WHISTLEBLOWING SYSTEM OF TENACTA GROUP
S.P.A unipersonale

POLICY ON THE PROCESSING OF PERSONAL DATA PURSUANT TO ARTICLES 13 AND 14 OF THE EUROPEAN DATA PROTECTION REGULATION (GDPR)

Dear User,

*At TENACTA GROUP S.p.A. unipersonale (the "***Company***"), we wish to be promptly informed of any suspected breaches or concerns of breaches of laws, regulations, or internal policies and procedures. Reports can be made through various channels, including the digital platform eWhistle ("***Platform***") and the recorded telephone line/recorded voicemail system accessible via landline or mobile phone ("***Telephone Line***").*

Regardless of the channel used, the receipt and analysis of a report, as well as any subsequent investigations conducted, shall involve the processing of personal data by the Company.

The Company takes the protection of your personal data seriously and invites you to read the following policy – drawn up in accordance with Italian Legislative Decree 196/2003, as amended, and EU Regulation 2016/679 on personal data protection – to help you understand how we process and manage your personal data and the information contained in your report, and to inform you about your rights in this regard.

For any questions or concerns regarding this policy, please contact the Company at the following email address: info@tenactagroup.com.

1. GENERAL INFORMATION AND PURPOSES OF PROCESSING

The Company has set up a platform and a telephone line to enable any individual, including employees, self-employed workers, collaborators, including volunteers and interns, workers or staff of suppliers, freelancers and consultants, administrators, members of supervisory bodies, and shareholders of the Company, to report suspected breaches or concerns of breaches of laws, regulations, or internal policies and procedures. For the purposes of this Policy, "User" refers to the person submitting a report via the platform or telephone line.

Specifically, reports may concern behaviours that constitute actions or omissions, whether committed or attempted:

- Penal, civil, or administrative infringements, or accounting breaches;
- Involving legal representatives, administrators, executives, and/or employees of the Company [or subsidiaries, companies that are not subsidiaries in which the

Company holds significant equity interests], joint ventures, or – in any case – anyone acting on behalf of the Company (e.g., consultants, suppliers, etc.);

- Carried out in violation of the 231 Model or other company Policies or procedures;
- Likely to cause financial or reputational damage to the Company;
- Potentially constituting conflicts of interest;
- Likely to cause harm to employee health or safety, or environmental damage;
- Likely to constitute a breach of regulations, including, but not limited to, the following areas:
  - Public contracts;
  - Services, products, and financial markets, and prevention of money laundering and terrorist financing;
  - Product safety and compliance;
  - Transportation safety;
  - Environmental protection;
  - Public health;
  - Consumer protection;
  - In general, national or European legislation.

Personal data collected during the receipt, processing, and investigation of a report ("**Personal Data**") are processed by the Company to ensure its proper management. The Company shall process your Personal Data only for the following purposes:

- Managing the lifecycle of the report, conducting investigations with parties concerned, including public authorities;
- Enabling management of the platform and related reports;
- Determining whether an offense has occurred;
- Determining relevant sanctions and possible mitigation measures to prevent future offenses;
- Verifying and ensuring the correct and complete application of corporate policies, and carrying out subsequent and consequential activities to such checks, as well as fulfilling specific legal obligations, regulations, and applicable legislation with reference to specific needs connected to the Company's internal control and company risk monitoring, specifically required by law;
- Calculating statistics and reporting.

2. PERSONAL DATA AND CATEGORIES OF DATA PROCESSED

Personal Data refers to all information relating to an identified or identifiable natural person (the "data subject").

The provision of the User's Personal Data is **optional**. The option for anonymous reporting available on the platform and accessing the telephone line allows making a report without providing any User Personal Data.

In cases where the User voluntarily decides to provide their Personal Data, the following categories of data may be processed as part of report management by the Data Controller:

i. User's identifying data: name, surname, and contact information (unless the report is anonymous);

ii. Personal Data of the reported person or other mentioned parties, or data obtained by the Data Controller during investigations: name, surname, and Personal Data (e.g., description of roles and contact information); and

iii. Information related to the reported violation: description of the alleged breach, as well as a description of the circumstances of the case, or other information obtained during the investigation of the reported facts, records/summaries of the investigation, actions taken following the investigation.

