Privacy Policy Whistleblowing

Pursuant to Legislative Decree no. 196/2003 and subsequent amendments. (hereinafter the "Privacy Code"), EU Regulation 2016/679 (hereinafter "GDPR") as well as Legislative Decree 24/2023 implementing Directive EU 2019/1937 (collectively, Privacy Code, GDPR and Legislative Decree 24/2023 defined as "Applicable Legislation") in relation to the management of reports made by you through the internal Whistleblowing channel, we inform you that any information and personal data as defined in Applicable Legislation (hereinafter “Personal Data”) voluntarily provided through the aforementioned channel will be processed by Polynt S.p.A. as Data Controller of Personal Data (the "Data Controller") in accordance with the aforementioned Applicable Legislation.

1. Purpose and legal basis of data processing

Personal Data are processed for the management of internal reports of alleged violations, or conduct, acts or omissions that harm the public interest or the integrity of the private entity, as defined by art. 2 paragraph 1 letter a) of Legislative Decree 24/2023 of which the reporting person has become aware due to his or her collaboration relationship with the Data Controller. The Personal Data processed are those contained in the internal report, and/or in acts and documents attached to it that refer to the reporting person and any other person involved.
Personal Data may also be processed to carry out the necessary investigative activities aimed at verifying the validity of what has been reported, as well as, if necessary, for the adoption of appropriate corrective measures and the introduction of appropriate disciplinary and/or judicial actions against those responsible for the violations. The legal basis that legitimizes the processing of personal data is represented by the fulfilment of a legal obligation to which the Data Controller is subject (Article 6, paragraph 1, letter c) of the GDPR), and specifically, provided for by Legislative Decree 24/2023. The processing may also concern particular data and data relating to criminal convictions and offences if included in the report in accordance with the provisions of Articles 9 and 10 of the GDPR.

2. Data processing methods and retention time criteria

Personal Data will be processed by Data Controller through 1) the reporting form provided by the Data Controller or 2) through an internal portal provided by an external company (hereinafter "Whistleblowing Portal"), i.e. InsiderLog AB, a well-known company, specialized in the provision of information platforms for data collection.

In particular, InsiderLog AB has been duly appointed by the Data Controller, pursuant to Article 28 of the GDPR, as Data Processor and, in the execution of its obligations, guarantees an adequate level of security and confidentiality of Personal Data.

We inform you that there are two ways to submit the report: anonymous or identified manner. In the first case, the registration of reports in the Whistleblowing Portal is also anonymous. The only data that is recorded is the report itself. No logs are traced for the IP address or ID of the computer from which the report originated.
The Data Controller guarantees that your rights regarding the protection of Personal Data will be respected without limitation and will only be used as described in this policy.
The Data Controller will not share your personal information with third parties outside the organization except in the cases described below in the "Transfer and disclosure of Personal

Data" section.
In the event of identified reports, all subjects who use the reporting form or the Whistleblowing Portal agree to process their Personal Data for the purposes indicated in this policy.
All Personal Data (including the identity of the whistleblower and all other data provided) will remain strictly confidential and will not be shared with third parties outside the Data Controller's organization, including for the purpose of carrying out investigations related to the report (except in the cases described in the "Transfer and disclosure of Personal Data" section). In particular, whistleblowing reports as well as the information and Personal Data included therein will be processed by the Internal Auditor and/or the Group General Counsel/Group Director HR/IT, ("Directive Committee") both subjects specifically and internally appointed by the Data Controller pursuant to the Applicable Regulations.
If necessary for investigations, the whistleblowing report may be submitted to other individuals/employees who need to be involved in the investigations and who will be duly authorized to process the Personal Data contained therein. If necessary, the Data Controller will request your consent to disclose your identity to such individuals/employees.
In order to comply with legal obligations or in the event of legal proceedings following the analysis of the report, the Data Controller must disclose the identity of the reporting party.
Personal Data will be processed for the period strictly and objectively necessary to achieve the scope and purposes identified in paragraph 1 above. In the event that the Personal Data is no longer required, the Data Controller will securely delete or anonymize the Personal Data.
In any case, the Personal Data will be kept for a period not exceeding 5 (five) years from the notification of the final decision on the whistleblowing report and, subsequently, will be permanently deleted.

3. Transfer and Disclosure of Personal Data

The content of the report may be shared or disclosed to other companies of Polynt S.p.A. (affiliates, subsidiaries, etc.) that may process Personal Data as independent data controllers. All of these entities are bound by intercompany agreements entered into for this purpose.
In the event of a possible legal proceeding or if the Data Controller needs specific advice to analyze and better understand the content of the report, it may share the Personal Data with its legal advisors or competent authorities, duly authorized to process Personal Data.
In general, Personal Data will be stored and processed within the European Union (EU)/European European Economic Area (EEA) or any other non-EEA country that the European Commission deems to offer an adequate level of protection (so-called "white-listed" countries). In the event that it is necessary to transfer Personal Data to a non-EEA country that the European Commission does not consider offering an adequate level of protection, we will implement appropriate security measures and safeguards, including the applicable Standard Contractual Clauses adopted by the European Commission.
We hereby inform you that the Data Controller implements all possible and reasonable security measures during the collection and processing of your Personal Data but declines any responsibility for the security of your data during its transit in the web unless the Data Controller's liability explicitly derives from a legal obligation.
Notwithstanding the above, we inform you that the person against whom the report refers will not have access to the identity of the reporting party but may have access to the content of the report itself.

4. Your rights

As a reporting party/data subject (to whom the Personal Data refers), you are the owner of the rights conferred by the GDPR. In particular, pursuant to articles 15-22 of the GDPR, data subjects have the right to request and obtain, at any time, access to their Personal Data, information on the processing carried out, rectification and/or updating of Personal Data, cancellation and limitation of processing. You also have the right to object to processing and to request data portability *(i.e. to receive* your personal data in a structured, commonly used and machine-readable format, with the exception of personal data that may be essential for us to comply with legal obligations). Finally, data subjects always have the right to withdraw their consent at any time (this, in any case, will not affect the lawfulness of the processing carried out on the basis of the consent given before its withdrawal) and to lodge a complaint with the competent data protection authority (in Italy: "Garante per la protezione dei dati personali").

Requests relating to the exercise of the above rights should be sent to the following e-mail address: privacy@polynt.com.

To the same address indicated above, the interested party must also send requests relating to the recipients of Personal Data, as well as requests for clarification regarding this privacy policy.