- Shareholders and persons with administrative, managerial, control, supervisory or representative functions, even if such functions are performed only in fact;
- Those who do not yet have a legal relationship with the entity (pre-contractual stage), as well as those whose relationship has ended or who are in a trial period.

Due to the extension of the subjective scope of application of the reference legislation, the following are also recipients of the safeguards and protection guaranteed by the legislation:

- Facilitator, a natural person who assists (provides advice or support) to the Whistleblower in the reporting process, operating within the same work context;
- Persons in the same working context as the Whistleblower, who are linked to him/her by a stable emotional or family bond within the fourth degree;
- Work colleagues, who work in the same working context as the Whistleblower and who have a habitual and current relationship with this person;
- Entities owned by the Whistleblower, either exclusively or majority-owned by third parties, of the Whistleblower;
- Entities where the Whistleblower works;
- Entities that operate in the same working context as the Whistleblower.

2. SUBJECT OF THE REPORT

Information on violations of specific national and European Union regulations may be reported. There is no exhaustive list of crimes or irregularities that may be the subject of *whistleblowing*; reports concerning conduct, risks or irregularities, committed or attempted, to the detriment of the public interest or the integrity of the entity are considered relevant.

It should be noted that, according to the provisions of the Decree, the protection and safeguards provided for by the law do not apply to reports relating to:

a) Disputes, claims or requests related to a personal interest of the Whistleblower or that relate exclusively to their individual employment relationships;
b) Violations where they are already regulated by European Union or national acts (for example: financial services, money laundering and terrorism, transport security, environmental protection, consumer protection);
c) Violations of national security, as well as procurement related to aspects of defence or national security, unless such aspects fall under the relevant secondary legislation of the European Union.

Therefore, violations will 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 pursuant to Legislative Decree no. 231/2001;
3) Offences that fall within the scope of European Union or national acts (not already regulated on a mandatory basis);
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 concerning the internal market, pursuant to art. 26(2) TFEU (e.g. fraud of the EU budget and corrupt activities);
6) Acts or conduct that frustrate the object or purposes of the provisions of the European Union acts in the areas indicated in numbers 3), 4) and 5).

Whistleblowers must ensure that the report is as detailed as possible and that the information relating to the reported person as a potential perpetrator of the offence is such as to allow the identification and attribution of the reported facts. It is possible to attach documents to the report to demonstrate the truthfulness and validity of the reported facts.

In the case of a generic report, which does not contain sufficient information for the start of the investigation, the Committee must request the Whistleblower – through the appropriate Platform – to provide further details. If it is not possible to contact the Whistleblower or if the Whistleblower does not provide further details within fifteen working days of the request, the Committee will proceed to archive 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 (National Anti-Corruption Authority);
- 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 makes available to employees and external *stakeholders* a reporting channel accessible at the link in the "Whistleblowing" section on the *patriziapepe.com* website, which will lead directly to the online platform dedicated to receiving reports (hereinafter, also the "Platform").

The Platform allows you to make an "anonymous" report, without making any registration and without the need 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 total anonymity to the Whistleblower, it is recommended to report from a personal device via a private, non-corporate, network.

A WRITTEN REPORT may be made through the Platform, by filling in the appropriate fields with the required information, or A DIRECT MEETING WITH THE MEMBERS OF THE MANAGEMENT COMMITTEE may be requested (ORAL REPORT).
To request a face-to-face meeting, the fields on the Platform can be used to formulate your request. Required fields can be exceeded by entering at least one alphanumeric character or generic details.

It should be noted that if the Whistleblower opts for a face-to-face meeting, anonymity cannot be guaranteed, without prejudice to the Management Committee's commitment to ensuring maximum confidentiality, using all measures deemed necessary (for example, scheduling the meeting in an isolated meeting room, or in a single office or, again, with the provision of the meeting at a suitable time).
The Management Committee will replay to the Whistleblower through the Platform, informing about the place and manner of the direct meeting, which must be scheduled no later than ten [10] days from the request. During the face-to-face meeting, a report will be drawn up and must also be signed by the Whistleblower as well as by the person who received the declaration. A copy of the report must be given to the Whistleblower. After this initial stage, the procedure will follow the normal course set out in §3.1.2, below.

At the end of the electronic procedure carried out through the Platform, the Whistleblower is issued with a receipt number that identifies his communication and that he must subsequently use to view the progress of his report/request within the Platform.

No more than one report should be opened for the same fact. Any additions must be included in the same report.

3.1.1. MANAGEMENT COMMITTEE

The Management Committee (hereinafter also referred to as the "*Committee*") is the body responsible for receiving and managing reports. The Committee is composed of two members from within the Company, who are suitable to fill the role due to their professional skills and functions. In compliance with the principles of impartiality and confidentiality, the Committee carries out any activity deemed appropriate for the evaluation of the report, including the hearing of the subjects who may report on the facts reported.

