TESSILFORM S.p.A.

WHISTLEBLOWING POLICY

Version	Date of issue
v. 1.0.	10 July 2023
v. 1.1.	17 May 2024
v. 1.2.	3 February 2025
v. 1.3	19 March 2026

Contents

1. PURPOSE AND SCOPE OF APPLICATION

1.1 PURPOSE

The term *'whistleblowing'* refers to the reporting by an individual, known as *a whistleblower*, of wrongdoing that harms the public interest or the integrity of the organisation, occurring within the workplace and of which the individual has become aware.

Legislative Decree No. 24 of 10 March 2023 (hereinafter the "Decree"), implementing EU Directive 2019/1937, aims to strengthen the protection of whistleblowers and extend the scope of confidentiality protection to other individuals, other than the whistleblower, who may nevertheless be subject to retaliation, including indirectly, due to the role they have assumed in the reporting process and/or the particular relationship linking them to the whistleblower. The Decree also provides for the possibility of making anonymous reports.

This *policy* governs the procedures by which Tessilform S.p.A. (hereinafter "the Company") implements the legislation on whistleblowing and describes the process for handling reports received via the internal channel from anyone who is aware of acts and/or facts, even if only potentially, contrary to the law and internal company regulations.

1.2 RECIPIENTS OF THE 'WHISTLEBLOWING' POLICY

The following are covered by the safeguards and protection guaranteed by the legislation:

- Employees;
- Self-employed workers carrying out their work at the organisation;
- Suppliers, subcontractors and their employees;
- Freelancers and consultants;
- Temporary agency workers;
- Volunteers and trainees, whether or not they receive a reimbursement of expenses;
- Shareholders and persons holding administrative, managerial, supervisory, oversight or representative roles, even where such roles are exercised de facto;
- Those who do not yet have a legal relationship with the organisation (during pre-contractual negotiations), as well as those whose relationship has ceased or who are on probation or serving a notice period.

Given the broad scope of the relevant legislation, the following are also covered by the safeguards and protection guaranteed by the legislation:

- Facilitators, natural persons who assist (provide advice or support) the Whistleblower in the reporting process, operating within the same workplace;
- Persons in the same workplace as the Whistleblower, who are linked to them by a stable personal relationship or kinship up to the fourth degree;
- Work colleagues who work in the same workplace as the Whistleblower and who have a regular and ongoing relationship with that person;
- Entities owned by the Whistleblower, either exclusively or through a majority shareholding by third parties;
- Entities at which the Whistleblower works;
- Entities operating in the same workplace as the Whistleblower.

2. SUBJECT OF THE REPORT

Information regarding breaches of specific national and European Union regulations may form the subject of a report. There is no exhaustive list of offences or irregularities that may constitute the subject of *whistleblowing*; reports concerning conduct, risks or irregularities, whether committed or attempted, to the detriment of the public interest or the integrity of the organisation, are considered relevant.

It should be noted that, in accordance with the provisions of the Decree, the protection and safeguards provided for by the legislation do not apply to reports relating to:

a) Disputes, claims or requests linked to the personal interests of the whistleblower or which relate exclusively to their individual employment relationship;
b) Violations where these are already mandatorily regulated by European Union or national legislation (for example: financial services, money laundering and terrorism, transport safety, environmental protection, consumer protection);
c) Violations relating to national security, as well as contracts concerning defence or national security aspects, unless such aspects fall within the relevant secondary legislation of the European Union.

The managing entity shall keep a written record of all reports received by maintaining a dedicated Report Register, kept via an independent logging system or other suitable means to ensure the confidentiality, traceability and security of the data contained therein. Periodic checks are carried out to ensure that all reports received have been processed and entered into the Report Register.

In the event that a report received does not meet the requirements to be considered relevant for the purposes of whistleblowing legislation (for example, because it does not fall within the objective scope of application of Legislative Decree 24/2023 or because the whistleblower is not among the eligible persons), the confidentiality of the whistleblower will nevertheless be ensured. The report will nevertheless be recorded in the Report Register, stating the reasons why no further investigation was carried out, and the whistleblower will be informed of the closure of the case whilst maintaining the utmost confidentiality regarding their identity.

