

PRIVACY NOTICE FOR THE PROCESSING OF PERSONAL DATA

(Prepared pursuant to Article 13 of the European Regulation No. 679/2016)

LimoLane Holding S.r.l. provides this notice regarding the processing of personal data in compliance with the European Regulation on the protection of personal data No. 679/2016 (“GDPR”).

The processing of personal data related to the receipt and management of whistleblowing reports will be carried out in accordance with European and national principles on personal data protection, as well as in compliance with Legislative Decree 24/2023, providing appropriate information to whistleblowers and persons involved, and implementing appropriate security measures to safeguard the rights and freedoms of the data subjects.

Data Controller

The Data Controller is:

- LimoLane Holding S.r.l.,
- Via per Monzoro n. 41/43, Cornaredo (MI), C.F./P.I. 05939340963, represented by Mr. Francesco Righetti.

Types of Data Processed

In the context of receiving and managing reports of violations, the Data Controller may process the following types of personal data:

- Personal identification data (e.g., name, surname, residential address, place and date of birth),
- Contact data (e.g., email and telephone),
- Identity documents (e.g., ID card, driver’s license),
- Special categories of personal data (e.g., health conditions, sexual orientation, trade union membership under Art. 9 GDPR),
- Data relating to criminal convictions and offenses (under Art. 10 GDPR).

These data are processed to conduct necessary investigations to verify the validity of the report and, where appropriate, to adopt corrective measures and initiate disciplinary and/or legal proceedings against those responsible for unlawful conduct.

Purpose and Legal Basis of the Processing

Personal data are collected and processed for the following purposes:

- a) To receive and manage reports of misconduct involving acts or omissions that harm the public interest or the integrity of public administration or private entities, including:
- Administrative, accounting, civil, or criminal offenses,
 - Conduct relevant under Legislative Decree 231/2001 or violations of organizational and management models,
 - Violations of EU or national acts in areas such as: public procurement, financial services and markets, AML/CFT, product safety, transportation safety, environmental protection, nuclear safety, food safety and animal health, public health, consumer protection, privacy and data protection, and cybersecurity,
 - Acts that harm the EU's financial interests,
 - Acts affecting the internal market,
 - Conduct undermining the purpose of EU legislation.
- b) To establish, exercise, or defend a legal right or legitimate interest of the Controller.

The legal basis for the processing referred to in purpose a) is the need to fulfill a legal obligation to which the Data Controller is subject pursuant to Art. 6, paragraph 1, letter c) of the GDPR. Specifically, the legal obligations are set forth in the provisions of Legislative Decree no. 24 of 10 March 2023, "Implementation of Directive (EU) 2019/1937 on the protection of persons reporting breaches of Union law and containing provisions on the protection of persons reporting breaches of national legislation" and in Legislative Decree no. 231 of 8 June 2001, "Regulation of the administrative liability of legal persons, companies and associations, including those without legal personality."

The legal basis for purpose b) is the need to pursue the legitimate interest of the Data Controller pursuant to Art. 6, paragraph 1, letter f) of the GDPR.

Nature of Data Provision

The provision of personal data is optional; however, failure to provide it may jeopardize the investigation of the report. Anonymous reports, in fact, will be taken into consideration only if they are adequately detailed and rendered in great detail, in order to bring out facts and situations connected to specific contexts, they will be equated with ordinary reports and, as such, may be treated in compliance with internal regulations.

Processing Methods

The Data Controller undertakes to process, in a lawful, correct, and transparent manner, only the data necessary to achieve the purposes essential for carrying out the activities reported.

The Data Controller processes data using electronic and/or paper-based media.

The report of the wrongdoing will be collected and managed via an electronic platform in compliance with current regulations on the protection of personal data, as well as with the provisions of Legislative Decree 24/2023, in order to guarantee the security and confidentiality of the whistleblower's identity.

Data Recipients

The personal data of the reporting party and of the persons identified as potentially responsible for the unlawful conduct, as well as of the persons involved in any capacity in the reported incidents, will not be disclosed.

