WHISTLEBLOWING
Privacy Policy
In accordance with Articles 13 and 14 of Regulation (EU) 2016/679 ("GDPR")

Introduction

Below, Rheavendors Industries S.p.A., as the Data Controller, provides information regarding the processing of personal data of individuals carried out in the context of managing whistleblowing reports, i.e., illicit behaviors or violations referred to in Article 2.1, letter a) of Legislative Decree 24/2023 (hereinafter, "**Whistleblowing Decree**").

Under the GDPR, "data subjects" are natural persons to whom the data relates. In this case, data subjects include whistleblowers, the reported individual, and any individuals mentioned in the report.

Reports can be made through the channels and methods specified in the whistleblowing procedure (hereinafter, "**Procedure**"), including:

a) in writing, through the dedicated software platform available at the link https://rhea.segnalazioni.info/#/

b) orally, through the specific functionality available via the software platform mentioned above, with the acquisition of the corresponding audio file;

c) exceptionally, at the whistleblower's request, during an in-person meeting (to be requested through the online platform in any case).

1. Data Controller

The Data Controller is Rheavendors Industries S.p.A., with registered office at Via Valleggio 14, 22100 Como (CO), tel. +39 02966551, email segnalazioni@rheavendors.com

2. Categories and Source of Processed Data

In the context of whistleblowing reports, the following data will be processed:

- Personal and contact data of the whistleblower, if voluntarily disclosed by them;
- Data related to the reported individual and other individuals involved in the report, potentially including data related to the commission of illicit activities;
- Data related to work activities within the organizational framework;
- Any other data (potentially even sensitive, if relevant to the report) contained in the report or acquired during the investigative phase.

The data of the whistleblower, the reported individual, and/or third parties are provided directly by the whistleblower and/or acquired during subsequent investigative activities.

3. Purposes of processes, legal bases and data retention periods

Why are personal data processed?	What is the legal basis for the processing?
For the management of whistleblowing reports, including investigative activities following the report	The fulfillment of a legal obligation to which the Data Controller is subject, as provided for in Article 6, paragraph 1, letter c) of the GDPR
If necessary, for the adoption of measures following the report and, in general, for the protection of the rights of the Data Controller.	Legitimate interest of the Data Controller pursuant to Article 6, paragraph 1, letter f) of the GDPR
For the disclosure of the whistleblower's identity (if known) only in cases provided for by law, e.g., to allow the reported individual to defend themselves in the context of a disciplinary proceeding (Article 12, paragraphs 5 and 6 of the Whistleblowing Decree).	Consent of the data subject pursuant to Article 6, paragraph 1, letter a) of the GDPR
For the documentation of a report made through the recorded voice messaging system, through further recording on a device suitable for storage and playback, or by means of full transcription (Article 14, paragraph 2 of the	Consent of the data subject pursuant to Article 6, paragraph 1, letter a) of the GDPR

Whistleblowing Decree)	

For the management of any data, included in the report or emerged during the investigation, related to criminal convictions and offenses or related security measures.	The processing is authorized by Union or Member State law (specifically, by the Whistleblowing Decree), as provided for in Article 10 of the GDPR
For the management of special category data (namely, data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, and data concerning health or sexual life) relevant to the reported case.	The processing is allowed for reasons of substantial public interest (specifically, to fulfill the provisions of the Whistleblowing Decree) and/or the processing is necessary for the establishment, exercise, or defense of legal claims, in accordance with Article 9, paragraph 2, letters f) and g) of the GDPR
What is the data retention period?	
The data is retained for a maximum period of 5 years from the date of communication of the final outcome of the whistleblowing procedure, unless a judicial or disciplinary proceeding is initiated as a result of the report. In such cases, the data will be kept for the entire duration of the proceedings, until their conclusion, and the expiration of any appeal periods. Personal data that is evidently not useful for the management of a specific report is not collected, or if collected accidentally, is immediately deleted. After the above-mentioned retention periods have elapsed, the data will be destroyed, deleted, or anonymized, in line with the technical timelines for deletion and backup.	