The following violations may therefore be reported: conduct, acts or omissions that harm the public interest or the integrity of the organisation, consisting of:

1) Administrative offences;
2) Predicate offences under Legislative Decree No. 231/2001;
3) Offences falling within the scope of application of European Union or national legislation (not already subject to mandatory regulation);
4) Acts or omissions that harm the financial interests of the European Union as referred to in Article 325 of the TFEU (e.g. fraud and illegal activities);
5) Acts and omissions relating to the internal market, as referred to in Article 26(2) of the TFEU (e.g. fraud against the European Union budget and corrupt practices);
6) Acts or conduct that undermine the purpose or objectives of the provisions set out in European Union legislation in the sectors referred to in points 3), 4) and 5).

Reporting parties must ensure that the report is as detailed as possible and that the information relating to the reported party as the potential perpetrator of the offence is sufficient to enable their identification and the attribution of the reported facts. Documents may be attached 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 to initiate an investigation, the Manager must request the Reporter – via the dedicated Platform – to provide further details. If it is not possible to contact the Reporter or if the Reporter does not provide further details within fifteen working days of the request, the Manager will proceed to close the report.

3. REPORTING CHANNELS

The provisions of the Decree require that three reporting channels be made available to the *whistleblower*:

- The internal channel, set up by the Company
- The external channel, set up by ANAC (National Anti-Corruption Authority)
- Public disclosures, via the press or social media

The regulations stipulate that, as a matter of priority, whistleblowers must use the internal channel and may only make an external report or public disclosure if certain conditions are met.

3.1 INTERNAL CHANNEL

The Company provides employees and external *stakeholders* with a reporting channel accessible via the link in the dedicated Whistleblowing section on the *patriziapepe.com* website, which leads directly to the IT platform dedicated to receiving reports (hereinafter also referred to as the "Platform").

The Platform allows for "anonymous" reporting, without the need to register or provide personal details. In this regard, should the Reporter wish to remain anonymous, they are advised to remove any reference to their identity from the subject line of the report and any attachments.

To ensure the Reporter's complete anonymity, it is recommended that the report be submitted from a personal device via a private, non-corporate network.

Through the Platform, a WRITTEN REPORT may be submitted by completing the relevant fields with the required information, or a FACE-TO-FACE MEETING WITH THE INTERNAL CHANNEL MANAGER (ORAL REPORT) may be requested.

To request a face-to-face meeting, the fields on the Platform may be used to submit your request. Mandatory fields may be bypassed by entering at least one alphanumeric character or general details.

Please note that if the Whistleblower opts for a face-to-face meeting, anonymity cannot be guaranteed, without prejudice to the Manager's commitment to ensuring the utmost confidentiality by taking all measures deemed necessary (for example, scheduling the meeting in a secluded meeting room, or in a private office, or arranging the meeting at a suitable time).

The Manager will respond to the Whistleblower via the Platform, providing details of the venue and arrangements for the face-to-face meeting, which must be scheduled no later than ten [10] days from the request. During the face-to-face meeting, minutes shall be drawn up and signed by both the Whistleblower and the person who received the statement. A copy of the minutes shall be provided to the Whistleblower. Following this initial phase, the procedure shall proceed as set out in §3.1.2 below.

Upon completion of the online procedure carried out via the Platform, the Reporter is issued with a reference number identifying their report, which they must subsequently use to view the progress of their report/request within the Platform.

No further reports should be opened for the same matter. Any additional information must be included within the same report.

The activation of the internal channel was preceded by the involvement of trade unions in accordance with Article 4, paragraph 1, of Legislative Decree No. 24/2023. In particular, the company trade union representatives (RSA/RSU) or, in their absence, the corresponding regional organisations of the most representative trade union associations at national level, were informed in advance of the activation of the internal channel and/or its update by means of a formal communication containing the organisational document and an indication of a deadline for any requests for clarification and/or meetings.

3.1.1. MANAGER OF THE INTERNAL CHANNEL

The management of the internal reporting channel is entrusted to a person external to the Company, namely Ms Eleonora Netti (hereinafter also the "Manager"), a professional possessing autonomy, competence and independence, and suitable to fulfil the role by virtue of her specific professional expertise. The Manager, in accordance with the principles of impartiality and confidentiality, carries out any activity deemed appropriate for the assessment of the report, including hearing from individuals who can provide information on the reported facts.

In the event of a conflict of interest, namely where the Manager is the same person as the Reporting Party, the Party Against Whom the Report is Made, or is otherwise a person involved in or affected by the report, the report shall be referred to the Company's Board of Directors, always in compliance with the confidentiality obligation provided for by the regulations.