Depending on the laws in force in the country where the whistleblower resides, anonymous reporting may not be permitted; in such cases, Personal Data will still be processed confidentially and will only be communicated according to the rules outlined below.

Please keep in mind that the information contained in some reports may include **special categories of Personal Data**. According to Article 9 of the GDPR, "special categories" of data are those that may reveal racial or ethnic origin, religious or philosophical beliefs, political opinions, membership in parties or trade unions, data concerning health and sexual orientation, or criminal proceedings.

The GDPR imposes greater restrictions on such data, which shall only be processed if and when relevant to the purpose of the report and only to the extent permitted by applicable law and/or necessary to establish, exercise or defend a legal claim in a pending court proceeding pursuant to Article 9(2)(f) of the GDPR. If, instead, such data are not relevant for the purpose of the report and are outside the scope allowed by applicable law and/or are not necessary to establish, exercise or defend a legal claim in a pending court proceeding, the data shall be promptly and securely erased and not further processed.

3. PROCESSING OF PERSONAL DATA

"Processing of Personal Data," as defined under Article 4(2) of the GDPR, refers to any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, and dissemination.

The Personal Data provided shall be processed by the Company in accordance with applicable law, respecting the principle of data minimisation and through methods suitable to ensure their security and confidentiality. Specifically, the processing of such data shall be carried out:

- ✓ through digital or audio support, depending on the channel used for making the report;
- ✓ in a manner that ensures the highest standards of confidentiality and to prevent or minimise the risks of destruction or loss, including accidental, of data, of unauthorised access, or of processing not allowed or not in accordance with the purposes of collection.

In compliance with the GDPR, the Personal Data obtained may be used to update and correct information previously collected.

To ensure the confidentiality of the whistleblower throughout the management of the internal report, their identity will be known only to those expressly authorised to process the reports. The identity of the Whistleblower is protected in every context following the

report and cannot be disclosed without their express consent, and all those who receive or are involved in managing the report are required to protect the confidentiality of such information.

4. DATA CONTROLLER

The Data Controller is TENACTA GROUP S.P.A. unipersonale, with its registered office at Via Piemonte 5/11, 24052 Azzano S. Paolo (BG), in the person of its pro-tempore legal representative ("**Data Controller**").

5. LEGAL BASIS FOR PROCESSING

Legal obligation: Your Personal Data shall be processed for **mandatory** purposes related to compliance with applicable laws and regulations and to satisfy any requests received from competent authorities.

Legitimate interest: We shall also retain your Personal Data based on the legitimate interest of the Company in properly managing the received reports, in line with the relevant *Policy* for managing reports, to prevent and investigate the alleged breaches listed in the previous paragraph I, and to defend our rights in (or initiate) a legal proceeding as a consequence.

The User's Personal Data and the persons mentioned in the report may be processed without their consent, in cases where this is necessary to pursue the legitimate interest of the Data Controller in receiving and processing reports of actual or suspected breaches of laws or regulations applicable to the Companies, as well as internal policies and procedures.

The processing of data shall in any case be carried out according to applicable principles in terms of purpose, relevance, adequacy, and limitation.

6. COMMUNICATION OF PERSONAL DATA

For the purposes described in the previous paragraph 1, the Personal Data provided may be transmitted in the following areas:

A. Within the Company - The data may be used by Company personnel tasked with processing, who have been assigned a specific role as data processor and commit to maintaining confidentiality and have been given appropriate instructions.

Your Personal Data shall be made accessible only to those within the Company who need the data due to their duties or hierarchical position. Such individuals shall be appropriately instructed to avoid loss, destruction, unauthorised access, or unauthorised processing of the data.

