Privacy policy for the RAG whistleblower system

As part of its compliance management system, RAG pursues the goal of ensuring compliant and ethical conduct in the course of its business activities through a range of measures measures. A group-wide whistleblower system has been set up to enable the early detection of misconduct, wrongdoing or violations of rules (hereinafter referred to as „violations“). This is intended to help RAG quickly address and remedy any misconduct by employees or business partners. The whistleblower system can be used to report violations on predefined topics electronically, either by disclosing one‘s identity or anonymously.

The following information serves to explain the processing of **personal data** in the course of using the whistleblower system. This is done in accordance with the provisions of the Whistleblower Protection Act (Hinweisgeberschutzgesetz, “HSchG”), the Data Protection Act (Datenschutzgesetz, “DSG”), and the General Data Protection Regulation (GDPR). The aim is to process incoming reports securely, confidentially, and in a manner that protects the rights of both the whistleblower and any persons affected.

Name and contact details of the controller

RAG Austria AG, Schwarzenbergplatz 16, 1015 Vienna, is responsible for data processing; it is represented by its Executive Board. The data protection officer can be contacted at datenschutzbeauftragter@rag-austria.at.

Purpose and legal basis of data processing

Personal data is processed exclusively for the purpose of receiving incoming reports for the detection, investigation, and elimination of potential violations on predefined topics. It is generally possible to submit a report without providing personal data. However, in the course of the whistleblowing process, personal data may be disclosed on a voluntary basis in open text fields, uploaded documents, or within the communication options used via the whistleblowing system. Processing is strictly purpose-specific and is only carried out by authorized and trained persons who are bound to confidentiality.

Depending on the content of a report, the following data may be processed:

- Information about the whistleblower (e.g., name, contact details, position), unless the report is anonymous
- Information about the person(s) concerned, such as the accused, witnesses, or persons with knowledge of the matter (e.g., name, position, behavior)
- Factual information, descriptions, evidence, or other documents
- Communication and procedural data (e.g., queries, internal processing notes).

The processing of personal data is based on:

- **Art. 6 (1) (c) GDPR** in conjunction with **Sections 11 et seq. HSchG**: to fulfill the legal obligation to set up and operate an internal reporting channel, as well as on the basis of Section 8 HSchG;
- **Art. 6 (1) (f) GDPR**: to safeguard RAG‘s legitimate interests in detecting and preventing violations

Insofar as **special categories of personal data** are processed in the context of a report, the processing is based – depending on the type of data and the subject matter of the report - on **Art. 9 (2) (f) GDPR, Art. 9 (2) (g) GDPR**, or **Art. 10 GDPR** in conjunction with Section 8 (6) HSchG and **Section 4 (3) DSG**.

Confidentiality and protection of your identity as a whistleblower

If you disclose your identity as a whistleblower, it will always be treated confidentially and will only be disclosed to authorized employees of the internal reporting channel. Any further disclosure of information about your identity will only take place if there is a legal obligation to disclose it. If a report is knowingly false, there is no entitlement to confidentiality protection.

If a report contains personal data of third parties, known as „affected individuals“ by the report, they will be given the opportunity to comment on the report. In this case, the person affected may be informed about the report. The confidentiality of the whistleblower is maintained, as the person affected will not be given any information about the identity of the whistleblower, as far as legally possible.

Both the provider‘s whistleblower system and RAG‘s internal processes are designed to ensure the highest possible level of protection for your data. All information is transmitted in the whistleblower system using end-to-end encryption and stored in a specially secured database. Neither employees of the software provider nor unauthorized third parties have access to your report. No IP addresses, location data, or any other technical metadata that could be used to identify you are stored.

Processors

The technical implementation of the whistleblower system is carried out by Formalize ApS, Kannikegade 4, DK-8000 Aarhus C, Denmark, CVR 42 04 51 36. For this purpose, a data processing agreement in accordance with Art. 28 GDPR has been concluded to ensure data protection.

Recipients of the data

In addition to the employees of the internal reporting channel, other persons whose information is required for this purpose may be involved in clarifying the facts. The identity of the persons affected by the report will only be disclosed under the legal requirements, and all persons providing information are expressly obliged to maintain strict confidentiality.

If, in the course of investigating reports, there are valid indications of possible administrative offenses, criminal offenses, or other prohibited conduct, RAG may transmit the relevant information to the competent authorities for the necessary implementation of follow-up measures, or RAG may even be obliged to do so. There, they are subject to the applicable procedural and confidentiality regulations. RAG may also forward the relevant data to its legal advisors, who are subject to professional and ethical confidentiality obligations, in order to clarify the underlying facts.

Data access and storage period

Only employees of RAG‘s internal reporting channel who are authorized to process data have access to your data.

Personal data that is not required for the processing of a report will be deleted immediately. Otherwise, your personal data will be deleted **five years** after it was last processed or transmitted, unless longer storage is necessary, for example due to ongoing proceedings. All processing operations are logged. The log data is stored for **three years** after the last processing or transmission, after the five-year retention period has expired, before being deleted. Sections 8 (11) and (12) HSchG apply.

Your rights as a data subject

Persons who are named in a report or whose personal data is processed in the course of processing (accused persons, witnesses, third parties) have the right to be informed, the right of access, rectification, erasure, restriction, data portability, withdrawal of consent, and objection within the framework of the legal requirements. To assert these rights, data subjects can contact datenschutzbeauftragter@rag-austria.at. However, the exercise of these rights may be restricted in accordance with the Data Protection and Whistleblower Act – this applies in particular if it is necessary to protect the identity of a person who is protected accordingly and/or to prevent attempts to obstruct the reporting of violations or follow-up measures based on them.

In addition, there is the right to complain to the competent data protection authority if there is suspicion of unlawful data processing.

If a report results in proceedings before a court or an authority, or if the public prosecutor's office becomes responsible, the rights of the persons concerned (also) arise from the applicable procedural rules.

By using the whistleblower system, you acknowledge and agree to this privacy policy and the processing of your personal data as described herein.