



## Obligation to provide information pursuant to Art. 13 and Art. 14 GDPR for customers / business partners / suppliers

The protection of your data and transparency about its processing is very important to us. Therefore, we hereby comply with our obligation to inform about the circumstances of processing in accordance with Art. 13 and Art. 14 of the General Data Protection Regulation (GDPR).

*Note: For better readability, the masculine form is used in this document. Of course, this always means all genders equally.*

The processing of your personal data gives you the following rights:

- a. Right to information (see Art. 15 GDPR)
- b. Right to rectification (see Art. 16 GDPR)
- c. Right to erasure (see Art. 17 GDPR)
- d. Right to restriction of data (see Art. 18 GDPR)
- e. Right to object (see Art. 21 GDPR)
- f. Right to data portability (see Art. 20 GDPR)
- g. Right of withdrawal: If the processing is based on Art. 6 GDPR (1) (a) or Art. GDPR 9 (2) (a), you have the right to withdraw your consent at any time. Previously processed data remains unaffected by the revocation.

Contact details of the data protection officer: Jasmin Muhmenthaler-Sturm, Datenbeschützerin GmbH, Unterer Sand 9, 94209 Regen, E-Mail: [info@datenbeschuetzerin.de](mailto:info@datenbeschuetzerin.de), Tel: 09921 22 88 9000

You have the right to lodge a complaint with a supervisory authority if you believe that the processing of your personal data is unlawful.

The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg  
Lautenschlagerstraße 20  
P.O. Box 10 29 32  
70025 Stuttgart

Phone: 0711/615541-0

Fax: 0711/615541-15

E-Mail: [poststelle@lfdi.bwl.de](mailto:poststelle@lfdi.bwl.de)

The data controller is:

Heidelberg Instruments Mikrotechnik GmbH  
Represented by: Mr. Konrad Roessler  
Mittelgewannweg 27  
69123 Heidelberg

Phone: (+49) 6221 728899 0

E-Mail: [info@heidelberg-instruments.com](mailto:info@heidelberg-instruments.com)

Furthermore, it should be mentioned here:

Nanoscribe GmbH & Co. KG  
Represented by: Martin Hermatschweiler and Lars Tritschler  
Hermann-von-Helmholtz 6th place  
76344 Eggenstein-Leopoldshafen

Phone: +49 (0) 721 981 980 0

E-Mail: [info@nanoscribe.com](mailto:info@nanoscribe.com)



The controller is the natural or legal person who, alone or jointly with others, decides on the purposes and means of the processing of personal data (e.g. names, e-mail addresses, etc.).

Data will only be transferred to third countries (countries outside the European Economic Area – EEA) if this is necessary for the execution of the service contract or if you have given us your consent or if this is otherwise legally permissible. In this case, we take measures to ensure the protection of your data, for example through contractual arrangements. We only transmit data to recipients who ensure the protection of your data in accordance with the provisions of the GDPR for transfer to third countries (Art. 44 to 49 GDPR).

The decision on our contractual relationship is not based on automated processing or profiling, i.e. there is no automated decision-making within the meaning of Art. 22 GDPR for the establishment, implementation and processing of the contractual relationship.

If this procedure is used in individual cases, we will inform you separately if this is required by law.

Within the framework of our customer relationship, only the personal data that is necessary for the establishment, implementation and termination of the customer relationship and the fulfilment of the associated contractual obligations or that we are legally obliged to collect are to be provided. Without this data, we will otherwise generally not be able to perform the contract or customer relationship with you.

As a rule, we collect your personal data directly from you. If, exceptionally, data comes from other sources, you will be informed separately.



# 1 Data processing in the context of order processing

## 1.1 Order entry and processing

In order to process your order or request, we collect personal data from contact persons (name, address, e-mail address, telephone number, mobile phone number) as part of the process. Your data will be entered and stored in our central system. The provider of the system is Aptean Germany GmbH, Pforzheimer Str. 128, 76275 Ettlingen

For the written activity planning of our projects, we have a weekly plan, which may also contain personal data in the form of customer master data and project information.