Furthermore, the data may be used by third-party companies or individuals performing instrumental activities on behalf of the Company, such as:

i. Service providers: the external company that provides the Company with the necessary services for managing reports and the providers of the platform and telephone line, who shall access the data only for system maintenance purposes or technical support for the User; such providers are duly appointed as Data Processors in accordance with the provisions of the GDPR;

ii. External consultants for managing the investigative process and legal assistance, companies, and firms operating in the context of assistance and consultancy relationships.

These companies operate as Data Processors and under the direction and monitoring of the Company.

In any case, your report will be processed only by internal staff or external autonomous, dedicated personnel that has been specifically appointed and trained also in terms of constraints imposed by legislation on the protection of Personal Data, based on the *need-to-know* principle expressed by the GDPR.

The protection of your Personal Data and the legitimacy of the processing are ensured by appropriate appointment as Data Processors of all third parties who perform processing on behalf of the Company. All our Data Processors are therefore required to comply with current privacy laws and to implement adequate security measures.

B. Outside the Company (public entities or supervisory bodies) - Furthermore, always for purposes strictly instrumental to assessing the reports and in implementation of legal or contractual provisions, in some circumstances, the Company may need to transmit, directly or indirectly, some of the Personal Data contained in the report - according to a stringent criterion of relevance - to the following categories of subjects:

i. Public security authorities;

ii. Judicial authorities.

These subjects shall act as independent Data Controllers (of their respective processing), unless they act on behalf of the Company as Data Processors and have therefore signed a specific contract regulating the processing entrusted to them, pursuant to Article 28 of the GDPR.

Please note that the identity of the User, acting as a whistleblower, shall only be disclosed if required by legal or regulatory obligation, previously mentioned request for exhibition, or to ensure the right of defense of the reported individual, in case the whistleblower has expressed their consent.

The Company shall implement in any case appropriate security measures to safeguard your Personal Data from unauthorised access, disclosure, or accidental erasure:

- We shall apply reasonable measures to ensure that Personal Data are collected in accordance with the principles of minimisation and limitation of purposes;
- We shall store your Personal Data for a limited time as specified in paragraph 8 below, unless the extension of the retention period is required or permitted by law;
- We shall use advanced technologies to ensure the confidentiality of Personal Data, ranging from encryption, the use of complex *passwords* and two-factor authentication, to *firewalls* and dedicated *software* to protect *servers* from external attacks;
- We shall select our business partners and service providers based on rigorous qualification criteria and the obligation to respect our security standards guaranteed by specific contractual provisions and perform *audits* and other assessments to verify their compliance with the above requirements;
- We shall conduct specific training sessions on *privacy* and data protection and tests to verify the learning of the personnel and other activities to increase awareness of privacy issues among employees and collaborators.

7. INTERNATIONAL TRANSFERS OF DATA

Your Personal Data is stored on the servers of the providers of the platform and the telephone line (specifically appointed as Data Processors) located in Italy or within the European Union. Depending on the specific characteristics and content of your report, your Personal Data may be transferred to other countries, including those outside the European Union. The Company has assessed the impact of international transfers that may fall within the scope of the reports and has implemented appropriate safeguards.

Should it be necessary to transfer – for needs related to the management of reports - your Personal Data to countries outside the European Union, which do not guarantee an adequate level of protection of Personal Data as per the GDPR, the Company shall transfer your data only to countries for which the European Commission has declared an adequate level of security, or alternatively, will adopt contractual measures to ensure that all recipients provide an adequate level of data protection (e.g., through the implementation of *Standard Contractual Clauses* approved by the European Commission).

8. STORAGE OF PERSONAL DATA

Your Personal Data shall be processed and stored by the Data Controller, for the time strictly necessary for the management of reports, consistently with the needs that may arise during the management of your report (e.g., legal action, proceedings at public authorities) or to meet legal obligations. The data shall be deleted from the platform and the telephone line after 5 years from the closure of the investigation, unless the Data Controller is required to retain them for a further period to comply with legal obligations or to ensure the possibility of legal defense. In any case, your data shall not be subject to further processing.

