

Privacy Notice for the Whistleblower System

1 General

1.1 Objectives and Responsibilities

- (1) The purpose of this Privacy Notice is to inform you about the nature, scope, and purpose of the processing of personal data in our reporting portal based on the “EQS Integrity Line” software from the EQS Group and the associated functionalities and content (hereinafter referred to as the “Whistleblower System”).
- (2) The provider of the whistleblower system and the data controller under data protection law is Heraeus Holding GmbH, Heraeusstraße 12-14, 63450 Hanau, Germany (hereinafter “Heraeus,” “we,” or “us”).

Heraeus Holding GmbH and the other Heraeus Group companies also process certain personal data within the framework of the Whistleblower System as joint controllers within the meaning of Article 26 of the GDPR.

The technical provision and operation of the “EQS Integrity Line” software are carried out by EQS Group, Karlstr. 47, 80333 Munich, which acts on our behalf as a data processor within the meaning of Article 28 of the GDPR (see Sections 1.6 and 2.4).

Depending on the nature and scope of the measures required, we may, if necessary, entrust service providers with the specific implementation of the corresponding investigative and clarificatory measures. These service providers may include, for example, auditors, law firms, or tax advisors. In this case, the service providers often act as separate data controllers within the meaning of Article 4(7) of the GDPR.

- (3) You can contact our Data Protection Officer at the following email address: dataprotection@heraeus.com or by mail:

Data Protection Officer
c/o Heraeus Business Solutions GmbH
Heraeusstr. 12-14
63450 Hanau

- (4) The term “whistleblower” refers to any person who submits a report via the reporting portal. This may include both Heraeus employees and external individuals.

1.2 Legal Basis

Personal data is collected and processed on the following legal basis:

- a) Processing to fulfill a legal obligation pursuant to Art. 6(1)(c) of the GDPR, i.e., data processing is required by law or another legal requirement. This refers in particular to Art. 17 of Directive (EU) 2019/1937 (“EU Whistleblower Directive”) in conjunction with the national regulations implementing it. Under the EU Whistleblower Directive and the national regulations implementing it, we are legally required to provide a whistleblower system.
- b) Processing to safeguard legitimate interests pursuant to Article 6(1)(f) of the GDPR, i.e., processing is necessary to safeguard our legitimate interests or those of a third party, provided that such interests do not override the fundamental rights and freedoms of users who require the protection of personal data. Our legitimate interest consists of the prevention and detection of criminal offenses, breaches of duty, and other violations within our company, in conjunction with any applicable national regulations; the associated prevention of damages and liability risks for our company; the review of internal processes for their legality; and the preservation of our company’s integrity.

- c) To the extent that, in the context of reports or subsequent investigative proceedings, special categories of personal data within the meaning of Article 9(1) of the GDPR – such as information regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, health data, or data concerning sex life or sexual orientation, are entered into the whistleblower system, we process such data on the legal basis of Article 9(2)(b) of the GDPR in conjunction with Article 9(2)(f) of the GDPR and applicable national regulations.

1.3 Rights of the Data Subject

You may exercise your rights as a data subject with respect to your processed personal data at any time by contacting the Data Protection Officer using the contact information provided above, either in writing by mail or by email. As a data subject, you have the following rights.