The processing is based on a contract or pre-contractual measure in accordance with Art. 6 (1) (b) GDPR.

This is forwarded internally to the necessary departments and, if necessary, to external bodies (e.g. legal advice, press) that are subject to secrecy / (e.g. shipping service providers/business partners/subcontractors) in order to be able to continue processing the order. We have commissioned an external service provider for the technical support of our IT systems: LAB14 GmbH, Margot-Becke-Ring 8, 69124 Heidelberg. A data processing agreement has been concluded with the service provider.

The data is stored within the framework of the statutory retention obligations. If no contractual relationship is established, your data will be deleted after one year without active contact.

## 1.2 Ordering and Shipping

Personal data is collected for ordering and shipping in order to be able to assign the goods to the customers. If you order directly through us, you will receive a delivery note created by us. For the processing of the shipment, your data (name, address) will be transmitted to the shipping service provider.

The processing is based on a contract or pre-contractual measure in accordance with Art. 6 (1) (b) GDPR.

The data will be passed on to internal bodies as well as to the shipping service provider.

The data is stored within the framework of the statutory retention obligations.

## 1.3 Digital signing of documents

To simplify contract signing, we use digital signature solutions or providers of electronic signatures. We use your e-mail address to send the digital document.

As part of the signing, your digital signature, timestamp and name will be processed and stored.

We use the following provider to carry out the digital signature: DocuSign Germany GmbH, Mies-van-der-Rohe-Straße 6, 80807 Munich.

Your data is processed on the basis of a legitimate interest in accordance with Art. 6 (1) (f) GDPR. The controller pursues the goal of efficient, paperless management and signing of contracts and documents. In addition, the processing is based on the implementation of pre-contractual measures or the performance of a contract in accordance with Art. 6 (1) (b) GDPR. If qualified electronic signatures are used, the processing is also carried out on the basis of legal obligations in accordance with Art. 6 (1) (c) GDPR.

The data is stored internally. A data processing agreement has been concluded with the provider of the signature solution in accordance with Art. 28 GDPR.

The documents and documents are stored in accordance with the statutory retention periods



## 1.4 Communication by e-mail / telephone

To get in touch with you, we will send you an e-mail with further information, to process your request, your order or as part of our general business relationship. For this purpose, your e-mail address, the e-mail content and the history of communication are recorded. The e-mails are hosted by an external service provider. The provider is IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Germany. A data processing agreement has been concluded with the provider.

Furthermore, we can also call you by phone via the telephone or mobile phone number we have on file.

The processing of the data is based on the performance of a contract in accordance with Art. 6 (1) (b) GDPR, which permits the processing of data for the performance of a contract or pre-contractual measures (customer relationship, contracts with business partners).

The data will only be passed on if this has been agreed with you or is necessary for the current business transaction.

Your data will be stored by us on our systems within the framework of the statutory retention obligation.

## 2 Data Processing in IT Systems

### 2.1 Contact and address management

To manage the contact information of our customers and business partners, we store it in our system. The provider of the system is: Salesforce, 415 Mission St FL 3, San Francisco, CA 94105. The following data is processed: name, contact person if applicable, address, telephone number, mobile phone number and e-mail address.

The data is collected on the basis of a legitimate interest in accordance with Art. 6 (1) (f) GDPR in order to be able to manage the contact information in a structured and efficient manner.

Only our employees have access to the system. A data processing agreement has been concluded with the provider of the administrative software in accordance with Art. 28 GDPR.

Your contact details will be stored within the framework of the statutory retention period.

We have entered into a joint controller agreement with the above-mentioned party (Nanoscribe) in accordance with Art. 26 GDPR. The data will only be passed on if this has been agreed with you or is necessary for the current business transaction.

The company is certified according to the "EU-US Data Privacy Framework" (DPF). The DPF is an agreement between the European Union and the USA that is intended to ensure compliance with European data protection standards for data processing in the USA. Every company certified according to the DPF is committed to complying with these data protection standards. Further information on this can be obtained from the provider under the following link: <https://www.dataprivacyframework.gov/list>.

