Personal Data Processing Notice Relating to the Whistleblowing Procedure Pursuant to Article 13 of Regulation (EU) 2016/679 ("GDPR")

This notice is issued by **DELTA PREG S.p.A. - Località Tei 10, 55011 Altopascio (Lucca), Italy - VAT No. 01723910467**, acting as *Data Controller*, to describe the methods of processing personal data contained in reports of unlawful conduct pursuant to Legislative Decree No. 24/2023 (the "Whistleblowing Decree"), implementing Directive (EU) 2019/1937.

1. PARTIES INVOLVED IN DATA PROCESSING

The *Data Controller of the personal data* you provide is identified as the current legal representative.

The Data Controller has appointed *Authorized Persons* to process data for the fulfilment of legal obligations and has appointed *external Data Processors* to whom certain activities have been outsourced.

2. CATEGORIES OF DATA PROCESSED

For the management of the whistleblowing procedure, the *Data Controller* processes:

- ***Common Personal Data*** (for example: first name, last name, address, email address and other identifying information or contact details):
  - of the **reporting person (whistleblower)**, only in the case of non-anonymous reports;
  - of the **reported persons allegedly responsible for the violations**, in all cases;
  - of **third parties mentioned by the reporting person for any reason** (witnesses, so-called facilitators, etc.), where applicable.
- ***Special Categories of Personal Data*** pursuant to Article 9 GDPR relating to health, political opinions, trade union membership, or judicial data (e.g., criminal convictions), where included in the report, inferred from it, or necessary for its management.

Any data communicated that are not useful for handling a specific report will not be processed or, if collected inadvertently, will be promptly deleted.

3. PURPOSES OF PROCESSING AND LEGAL BASIS

Your personal data are processed exclusively for:

a) managing the report;

b) complying with obligations arising from Legislative Decree No. 24/2023, Legislative Decree No. 231/2001, or other national and European regulations;

c) establishing, exercising, or defending legal claims in civil, administrative, or criminal proceedings.

The legal basis for processing is:

- for the purposes under points a) and b), compliance with a legal obligation to which the Data Controller is subject (Article 6(1)(c) GDPR);
- where the report is made orally, the legal basis is the data subject's consent pursuant to Article 6(1)(a) GDPR and Article 12 of Legislative Decree No. 24/2023;
- for the purpose under point c), the legitimate interest of the Data Controller pursuant to Article 6(1)(f) GDPR.

Where, for procedural reasons or to comply with additional legal obligations, it is necessary to disclose the identity of the reporting person to third parties other than those authorized to receive and manage the report, the reporting person will be asked to provide specific and explicit consent, provided that the report is not anonymous.

In such cases, the legal basis for processing shall be consent pursuant to Article 6(1)(a) GDPR and Article 12 of Legislative Decree No. 24/2023.

4. NATURE OF DATA PROVISION AND CONSEQUENCES OF REFUSAL

Providing personal data for the purposes described in Section 3 is optional, as reports may also be submitted anonymously.

However, refusal to provide such data, in whole or in part, may make it impossible for the Company to follow up on the report.

5. PROCESSING OPERATIONS AND METHODS

The processing of your Personal Data is carried out through some of the operations referred to in Article 4(2) of the GDPR, namely: collection, recording, organisation, storage, use, disclosure by transmission, restriction, erasure and destruction of Data.

Such Data may be collected through a digital platform or directly by the Data Controller in written or oral form (for example, in the event of a meeting requested by the reporting person with the member(s) of the REPORT MANAGEMENT BODY (Supervisory Body, ad hoc appointed internal committee, or professional specifically authorised to perform this role)) and shall be processed in compliance with the aforementioned legislation.

The *Data Processing* shall be carried out by automated and/or manual means, implementing all technical and organisational measures appropriate to ensure a level of security commensurate with the risk, as required by Article 32 of the GDPR. Processing shall be performed by the persons identified in the following section, namely internal personnel of the Company acting as Authorised Persons, and external parties acting as Data Processors, in accordance with Article 29 of the GDPR.

Data collected through the whistleblowing platform are processed using encryption techniques.

The system provider has adopted technical and organisational measures consistent with the requirements of the GDPR, including through the performance of preliminary risk assessments concerning the processing activities carried out.

The IT platform used for managing reports has been designed and developed in accordance with the principles of “privacy by design” and “privacy by default”, ensuring the protection of personal data from the earliest stages of system development.

Given the specific nature of whistleblowing-related processing activities, the Company adopts enhanced technical and organisational security measures aimed at ensuring:

• the confidentiality of the identity of the reporting person and the individuals involved;

• the protection of data against unauthorised access;

• the traceability of access and operations performed;

• the use of encryption systems and security protocols for the transmission and storage of data.

Such measures are subject to periodic review and updating, also in light of regulatory developments and identified risks.

6. RECIPIENTS OF YOUR PERSONAL DATA

The Company has established a governance model for the internal reporting channel in compliance with Legislative Decree No. 24/2023 and the ANAC Guidelines, identifying individuals expressly authorised to receive, analyse and manage reports, who possess appropriate levels of autonomy, independence and expertise. These individuals operate on the basis of documented instructions and in compliance with specific confidentiality obligations, ensuring a functional separation between those who receive the report and any functions involved in investigative activities.

