
Data Privacy Statement

We are very pleased about your interest in our company.

The topic data security has a particularly high value for the management of FIR e. V. A use of the Internet sides of FIR e. V. is generally possible without any indication of personal data. However, if you wish to take advantage of a special service offered by our company via our Internet pages, it may be necessary to process personal data.

If it is necessary to process personal data and there is no legal basis for such processing, we generally obtain the consent of the data subject. The processing of personal data, such as the name, address, e-mail address or telephone number of a data subject, is always carried out in accordance with the basic data protection regulation and in compliance with the applicable country-specific data protection regulations.

For this reason, you cannot use our website to collect your data without the corresponding confirmation, as we are obliged by the relevant regulations (e.g. the European General Data Protection Regulation and other regulations on data protection) to fulfil the transparency obligations contained therein.

By means of this Data Privacy Statement, our company wishes to inform the public about the type, scope and purpose of the personal data collected, used and processed by us. Furthermore, this Data Privacy Statement informs data subjects of their rights.

FIR e. V. as the controller responsible for the processing has implemented numerous technical and organisational measures to ensure the most complete protection of the personal data processed via these Internet pages. Nevertheless, Internet-based data transmissions can generally have security gaps, so that absolute protection cannot be guaranteed. For this reason, every data subject is free to transmit personal data to us by alternative means, for example by telephone.

Table of Contents

- [1. Definitions](#)
- [2. Name and address of the controller](#)
- [3. Contact details of the data protection officer](#)
- [4. Contact details of the competent supervisory authority for data protection](#)
- [5. Purposes of the processing](#)
- [6. Categories of data](#)
- [7. Recipient of data](#)
- [8. Transfer to a third country](#)
- [9. Collection of general data and information on our Internet pages](#)
- [10. Contact possibility via the Internet pages](#)
- [11. Routine deletion and blocking of personal data](#)
- [12. Rights of the data subject](#)
- [13. Data protection for applications and the application process](#)
- [14. Newsletter](#)
- [15. Allowing the use of cookies](#)
- [16. Function of the web analysis tool MATOMO](#)
- [17. Microsoft Teams](#)
- [18. Online presence in social media](#)
- [19. Legal basis of the processing](#)
- [20. Legitimate interests in the processing pursued by the controller or a third party](#)
- [21. Duration for which the personal data are stored](#)
- [22. Legal or contractual provisions on the provision of personal data](#)
- [23. Existence of an automated decision making process](#)

1. Definitions

The data protection declaration of FIR e. V. is based on the terminology used by the European Directive and Regulation Giver in the adoption of the General Data Protection Regulation (GDPR) and in the “German Act on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and Implementation of Directive (EU) 2016/680 (DSAnpUG-EU)”.

To ensure this, we would like to explain the terms used in advance.

Personal data

Personal data means any information relating to an identified or identifiable natural person (hereinafter referred to as “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, on-line identification, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data subject

Data subject means any identified or identifiable natural person whose personal data are processed by the controller.

Processing

Processing is any operation or set of operations, performed with or without the aid of automated means, which is performed upon personal data, such as collection, recording, organisation, organisation, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restriction of processing

Restriction of processing is the marking of stored personal data with the aim of limiting their future processing.

Profiling

Profiling is any automated processing of personal data consisting of the use of such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects relating to the performance of work, economic situation, health, personal preferences, interests, reliability, conduct, location or change of location of that natural person.

Pseudonymisation

Pseudonymisation is the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to technical and organisational measures which ensure that the personal data is not attributed to an identified or identifiable natural person.

Controller

Controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or national law, the controller or the specific criteria for his designation may be provided for by Union or national law.

Processor

Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient

The recipient is any natural or legal person, public authority, agency or other body to whom personal data are disclosed, whether or not that person is a third party. However, authorities which may receive personal data in the context of a specific investigation mandate under Union or national law shall not be considered as recipients.

Third party

Third party means any natural or legal person, public authority, agency or body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the personal data.