### 2.2 Audio and video conferencing

#### 2.2.1 Data processing

For communication with our customers, we use online conference tools, among other things. The specific tools we use are listed below. If you communicate with us via video or audio conference via the Internet, your personal data will be collected and processed by us and the provider of the respective conference tool.



The conference tools collect all data that you provide/use to use the tools (e-mail address and/or your telephone number). In addition, the conference tools process the duration of the conference, the start and end (time) of participation in the conference, the number of participants and other "contextual information" related to the communication process (metadata).

Furthermore, the provider of the tool processes all technical data required to handle online communication. This includes, but is not limited to, IP addresses, MAC addresses, device IDs, device type, operating system type and version, client version, camera type, microphone or speakers, and the type of connection.

If content is exchanged, uploaded or otherwise made available within the tool, this is also stored on the servers of the tool providers. Such content includes, but is not limited to, cloud recordings, chat/instant messages, voicemails, photos and videos uploaded to voicemails, files, whiteboards, and other information shared while using the Service.

Please note that we do not fully influence the data processing processes of the tools used. Our options are largely based on the corporate policy of the respective provider. Further information on data processing by the conference tools can be found in the privacy policies of the respective tools used, which we have listed below this text.

### 2.2.2 Purpose and legal basis

The conference tools are used to communicate with prospective or existing contractual partners or to offer certain services to our customers (Art. 6 para. 1 lit. b GDPR). Furthermore, the use of the tools serves to generally simplify and accelerate communication with us or our company (legitimate interest within the meaning of Art. 6 para. 1 lit. f GDPR). If consent has been requested, the use of the tools in question is based on this consent; consent can be revoked at any time with effect for the future.

### 2.2.3 Storage period

The data collected directly by us via the video and conference tools will be deleted from our systems as soon as you ask us to delete it, revoke your consent to its storage or the purpose for which it was stored no longer applies. Stored cookies remain on your device until you delete them. Mandatory statutory retention periods remain unaffected.

We have no influence on the storage period of your data, which is stored by the operators of the conference tools for their own purposes. For details, please contact the operators of the conference tools directly.

### 2.2.4 Conference tools used

We use the following conference tools:

#### 2.2.5 Microsoft Teams

We use Microsoft Teams. The provider is Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Details on data processing can be found in the Microsoft Teams privacy policy: <https://privacy.microsoft.com/de-de/privacystatement>.

The company is certified according to the "EU-US Data Privacy Framework" (DPF). The DPF is an agreement between the European Union and the USA that is intended to ensure compliance with European data protection standards for data processing in the USA. Every company certified according to the DPF is committed to complying with these data protection standards. Further information on this can be obtained from the provider under the following link: <https://www.dataprivacyframework.gov/participant/6474>.

## 2.3 Video Conferencing Recording

It is possible to record the online meeting. This serves the purpose of making the online meeting available to you afterwards and viewing the content from the meeting for follow-up. We need your consent for the recording. You can decide at the beginning of the meeting whether or not to allow the recording to take



place. Your consent will be stored in video form. Your name, the content of the conversation and the shared screen content are processed and stored in the recording.

The processing of the data is based on voluntary consent in accordance with Art. 6 (1) (a) GDPR. The data subject can revoke the consent at any time by sending an informal notification. Processing that has already been carried out remains unaffected by the revocation.

The content of the video remains internal.

The recordings will be stored until you revoke your consent.

## 2.4 File exchange via OneDrive / SharePoint

We use OneDrive / SharePoint to exchange files with you. The provider is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA (hereinafter referred to as "OneDrive" or "SharePoint").

OneDrive/SharePoint allows us to include a folder structure on our system where you can upload content. When you upload content, it is stored on the servers of OneDrive /SharePoint. It also connects to OneDrive/SharePoint so that OneDrive/SharePoint can determine that you have visited our system.

The use of OneDrive / SharePoint is based on Art. 6 para. 1 lit. f GDPR. The controller has a legitimate interest in a reliable and efficient data exchange system.