- (1) **Right of Access:** Pursuant to Article 15 of the GDPR, you may request confirmation as to whether your data is being processed. If this is the case, you have the right to receive information about such processing free of charge. In this context, you also have the right to receive a copy of the personal data that is the subject of the processing.
- (2) **Right to Rectification:** If personal data was processed while it was inaccurate, you have the right, pursuant to Article 16 of the GDPR, to request the rectification of such data without delay. You also have the right to request that incomplete personal data be completed.
- (3) **Right to erasure:** If you have withdrawn your consent, objected to the processing of your personal data (and there are no overriding legitimate grounds for the processing), if your personal data is no longer necessary for the original purpose of processing, if there is a corresponding legal obligation, or if personal data has been processed unlawfully, you have the right to request the erasure of your personal data pursuant to Article 17 of the GDPR, provided that no obstacles to erasure – such as statutory retention periods – prevent it.
- (4) **Right to Restriction of Processing:** Under the provisions of Article 18 of the GDPR, you have the right to request the restriction of the processing of your personal data.
- (5) **Obligation to Notify and Right to Be Informed:** Pursuant to Article 19 of the GDPR, we are obligated to inform all recipients to whom your data has been disclosed about any rectification or erasure of your data or any restriction on processing, unless this proves impossible or involves disproportionate effort. You have the right to be informed of these recipients.
- (6) **Right to Object:** If the processing of personal data is necessary to safeguard the legitimate interests of our company pursuant to Article 6(1)(f) of the GDPR, you may, pursuant to Article 21(1) of the GDPR, object to the processing at any time on grounds relating to your particular situation. The objection may be submitted in any form. If you object, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or the processing is necessary for the establishment, exercise, or defense of legal claims.
- (7) **Right to lodge a complaint:** Pursuant to Article 77 of the GDPR, you have the right to lodge a complaint with any supervisory authority of your choice – in particular, in the EU Member State where you reside, where you work, or where the alleged infringement occurred – if you believe that the processing of your personal data violates the legal provisions. This does not affect any other administrative or judicial remedies.

1.4 Deletion of Data

Your personal data will be deleted as soon as the purpose for which it was collected no longer applies and there are no other statutory or contractual retention obligations.

A case is considered closed when no further findings regarding the matter are expected, the investigative measures have been completed, and any necessary measures in response to the report have been implemented. Personal data from the whistleblower system is generally deleted within two

months after the conclusion of the respective investigation, unless it must be further processed for other purposes, e.g., to fulfill statutory retention and documentation obligations or to exercise, assert, or defend legal claims.

1.5 Security Measures

- (1) Organizational and technical security measures in line with the current state of the art are in place to ensure compliance with the relevant legal provisions and to protect personal data against accidental or intentional manipulation, loss, destruction, or access by unauthorized persons.
- (2) The data provided via the whistleblower system is stored in a highly secure EQS Group database located in the European Union. All data stored in the database is encrypted using state-of-the-art technology. Only Heraeus has access to the data. Neither the EQS Group nor any other third party has the ability to decrypt this data and make it readable.

1.6 Disclosure of Data to Third Parties and Third-Party Providers

- (1) Heraeus transfers data to third parties exclusively in accordance with legal provisions. We transfer data to third parties only when necessary, or for other purposes required to fulfill our contractual obligations toward whistleblowers or to comply with legal requirements. Data transfer and processing are always purpose-limited and based on a legal basis.
- (2) To the extent that we use subcontractors to provide our services, we take appropriate legal precautions as well as technical and organizational measures to protect personal data in accordance with applicable legal provisions. The EQS Group is our technical service provider for the whistleblower system and acts as a data processor on the basis of a data processing agreement pursuant to Article 28(3) of the GDPR. In addition, your personal data may be disclosed to other external service providers within the scope of contract processing subject to our instructions (e.g., IT service providers for remote maintenance and support, among other things).
- (3) If, within the scope of this Privacy Notice, we use content, tools, or resources from other providers (hereinafter collectively referred to as “third-party providers”) based in a third country, or if we transfer data to group companies based in a third country, it can be assumed that data will be transferred to such third countries.
- (4) Third countries are countries in which the GDPR does not apply directly, i.e., in principle, all countries outside the EU or the European Economic Area. Data may only be transferred to third countries if an adequate level of data protection is ensured, you have given your consent, or the transfer of such data is permitted by law. The Heraeus group companies to which your personal data may be transferred are located in Germany as well as, in some cases, in European and non-European countries. In non-European countries, the level of data protection may not be equivalent to the level of data protection provided by the GDPR in the European Union. In such cases, we ensure the protection of personal data in the recipient country through appropriate safeguards, such as the European Union’s standard contractual clauses pursuant to Article 46(2)(c) of the GDPR.
- (5) To the extent that the transfer of your personal data to a court or public authority in a non-European country without an adequate level of data protection is necessary and legally permissible for the assertion, exercise, or defense of our company’s legal claims, such transfer may take place on the basis of Article 49(1), first sentence, (e) of the GDPR.
- (6) You may request further information regarding the recipients of your personal data and any safeguards by contacting the Data Protection Officer using the contact information provided above.