4. Nature of Data Provision

In the reporting phase, the provision of data is at the discretion of the whistleblower, provided that excessively generic and unsubstantiated reports cannot be effectively handled.

During the investigative phase, the Data Controller may acquire additional data by requesting them from the parties involved or conducting inquiries on its own.

The whistleblowing management process ensures the confidentiality of the whistleblower's identity (if disclosed), from the moment of receipt and throughout any subsequent contact, as well as the confidentiality of individuals subject to the report or mentioned in it.

In any case, any anonymous reports will be considered only if adequately detailed, based on concrete elements, and provided with an abundance of particulars, making the reported facts appear credible.

5. Data recipients

Personal data related to the management of the above-mentioned reports are processed by the following entities:

- The HR Director of Rhea Vendors Group S.p.A., acting as the Reporting Manager on behalf of the Data Controller, designated as Data Processors under Article 28 of Regulation (EU) 2016/679;
- GRC Team S.r.l., the provider of the whistleblowing software platform, designated as a Data Processor under Article 28 of Regulation (EU) 2016/679.

Any sharing of the report and documentation provided by the whistleblower with other company functions or external professionals for investigative purposes is carried out in compliance with the Procedure, the Whistleblowing Decree, and data protection regulations, with utmost care to protect the confidentiality of the whistleblower and the reported individual, omitting any communication of data that is not strictly necessary.

It is emphasized that the identity of the whistleblower (and any other information from which it can be inferred, directly or indirectly) will not be disclosed, without their consent, to parties other than the Reporting Manager and (when necessary) the professionals assisting them in the investigative activity, except as required by applicable regulations.

Data may be communicated to the Judicial Authority and other public entities authorized to receive them, such as ANAC, in cases and methods provided by the Whistleblowing Decree and the Procedure.

In the context of a potential criminal proceeding, the identity of the reporting person is protected by secrecy in the ways and limits provided by Article 329 of the Criminal Procedure Code.

In the context of a potential proceeding before the Court of Auditors, the identity of the reporting person cannot be revealed until the conclusion of the investigative phase.

6. Transfer of Data outside the EU

The data is not transferred outside the European Union.

7. Features of the software platform for submitting reports

The platform for submitting reports has the following characteristics:

- it uses the open-source software GlobaLeaks, developed following the OWASP development guidelines, and is already employed by ANAC for the creation of its OpenWhistleblowing portal;
- it is is provided and maintained by the supplier GRC Team S.r.l., without involvement from the Data Controller's Information Systems;
- it generates exclusively anonymous logs regarding the activities performed by the whistleblower, preventing their identification;
- it is protected by security measures appropriate to the risk, including foremost data encryption for stored information.

8. Rights of the Data Subjects

It is possible to exercise, in relation to the data processing described above, the rights recognized by the GDPR to the data subjects, including the right to:

- request access to the data and information as per Article 15 (processing purposes, categories of personal data, etc.);
- obtain the rectification of inaccurate data or the integration of incomplete data under Article 16;
- request the erasure of personal data in the cases provided for by Article 17, if the Data Controller no longer has the right to process them;
- obtain the restriction of processing (i.e., the temporary limitation of data to storage operations only) in cases provided for by Article 18 of the GDPR;
- object at any time, for reasons related to their particular situation, to the processing of their personal data based on legitimate interest under Article 6.1, letter f) of the GDPR.

To exercise these rights, it is possible to contact the Reporting Manager at Rhea Vendors Group S.p.A., with registered office at Via Valleggio 14, 22100 Como (CO), tel. +39 02966551, emaile segnalazioni@rheavendors.com

Data subjects have the right to lodge a complaint with the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) or to take legal action if they believe that the processing of their personal data is contrary to the applicable regulations.

It is noted that, pursuant to Article 2-undecies of Legislative Decree no. 196/2003 ("Privacy Code"), the rights under Articles 15 to 22 of the GDPR cannot be exercised if the exercise of these rights could result in a real and concrete harm to the confidentiality of the whistleblower's identity. In this case, the rights in question can be exercised through the Italian Data Protection Authority, following the procedures specified in Article 160 of the Privacy Code.