The company is certified according to the "EU-US Data Privacy Framework" (DPF). The DPF is an agreement between the European Union and the USA that is intended to ensure compliance with European data protection standards for data processing in the USA. Every company certified according to the DPF is committed to complying with these data protection standards. For more information, please contact the provider at the following link: <https://www.dataprivacyframework.gov/participant/647>

## 2.5 IT ticket system

To ensure IT support, to prioritize and document requests, we use a ticket tool in IT. When you submit a ticket, we record the following from the processor: surname, first name. From the requester we record: surname, first name, department. Depending on the type of error, personal data may also be included in the error description itself.

The ticket system is provided by Salesforce, 415 Mission St FL 3, San Francisco, CA 94105

The processing of the data is based on a business purpose in accordance with Art. 6 (1) (f) GDPR. The controller has a legitimate interest in optimizing IT processes.

The data will be processed in the IT department and, if necessary, passed on to an external support service provider for processing the case. An order processing agreement was concluded with the external IT support and the provider of the ticket system.

We have entered into a joint controller agreement with the above-mentioned party (Nanoscribe) in accordance with Art. 26 GDPR. The data will only be passed on if this has been agreed with you or is necessary for the current business transaction.

Your personal data will be stored as part of the processing and then deleted. Statutory retention periods remain unaffected.

The company is certified according to the "EU-US Data Privacy Framework" (DPF). The DPF is an agreement between the European Union and the USA that is intended to ensure compliance with European data protection standards for data processing in the USA. Every company certified according to the DPF is committed to complying with these data protection standards. Further information on this can be obtained from the provider under the following link: <https://www.dataprivacyframework.gov/list>.



## 2.6 Guest Wi-Fi

We offer our guests the possibility of internet access. For this purpose, you will receive access to our guest Wi-Fi. You can get access by asking the managing director or a responsible employee.

Your name and the log data will be stored in our system.

The use of the WLAN is based on voluntary consent in accordance with Art. 6 (1) (a) GDPR. You can revoke your consent informally at any time. However, this will result in you no longer being able to use internet access.

The data will only be passed on if this has been agreed with you or is necessary for the current incident. The external service provider LAB14 GmbH, Margot-Becke-Ring 8, 69124 Heidelberg, Germany, was commissioned to provide technical support. A data processing agreement has been concluded with the service provider.

The log data is stored for three months and then deleted from the system.

## 3 Sales & Marketing

### 3.1 Sending newsletters to existing customers

If you order goods or services from us and provide your e-mail address, this e-mail address may subsequently be used by us to send newsletters, provided that we inform you in advance. In such a case, the newsletter will only be used to send direct advertising for its own similar goods or services. You can cancel the sending of this newsletter at any time. For this purpose, there is a corresponding link in every newsletter. In this case, the legal basis for sending the newsletter is Art. 6 para. 1 lit. f GDPR in conjunction with § 7 para. 3 UWG.

After you have unsubscribed from the newsletter distribution list, your e-mail address may be stored in a blacklist by us in order to prevent future mailings to you. The data from the blacklist will only be used for this purpose and will not be merged with other data. This serves both your interest and our interest in complying with the legal requirements when sending newsletters (legitimate interest within the meaning of Art. 6 para. 1 lit. f GDPR). The storage in the blacklist is not limited in time. You can object to the storage if your interests outweigh our legitimate interest.

### 3.2 Exhibition stand

In order to be able to provide you with further information about our companies and offers as well as services after the fair, we will collect the following data from you at our booth: name, e-mail address, telephone number / mobile number. The data is then entered into our CRM system.

The processing is based on a contract or pre-contractual measure in accordance with Art. 6 (1) (b) GDPR.

Only our employees have access to our system.

Your contact details will be stored within the framework of the statutory retention period.



### 3.3 Invitation to company events

Personal data from you will be processed for the planning, organisation and implementation of company events (e.g. summer party, open day, etc.). This serves communication, event coordination and the consideration of individual needs (e.g. food preferences, confirmation of participation).

The following data will be processed: name, e-mail address, participation information (e.g. acceptance or rejection), any special information (e.g. meal requests, accompanying persons).

