PRIVACY NOTICE ON THE PROCESSING OF PERSONAL DATA – WHISTLEBLOWING PURSUANT TO REGULATION (EU) 2016/679 (GDPR) AND APPLICABLE NATIONAL LAWS (Legislative Decree No. 196/2003, as amended by Legislative Decree No. 101/2018)

Dear Sir/Madam,
Ecopneus S.c.p.a., in its capacity as Data Controller, hereby provides you with the information set out below pursuant to and for the purposes of Article 13 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (hereinafter also referred to as the "Regulation" or the "GDPR").

1 DATA CONTROLLER AND DATA PROTECTION OFFICER

The **Data Controller** is ECOPNEUS S.C.P.A., VAT No. 06516590962, with registered office at Via Messina 38, Torre B, 20154 Milan (hereinafter the "Controller"), which may be contacted for these purposes at the following email address: privacy@ecopneus.it.
The Company has also appointed a Data Protection Officer (DPO), Avv. Diego Perini, who may be contacted at the following email address: diego@studiolegalediegoperini.it.

2 CATEGORIES OF DATA PROCESSED

- Data concerning the reporting person: ordinary personal data within the meaning of Article 4(1) GDPR concerning the reporting person (where reports are not anonymous), as well as any persons involved in or mentioned in the report and facilitators, as defined in the Whistleblowing Procedure (hereinafter the "Data Subjects"), including: personal details (e.g. first name, surname, date and place of birth), contact details (e.g. landline and/or mobile telephone number, postal/email address), and company position, role or title. Special categories of personal data within the meaning of Article 9 GDPR, if included in the report, which the Controller will process pursuant to Article 9(2)(g) GDPR.
- Data concerning the reported person: the data that the reporting person has chosen to provide in order to describe the facts set out in the report. In this case, the Controller cannot determine in advance the data that may be included in the report, which may therefore also include criminal-offence data within the meaning of Article 10 GDPR (e.g. criminal convictions, offences, etc.).

3 PURPOSES OF THE PROCESSING

The above personal data are processed by the Controller for the following purposes: managing reports submitted pursuant to Legislative Decree No. 24/2023; complying with obligations imposed by law or EU legislation; defending or establishing the Controller's rights in civil, administrative or criminal proceedings; and internal control and monitoring of corporate risks.

4 LEGAL BASIS FOR THE PROCESSING

The legal basis for the processing is: for the purposes referred to in points (a) and (b), compliance with a legal obligation to which the Controller is subject (Article 6(1)(c) GDPR); for the purposes referred to in points (c) and (d), the Controller's legitimate interests (Article 6(1)(f) GDPR).

5 METHODS OF PROCESSING

The data are processed manually and/or by means of automated IT and electronic tools, using procedures related to the purposes set out above and, in any event, in a manner that ensures their security and confidentiality. At every stage, the report management system safeguards the confidentiality of the identity of the reporting person, the persons involved in and/or otherwise mentioned in the report, the content of the report and the related documentation, without prejudice to Article 12 of Legislative Decree No. 24/2023.

6 RECIPIENTS OF THE DATA

In pursuit of the above purposes, the personal data provided are made accessible only to those within the Company who are responsible for receiving reports or for taking follow-up action, including the analysis, investigation and management of reports and any resulting action (such as the Supervisory Body). These persons are appointed as persons authorised to process personal data pursuant to Article 29 GDPR and are duly trained and instructed to prevent the loss of data, access by unauthorised persons or unauthorised processing, and, more generally, to ensure compliance with personal data protection obligations. Certain processing activities may also be carried out by third parties to whom the Controller entrusts certain activities, or parts thereof, for the purposes referred to in section 2. Such third parties will act either as independent controllers or as processors pursuant to Article 28 GDPR (subject to the execution of an appropriate legal instrument) and will essentially include the following categories: consultants (organisation, litigation, law firms, etc.); companies responsible for personnel administration and management; audit firms; investigation agencies; providers of the whistleblowing IT platform; public institutions and/or authorities; judicial authorities; and law enforcement agencies.



7 DISCLOSURE AND PROFILING

The personal data processed by the Controller are not disclosed and are not subject to any solely automated decision-making process, including profiling.

8 TRANSFER OF DATA TO A THIRD COUNTRY AND/OR AN INTERNATIONAL ORGANISATION

The personal data are not transferred to third countries and/or international organisations. It is understood that, should the need arise, the Controller may relocate the servers within the European Union and/or to countries outside the EU. In such cases, the Controller hereby assures that any transfer of data outside the EU will take place in accordance with Articles 44 et seq. of the Regulation and the applicable legal provisions, and that, where necessary, agreements ensuring an adequate level of protection will be entered into. In particular, the Controller will ensure that appropriate technical and organisational measures are in place so that the processing complies with the requirements of the Privacy Code and the GDPR, that the rights of third-party Data Subjects are protected, that data transfers can be tracked, and that appropriate security measures can be documented.



9 DATA RETENTION

The Controller retains personal data for the period provided for in Article 14 of Legislative Decree No. 24/2023, namely for as long as necessary to process the report and, in any event, for no longer than five years from the date on which the final outcome of the report is communicated to the Supervisory Body. Personal data that are manifestly not useful for processing a specific report are not collected or, if collected accidentally, are promptly deleted.



10 CONSEQUENCES OF FAILURE TO PROVIDE PERSONAL DATA

The reporting person is not required to provide personal data and may remain anonymous. However, the reporting person's identity may also be inferred from contextual information or elements of the report, in which case the report cannot technically be regarded as anonymous. In such circumstances, the reporting person's wish to remain anonymous will nevertheless prevail and the confidentiality of their identity will be safeguarded. In any event, personal data contained in the report will be processed only where relevant and necessary for the analysis of the reported event.

11 DATA SUBJECT RIGHTS

The Data Subject, where they are the reporting person or a facilitator, is entitled at any time to access the data concerning them and to exercise the rights provided for in Articles 15 to 22 GDPR, where applicable (including the right of access to personal data, the right to rectify them, the right to obtain their erasure or the so-called "right to be forgotten", the right to restriction of processing, the right to data portability and the right to object to processing), by sending an email or letter to the Controller and/or the DPO at the addresses set out in section 1. The above rights may not be exercised by the person involved in or mentioned in the report for such time and to the extent that this constitutes a necessary and proportionate measure, pursuant to Article 2-undecies of the Privacy Code (Legislative Decree No. 196/2003, as amended by



Legislative Decree No. 101/2018) and Article 23 GDPR, since exercising those rights could cause actual and specific prejudice to the protection of the confidentiality of the reporting person's identity.

The Data Subject is also entitled to lodge a complaint with the supervisory authority if they consider that their rights have been infringed. In Italy, the supervisory authority is the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) (www.garanteprivacy.it).