1.7 Automated Decision-Making

We do not intend to use the personal data collected from you for automated decision-making (including profiling).

2 Data Processing in Detail

2.1 Data or Data Categories

As part of investigative and fact-finding measures, the following data or categories of data are processed, provided that they are disclosed by the whistleblower or entered into the whistleblower system during subsequent investigative proceedings:

- The whistleblower's identity, such as first and last name, job title, place of work, and work contact information, to the extent that the whistleblower discloses their identity in the report (non-anonymous report)
- The fact that the whistleblower used the whistleblower system to file a report
- Company-related information, such as the role within the company, job title, potential supervisory position, place of employment, work email address, and work phone number of the individuals concerned
- Personal information, such as the name, home address, home phone number, and personal email address of the individuals concerned
- Information regarding relevant facts, in particular regarding the reported conduct of the individuals concerned
- Company documents such as performance records, travel expense reports, logbooks, invoices, and similar documents that may also contain personal data, to the extent that they are necessary to investigate the reported matter
- Information regarding behavior when using company communication systems, such as metadata, log data, or the content of company emails, to the extent that such information is necessary to investigate the reported matter
- Data regarding criminal convictions and offenses
- In individual cases, special categories of personal data as defined in Article 9(1) of the GDPR

2.2 Purpose of Data Processing

- (1) Heraeus seeks to ensure compliance with laws and regulations as well as internal policies through an appropriate compliance organization, suitable processes, and measures to prevent and respond to potential violations. These measures include, among other things, the implementation and operation of a whistleblower system. The whistleblower system is designed to receive and process reports from employees and external individuals regarding conduct that is unlawful or contrary to the objective or purpose of legal provisions in a secure and confidential manner.
- (2) Heraeus is subject to comprehensive statutory supervisory and compliance obligations. These include, in particular, the provisions of commercial and tax law, criminal and administrative offense law, labor law, antitrust law, and data protection law. In addition, there are comprehensive legal regulations in countries outside the EU where Heraeus operates. Failure to adequately fulfill these legal obligations may result in significant adverse consequences, such as fines, claims for damages, the revocation of necessary permits, reputational damage, and the loss of business relationships. The implementation of the whistleblower system and the associated investigative and clarifying measures serve to fulfill these legal obligations in accordance with Article 6(1)(c) of the GDPR in conjunction with Article 17 of the EU Whistleblower Directive and the national regulations implementing it, as well as to improve compliance structures by identifying and addressing weaknesses in the internal compliance organization.

- (3) Heraeus processes the data of whistleblowers and data subjects for the following investigative and clarifying purposes:
- Verifying the plausibility of reports, in particular whether they suggest a violation of laws or other legally binding requirements or breaches of employment contract obligations
 - Investigating misconduct
 - Preventing future misconduct
 - Investigative and fact-finding measures to mitigate and prevent impending financial or other damages
 - Clearing the names of employees who have been wrongly suspected
 - Legal defense: Assertion, defense, and enforcement of legal claims
 - Fulfillment of any obligations to cooperate in the context of investigations by law enforcement or other authorities

2.3 Use of the Whistleblower System

- (1) Use of the whistleblower system is voluntary. The data processed by Heraeus depends on the information submitted by the whistleblower (see 2.1 Data and Data Categories).

