

## **Privacy Policy for Suppliers and Service Providers**

Information pursuant to Articles 13, 14 and 21 of the General Data Protection Regulation (GDPR)

The purpose of this Privacy Policy is to inform suppliers, service providers and other business partners of Heraeus (hereinafter referred to as business partners) about how Heraeus uses their data and what rights they have under the GDPR regarding these data.

The type of business partner data processed and used by Heraeus largely depends on the business relationship between Heraeus and each individual business partner.

### **1. Who is responsible for the processing of data and who is the point of contact at Heraeus for our business partners?**

The legal entity responsible for the processing of data within the meaning of data protection legislation is the Heraeus company in whose name products or services are ordered from a business partner or in whose name business contacts are established with a business partner (hereinafter referred to as Heraeus). The exact name and address of the relevant Heraeus company will be stated in each order, inquiry or request. Any inquiries or requests for information under data protection law must be addressed directly to the Heraeus company responsible for the processing of data. If the responsible Heraeus company has its registered office in Germany, any inquiries or requests for information under data protection law may also be directed to the Heraeus Data Protection Officer.

The Heraeus Data Protection Officer may be contacted at [datenschutzbeauftragter@heraeus.com](mailto:datenschutzbeauftragter@heraeus.com) or

Data Protection Officer  
c/o Heraeus Business Solutions GmbH  
Heraeusstraße 12-14  
63450 Hanau  
Germany

### **2. What sources are used and what data are processed by Heraeus?**

Heraeus primarily processes data that are directly provided by business partners or their employees. Heraeus also processes data that originate from public sources (e.g., commercial registers, press releases, websites, social media etc.) or that may be legitimately obtained from third parties, e.g., credit reporting agencies.

Relevant personal data are personal details of business partners (name, address and other contact data) as well as personal data of their employees (name, title, position and function at the business partner's company, business address and other business contact data) and all data relevant for the business relationship - whether or not these data can be attributed to a specific person - if these data are necessary for the initiation, the conclusion, the execution or the termination of contracts. Heraeus processes the private addresses and other private contact details as well as the date of birth, place of birth, nationality and information regarding residence permits or work permits of business partners or their employees only if such processing is required by mandatory law.

Furthermore, Heraeus processes data regarding the creditworthiness of its business partners, in particular if Heraeus is required to make advance payments, as well as advertising data (documentation data, data from public registers, data regarding the use of telemedia, e.g., time of access to Heraeus websites, apps or newsletters, provided that the business partner has not objected to the processing of such data) and other similar data. Further details are provided in the Heraeus Privacy Policy which can be viewed and printed at [www.heraeus.com](http://www.heraeus.com).

### **3. Where does Heraeus store business partner data?**

Heraeus stores business partner data in the IT systems of Heraeus and of any third-party data processors commissioned by Heraeus.

### **4. For which purpose does Heraeus process data and on which legal basis?**

Heraeus processes personal data in accordance with the provisions of the General Data Protection Regulation (GDPR) and other applicable laws requiring and/or authorizing Heraeus to process data of its business partners and their employees:

#### **4.1 For the performance of contractual obligations pursuant to Art. 6 (1) b) GDPR**

Business partner data are primarily processed for the initiation, the conclusion, the execution and the termination of contracts with the relevant business partners.

The purpose for which the data are processed in each case depends on the specific transaction (e.g., purchase of products, services, research and development services etc.). Data may be processed, inter alia, for credit assessments and creditworthiness checks with regard to business partners, especially if Heraeus is required to make advance payments.

Further details regarding the purpose of the data processing will be stipulated in the written or oral contract or other document pertaining to the individual transaction.

