INFORMATION ON THE PROCESSING OF PERSONAL DATA, PURSUANT TO ART. 13 AND 14 OF REGULATION (EU) 2016/679 ("GDPR") CONCERNING THE SYSTEM ADOPTED BY THE COMPANY TO COLLECT REPORTS OF UNLAWFUL CONDUCT OR VIOLATIONS OF THE ORGANIZATION, MANAGEMENT AND CONTROL MODEL PURSUANT TO LEGISLATIVE DECREE 231/2001

	DATA CONTROLLER	**Lamberti S.p.A.** Via Piave, 18 - 21041 - Albizzate (VA) VAT number 01425250121 privacy@lamberti.com ("**Company**" or "**Data Controller**")
	DATA PROTECTION OFFICER (DPO)	The **DPO** can be contacted at the e-mail address: dpo@lamberti.com

TYPE OF DATA PROCESSED AND SOURCE OF DATA

Lamberti allows the submission of detailed reports of unlawful conducts with regards to:

- violations of national and European provisions consisting of offences concerning – by way of example but not limited to – the following sectors:
  - procurement;
  - financial services, products and markets and the prevention of money laundering and terrorist financing;
  - product safety and compliance;
  - transport safety;
  - environmental protection;
  - radiation protection and nuclear safety;
  - food and feed safety and animal health and welfare;
  - public health;
  - consumer protection;
  - protection of private life and protection of personal data and security of network and information systems.
- violations of European provisions consisting of:
  - acts and omissions affecting the financial interests of the Union;
  - acts and omissions concerning the internal market;
  - acts and conduct which undermine the object or purpose of the provisions of EU acts in the areas referred to above;
- violations of national provisions consisting of:
  - administrative, accounting, civil or criminal offences;
  - relevant unlawful conduct pursuant to Legislative Decree no. 231/2001;
- violations of the Company's internal provisions, such as:
  - Organisation, Management and Control Model adopted pursuant to Legislative Decree 231/2001, as well as the related procedures;
  - Code of Ethics;
  - National collective agreements and, more generally, internal regulations (procedures, policies, operating instructions, etc.);

digitally through its "*whistleblowing platform*".

Reports can be **nominative or anonymous**:

- in the case of anonymous reports, the company's IT systems **will not be able to identify the whistleblower** from the access point to the portal (IP address);
- in the case of nominative reports, at the choice of the whistleblower, the personal data of the latter will be associated with the report. Within the form, made available on the "*whistleblowing platform*", the whistleblower may indicate his/her personal data, in the case of nominative reports (and, specifically, personal data and contact details), as well as personal data of the reported person and/or any third parties (hereinafter the "**Data**").

	The "*whistleblowing platform*" also provides the whistleblower with the possibility, on a completely optional basis, to make reports by voice recording, in which case the Data collected will also include the voice of the whistleblower. The Data of the whistleblower, if provided, are submitted directly by the whistleblower (and therefore acquired by the Data Controller from the data subject pursuant to Article 13 of the GDPR); the Data of the person concerned and/or third parties are provided by the whistleblower (and therefore acquired by the Data Controller from third parties pursuant to Article 14 of the GDPR). In addition, in the context of this activity, special categories of personal data (e.g. health data) and criminal offence data (in particular, data relating to alleged crimes) may also be processed if they are directly provided by the whistleblower; as a matter of fact, the provision of these categories of data is not mandatory in order to send the report.

PURPOSE OF THE PROCESSING	**LEGAL BASIS OF THE PROCESSING**	**DATA RETENTION PERIOD**
Management of detailed reports of unlawful conduct or violations of the Management Model, carried out in written and oral form, including preliminary activities aimed at verifying the validity of the reported facts and the adoption of the consequent measures in accordance with the provisions of the Management Model.	Fulfilment of a legal obligation to which the Data Controller is subject pursuant to Legislative Decree no. 231/2001, as amended by Law no. 179/2017 as well as by EU Directive no. 2019/1937 as transposed by Legislative Decree no. 24/2023, as well as art. 6 (1) lit. c) GDPR. The processing of special data is based on the fulfilment of obligations and the exercise of specific rights of the Company and the data subject in the field of labour law pursuant to art. 9, par. 2, letter b) of the GDPR. The processing of data relating to criminal convictions and offences is based on art. 10 of the GDPR. With reference exclusively to the making of reports by voice recording, the Data will be processed subject to the consent of the interested party, pursuant to art. 14 of Legislative Decree no. 24/2023.	The Data are stored for the time necessary to process the report and in any case no longer than 5 years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations referred to in Article 12 of Legislative Decree No. 24/2023 and the principle referred to in Article 5 (1) letter e) of the GDPR. If the report involves the establishment of a dispute or disciplinary proceedings against the reported person or the whistleblower, the Data will be stored for the duration of the judicial and/or extrajudicial proceedings until the expiry of the time limit for appeals.
If necessary, to ascertain, exercise or defend the rights of the Data Controller in court.	Legitimate interest of the Data Controller pursuant to art. 6, par.1, letter f) of the GDPR. The processing of special data is based on the establishment, exercise or defence of legal claims pursuant to Article 9(2)(f) GDPR. The processing of data relating to criminal convictions and offences is based on art. 10 of the GDPR.	The Data will be stored for the entire duration of the judicial proceeding or until the time limit for appeals has been exhausted.
Once the above-mentioned retention terms have expired, the Data will be destroyed, deleted or made anonymous, compatibly with the technical procedures of cancellation, backup, as well as accountability of the Data Controller.		