If an internal report is submitted outside the internal reporting channel and it is clear that it constitutes a whistleblowing report, it must be forwarded to the Internal Reporting Channel Manager within seven [7] days of receipt, without retaining a copy, and the Reporter must be notified of the forwarding at the same time.

3.1.2. PRELIMINARY INVESTIGATION AND INTERNAL INVESTIGATIONS

The Manager receives reports via notification of a report submitted through the Platform. The Manager issues an acknowledgement of receipt to the Whistleblower within seven [7] days of the date of receipt. At the same time, a communication channel is established between the Whistleblower and the Manager for any queries or additional information. For this reason, the Reporting Party must regularly access the Platform and monitor the status of the investigation by entering the receipt number issued upon completion of the reporting form.

The Manager, in accordance with the principles of impartiality and confidentiality, may decide, in order to follow up on reports diligently, to involve Authorised Collaborators, who are also specifically trained and authorised, to verify:

- that the Whistleblower is among those qualified to make a report;
- that the breach is one that can be reported;
- the merits of the report, dismissing it if found to be lacking merit and proceeding with internal investigations if deemed well-founded.

The Manager shall respond to the report within three [3] months of the date of the acknowledgement of receipt or, in the absence of such acknowledgement, within three [3] months of the expiry of the seven [7] day period following the submission of the report or the date on which the face-to-face meeting took place, where the Reporting Person has used this method of reporting.

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

- ✓ analyse databases to identify possible links between the Reported Party and third parties;
- ✓ collect relevant company documents;

- ✓ analyse the *devices* assigned to the Reported Party to verify the existence of evidence confirming the report, such as emails or messages, in accordance with the Company Regulations on the use of IT devices;
- ✓ conduct interviews with individuals who can provide relevant information to substantiate the reported breaches.

For the purposes of the investigation, the Manager may delegate the investigation to specialist departments and/or third parties, taking care to:

- issue a formal mandate, defining the scope of action and specifying the information to be obtained from the requested investigation;
- omit any information that could, even indirectly, lead to the identification of the Whistleblower;
- omit any information relating to the subject of the report, unless strictly necessary for the proper performance of the assigned task;
- reaffirm to the appointed party the obligation of confidentiality regarding the data processed (in the case of parties external to the Company, this obligation must be formalised in the service contract on behalf of the Manager).

For the purposes of admissibility, the report must clearly state:

- ✓ the time and place at which the incident forming the subject of the report occurred;
- ✓ a description of the facts forming the subject of the report, containing details of the circumstantial evidence and, where applicable, the manner in which the Reporting Party became aware of the facts;
- ✓ the personal details or other information enabling the identification of the person to whom the reported facts are attributed.

At the end of the three [3] months, the Manager shall notify the Reporter:

- ➢ that the report has been closed, stating the reasons;
- ➢ that the report has been found to be well-founded and has been forwarded to the relevant internal bodies;
- ➢ the actions taken to date and/or the actions intended to be taken. In the latter case, the Whistleblower will also be informed of the final outcome of the investigation (dismissal or confirmation of the validity of the report with referral to the competent bodies).

To ensure complete transparency of the process, reports closed as irrelevant are recorded, stating the subject of the report and the reasons why no further investigation was carried out.

3.2 EXTERNAL CHANNEL

The Whistleblower may submit a report via the external channel set up by ANAC (National Anti-Corruption Authority) if, at the time of submission, one of the following conditions applies:

a. there is no requirement within their workplace to use the internal reporting channel, or, even if mandatory, it is not active, or, even if active, it does not comply with the provisions of the legislation;
b. the Whistleblower has already made an internal report following the procedure established by their organisation but no action was taken;

c. the Whistleblower has reasonable grounds to believe that, if they were to make an internal report, it would not be effectively followed up, or that making such a report could result in 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 writing via the IT platform provided by ANAC, or orally via telephone lines or voice messaging systems, or, at the Whistleblower's request, through a face-to-face meeting arranged within a reasonable timeframe.

The procedures for handling reports have been set out in the ANAC Regulations, which are available on the ANAC website.

Any external report submitted to a body other than ANAC shall be forwarded to ANAC within seven days of receipt, and the reporter shall be notified of this forwarding at the same time.