Consent

Consent shall mean any freely given and informed unequivocal expression of the data subject's wishes in the specific case, in the form of a statement or any other unequivocal affirmative act by which the data subject signifies his or her consent to the processing of personal data relating to him or her.

2. Name and address of the controller

The person responsible within the meaning of the Basic Data Protection Regulation, other data protection laws applicable in the Member States of the European Union and other provisions of a data protection nature is

Forschungsinstitut für Rationalisierung e. V. an der RWTH Aachen
Campus-Boulevard 55
52074 Aachen, Germany
Phone: +49 241 47705-0
Fax: +49 241 47705-199

3. Contact details of the data protection officer

Hans-Jürgen Fellgiebel
imatec GmbH
Bickerather Straße 3
52152 Simmerath, Germany
Phone: +49 2473 92879-0
E-mail: datenschutz@fir.rwth-aachen.de

4. Contact details of the competent supervisory authority for data protection

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
(The State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia)
Postfach 20 04 44
40102 Düsseldorf, Germany
Kavalleriestraße 2-4
40213 Düsseldorf, Germany
Phone: +49 211 38424-0
Fax: +49 211 38424-10
E-mail: poststelle@ldi.nrw.de Internet: www.ldi.nrw.de

5. Purposes of the processing

We process your data for the following purposes:

To fulfil a contract concluded with you or to carry out pre-contractual measures (in accordance with Article 6 (1) b) of the EU-GDPR)

such as

- Examination of the conclusion of the contract and the decision on the acceptance of the contract
- Research applications and projects
- Proposal preparation and project processes for industrial projects
- Handling the business
- Invoicing
- Defence or settlement of any liability claims as well as for the assertion of any own claims from the business relationship.

In order to fulfil your wishes, to improve our services and to strengthen the customer relationship, taking into account the consent you have given in the approval in the scope of the Data Privacy Statement (in accordance with Article 6 para 1 a) EU GDPR),

such as

- Sending interesting information about our products and services, satisfaction surveys

To fulfil legal obligations (in accordance with Article 6(1)(c) EU GDPR),

such as

- under the Money Laundering Act
- due to tax regulations and due to employment relationships / administration.

For purposes of legitimate interest (in accordance with Article 6 (1) f) EU GDPR)

such as

- Continuation or reactivation of a business relationship for good cause
- Video surveillance to protect against property damage, personal injury and theft

6. Categories of data

We regularly process the following data in particular within the scope of our business activities:

Last name, first name, title, position/function, company and company address (street with house number, postal code, city), contact details (telephone number, fax number, e-mail address), web address

7. Recipient of data

Your data will be processed within the responsible department by our employees, who are regularly trained and committed to data protection. Furthermore, your data will only be passed on to recipients outside our company in compliance with legal regulations or on the basis of your consent. In order to be able to carry out our business operations (see section 5), we also work together with other companies to whom we transfer your data in specific individual cases. These include in particular the following:

- Service providers for the printing and dispatch of publications and information brochures

- Service providers for the dispatch of digital information
- Service providers for the implementation and accounting of further education offers and events
- Cooperation partners for the implementation of Assessment Centres Contracts for commissioned data processing exist with all service providers.

8. Transfer to a third country

A transfer of your data to a third country (outside the EU) does not take place and is not planned. However, as explained in this privacy policy, we use tools whose providers are partly located in so-called third countries (such as the USA), i.e. countries whose level of data protection does not correspond to that of the European Union. When these tools are active, your personal data may be transferred to the US servers of these companies. We must point out that the USA is not a safe third country within the meaning of EU data protection law. US companies are required to release personal data to security authorities without you as the data subject being able to take legal action against this. The possibility cannot therefore be excluded that US authorities (e.g. secret services) may process, evaluate and permanently store your data on US servers for monitoring purposes. We have no influence over these processing activities.

9. Collection of general data and information on our Internet pages

The web pages of FIR e. V. collect with each call of the web pages by a data subject or an automated system a set of general data and information. This general data and information is stored in the log files of the server.