However, the Data Controller may disclose, in accordance with the purposes of the processing and based on the same lawfulness requirements indicated above, the personal data collected to third parties belonging to the following categories:

- the Judicial Authority or the National Anti-Corruption Authority (ANAC). These entities are independent data controllers,
- police forces, competent authorities, and other public administrations. These entities will act as data controllers,
- the company providing the certified email service,
- legal and auditing/reviewing or consulting firms may perform, for example, consulting activities, support for the provision of services, etc., and will act, as appropriate, as independent data controllers or data processors based on a specific agreement on the processing of personal data concluded pursuant to Article 28 of the GDPR. The report and the identity of the whistleblower cannot be accessed either through document access or through general public access.
- the company providing the IT platform for receiving and managing reports of unlawful conduct. This entity acts as data processor pursuant to Article 28 of the GDPR under the direction and control of the Data Controller.

Natural persons such as employees, collaborators, and consultants assigned to and supporting central corporate functions and operational activities related to reporting may also access the data, acting as "authorized data processors."

The updated list of Data Processors designated by the Data Controller for the provision of services is kept at the Company's registered office.

Data transfer abroad

The personal data of the interested parties will not be communicated or transferred to countries located outside the European Union.

Automated decision-making processes

The Data Controller does not use any automated decision-making processes involving the data subject's personal data.

Data retention period

In relation to the aforementioned purposes, personal data will be collected and retained for the period established by the Whistleblowing legislation (Article 14, paragraph 1, of the Whistleblowing Decree), which establishes the deletion of reports and related documentation no later than 5 years from the date of communication of the final outcome of the reporting procedure and, in any case, for a period no longer than is necessary to achieve the purposes for which they were collected or subsequently processed.

Personal data may also be processed for the activation of judicial and/or disciplinary protection connected to the report, or communicated to the competent Authorities in the event of violations of the applicable regulations, as well as being transmitted in response to a binding order from the same Authorities.

Data Subject Rights

The data subject may exercise their rights, listed below, at any time, in accordance with EU Regulation 679/2016 and applicable national legislation:

- Right of access: The data subject has the right to obtain confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to their personal data. They may request access to the following information at any time: the purposes of the processing, the categories of data processed, the recipients to whom the personal data has been or will be disclosed, the data retention period, the existence of rights in their favor, the source of the data, and whether automated processing is used.
- Right to rectification: The data subject has the right to obtain from the data controller without undue delay the rectification of inaccurate personal data concerning them. Furthermore, they have the right to have incomplete personal data completed, including by means of providing a

supplementary statement. In this case, the data controller will be required to inform each recipient to whom the personal data has been disclosed of any rectifications.

- Right to erasure: The data subject has the right to obtain the erasure of personal data concerning him or her without undue delay and to request its deletion. Furthermore, if his or her data has been made public, the data controller will erase it and will take reasonable steps, including technical measures, to inform data controllers processing the personal data of the data subject's request to erase any copies of his or her personal data.
- Right to restriction of processing: If the data subject deems it appropriate, he or she may request the restriction of processing of his or her personal data and limit its processing in the future. In this case, the data controller will communicate any restrictions to processing to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.
- Right to lodge a complaint with the Supervisory Authority: If the data subject believes that his or her data has been processed unlawfully and violates the rules and principles regarding personal data protection, he or she has the right to contact the Supervisory Authority (Privacy Guarantor) to lodge a complaint, according to the procedures established by the latter.

The Data Controller reserves the right to limit or delay the exercise of these rights, within the limits established by applicable laws, in particular where there is a risk that the confidentiality of the Reporting Party may be subject to actual, concrete, and otherwise unjustified harm, and that the ability to effectively verify the validity of the Report or to gather the necessary evidence pursuant to Articles 2-*undecies* and 2-*duodecies* of the Privacy Code and Article 23 of the GDPR may be compromised.