3.3 PUBLIC DISCLOSURE

Finally, Legislative Decree 24/2023 established the **Public Disclosure** channel, which involves making information on violations public through the press, electronic media or, generally, by using means of dissemination capable of reaching a large number of people (e.g. TV, radio, social media). This channel is to be used as a last resort, namely when:

i. reports made via other channels have not been followed up;
ii. the use of other channels exposes the whistleblower to a risk of retaliation (e.g. where there is a well-founded fear that the person to whom the report was made is colluding with the perpetrator of the breach or is even personally involved);
iii. the breach constitutes an imminent or obvious danger to the public interest.

4. RETENTION OF DOCUMENTATION AND DATA PROTECTION

The data and any documentation attached to the report will be retained for the time necessary to manage and assess the report, but in any event for no longer than five [5] years from the date of notification of the final outcome of the reporting procedure.

5. PROTECTION OF THE WHISTLEBLOWER

The identity of the Whistleblower and of other persons to whom the *whistleblowing* legislation extends protection may not be disclosed to anyone other than the Manager responsible for receiving and handling reports, unless specifically authorised.

The measures adopted to guarantee the confidentiality of the Whistleblower are not limited to protecting identifying data, but also cover all elements of the report from which their identity may be inferred, even indirectly. Any disclosure of the Whistleblower's identity to persons other than those authorised to receive or follow up on reports, or otherwise authorised, shall take place with the Whistleblower's express consent.

The Company undertakes to ensure protection against any act of retaliation, discrimination or penalisation, whether direct or indirect, against the Whistleblower for reasons directly or indirectly linked to the report. All staff involved, in any capacity, in the various stages of report handling are required to ensure the highest level of confidentiality regarding the content of the reports and the persons involved in the reporting process.

A further safeguard afforded to the Whistleblower by the legislation is the limitation of their liability in relation to the disclosure of certain categories of information, which could expose them to criminal, civil and administrative liability, provided that:

- at the time of disclosure or dissemination, there are reasonable grounds to believe that the information is necessary to reveal the breach being reported;
- the report is made in accordance with the conditions set out in the Decree to benefit from protection against retaliation (reasonable grounds to believe the reported facts to be true, the breach is among those that may be reported, and the procedures and conditions for making the report are complied with).

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

- disclosure and use of official secrets (Article 326 of the Italian Criminal Code);
- disclosure of professional secrecy (Article 622 of the Italian Criminal Code);
- disclosure of scientific and industrial secrets (Article 623 of the Italian Criminal Code);
- breach of the duty of fidelity and loyalty (Article 2105 of the Italian Civil Code);
- breach of provisions relating to copyright protection;
- breach of provisions relating to the protection of personal data;
- disclosure or dissemination of information regarding breaches that damage the reputation of the person concerned.

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

- is not connected to the report;
- is not strictly necessary to disclose the breach;
- constitutes the unlawful acquisition of information or access to documents.

Protection for the Whistleblower cannot be guaranteed if the report is found to be unfounded and defamatory, thereby constituting malicious conduct on the part of the Whistleblower.

6. PROTECTION AGAINST DEFAMATORY REPORTS AND PROTECTION OF THE REPORTED PARTY

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

In this context, should the report be found to be unfounded at the conclusion of the verification phase, and should the Reporter's malicious intent and/or gross negligence be established, the Company will take appropriate measures to protect itself and its employees.

The Company adopts similar measures to safeguard the privacy of the Reporting Party, including for the alleged perpetrator of the breach, subject to the applicable legal provisions.

7. SANCTIONS AND MEASURES

Should the investigations into reports, conducted in accordance with this document, reveal unlawful conduct attributable to employees, the Company will act promptly and immediately, through appropriate and proportionate disciplinary measures and sanctions, taking into account the seriousness and criminal relevance of such conduct and the initiation of criminal proceedings in cases where it constitutes a criminal offence under current national legislation.

Should the investigations reveal intentional or negligent conduct on the part of third parties who have had or currently have dealings with the Company, the Company shall act promptly by implementing all measures deemed necessary for its own protection.

8. INFORMATION FLOWS TO THE SUPERVISORY BODY

Company staff involved are required to promptly report any breaches of this protocol to the Supervisory Body (hereinafter also referred to as the "SB") atorganismodivigilanza@adrfirm.it , providing evidence and describing the incident in as much detail as possible.

The Area Managers concerned shall ensure, by coordinating the departments under their responsibility, the traceability of the process and proof of compliance with the regulations and this protocol, making all necessary documentation available to the SB in a well-organised archive.

Information must be sent to the SB primarily via email to the dedicated address mentioned above, taking care to specify in the subject line the name of the Company on whose behalf the report is being made.

