




NOTICE REGARDING THE PROCESSING OF PERSONAL DATA, PURSUANT TO ARTICLES 13 AND 14 OF REGULATION (EU) 2016/679 ("GDPR") ARISING FROM THE SYSTEM ADOPTED BY THE COMPANY TO COLLECT REPORTS OF UNLAWFUL CONDUCT OR VIOLATIONS OF THE ORGANIZATIONAL, MANAGEMENT AND CONTROL MODEL PURSUANT TO LEGISLATIVE DECREE 231/2001 AND THE REPORTS PROVIDED FOR BY LEGISLATIVE DECREE 24/2023

	<p align="center">DATA CONTROLLER</p>	<p>Exelite S.p.A. (already known as Liu.Jo S.p.A.) Address: Viale J. A. Fleming, 17 - 41012 - Carpi (MO) E-mail address: privacyconsumer@liujo.it (hereafter also referred to as the "Company" or the "Data Controller").</p>
	<p align="center">DATA PROTECTION OFFICER (DPO)</p>	<p>The Data Controller has appointed a DPO who can be contacted at dpo@liujo.it</p>




	<p align="center">TYPE OF DATA PROCESSED AND SOURCE OF DATA</p>
	<p>The Company allows detailed written or oral reports of:</p> <ul style="list-style-type: none"> • unlawful conduct of an administrative, accounting, civil or criminal nature, including pursuant to Legislative Decree 231/2001. • violations of the Company's internal provisions, such as: <ul style="list-style-type: none"> a) Organization Management and Control Model that may have been adopted by the Company pursuant to Legislative Decree 231/2001, as well as related procedures; b) Code of Conduct and Anti-Corruption Regulations; c) Antitrust Regulation Compliance Program; d) Policies pertaining to Diversity, Inclusion and Gender Equality; e) National collective agreements and, more generally, internal regulations (procedures, policies, operating instructions, etc.); • violations of European provisions consisting of: <ul style="list-style-type: none"> a) acts and omissions that harm the financial interests of the Union;; b) acts and omissions affecting the internal market; c) acts and conduct that frustrate the object or purpose of the provisions of Union acts in the above-mentioned areas; • violations of national and European provisions consisting of offenses concerning - but not limited to - the following areas: <ul style="list-style-type: none"> a) public procurement; b) financial services, products and markets and prevention of money laundering and terrorist financing; c) product safety and compliance; d) transportation security; e) environmental protection; <p>digitally through its "<i>Whistleblowing platform</i>".</p> <p>Reports can be nominal or anonymous:</p> <ul style="list-style-type: none"> • in the case of anonymous reports, the company's computer systems will not be able to identify the reporter from the portal access point (IP address); • in the case of written or oral and nominal reports, at the choice of the whistleblower, the whistleblower's personal data will be associated with the report. Within the form, made available in

the "*Whistleblowing platform*", the whistleblower will be able to indicate his or her personal data, in the case of reports nominal (and, specifically, personal data and contact details), information pertaining to the relationship with the Data Controller, the circumstances and description of the fact that is the subject of the report as well as personal data of the reported and/or any third parties (hereinafter the "**Data**").


The "*Whistleblowing platform*", moreover, provides the whistleblower, on a completely optional basis, with the possibility of making reports by voice recording, subject to express consent, in which case the Data collected will also include the voice of the whistleblower himself. The "*Whistleblowing platform*" also makes it possible, at the request of the whistleblower, to schedule a direct meeting with the company functions deputized and expressly authorized for processing and which have received appropriate operational instructions. The meeting, subject to the consent of the whistleblower, will be specially documented.

The Data of the reported person, if any, are provided directly by the reported person (and thus acquired by the Data Controller from the data subject pursuant to Article 13 of the GDPR); Data of the reported person and/or third parties are provided by the reported person (and thus acquired by the Data Controller from third parties pursuant to Article 14 of the GDPR).

Any special categories of data (e.g., data pertaining to health status) are not required by the Data Controller. Should they be shared by the reporter, they will be processed only if one of the conditions set forth in Art. 9 GDPR as indicated below is met; in the absence of such conditions, they will be immediately deleted. The same considerations apply to any judicial data (e.g., data relating to criminal offenses) that may be provided and, therefore, the same will not be considered or will be processed only where required by law under Art. 10 GDPR.

	PURPOSE OF PROCESSING	 LEGAL BASIS FOR PROCESSING	 DATA RETENTION PERIOD
	<p>Handling of circumstantiated reports of unlawful conduct or violations of the Management Model, made in written and oral form, including investigative activities aimed at verifying the justification of the reported facts and the adoption of the consequent measures in accordance with the provisions of the Management Model/offenses and/or irregularities of within the framework of pre-contractual, contractual, probationary period intercurrent relations with the Data Controller or after the dissolution of the legal relationship if the information on violations was acquired in the course of the same legal relationship as</p>	<p>The Data are processed to fulfill 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 EU Directive No. 2019/1937 as transposed by Legislative Decree No. 24/2023, Art. 6 (1) lett. c) of the GDPR.</p> <p>The processing, if any, of special categories of data is based on the fulfillment of obligations and the exercise of specific rights of the Data Controller and the data subject in the field of labor law pursuant to Article 9 (2) (b) of the GDPR.</p> <p>Any data relating to criminal convictions and offenses will be processed only in cases</p>	<p>The Data shall be kept for as long as necessary for the processing of the report and, in any case, no longer than 5 years from the date of the communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set forth in Article 12 of Legislative Decree No. 24/2023 and the principle set forth in Article 5 (1) letter e) of the GDPR.</p> <p>If the report results in the initiation of litigation or disciplinary proceedings against the reporter or whistleblower, the Data will be retained for the duration of the litigation or out-of-court proceedings until the expiration of the time limit for appeal actions.</p>