The following information can be recorded:

- Used browser type and version,
- Operating system used by the accessing system,
- Website from which an accessing system accesses our website (so-called referrer),
- Sub-websites, which are accessed via an accessing system on our Internet pages,
- Date and time of access to the Internet pages,
- Internet Protocol (IP) address,
- Internet service provider of the accessing system and
- Other similar data and information which serve to avert danger in the event of attacks on our information technology systems.

When using this general data and information, our company does not draw any conclusions about the data subject.

This information is rather needed:

- to deliver the contents of our Internet pages correctly,
- to optimise the contents of our internet pages as well as the advertising for them,
- to guarantee the permanent functionality of our information technology systems and the technology of our Internet pages, and
- to provide law enforcement authorities with the information necessary for prosecution in the event of a cyber-attack.

This anonymously collected data and information is evaluated by our company on the one hand statistically and also with the aim of increasing data protection and data security in our company, in order to ultimately ensure an optimum level of protection for the personal data processed by us. The anonymous data of the server log files are stored separately from all personal data provided by a data subject.

10. Contact possibility via the Internet pages

The Internet pages of FIR e. V. contain due to legal regulations data, which make a fast electronic establishment of contact to our enterprise possible as well as a direct communication with us, which likewise covers a general address of the so-called electronic post (E-mail address). Where a data subject contacts the controller by e-mail or via a contact form, the personal data transmitted by the data subject are automatically stored. Such personal data provided voluntarily by a data subject to the controller are stored for the purposes of processing or for contacting the data subject. This personal data will not be passed on to third parties.

11. Routine deletion and blocking of personal data

The controller shall process and store personal data relating to the data subject only for the period of time necessary to achieve the purpose of storage or where provided for by the European legislator or other legislator in laws or regulations to which the controller is subject.

If the purpose of storage ceases to apply or if a storage period prescribed by the European Directive and Regulation Giver or another competent legislator expires, the personal data will be blocked or deleted as a matter of routine and in accordance with the statutory provisions.

12. Rights of the data subject

Right of appeal to the competent supervisory authority

In the event of breaches of the GDPR, data subjects shall have a right of appeal to a supervisory authority, in particular in the Member State of their habitual residence, their place of work or the place of the alleged breach. The right of appeal is without prejudice to other administrative or judicial remedies.

Right to confirmation

Every data subject shall have the right to obtain confirmation from the controller as to whether personal data relating to him or her are being processed.

Right to information

Any data subject concerned by the processing of personal data has the right to obtain at any time and free of charge from the controller information on personal data relating to him/her and a copy thereof. Furthermore, the European Directive and Regulation maker has granted the data subject access to the following information:

- The processing purposes
- The categories of personal data processed,
- The recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular to recipients in third countries or international organisations.
- If possible, the planned duration for which the personal data will be stored or, if this is not possible, the criteria for determining this duration.
- The existence of a right of rectification or erasure of personal data relating to him or her or of a restriction on processing by the controller or a right to object to such processing.
- If the personal data have not been collected from the data subject: All available information about the origin of the data.
- The existence of automated decision-making, including profiling, in accordance with Article 22(1) and (4) of the DPA and, at least in these cases, meaningful information about the logic involved and the scope and intended impact of such processing on the data subject.

The data subject shall also have the right to obtain information as to whether personal data have been transferred to a third country or to an international organisation. If this is the case, the data subject shall also have the right to obtain information on the appropriate guarantees in connection with the transfer.

Right of rectification

Any data subject concerned by the processing of personal data shall have the right to obtain the rectification without delay of inaccurate personal data relating to him/her. Furthermore, the data subject shall have the right to obtain, having regard to the purposes of the processing, the completion of incomplete personal data, including by means of a supplementary declaration.