Your Personal Data may be made accessible, for the purposes referred to in Section 3, to:

- the member(s) of the REPORT MANAGEMENT BODY (Supervisory Body, ad hoc appointed internal committee, or professional specifically authorised to perform this role), acting as authorised persons for data processing;
- the third-party company providing the reporting reception service through an online platform. In such case, the processing shall be carried out on the basis of specific written instructions issued by the Data Controller, aimed at ensuring compliance with data protection legislation, under the Data Controller's general and periodic supervision of the security measures adopted by the third party;
- any external professionals (e.g. lawyers, investigation agencies, internal audit experts, forensic investigation specialists, etc.) who may be appointed to carry out investigations or verifications regarding the reported facts on behalf of the Data Controller. Such parties shall act as Data Processors pursuant to Article 28 of the GDPR.

The list of Data Processors is contained in the Company's Process Management and Data Protection Register, which is kept at the Company's registered office and may be consulted upon express request submitted through the contact details indicated in the Contact Information section

7. DISCLOSURE TO THIRD PARTIES

Without the need for specific consent (Article 6 GDPR), and in compliance with legal obligations, the Data Controller may disclose your Personal Data, for the purposes referred to in Section 3, to the National Anti-Corruption Authority (ANAC), law enforcement authorities and judicial authorities.

Your Personal Data may also be disclosed to the ordinary judicial authorities where the Data Controller intends to take legal action against the reporting person for slander (calunnia) or defamation.

In all other cases, as specified above, specific consent will be requested where required.

Your Personal Data will not be disclosed to the public.

8. DATA TRANSFERS

Your personal data are not subject to international transfer.

9. DATA RETENTION METHODS AND PERIOD

All Personal Data provided will be processed in compliance with the principles of lawfulness, fairness, relevance and proportionality set out in the GDPR, Legislative Decree No. 24/2023, the ANAC Guidelines on whistleblowing, and Legislative Decree No. 231/2001, where applicable. Such processing will be carried out using electronic and/or telematic means strictly necessary to achieve the purposes described above and always with a view to ensuring the confidentiality of the identity of both the reported person and the reporting person.

The whistleblowing management system guarantees, at every stage of the process, the confidentiality of the identity of the reporting person, the persons involved and/or otherwise mentioned in the report, the content of the report, and the related documentation, without prejudice to the provisions of Article 12 of Legislative Decree No. 24/2023.

Personal data processed in paper format are stored in an identified location, access to which is restricted to the member(s) of the REPORT MANAGEMENT BODY (Supervisory Body, ad hoc appointed internal committee, or professional specifically authorised to perform this role).

Personal data processed in electronic format are stored on the dedicated platform or in a directory protected by authentication credentials known only to the member(s) of the REPORT MANAGEMENT BODY (Supervisory Body, ad hoc appointed internal committee, or professional specifically authorised to perform this role) and/or to persons expressly authorised by such body.

*

Pursuant to Article 14 of Legislative Decree No. 24/2023, Personal Data shall be retained for the time necessary to process the report and, in any event, for no longer than five years from the date of communication of the final outcome of the procedure.

10. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Considering the nature of the processing and the potentially high risks to the rights and freedoms of data subjects, the Company has carried out a **Data Protection Impact Assessment (DPIA)** pursuant to Article 35 GDPR.

The DPIA assessed the processing activities related to the whistleblowing channel and identified suitable technical and organizational measures to mitigate risks, particularly regarding confidentiality, data security, and lawful processing.

The DPIA is periodically reviewed and updated according to developments in processing activities, technologies, and applicable regulations.

11. DATA STORAGE LOCATION

Data collected by the Data Controller are stored within the IT infrastructure of the reporting platform managed by the appointed Data Processor.

12. DATA SUBJECT RIGHTS

As a data subject, you have the rights provided under Articles 15 et seq. GDPR, including the right to:

a) obtain confirmation as to whether personal data concerning you are being processed and access such data;

b) obtain rectification of inaccurate personal data;

c) obtain erasure of personal data where grounds exist;

d) obtain restriction of processing under the conditions provided by law;

e) receive your personal data in a structured, commonly used, machine-readable format;

f) object at any time, on grounds relating to your particular situation, to processing based on Article 6(1)(e) or (f) GDPR;

g) not be subject to decisions based solely on automated processing, including profiling, producing legal effects concerning you or similarly significantly affecting you;

h) lodge a complaint with a supervisory authority.

Note: The above rights cannot be exercised by the reported person or any person mentioned in the report, for the period and to the extent that such restriction constitutes a necessary and proportionate measure pursuant to Article 2-undecies of the Italian Privacy Code, where exercising those rights could cause actual and concrete prejudice to the protection of the reporting person's identity.

13. CONTACT DETAILS

You may contact the Company or exercise the rights referred to above by writing to the Data Controller: **DELTA PREG S.p.A., Località Tei 10, 55011 Altopascio (Lucca),** Italy or by email at: privacy.dltp.mb@delta.toray