<p>provided for by Legislative Decree 24/2023.</p>	<p>where it is required by law under Article 10 of the GDPR.</p> <p>With reference exclusively to the making of reports by voice recording, the recording will be processed with the express consent of the person concerned, pursuant to Article 14 of Legislative Decree No. 24/2023.</p>	<p>Exceptions to the aforementioned five-year retention period are reports whose contents are completely unrelated to the purpose of use of the whistleblowing channel (e.g., but not limited to, complaints, insults, suggestions), which will be deleted within the two-month period after the analysis is completed, documenting the reasons why they were not deemed relevant.</p>
<p>If necessary, to ascertain, exercise or defend the Data Controller's rights in court.</p>	<p>Legitimate interest of the Data Controller pursuant to Art. 6(1)(f) of the GDPR.</p> <p>Any categories of special data will be processed to establish, exercise, or defend a right in court pursuant to Art. 9(2)(f) of the GDPR.</p> <p>Processing of data related to criminal convictions and offenses, if sent, will be processed only in cases where it is required by law under Article 10 GDPR.</p>	<p>Data will be retained for the duration of the court proceedings or until the time for appeal has passed.</p>
<p>After the above retention periods have elapsed, the Data will be destroyed, erased, or anonymized, consistent with the technical erasure, backup, and accountability procedures of the Data Controller.</p>		

	<p>MANDATORY NATURE OF DATA PROVISION</p>
	<p>The provision of Data is optional.</p> <p>In particular, in case of failure to provide the Identifying Data of the reporter, the report will be made anonymously. The information reported in the report (e.g., the circumstances and description of the fact being reported with reference to the reported 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 as amended and Legislative Decree 90/2017 as amended and Legislative Decree 24/2023.</p> <p>Particular Categories of Data and/or judicial data are not requested by the Data Controller and may be processed, where sent by the reporter, only in the presence of the conditions listed above. In the absence of such conditions, they will be immediately deleted.</p>



MODE OF PROCESSING

The processing of the Data, with reference to both written and oral reports, will take place 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 face-to-face meeting is requested, the meeting will be documented, with prior consent, by the personnel in charge by means of minutes.



DATA RECIPIENTS

The Data may be disclosed to parties acting 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 matter in compliance with the confidentiality obligations set forth in Article 12 of Legislative Decree no. 24/2023.

The Data are also to be processed, on behalf of the Data Controller, by the supplier that manages the "*Whistleblowing platform*" (as well as the storage of the information and Data contained therein) as well as by the supplier that manages the reports, to whom appropriate operational instructions are given and specifically appointed as the Data Processor pursuant to Article 28 of the GDPR. In exceptional cases, if from the report the Companies initiate disciplinary proceedings against the reported person that are based solely on the report, the Data of the reporter may be disclosed to the reported person, exclusively for the purpose of having the latter's right of defense exercised in compliance with the confidentiality obligations set forth in Article 12 of Legislative Decree No. 24/2023.



SUBJECTS AUTHORIZED TO PROCESS

The Data may be processed by authorized personnel, members of the Supervisory Board and instructors 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 TO COUNTRIES OUTSIDE THE EU

There are no transfers of Data outside the European Economic Area (EEA), with regard to the processing in question.

Should it become necessary for technical and/or operational issues to use entities located outside the EEA or should it become necessary to transfer some of the collected data to technical systems and cloud managed services located outside the EEA area, the processing will be regulated in accordance with the provisions of Chapter V of the GDPR.



RIGHTS OF THE DATA SUBJECT AND COMPLAINT TO THE SUPERVISORY AUTHORITY

The data subject will be able, through the Platform, to check the status of his or her report. In the case of anonymous reports, it is not possible to exercise the rights referred to in this paragraph because the exercise of rights implies the identification of the data subject in order to follow up on them.

In the case of nominal reports, by contacting the Company by e-mail at privacyconsumer@liujo.it, data subjects may request from the Data Controller access to the Data concerning them, their deletion in the cases

provided for by Art. 17 GDPR, the rectification of inaccurate data, the integration of incomplete data, the limitation of processing in the cases provided for by Art. 18 GDPR, as well as the opposition to the processing, for reasons related to their particular situation, in cases of legitimate interest of the Data Controller.

In the case of a face-to-face meeting, at the request of the reporter, the report (prepared with the consent of the reporter) may be verified, corrected, and confirmed by the reporter by his or her signature. In the case of an oral report, express consent of the reporter will be required, and in the case of a transcript of the oral report, the content of the transcript may be verified, rectified, or confirmed by the reporter by his or her own signature.

Data subjects have the right to lodge a complaint with the competent supervisory Authority in the member state where they usually reside or work or the state where the alleged violation occurred.

Pursuant to Article 2-undecies of Legislative Decree No. 196/2003, as amended by Legislative Decree No. 101/2018 (hereinafter, "**Privacy Code**"), the rights set forth in Articles 15 to 22 of the GDPR may not be exercised if the exercise of such rights may result in 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 such a case, the rights in question may be exercised through the Garante (in the manner set forth in Article 160 of the Privacy Code itself), which informs the person concerned that it has carried out all the necessary verifications or has carried out a review, as well as the right of the person concerned to seek judicial redress.