Right of cancellation (right to be forgotten)

Any data subject concerned by the processing of personal data shall have the right to obtain from the controller the erasure without delay of personal data relating to him/her, where one of the following reasons applies and insofar as the processing is not (or is no longer) necessary

- The personal data has been collected or otherwise processed for purposes for which it is no longer necessary.
- The data subject withdraws his or her consent on which the processing was based pursuant to Art. 6 para. 1 lit. a GDPR or Art. 9 para. 2 lit. a GDPR and there is no other legal basis for the processing.
- The data subject lodges an objection to the processing pursuant to Art. 21 para. 1 GDPR and there are no overriding legitimate reasons for processing, or the data subject lodges an objection to the processing pursuant to Art. 21 para. 2 GDPR.
- The personal data were processed unlawfully.
- The deletion of personal data is necessary to comply with a legal obligation under Union law or the law of the Member States to which the controller is subject.
- The personal data were collected in relation to information society services offered in accordance with Art. 8 para. 1 GDPR.

If any of the above reasons apply and a data subject wishes to request the deletion of personal data, he or she may at any time contact our data protection officer or another employee of the data controller. The data protection officer or another employee will arrange for the deletion request to be complied with.

If the personal data has been made public by FIR e. V. and our company as the responsible party is obliged to delete the personal data in accordance with Art. 17 para. 1 GDPR, we will take reasonable measures, including technical measures, taking into account the available technology and the implementation costs, to inform other controllers who process the published personal data that the data subject has requested these other controllers to delete all links to these personal data or copies or replications of these personal data, unless the processing is necessary. The data protection officer or another member of staff will arrange the necessary steps in individual cases.

Right to restriction of processing

Any data subject concerned by the processing of personal data shall have the right to obtain from the controller the restriction of the processing if one of the following conditions is met:

- The accuracy of the personal data is contested by the data subject, for a period of time that allows the controller to verify the accuracy of the personal data.
- The processing is unlawful, the data subject refuses to have the personal data deleted and instead requests that the use of the personal data be restricted.

- The controller no longer needs the personal data for the purposes of the processing, but the data subject needs them for the purpose of asserting, exercising or defending legal claims.
- The data subject has lodged an objection to the processing pursuant to Art. 21 para. 1 GDPR and it is not yet clear whether the legitimate reasons of the controller outweigh those of the data subject.

If one of the above-mentioned conditions is given and a data subject wishes to request the restriction of personal data stored by FIR e. V., he/she can contact our data protection officer or another employee of the data controller at any time. The data protection officer or another member of staff will arrange for the processing to be restricted.

Right to data portability

Every data subject has the right to obtain, in a structured, standard and machine-readable format, the personal data concerning him/her which have been supplied by the data subject to a controller. The data subject also has the right to transfer these data to another controller without hindrance from the controller to whom the personal data have been made available, provided that the processing is based on the consent pursuant to Art. 6 para. 1 lit. a GDPR or Art. 9 para. 2 lit. a GDPR or on a contract pursuant to Art. 6 para. 1 lit. b GDPR and that the processing is carried out by means of automated procedures, unless the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Furthermore, in exercising their right to data transfer, the data subject has the right, in accordance with Art. 20 para. 1 GDPR, to obtain that personal data be transferred directly from one controller to another controller, insofar as this is technically feasible and provided that it does not adversely affect the rights and freedoms of other persons.

In order to assert the right to data transferability, the data subject may at any time contact the appointed data protection officer or another employee.

Right to object

Any data subject concerned by the processing of personal data has the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her carried out pursuant to Art. 6 para. 1 lit. e or f GDPR. This also applies to profiling based on these provisions.

FIR e. V. shall no longer process the personal data in the event of an objection, unless we can prove compelling reasons for processing worthy of protection which outweigh the interests, rights and freedoms of the data subject, or the processing serves to assert, exercise or defend legal claims. If FIR e. V. processes personal data for the purpose of direct marketing, the data subject shall have the right to object at any time to the processing (with effect for the future) of personal data for the purpose of such marketing. This also applies to profiling, insofar as it is associated with such direct mail. If the data subject objects to the processing for direct marketing purposes, FIR e. V. shall no longer process these personal data for these purposes.

In addition, the data subject has the right to object, for reasons arising from his or her particular situation, to the processing of personal data concerning him or her which is carried out at FIR e. V. for the purposes of scientific or historical research or for statistical purposes in accordance with Art. 89 para. 1 GDPR, unless such processing is necessary for the performance of a task carried out in the public interest.