#### 4.2 For the safeguarding of legitimate interests pursuant to Art. 6 (1) f) GDPR

Furthermore, Heraeus processes data beyond the actual transaction of any business to safeguard its legitimate interests pursuant to Art. 6 (1) f) GDPR, in particular in the following cases:

- a) Processing of names, positions, functions and contact addresses of business partners' employees disclosed by business partners to Heraeus that are required for the initiation, conclusion, execution and termination of business transactions, including for complaint management and business partner relationship management. Heraeus trusts that its business partners are authorized to disclose these employee data for the aforementioned purpose and that they have made the necessary arrangements with their employees;
- b) consultation of, and exchange of data with, information offices to determine credit and default risks;
- c) assessment and optimization of procedures for direct business partner approach, including tendering and award procedures;
- d) assertion of legal claims and defense in legal disputes;
- e) prevention and investigation of criminal offenses, in particular investigations under the Anti-Money Laundering Act as well as measures for the prevention of undeclared work and unlawful employment, or violations of the right of residence;
- f) video surveillance of entrance areas and traffic routes on the fenced in Heraeus business premises, as well as building and plant security measures (e.g., access controls), protection of domestic authority, and all measures relating to IT security at Heraeus;
- g) Transmission of data to other Heraeus companies who are interested in the procuring products and/or services from the respective business partner;
- h) transmission of data to other Heraeus departments or other Heraeus companies to the extent that such transmission serves the purpose of complying with legal or statutory obligations (e.g., transmission of data to the legal department, the tax department, the corporate accounting department etc.) or serves the business relationship (e.g., global procurement department, corporate communication department etc.);
- i) transmission of data to third parties who assist Heraeus in the performance of its legal obligations (such as tax consultants, auditors, external lawyers etc.);

- j) measures for business management and the further development of products and services of the business partner.

#### 4.3 Based on consent given pursuant to Art. 6 (1) a) GDPR

Heraeus also processes personal data for purposes to which its business partners have expressly consented.

Any consent already given may be withdrawn at any time. This right of withdrawal also applies to any consent given prior to the effective date of the GDPR. Such withdrawal of consent is only of effect for the future and does not affect the processing operations that were performed prior to such withdrawal.

#### 4.4 For compliance with legal obligations (pursuant to Art. 6 (1) c) GDPR) or for the performance of a task carried out in the public interest (Art. 6 (1) e) GDPR).

As a business enterprise, Heraeus is subject to various statutory obligations, e.g., obligations under anti-money laundering, under combating undeclared work and unlawful employment, anti-corruption, minimum wage, or anti-terrorist legislation etc. Heraeus processes data to ensure compliance with these laws (e.g., in connection with identity verification measures, for the prevention of undeclared work and unlawful employment, for the compliance with minimum wage legislation and other public-law provisions, for the fulfillment of control and reporting obligations under public law, and for the assessment and management of legal risks).

### 5. To whom are the data disclosed?

Within the Heraeus Group, the disclosure of data is limited to those employees who have a need to know such data for the performance of contractual and legal obligations. The data will also be disclosed to other Heraeus companies if they are involved in the conclusion and/or the processing of business transactions with business partners or if their assistance is required in fulfilling any legal and statutory obligations towards business partners or third parties. The foregoing provision also applies to third-party processors within the meaning of Art. 28 GDPR, or to service providers who are not third-party processors. These third-party processors and service providers are, in particular, companies active in the fields of IT, logistics, telecommunications, payment transactions, procurement and communication.

Other Heraeus companies also receive data from business partners based on the procurement of the same or similar products or services or due to the fact that Heraeus believes that other Heraeus companies are also interested in the products and/or services which are offered by these business partners or that other Heraeus companies wish to enter into business relationships with these business partners, always provided

that that the respective business partner has not objected to the transmission of such data.

In addition, Heraeus is under the legal obligation to transfer business partner data to public authorities or third parties who assist Heraeus in the performance of its legal or statutory obligations (such as legal and tax consultants and auditors).

## **6. How long will the data be stored?**

Heraeus stores data in accordance with the applicable statutory retention and documentation obligations. As a rule, the statutory retention and documentation periods range from two to ten years, and generally commence at the end of the calendar year in which Heraeus received the data.