Once the report has been received, the SB may request that the reporting party prepare the documentation to be presented at a specific meeting. Any interviews with managers will be aimed at providing updates or further details on information, events or significant data useful for assessing activities at risk and the related management procedures.

The above is intended to keep the Supervisory Body constantly updated and to enable it to continuously assess the adequacy of this protocol and, more generally, of the Organisation, Management and Control Model pursuant to Legislative Decree No. 231/2001 adopted by the Company, as well as any need to update or implement them.

9. PRIVACY NOTICE

Information provided pursuant to Articles 13 and 14 of EU Regulation 679/2016 (GDPR) on the processing of personal data relating to natural persons.

Through this notice, Tessilform S.p.A. (hereinafter also "the Company") provides information regarding the processing of personal data of the data subject making a report (hereinafter, "the Whistleblower") and of other data subjects mentioned or involved in the report itself, including those potentially responsible for the offences being reported (hereinafter, "the Reported Party"). 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 current legal representative, with registered office at Via Gobetti 7/9, 50013 Capalle, Campi Bisenzio (FI). Email: *privacy@patriziapepe.it*

DATA PROTECTION OFFICER (DPO)

The DPO can be contacted at the email address *dpo@patriziapepe.it*

SOURCE OF THE DATA PROCESSED

Information may be provided:

- in the report, by the Reporting Party;
- during the necessary preliminary investigations (for example, from public sources, third-party interviewees, etc.);
- during the report handling process;

- through traffic logs relating to connections to the Reporting Platform recorded on the Company's systems.

To ensure the Whistleblower's complete anonymity, it is recommended that the report be submitted from a personal device via a private, non-company network.

TYPE OF DATA PROCESSED

- Should the Whistleblower choose not to remain anonymous, personal data relating to them may be processed, specifically:
  - personal details; or contact details;
  - any special category data within the meaning of Article 9 of the GDPR, *insofar as it is capable of revealing a general state of health (absences due to illness, maternity leave, injury, etc.), fitness to perform specific duties, membership of a trade union and/or a political party, holding of elected public office, or religious beliefs;*
  - any so-called judicial data within the meaning of Article 10 of the GDPR, insofar as it relates *to criminal convictions and offences or related security measures;*
  - any personal data contained in the subject of the report.

- Following the report, personal data relating to third parties (potential perpetrators of an offence or irregularity falling within the scope of reportable matters, or individuals informed of the facts) may be processed, specifically:
  - personal details;
  - contact details;
  - any special categories of data within the meaning of Article 9 of the GDPR, *insofar as they are capable of revealing a general state of health (absences due to illness, maternity leave, accident, etc.), fitness to perform specific duties, membership of a trade union and/or a political party, holding of elected public office, or religious beliefs;*
  - any so-called judicial data within the meaning of Article 10 of the GDPR, insofar as it relates *to criminal convictions and offences or related security measures;*
  - any personal data contained in the subject of the report.

- Any personal data that may emerge from subsequent investigations;
- Traffic logs relating to connections to the reporting platform recorded on company systems *(Generally speaking, logs are files that record – and thus allow the reconstruction of – the entire 'history' of operations carried out by a user or a machine. Through logs, in fact, all operations are recorded, in chronological order, as they occur during the normal use of software, an application or, quite simply, a computer. The log also records all operations that a computer performs autonomously, without the need for human intervention. Log management at a company-wide level enables the monitoring of a range of activities, including system accesses made within a given time frame (including those outside working hours, unsuccessful attempts, or those via VPN), failed transactions, any anomalies (both software and hardware), and potential malware threats. This information is necessary to understand the state of the company's IT security: both when the system is operating normally and, above all, in the event of errors and problems, such as potential hacker attacks, thereby enabling the IT department to investigate the causes and find a resolution, preventing or promptly blocking harmful situations).*

Only personal data that is strictly necessary and relevant to the purposes set out below will be collected, in accordance with the principle of data minimisation referred to in Article 5(1)(c) of the GDPR.