2.4 Categories of Recipients

- (1) The data submitted by the whistleblower is processed by Heraeus. It is possible that the data submitted by the whistleblower may need to be accessed by other departments of the data controller or by other companies within the Heraeus Group, provided this is necessary to clarify the facts of the matter, particularly if these entities are also or solely affected by the reported matter.
- (2) The EQS Group acts as a technical service provider and data processor for Heraeus in accordance with Article 28 of the GDPR. It may have access to the encrypted data in the course of maintenance work, but not in a readable form.
- (3) If the processing of the report leads to the conclusion that a violation has occurred, Heraeus may disclose the results of investigative and clarifying measures – for example, in the context of criminal investigations – to public authorities. This applies, for instance, to German or foreign public prosecutors' offices, law enforcement agencies, courts, or other authorities. In doing so, personal data of the accused person or – in the case of non-anonymous reports – also of the whistleblower may be disclosed.
- (4) To the extent necessary to assert and enforce Heraeus's claims, and provided that no legitimate interests of data subjects preclude such disclosure, personal data may also be transferred to opposing parties in litigation or to insurers.
- (5) When conducting investigative and fact-finding measures, Heraeus may also rely on the assistance of external service providers, such as law firms, consultants, or auditing firms. In addition, data may be disclosed to external audit firms for the purpose of conducting an audit. Appropriate measures are taken to ensure that these service providers process your data only in accordance with the relevant data protection regulations.

2.5 Confidentiality of the Whistleblower's Identity and Notification of Affected Individuals

- (1) The identity of the whistleblower will be treated confidentially. If a report was not submitted anonymously, Heraeus will not disclose the whistleblower's identity – to the extent permitted by law – and will ensure that no other conclusions regarding the whistleblower's identity can be drawn.
- (2) All persons authorized to review the reports are expressly bound by confidentiality.

- (3) In certain cases, Heraeus is obligated to inform the accused individuals that Heraeus has received a report concerning them, as soon as this information no longer objectively jeopardizes the investigation of the reported matter or the follow-up on the report. The identity of the whistleblower will not be disclosed in this process.
- (4) In the event of a knowingly false report made with the intent to discredit another person, Heraeus may be obligated to disclose the identity of the whistleblower to that person.

2.6 Criteria for Determining the Retention Period

The data will be retained until the aforementioned purposes have been fulfilled or until the whistleblower's report regarding compliance-related matters has been fully processed, and to the extent required by applicable laws. This may vary depending on the complexity of the matter and the duration of the investigation.

The retention period is determined in particular by the completion of the investigative and clarification measures, the implementation of any follow-up measures, existing legal retention and documentation obligations, and whether legal consequences are still to be expected from the matter. Data from which legal consequences are expected will be retained until it is established that no further legal consequences are to be expected, or for as long as they are necessary for the exercise, assertion, or defense of legal claims. Details regarding deletion, including the deletion period, are set forth in Section 1.4 (Deletion of Data).

2.7 Technical Implementation, Anonymity, and Use of IP Addresses

- (1) The whistleblower system is provided by the EQS Group as the software provider and enables the submission of anonymous reports as well as anonymous communication via an encrypted connection.
- (2) When using the whistleblower system, the whistleblower's IP address and current location are not stored at any time.
- (3) After submitting a report, the whistleblower receives login credentials for a secure mailbox within the whistleblower system to continue communicating with Heraeus securely – even in the case of an anonymous report.
- (4) The data provided via the whistleblower system is stored in encrypted form in an EQS Group database located in the European Union; only Heraeus has access to this data (see Section 1.5 (2) for details).

2.8 Guidance for Employees

Heraeus employees can find further information regarding the processing of their personal data in the "Data Protection Guideline for Heraeus Employees".

3 Changes to the Privacy Notice

- (1) We reserve the right to amend this Privacy Notice to adapt it to changes in the legal landscape or to changes in our services and data processing practices. However, this applies only to guidelines regarding data processing.
- (2) Users are asked to familiarize themselves with the content of the Privacy Notice on a regular basis.

Last updated: September 30, 2026