In the event of a conflict of interest, i.e. in the event that one or more members of the Management Committee coincide with the Whistleblower, the Reported or are in any case persons involved or interested, the report will be addressed to the company's top management, always in compliance with the obligation of confidentiality provided for by the regulations.

If the internal report is submitted outside the internal channel and it is clear that it is a whistleblowing report, it must be transmitted, within seven [7] days of its receipt and without retaining a copy, to the Management Committee, at the same time informing the Whistleblower of the transmission.

3.1.2. ENQUIRY PHASE AND INTERNAL INVESTIGATIONS

The Committee receives reports through the notification of the presence of a report made through the Platform. The Committee shall send a notice of acceptance to the Whistleblower **within seven [7] days** from the date of receipt. At the same time, a channel of communication 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 collegial composition and in compliance with the principles of impartiality and confidentiality, may decide, in order to diligently follow up on reports, to involve Collaborators, who are also specifically trained and authorised, to verify:

- that the Whistleblower is one of the persons qualified to make a report;
- that the violation is among those that can be reported;
- the merits of the report, archiving it if unfounded, proceeding with internal investigations if deemed well-founded.

The Committee will provide feedback to the report **within three [3] months from the date of the acknowledgment of receipt** or, in the absence of such acknowledgement, **within three [3] months after the expiry of the period of seven [7] days from the submission of the report or from the date on which the face-to-face meeting took place**, if the Whistleblower has used this method of reporting.

As part of internal investigations, in order to verify the validity of the reports and the truthfulness of the facts reported, the Committee may:

- ✓ analyze databases to identify possible links between the Reported and third parties;
- ✓ collect relevant business documents;
- ✓ analyze the devices assigned to the Reported to verify the existence of evidence to confirm the report, such as e-mails or messages, in accordance with the provisions of the Company Regulations for the use of IT devices;
- ✓ Conduct interviews with people who may report impactful information to prove reported violations.

For the purposes of the verification activity, the Committee may confer a mandate for in-depth analysis to specialist offices and/or third parties, taking care of:

- confer a formal mandate, defining the scope of action and specifying the information it intends to obtain from the requested in-depth analysis;

- omit any information that could, even indirectly, lead back to the identity of the Whistleblower;

- omit any information relating to the Reported Person, where not strictly necessary for the proper performance of the assignment entrusted;

- reiterate to the person in charge the obligation of confidentiality of the data processed (in the case of parties external to the Company, this obligation must be formalized in the contract for the provision of services on behalf of the Management Committee).

In order to be admissible, it must be clear in the report:

- ✓ the circumstances of time and place in which the reported event occurred;
- ✓ a description of the facts covered by the report that contains details relating to the circumstantial information and, if any, also the manner in which the Whistleblower became aware of the facts;
- ✓ personal details or other elements that make it possible to identify the person to whom the reported facts can be attributed.

At the end of the three [3] months, the Management Committee will communicate to the Whistleblower:

- ➢ the dismissal of the report, justifying the reasons;
- ➢ ascertaining the validity of the report and transmitting it to the competent internal bodies;
- ➢ the activity carried out so far and/or the activity to be carried out. In the latter case, the Whistleblower will also be informed of the subsequent final outcome of the investigation (dismissal or verification of the validity of the report with transmission to the competent bodies).

For complete transparency of the process, reports dismissed as irrelevant are noted by reporting the subject of the report and the reasons why subsequent investigations were not carried out.

3.2 EXTERNAL CHANNEL

The Whistleblower may make a report through the external channel activated by ANAC (National Anti-Corruption Authority) if, at the time of its submission, one of the following conditions is met:

a. there is no mandatory activation of the internal reporting channel within his/her work context, i.e. this, even if mandatory, is not active or, even if activated, does not comply with the provisions of the legislation;
b. the Whistleblower has already made an internal report following the procedure established by their organization but the same has not been followed up;
c. the Whistleblower has reasonable grounds to believe that, if the Whistleblower were to make an internal report, it would not be effectively followed up or that the same report could lead to a risk of retaliation;
d. the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

External reports are made in written form through the online platform made available by ANAC or orally through telephone lines or voice messaging systems or, at the request of the Whistleblower, through a direct meeting set within a reasonable time.

The methods for managing reports have been established within the ANAC Regulation, accessible through the ANAC website.

The external report submitted to a party other than ANAC shall be transmitted to the latter, within seven days from the date of its receipt, at the same time giving notice of the transmission to the Whistleblower.

3.3. PUBLIC DISCLOSURE

The Whistleblower may make a public disclosure if one of the following conditions is met:

a) the Whistleblower has previously made an internal and external report or has directly made an external report and has not been responded to within the prescribed terms;
b) the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
c) the Whistleblower has reasonable grounds to believe that the external report may entail the risk of retaliation or may not be effectively followed up due to the specific circumstances of the specific case, such as those in which evidence may be concealed or destroyed or where there is a well-founded fear that the person receiving the report may be colluding with the infringer or involved in the violation itself.