Your Personal Data shall be processed according to the terms above or for a shorter period should you decide to exercise one of the rights listed in the subsequent paragraph 9. Please note that if you request the erasure of your Personal Data, we may not be able to respond to your report or conclude the investigation.

If the checks carried out in relation to the report do not show any evidence of breach (groundless report) or if the report does not fall within the scope of reportable conduct (irrelevant reports), the related Personal Data shall be immediately erased.

Upon expiration of the term, your Personal Data shall be erased or made anonymous according to our internal procedures, unless otherwise required by legal obligations or if your Personal Data is necessary to protect our rights before any judicial authority or other competent authority.

We also inform you that, under Articles 5 and 89.1 of the GDPR, your Personal Data may be stored in an anonymous form for longer periods than specified in the previous paragraph for statistical purposes only, subject to the implementation of appropriate technical and organisational measures necessary to protect your rights and freedoms.

9. RIGHTS OF THE DATA SUBJECT

Under Articles 15-22 of the GDPR, as a data subject, you have the right to exercise the following rights:

1. **Right of access**: the right to obtain confirmation from the Data Controller as to whether or not Personal Data concerning you is being processed and, if so, to gain access to the Personal Data and additional information on the origin, purpose, category of data processed, recipients of communication and/or data transfer, data retention period or criteria to determine it, and the data subject's rights.
2. **Right to rectification**: the right to obtain from the Data Controller:
    a. the rectification of inaccurate Personal Data without undue delay;
    b. the completion of incomplete personal data, even by providing a supplementary statement containing the information you request to be included.
3. **Right to erasure**: the right to obtain the erasure of Personal Data concerning you without undue delay from the Data Controller in cases where:
    a. the Personal Data is no longer necessary in relation to the purposes for which it was processed;
    b. the consent on which the processing is based is withdrawn and there is no other legal ground for processing;
    c. the Personal Data has been unlawfully processed;
    d. the Personal Data must be erased for compliance with a legal obligation in Union or Member State law to which the Data Controller is subject.
4. **Right to object to processing:** the right to object at any time, on grounds relating to your particular situation, to processing of personal data concerning you which is based on Article 6(1)(e) or (f) of the GDPR, including profiling based on those provisions.
5. **Right to restriction of processing**: the right to obtain restriction of processing from the Data Controller in cases where the accuracy of the Personal Data is contested (for the period necessary for the Data Controller to verify the accuracy of the personal data), if the processing is unlawful and/or the data subject has objected to processing.
6. **Right to data portability**: the right to receive the personal data concerning you in a structured, commonly used and machine-readable format and to transmit those data to another Data Controller, only for cases where the processing is based on consent and for data processed by electronic means.
7. **Right to lodge a complaint with a supervisory authority**: without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority in the Member State of your habitual residence or place of work, or of the place where the alleged infringement occurred, if you consider that the processing of your data violates the GDPR.

10. EXERCISING DATA SUBJECTS' RIGHTS

To exercise the rights described in paragraph 5), you may contact the Data Protection Officer (DPO) at the email address: dpo@tenactagroup.com.

The response period is one (1) month, extendable by two (2) months in cases of particular complexity; in these cases, the Company shall provide at least an interim communication within one (1) month of receipt of the request.

11. INFORMATION ON AUTOMATED DECISION-MAKING AND UPDATES

Your Personal Data is not subject to automated decision-making (including profiling). This information may be updated from time to time. Any update to this information shall become effective at the time of its publication on the platform.

12. DATA CONTROLLER AND DATA PROTECTION OFFICER

The Data Controller is the Company, with registered office at Via Piemonte 5/11, 24052, Azzano San Paolo (Bergamo), VAT and Taxpayer's ID No.: 02734150168. 02734150168.

The Data Protection Officer (DPO) can be contacted by regular mail at the following address: Via Piemonte 5/11, 24052, Azzano San Paolo (BG) or at the following email address: dpo@tenactagroup.com.

Date of Publication	Data Controller
14/12/2023	Tenacta Group S.p.A. Unipersonale