In order to exercise the right of objection, the data subject may contact the data protection officer or another member of staff directly. The data subject shall also be free to exercise his/her right of

objection in relation to the use of information society services, notwithstanding Directive 2002/58/EC, by means of automated procedures involving technical specifications.

Automated decisions in individual cases including profiling

Any data subject concerned by the processing of personal data shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her in a similar way, granted by the European legislator, provided that the decision

- is not necessary for the conclusion or performance of a contract between the data subject and the controller, or
- is authorised by Union or national legislation to which the controller is subject and that legislation provides for adequate measures to safeguard the rights and freedoms and legitimate interests of the data subject, or
- with the express consent of the data subject. If the decision
- is necessary for the conclusion or performance of a contract between the data subject and the controller, or
- it is carried out with the express consent of the data subject,

FIR e. V. shall take appropriate measures to safeguard the rights and freedoms as well as the legitimate interests of the data subject, which shall include at least the right to obtain the intervention of a person on the part of the controller, to present the own standpoint and to contest the decision.

If the data subject wishes to exercise rights relating to automated decisions, he or she may at any time contact the data protection officer or any other member of the controller's staff.

Right of revocation of a data protection consent

Every data subject affected by the processing of personal data has the right, granted by the European Directive and Regulation Giver, to revoke his or her consent to the processing of personal data at any time.

If the data subject wishes to exercise this right to withdraw consent, he or she may at any time contact our data protection officer or another employee of the controller.

13. Data protection for applications and the application process

The controller collects and processes the personal data of applicants for the purpose of processing the application procedure. The processing may also be carried out by electronic means. This is in particular the case if an applicant submits relevant application documents to the controller by electronic means, such as e-mail or a web form available on the website. If the controller concludes an employment contract with an applicant, the transmitted data is stored for the purpose of processing the employment in compliance with the statutory provisions. Applicant data may be passed on to another area within FIR e. V., if this area also has an open job advertisement with thematic relevance.

The application procedure for research assistants intending to do a doctorate is carried out via an assessment centre in cooperation with the career pool of WZL Aachen PS GmbH. For this purpose, the applicant data is transferred to the career pool and is thus also available to the authorised employees of the companies participating in the assessment centre (currently FIR e. V., the Fraunhofer Institute for Production Technology IPT, the WZL's Production Systematics Research Division and Schuh & Co. GmbH).

If the controller does not conclude an employment contract with the applicant, the application file will be automatically deleted 6 months after the notification of the decision of refusal, unless deletion is contrary to any other legitimate interest of the controller. Other legitimate interests in this sense

include, for example, a duty to provide evidence in proceedings under the General Equal Treatment Act (AGG).

14. Newsletter

If you would like to receive one of the newsletters offered on the website, we need an e-mail address from you as well as information that allows us to verify that you are the owner of the e-mail address provided and that you agree to receive the newsletter. In order to ensure that the newsletter is sent by mutual agreement, we use the so-called double opt-in procedure. In the course of this, the potential recipient can be included in a distribution list. Subsequently, the user receives a confirmation e-mail to confirm the registration in a legally secure manner. The address will only be actively included in the distribution list if confirmation is received.

We use this data exclusively for sending the requested information and offers.

Sendinblue is used as newsletter software. Your data will be transmitted to Sendinblue GmbH. Sendinblue is not allowed to sell your data and use it for other purposes than for sending newsletters. Sendinblue is a German, certified provider, which was selected according to the requirements of the General Data Protection Regulation and the Federal Data Protection Act.

You can find further information here:

<https://de.sendinblue.com/informationen-newsletter-empfaenger/>

You can revoke your consent to the storage of your data, your e-mail address and its use for sending the newsletter at any time, for example by clicking on the “Unsubscribe” link in the newsletter.

Sendinblue enables us to analyse our newsletter campaigns. For instance, it allows us to see whether a newsletter message has been opened and, if so, which links may have been clicked. This enables us to determine, which links drew an extraordinary number of clicks.