4. RETENTION OF DOCUMENTATION

Any data and documentation attached to the report will be kept for the time necessary for the management and evaluation of the report, in any case no longer than five [5] years from the date of communication of the final outcome of the reporting procedure.

5. PROTECTION OF THE WHISTLEBLOWER

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

The measures adopted to guarantee the confidentiality of the Whistleblower are not limited to protecting the identification data, but also all the elements of the report from which the identity of the Whistleblower can be deduced, even indirectly. Any disclosure of the identity of the Whistleblower to persons other than those competent to receive or follow up on the reports or otherwise authorised will take place with the express consent of the Whistleblower.

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

A further protection granted to the Whistleblower by law is the limitation of his/her liability with reference to the dissemination of certain categories of information, which could expose him/her to criminal, civil and administrative liability, always provided that:

- at the time of disclosure or dissemination, there are reasonable grounds to believe that the information is necessary to uncover the reported breach;
- the report is made in compliance with the conditions set out in the Decree to benefit from protection against retaliation (well-founded reasons to believe the reported facts to be true, the violation is among those that can be reported and the methods and conditions of access to the report are respected).

In particular, the Whistleblower will not be held liable either criminally, or in civil and administrative proceedings for:

- disclosure and use of professional secrecy (Article 326 c.p.);
- disclosure of professional secrecy (Article 622 c.p.);

- disclosure of scientific and industrial secrets (Article 623 c.p.);
- violation of the duty of fidelity and loyalty (Article 2105 c.c.);
- infringement of copyright protection provisions;
- violation of the provisions relating to the protection of personal data;
- disclosure or dissemination of information about violations that offend the reputation of the person involved.

In any case, liability is not excluded for conduct that:

- are not related to the report;
- are not strictly necessary to disclose the breach;
- constitute an unlawful acquisition of information or access to documents.

The protection of the Whistleblower cannot be guaranteed if it is ascertained that the report is unfounded and defamatory, thus constituting malicious conduct by the Whistleblower.

6. PROTECTION FROM DEFAMATORY REPORTS AND PROTECTION OF THE REPORTED

In order to protect the dignity, honour and reputation of everyone, the Company undertakes to offer maximum protection from defamatory reports.

In this context, if, at the end of the verification phase of the report, it is ascertained that it is unfounded and that the Whistleblower is guilty of wilful misconduct and/or gross negligence, the Company will take appropriate initiatives 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 the applicable legal provisions.

7. MEASURES AND SANCTIONS

If, from the verification of the reports, conducted pursuant to this document, it is found that unlawful conduct attributable to employees is found, the Company will act promptly and immediately, through appropriate and proportionate measures and sanctions, taking into account the seriousness and criminal relevance of such conduct and the establishment of criminal proceedings in cases where it constitutes a criminal offence under applicable national law.

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

8. INFORMATION FLOWS TO THE SUPERVISORY BOARD

The company staff involved are required to promptly notify the Supervisory Board (SB), through the use of the Whistleblowing system active in the Company, of any behavioural exception (deviation from correct behaviour) or any unusual event that may arise, indicating the reasons for the discrepancies and reporting the authorisation process followed.

The Supervisory Board may require staff, in various capacities involved, to periodically communicate compliance with the rules of conduct indicated for the performance of the tasks assigned.

The Area Managers involved will ensure, by coordinating the structures under their competence, the traceability of the process to demonstrate compliance with the law, keeping all the necessary documentation available to the Supervisory Board, in an orderly archive.

The synoptic table, provided below, collects the following data: "Activity sensitive to the risk of committing the predicate crime"; "Information for the Supervisory Board"; "Responsibility for preparing and/or sending to the SB"; "Action / Periodicity".

Among the possible actions required we have:

• Sending: the information flows must reach the SB mainly by telematic transmission to the dedicated e-mail box;

• Preparation: the SB requires the preparation of the required documentation to be shown on the occasion of a specific convocation that can be requested at any time; the interviews of the Managers are mainly aimed at providing updates and insights on significant information or data useful for the assessment of risk activities or about the way to manage them.

Synoptic table of information flows to the SB

Activity sensitive to the risk of committing the predicate crime	Information for the Supervisory Board	Responsibility for preparing and/or sending to the SB	Action / Periodicity
All company activities sensitive to the risk of committing one of the crimes punished by Legislative Decree no. 231 / 2001 taking into account the risk areas specified in the Guidelines of Conduct.	Occurrence of an accident or a near-accident that may impact with Legislative Decree no. 231 / 2001. Abnormal behaviour or non-compliant with this procedure by Tessilform S.p.A. staff. Results of the inspection visits by the Control Bodies.	CEO	Whenever necessary / on request

9. 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, the Supervisory Board (SB). 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.