1 General

1.1 Goals and responsibilities

(1) The purpose of this privacy policy is to inform you about the nature, scope and purpose of the processing of personal data in our Heraeus SpeakUp reporting portal, as well as 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 Business Solutions GmbH, Heraeusstrasse 12-14, 63450 Hanau, Germany (hereinafter referred to as "Heraeus", "we" or "us").

Heraeus Business Solutions GmbH and the other group companies of Heraeus also process some personal data within the framework of the whistleblower system as joint data controllers within the meaning of Art. 26 GDPR.

Depending on the type and scope of the measures required, Heraeus Business Solutions GmbH will – if necessary – entrust service providers with the specific implementation of the corresponding investigation and clarification measures. Said service providers may include auditors, law firms or tax consultants. In this case, the service providers often act as their own data controllers within the meaning of Art. 4 No. 7 GDPR.

(3) You can reach our data protection officer at the following e-mail address: dataprotection@heraeus.com or by post:

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

(4) The term "whistleblower" includes all persons who submit a report via the designated portal.

1.2 Legal basis

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

a) Necessity for the performance of a contract or for the implementation of pre-contractual measures in accordance with Art. 6 (1) lit. b GDPR, i.e. the data is necessary for us to fulfil our contractual obligations or we need the data to prepare a contract.

b) Processing for compliance with a legal obligation pursuant to Art. 6 (1) lit. c GDPR, i.e. the data processing is necessary due to a law or another requirement.

c) Processing for the protection of legitimate interests pursuant to Art. 6 (1) lit. f GDPR, i.e. processing is necessary for the protection of our legitimate interests or those of a third party, provided that the interests do not override the fundamental rights and freedoms of users who require the protection of personal data.

1.3 Rights of the data subject

You may exercise your rights as a data subject in relation to your personal data processed at any time by contacting the Data Protection Officer using the contact details provided above. As a data subject, you enjoy the following rights.

(1) Right to withdraw consent: If personal data is processed on the basis of consent, you have the right to revoke this consent at any time for the future in accordance with Art. 7 GDPR.

(2) Right of disclosure: In accordance with Art. 15 GDPR, you can request confirmation as to whether your data is being processed. If this is the case, you have the right to the disclosure of this information to you free of charge.

(3) Right of rectification: If your personal data was processed while inaccurate, you have the right to request that this data be corrected without delay in accordance with Art. 16 GDPR.

(4) 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), your personal data is no longer necessary for the original processing purpose, there is a corresponding legal obligation or personal data has been processed unlawfully, you have the right to request the erasure of your personal data in accordance with Art. 17 GDPR.

(5) Right to restriction of processing: According to the provisions of Art. 18 GDPR, you have the right to request the restriction of the processing of your personal data.

(6) Right to data portability: In accordance with Art. 20 GDPR, you have the right to receive the personal data you have provided in a structured, common and machine-readable format.

(7) Right to lodge an objection: If the processing of personal data is necessary to protect the legitimate interests of our company, you may object to the processing at any time in accordance with Art. 21 GDPR.

(8) Right to register a complaint: You have the right to register a complaint with the competent supervisory authorities in accordance with Art. 77 GDPR.

1.4 Data deletion

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

A case is considered closed when no further findings on the facts of the case are to be expected, the investigative measures have been completed, and any necessary measures have been implemented in response to the whistleblowing tip. After three years from the time when the case can be considered closed and is accordingly marked as closed, the documentation pertaining to the case is deleted. The case itself shall be continued, but under a title that does not allow any conclusion to be drawn about the whistleblower or the affected person and without documentation on the case.

1.5 Security measures

State-of-the-art organisational and technical security measures are in place to ensure compliance with all relevant legal provisions, and to protect personal data against accidental or intentional manipulation, loss, destruction or against access by unauthorised persons.

1.6 Disclosure of data to third parties and third-party providers

(1) Heraeus shall transmit data to third parties exclusively within the scope of the statutory provisions. We shall only transfer data to third parties if this is necessary, or for other purposes deemed essential, in order to fulfil our contractual obligations to whistleblowers or legal requirements.

(2) Insofar as we use subcontractors to render our services, we take appropriate legal precautions, as well as technical and organisational measures to protect personal data in accordance with the applicable legal provisions.

(3) If we use content, tools or resources of other providers (hereinafter collectively referred to as “third party providers”) based in a third country within the scope of this privacy policy, it is to be assumed that data will be transferred to such third countries.

(4) Third countries are countries in which the GDPR is not directly applicable, i.e. Essentially 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 guaranteed, you have consented or the transfer of such data is permitted by law.