PURPOSES AND LEGAL BASES OF THE PROCESSING

The Data Controller will process the aforementioned personal data:

1. In order to manage and diligently follow up on reports received, including verification activities and internal investigations relating to the conduct reported, and the initiation of proceedings, including disciplinary proceedings, within the limits required by applicable regulations. Furthermore, personal data may be processed to respond to requests from the competent administrative or judicial authority and, more generally, from public bodies in accordance with legal formalities. The data will also be processed to effectively prevent and combat fraudulent behaviour and unlawful or irregular conduct.
   Therefore, the legal basis justifying the lawfulness of the processing is the need to comply with legal obligations and to carry out tasks in the public interest to which the Data Controller is subject, as well as provisions issued by authorities authorised by law [Art. 6(1)(c) and (e); Art. 9(2)(b) and (g); Article 10 of the GDPR].
   Any disclosure of the identity of the Reporting Person to persons other than those competent to receive or follow up on reports, or otherwise authorised, shall take place with the express consent of the Reporting Person [Art. 6(1)(a) GDPR].

2. For the purpose of: i) meeting the Data Controller's internal control requirements and monitoring corporate risks, as well as optimising and improving the efficiency of internal corporate management and administrative processes; ii) establishing, exercising or defending a right or a legitimate interest of the Data Controller in any competent forum to ensure the exercise of the right of defence pursuant to Article 24 of the Constitution; iii) managing IT security and safeguarding assets and data security, providing user support and maintaining security and perimeter protection systems for traffic logs relating to connections to the *whistleblowing* platform recorded on the company's systems.
   Therefore, the legal basis justifying the lawfulness of the processing is the need to pursue a legitimate interest of the Data Controller [Article 6(1)(f) of the GDPR].

METHODS OF PROCESSING

The information identified above is processed by the Internal Channel Manager, a person specifically appointed as an authorised representative and adequately trained for this purpose. Data is collected electronically via the dedicated reporting platform, in accordance with the Whistleblowing Policy, so as to ensure the anonymity of whistleblowers and any other individuals involved, as well as the confidentiality of the information contained within the reports. The platform used to receive reports is hosted on the company's servers.

RECIPIENTS AND SCOPE OF DATA DISCLOSURE

Other parties whose involvement is necessary to carry out the necessary investigations, aimed at verifying the validity of the matter reported, as well as the adoption of any measures, may become aware of the personal data collected.
In particular, depending on their roles and job responsibilities, the processing of personal data will be carried out by individuals specifically trained and authorised to perform processing operations, such as, for example, external consultants, managers of the department in which the reported individual works, the System Administrator, and the Supervisory Body (OdV). Please note that the information and data collected may be forwarded to the competent authorities.

Any disclosure of the identity of the Reporting Person to persons other than those competent to receive or follow up on reports, or otherwise authorised, shall take place with the express consent of the Reporting Person.

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

MANDATORY NATURE OF DATA PROVISION AND CONSEQUENCES OF ANY REFUSAL

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 staff to use such data for the purposes already stated. Failure to provide the data necessary to follow up on the report will prevent the activities from being carried out.

TRANSFER OF DATA ABROAD

The Data Controller does not transfer personal data to third countries. Should a transfer of data outside the EU become necessary, the Company will verify that the recipients provide adequate safeguards, as required by Articles 44 et seq. of the GDPR.

DATA RETENTION PERIODS

The personal data collected will be retained for the time strictly necessary to fulfil the purposes already indicated in the preceding paragraphs and, in any event, for no longer than five years from the date of notification of the final outcome of the report, unless further retention is necessary by virtue of legal obligations (for example, in the event of ongoing legal or disciplinary proceedings, until the conclusion thereof). Upon expiry of this period, the Data Controller will delete the personal data.

RIGHTS OF THE DATA SUBJECT

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

These rights may be exercised by contacting the Data Controller by sending a request to the email address *privacy@patriziapepe.it*

For any enquiries regarding this privacy policy, or in the event of any breaches of data protection legislation, please contact the DPO at *dpo@patriziapepe.it*

In this specific case, however, in accordance with the provisions of Articles 2-undecies and 2-duodecies of Legislative Decree 196/2003 "Italian Privacy Code", the Data Controller reserves the right to restrict or delay the exercise of such rights, within the limits established by the applicable legal provisions, in particular where there is a risk that actual, concrete and otherwise unjustified harm may be caused to the confidentiality of the Whistleblower's identity and that the ability to effectively verify the validity of the report or to gather necessary evidence may be compromised.

In particular, the exercise of such rights:

- shall be possible in accordance with the laws or regulations governing the sector (including Legislative Decree 231/2001 and subsequent amendments and additions);
- may be delayed, restricted or excluded, provided that the data subject is notified without delay and with a statement of reasons, unless such notification would undermine the purpose of the restriction, for as long and to the extent that this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the data subject, in order to safeguard the confidentiality of the Whistleblower's identity.

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