The processing is carried out on the basis of a legitimate interest in accordance with Art. 6 (1) (f) GDPR in order to enable customers to participate in internal events and to organise them efficiently.

The data will only be passed on to internal organizational units or external service providers who are commissioned to carry out the event.

The data will only be stored for as long as it is necessary for the organisation and implementation of the respective event and will then be deleted, unless there are any statutory retention obligations.

### 3.4 Creation and publication of photos and videos at company events

As part of corporate events, we take photos and videos that are used to document and present our events as well as for public relations. Our customers can also be recognizable in the recordings.

The following personal data will be processed: image and video recordings of the data subjects, if applicable, name and company affiliation (if mentioned in the context of the publication).

The processing is carried out on the basis of a legitimate interest in accordance with Art. 6 (1) (f) GDPR. Our interest lies in the presentation of our events and the promotion of our external presentation to business partners and the public.

The recordings can be published internally (e.g. intranet, presentations) as well as externally (e.g. website, social media, press releases). It cannot be ruled out that third parties may reuse or disseminate the published content.

The data will only be stored and used for as long as it is necessary for the aforementioned purposes or until a justified objection is filed.

## 4 Financial accounting

### 4.1 Sanction list check

EU companies are prohibited from checking and cross-checking employee data and business contacts for matches with the names on the sanctions lists. Sanctions lists are based on various EU regulations (including EU Regulation 2580/2001), the so-called anti-terrorism regulations and contain names of persons, companies and states against which sanctions have been imposed for foreign or security policy reasons. For this purpose, the name of the data subject is processed.

The review is carried out on the legal basis of Art. 6 (1) (c) GDPR or Art. 6 (1) (f) GDPR. The controller has a legitimate interest in not entering into business relationships with sanctioned persons.

The data will only be passed on if this has been agreed with you or is necessary for the current business transaction.

Your data will be stored by us on our systems within the framework of the statutory retention obligation.



## 4.2 Financial accounting / cash register

To handle financial accounting and cash receipts, we mapped a process in the company in our IT systems. In the course of the process, personal data of contact persons or billing information (name, address, e-mail address, telephone number, mobile phone number) may be processed.

The processing is based on a legal requirement in accordance with Art. 6 (1) (c) GDPR. The processing is necessary for compliance with a legal obligation to which the controller is subject (principles of proper accounting).

It will be forwarded to our responsible tax advisor.

The data is stored within the framework of the statutory retention obligations.

## 4.3 Dunning

In the case of outstanding receivables, we reserve the right to send reminders and – in the event of non-payment – to forward them to external service providers (e.g. lawyers or collection agencies) for further processing. The following personal data is required and processed for this purpose: name, address and the amount of the outstanding claim.

Data processing is carried out on the basis of a contractual relationship or pre-contractual measures in accordance with Art. 6 (1) (b) GDPR.

The data will only be passed on to the commissioned service providers (e.g. lawyers, debt collection agencies).

The data is stored in compliance with the statutory retention periods.

# 5 Facility Management

## 5.1 Headquarters, visitor management

For internal organization, the incoming mail is distributed to the respective responsible departments or employees. Personally addressed letters will be forwarded unopened.

Central telephone calls are answered and forwarded to the responsible persons.

Visitors are greeted at the reception and recorded in a visitor list so that they can track which external persons are on the company premises at any time.

The following personal data is collected and processed: name of the employee, name of the business partner or visitor, attendance times of the visitor, signature of the visitor.

The processing of this data is carried out on the basis of a legitimate interest in accordance with Art. 6 (1) (f) GDPR in order to ensure security on the company premises and to grant access only to authorised persons.

The data will only be passed on if this has been agreed with you or is necessary for the processing of a specific business transaction.

The data is stored on our systems in compliance with the statutory retention periods.



## 5.2 Video surveillance system (access protection)

The data is recorded by video cameras in the entrance area of the company premises in order to be able to provide evidence for the law enforcement authority in the event of trespassing.

The processing of the data is based on a business purpose in accordance with Art. 6 (1) (f) GDPR. The controller has a legitimate interest in avoiding or recognizing access to the company premises for rules and criminal offences.