In particular, the following retention periods apply:

- a) six years for commercial correspondence, commencing at the end of the calendar year in which the relevant item of correspondence was received or sent, unless such item of correspondence qualifies as supporting document or record, in which case a ten-year retention period applies;
- b) ten years for master and contact data that are repeatedly needed in an ongoing business relationship with business partners for the conclusion, performance and termination of contracts; such retention period commencing at the end of the calendar year in which the business relationship with the business partner is discontinued;
- c) two years for data that qualify neither as commercial correspondence nor as supporting documents, unless shorter or longer retention periods apply in individual cases;
- d) a significantly shorter retention period applies to video recordings. This period is specified on the video surveillance signs on the Heraeus premises.
- e) a statutory retention period of generally three years (but up to thirty years in individual cases) for data required by Heraeus to take any legal action. The retention period for ongoing legal disputes is six months from the date on which such dispute was finally adjudicated.

## **7. Are data transferred to third countries?**

Data will be transferred to third countries (countries outside the European Economic Area – EEA) if such transfer is necessary for the initiation, the conclusion, the execution or termination of business transactions with a business partner, if such transfer is required by law, if Heraeus has a justified interest in such transfer, or if the respective business partner has given his/her consent to such transfer.

For the avoidance of doubt: Heraeus companies outside the EEA have access to their business partners' data stored in the IT systems of Heraeus companies located within

the EEA to the extent that such access is necessary to ensure the proper delivery or provision of products or services by the business partners to these Heraeus companies, provided that the respective business partner has not objected to the transfer of such data. Such data transfer is executed in accordance with the technical and organizational data protection measures that apply to the data transfer between Heraeus companies located within the EEA.

#### **8. What data protection rights do business partners have?**

Business partners have a right to information and access pursuant Art. 15 GDPR, a right to rectification pursuant to Art. 16 GDPR, a right to erasure pursuant to Art. 17 GDPR, a right to restriction of processing pursuant to Art. 18 GDPR and a right to data portability pursuant to Art. 20 GDPR.

In addition, business partners have the right to lodge a complaint with a supervisory authority.

#### **9. Are business partners obliged to make personal data available to Heraeus?**

As a rule, business partners only have to provide those personal data which are necessary for the initiation, execution and termination of a business relationship with Heraeus or data which Heraeus is legally required to collect (cf. 4.4 above).

#### **10. Does Heraeus use automated decision-making processes?**

As a matter of principle, Heraeus does not use fully automated decision-making processes within the meaning of Art. 22 GDPR for the initiation and execution of business transactions with business partners. If Heraeus should use such automated decision-making processes in individual cases in the future, Heraeus will inform the relevant business partners separately if so required by law. The same applies to profiling (scoring).

#### **11. Information on your right of objection pursuant to Art. 21 GDPR**

Business partners are entitled to object to the processing of their personal data at any time for reasons arising from their particular situation if the processing of their data is carried out pursuant to Art. 6 (1) e) or Art. 6 f) GDPR (data processing for the safeguarding of interests). This right of objection also applies to employees of business partners if these employees made available their personal data to Heraeus directly or through the business partner and if these data are processed by Heraeus in the public interest or for the safeguarding of interests. It is the business partners' responsibility to instruct their employees about this right of objection.

Based on a business partner's objection, Heraeus will stop processing such business partner's personal data unless Heraeus can prove that the processing of the data is necessary for compelling legitimate reasons which outweigh the business partner's interests, rights and freedoms, or if the processing of the business partner's data serves the assertion, exercise or defense of legal claims.

Heraeus processes personal data of business partners for direct marketing purposes. Business partners have the right to object to the processing of their personal data for direct marketing purposes at any time.

Based on such objection, Heraeus will stop processing the business partner's personal data for the purposes of direct marketing.

The objection may be informal and should be addressed to:

[Widerspruch@heraeus.com](mailto:Widerspruch@heraeus.com)

Business partners are asked to state as precisely as possible to which specific data processing they wish to object.

**Last update:** Hanau, in April 2022

**Version:** Privacy Policy for Suppliers and Service Providers V.2.0