1.7 Automated decision-making process

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

2 Data processing in detail

2.1 Data or data categories

The following data (or data categories) are processed within the scope of investigation and clarification measures, insofar as they are disclosed by the whistleblower:

- Identity of the whistleblower, insofar as the whistleblower discloses his or her identity in the context of the whistleblowing activity
- Company details, such as function in the company, job title, possible supervisor position, professional e-mail address, professional telephone number of the persons concerned
- Personal details, such as name, private address, private telephone number, private e-mail address of the data subjects
- Information on relevant facts
- Data on criminal convictions and offences
- In individual cases, special categories of personal data within the meaning of Art. 9 (1) GDPR

2.2 Purpose of the data processing

(1) Heraeus wishes to ensure compliance with the law and internal guidelines by means of an appropriate compliance organisation, suitable processes and measures, in order to prevent and respond to possible breaches of the rules. These measures include the introduction and operation of a whistleblower system.

(2) Heraeus is subject to comprehensive statutory supervisory and compliance obligations. The implementation of the whistleblower system and the associated investigation and clarification measures serve to implement these legal obligations pursuant to Art. 6 (1) lit. c GDPR, as well as to improve compliance structures by uncovering and eliminating weaknesses in the internal compliance organisation.

(3) Heraeus shall process whistleblower data for the following investigation and clarification purposes:

- Checking the plausibility of whistleblowing reports
- Clarification of misconduct
- Prevention of future misconduct
- Investigation and clarification measures to compensate for (and avert) imminent economic or other damage
- Relief for employees
- Right defence: Assertion, defence and exercise of legal claims

This data processing may be necessary, among other things, for the establishment, implementation or termination of the employment relationship with employees (Art. 6 [1] lit. b GDPR), as well as for the protection of legitimate interests pursuant to Art. 6 [1] lit. f GDPR.

2.3 Use of the whistleblower system

(1) The use of the whistleblower system is voluntary. The data processed by Heraeus depends on the information provided by the whistleblower (see 2.1 Data or data categories.

2.4 Recipient categories

(1) The data transmitted by the whistleblower shall be processed by Heraeus. It is possible that the data provided by the whistleblower will have to be viewed by other departments of the data controller or by other companies of the Heraeus Group if this is necessary to ascertain the underlying facts.

(2) Heraeus shall be obligated to inform the accused that Heraeus has received a tip-off concerning his person as soon as this information no longer jeopardises the follow-up of the tip-off. The identity of the whistleblower shall not be disclosed.

(3) Heraeus may also disclose the results of investigations and clarification measures to public authorities, e.g. in the context of criminal investigation proceedings. This applies, for example, to German or foreign public prosecutors' offices, courts or other authorities.

(4) In carrying out investigative and clarifying measures, Heraeus shall, if necessary, also have recourse to the support of external service providers – such as law firms or auditing companies. Appropriate measures are taken to ensure that these service providers only process your data in accordance with the relevant data protection regulations.

2.5 Criteria for the determination of the retention period

The data will be retained until the above-mentioned purposes have been fulfilled or until the whistleblower's report (with the reference to compliance-relevant facts) has been fully processed and is

required within the framework of the applicable laws. This can vary depending on the complexity of the facts and the duration of the clarification of the facts.

Data from which no legal consequences are to be expected is deleted immediately after the processing of the whistleblower's report has been completed, and data from which legal consequences are to be expected is retained until it has been established that no legal consequences are to be expected.

2.6 Use of cookies

(1) Communication between the whistleblower's terminal device and the whistleblower system shall take place via an encrypted connection.

(2) In order to maintain the connection to the whistleblowing system, a cookie is stored on the computer of the whistleblower which contains a session ID. This cookie is valid until the end of the whistleblower's session and is then deleted.

(3) The legal basis for the use of cookies, which are necessary for the proper functioning of the whistleblowing system, is Art. 6 (1) lit. f GDPR. Our legitimate interest is the user-oriented and economically efficient operation of our reporting portal.

2.7 Use of IP addresses

The software provider of the whistleblower system – People Intouch B.V., (Olympisch Stadion 6, 1076 DE Amsterdam, The Netherlands) – uses Amazon Web Services-hereafter referred to as "AWS"-as a cloud service.

Every request is logged by AWS. The logs contain the IP address and are automatically deleted after 90 days according to the deletion policy.

You can find further data protection information in the People Intouch privacy policy at https://privacystatement.speakup.peopleintouch.com/

3 Changes to the privacy policy

(1) We reserve the right to change the privacy policy in order to adapt it to changes in the underlying legal situation or to changes in our services and data processing. However, this only applies to data processing policies.

(3) Whistleblowers are requested to familiarise themselves with the content of the data protection notices on a regular basis.

Last updated: 29/08/2023

Version: 1.0