The data will not be stored or passed on. The video material is deleted after 72 hours.

# 6 Miscellaneous

## 6.1 Whistleblower Portal / Reporting to Internal Reporting Office

### 6.1.1 Data processing

With the HinSchG, the Federal Republic of Germany is implementing the requirements of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report violations of Union law ("Whistleblower Protection Directive").

In order to be able to report violations taking into account these objectives and purposes, companies and public bodies that fall within the scope of application are obliged to set up and operate a so-called "reporting office".

As part of the data processing activity "receiving, processing and advising", the following categories of personal data are expected to be processed by the whistleblower officer as the reporting office:

**Whistleblower:** Personal data (name and gender), contact details (private address, private telephone number, private e-mail address; if applicable, also professional contact data), data on professional activity (occupation, employer, function and position at the employer), if applicable, special categories of personal data in accordance with Art. 9 GDPR, if applicable, personal data on criminal offences in accordance with Art. 10 GDPR

**Persons who are the subject of a report:** personal data (name and gender), data on professional activity (occupation, employer, function and position with the employer), information on the conduct that the whistleblower considers to constitute the violation, information on the content of follow-up measures and the result of the investigations triggered by the report, if applicable, special categories of personal data in accordance with Art. 9 GDPR, if applicable. personal data about criminal offences in accordance with Art. 10 GDPR

**Other persons affected by a report:** personal data (name and gender), if applicable, contact details (private address, private telephone number, private e-mail address; if applicable, also professional contact details), data on professional activity (occupation, employer, function and position with the employer), if applicable, special categories of personal data in accordance with Art. 9 GDPR, if applicable, personal data on criminal offences in accordance with Art. 10 GDPR

### 6.1.2 Purpose and legal basis

The purposes of the processing are specifically specified by the legislator in the HinSchG.

The HinSchG itself states that the purpose of the Act is to protect natural persons who have obtained information about violations in connection with their professional activity or in the prior to a professional activity and who report or disclose it to the reporting offices provided for in this Act

(cf. §1 para. 1 HinSchG).



Furthermore, the purpose of the Act is also to protect persons who are the subject of a report or disclosure, as well as other persons who are affected by a report or disclosure (cf. §1 para. 2 HinSchG).

### 6.1.3 Storage period

With the completion of follow-up measures (§18 HinSchG) by the reporting office, the reporting procedure is also concluded.

The data will be deleted three years after the conclusion of the procedure pursuant to §11 (5) HinSchG.

The documentation may be retained for a longer period of time to meet the requirements of this Act or other legislation, as long as this is necessary and proportionate.

This may be the case in particular if internal investigations are ongoing or administrative and/or judicial proceedings have not yet been concluded due to the facts of the report.

## 6.2 Paper and file disposal / data carrier disposal

The destruction of paper documents and data carriers containing personal data that are no longer required is carried out. This means that the deletion periods after the retention period are met.

All data from the customer relationship can be found on the documents and paper carriers.

The processing of the data is based on a legal requirement pursuant to Art. 6 (1) (c) GDPR, the processing is necessary for the fulfilment of a legal obligation to which the controller is subject.

The data will be passed on to the certified disposal company REISSWOLF International GmbH, Wilhelm-Bergner-Straße 3 A, 21509 Glinde, which the controller commissions with the destruction and disposal. A data processing agreement was concluded with the waste disposal company.

## 6.3 Data protection management

You can contact the external data protection officer at any time by e-mail to [info@datenbeschuetzerin.de](mailto:info@datenbeschuetzerin.de) or by phone at 09921 88 22 9000.

Your name, reason for the request, facts, any data stored in the system of the person concerned will be collected and stored.

The processing of the data is based on the performance of a contract in accordance with Art. 6 (1) (b) GDPR, which permits the processing of data for the performance of a contract or pre-contractual measure (service contract, employment contract).

The information will only be passed on with your consent.

Your personal data will be stored for as long as necessary for the purpose. Statutory retention obligations remain unaffected.