	DATA PROVISION
	The provision of Identification Data is optional. In particular, in the event of failure to provide the identification data of the whistleblower, the report will be made anonymously. The information contained in the report (e.g. the circumstances and description of the fact that is the subject of the report with reference to the reported person and/or third parties) is necessary to allow the Data Controller to acquire, manage and initiate any preliminary investigation phase pursuant to Legislative Decree 231/01 and Legislative Decree 90/2017 as amended by Legislative Decree 24/2023.

	Special categories of data and/or judicial data are not required by the Data Controller and may be processed, if sent by the whistleblower, only in the presence of the conditions listed above. In the absence of these conditions, they will be immediately cancelled.

	**PROCESSING MODE** The Data shall be processed by means of paper, electronic or automated tools (*Whistleblowing platform*") with logics related to the purposes indicated above and, in any case, in such a way as to guarantee the security and confidentiality of the Data. Specific security measures are observed to prevent the loss of Data, illicit or incorrect use and unauthorized access. In cases where a direct meeting is requested by the whistleblower, the meeting will be documented, subject to consent, by the staff in charge by means of minutes.

	**DATA RECIPIENTS** The Data may be communicated to subjects operating as Data Controllers such as, by way of example, judicial authorities and other public entities entitled to request them, as well as persons, companies, associations or professional firms that provide assistance and advice on the subject in compliance with the confidentiality obligations referred to in Article 12 of Legislative Decree no. 24/2023. The Data are also processed, on behalf of the Data Controller, by the provider that manages the "*Whistleblowing platform*" (as well as the storage of the information and Data contained therein) as well as by the supplier who manages the reports, who are given adequate operating instructions and specifically appointed as Data Processor pursuant to art. 28 of the GDPR. In exceptional cases, if the Company initiates disciplinary proceedings against the reported person based solely on the report, the whistleblower's Data may be communicated to the reported person, exclusively for the exercise of the latter's right of defense.

	**PERSONNEL AUTHORISED TO PROCESS** The Data may be processed by the members of the Direct Channel, the Alternative Channel, as well as by the Company's personnel, members of the Supervisory Body and Investigating Subjects involved in the management of reports who act on the basis of specific instructions regarding the purposes and methods of processing and who will in any case be involved only in cases that are strictly necessary, taking care to preserve the absolute confidentiality of the data subjects.

	**DATA TRANSFER** No data transfers outside the European Economic Area (EEA) are envisaged, with regard to the processing in question.

	**RIGHTS OF THE DATA SUBJECT – COMPLAINT TO THE SUPERVISORY AUTHORITY** The whistleblower will be able to check the status of the report through the Platform. In the case of anonymous reports, it will not be possible for the whistleblower to exercise the rights referred to in this paragraph as the exercise of the rights implies the identification of the data subject in order to follow them up. By contacting the Companies by e-mail at dpo@lamberti.com, data subjects may ask the Data Controller for access to the data concerning them, their cancellation in the cases provided for by Article 17 of the GDPR, the correction of inaccurate data, the integration of incomplete data, the limitation of processing in the cases provided for by Article 18 of the GDPR, as well as the opposition to processing, for reasons related to their particular situation, in the event of the legitimate interest of the Data Controller. In the event of a direct meeting, at the request of the whistleblower, the minutes (drawn up with the consent of the whistleblower) may be verified, corrected and confirmed by the whistleblower by signing them. In the case of an oral report, the express consent of the whistleblower will be required and, in the case of a transcription of the oral report, it will be possible to verify, rectify or confirm the content of the transcript by means of one's signature. Data subjects have the right to lodge a complaint with the competent supervisory authority in the Member State in which they habitually reside or work or in the State where the alleged infringement occurred.

	Pursuant to Article 2-undecies of Legislative Decree No. 196/2003, as amended by Legislative Decree No. 101/2018 (hereinafter, the "**Privacy Code**"), the rights referred to in Articles 15 to 22 of the GDPR cannot be exercised if the exercise of these rights may result in an actual and concrete prejudice to the confidentiality of the identity of the employee who reports unlawful conduct of which he or she has become aware by reason of his or her office. In this case, the rights in question may be exercised through the Garante (in the manner set out in Article 160 of the same Code), which informs the data subject that it has carried out all the necessary checks or that it has carried out a review, as well as of the data subject's right to bring judicial appeals.