Sendinblue also enables us to divide the subscribers to our newsletter into various categories. For instance, newsletter recipients can be categorized based on gender or place of residence. This enables us to tailor our newsletter more effectively to the needs of the respective target groups.

If you do not want Sendinblue to analyse your data, you must unsubscribe from the newsletter. We provide a link for you to do this in every newsletter message.

The data protection measures are always subject to technical innovations; for this reason, we ask you to inform yourself about our data protection measures at regular intervals by consulting our Data Privacy Statement.

15. Allowing the use of cookies

If you agree to the storage and evaluation of your data when visiting one of our websites, you can consent to the storage and use of your data on the respective website with a mouse click by allowing us to use cookies for this website:

You will be asked to agree or decline the use of cookies the first time you visit the respective website. In the former case, a so-called opt-in cookie is stored in your browser, which means that session data can be collected. You can change the setting for the use of cookies at any time by clicking on the blue “Cookie settings” button, which becomes visible by moving the mouse to the bottom of the window. If you delete your cookies in the browser, the opt-in cookie would also be deleted and you would be prompted again to make your desired settings the next time you visit the website.

If you have rejected the use of cookies, you can of course still use our websites to their full extent.

16. Function of the web analysis tool MATOMO

Some of our web pages use the open source software Matomo (<https://matomo.org>) to analyse the website. Matomo uses (only if the surfer has given his/her consent, see 15.) so-called cookies (text files), which are stored on your computer for this purpose. The usage information generated by the cookies is transferred to the server and stored for analysis purposes. Your IP address is immediately anonymised during this process, so that you as a user remain anonymous to us. The server on which the statistical data is stored belongs to a German provider and is also physically located in Germany. The information generated by the cookies about your use of the site will not be disclosed to third parties.

17. Microsoft Teams

We use the 'Microsoft Teams' tool to conduct conference calls, online meetings, video conferences and/or webinars, and online training (hereinafter collectively 'Online Meetings'). 'Microsoft Teams' is software developed by Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 USA. 'Microsoft Teams' is part of the cloud application Office 365, for which a user account must be created.

The legal basis for the processing of data to conduct 'online meetings' via 'Microsoft Teams' is our legitimate interest in the effective conduct of 'online meetings' pursuant to Art. 6 para. 1 lit. f GDPR. Insofar as the 'online meetings' are conducted within the framework of existing contractual relationships, the legal basis is Art. 6 para 1 lit. b GDPR. If we use 'Microsoft Teams' in order to process personal data of our employees, the legal basis for the data processing is Art. 26 of the German Federal Data Protection Act (BDSG).

During an 'online meeting', the following data may be processed under certain circumstances:

- Participant details: display name, if applicable, first name, last name, telephone, email address, password (encrypted for authentication), profile picture;
- Metadata: Meeting topic and description, IP address, participant's phone number, type of device/software or operating system, time of participant's last activity on Teams, number of chat and channel messages, number of meetings attended, duration of audio, video and screen sharing time;
- For chat, or channel message usage: text data for display and logging, if applicable;
- For audio use: microphone recording data;
- For video use: recording data from the video camera;
- For recordings: Audio, video and screen sharing for storage in the cloud / Microsoft Stream;
- For telephone use: incoming and outgoing phone numbers, country name, start and end time, possibly other connection data such as the IP address of the device.

If we intend to record 'online meetings', we will transparently inform you beforehand and - where necessary – request for permission. The fact of the recording will also be displayed in the Teams app. If it is necessary for recording the results of an 'online meeting', we will record the chat content. However, this is generally not the case.

Personal data that is processed in the context of attending 'online meetings' will generally not be forwarded to third parties unless it is intended for disclosure. Please note that the content of 'online meetings', as well as personal meetings is frequently specifically intended for communicating information to third parties, and therefore intended for disclosure.

Microsoft may receive knowledge of the above-mentioned data as part data processing in order to process it. All data traffic is encrypted and data storage generally takes place on servers in the European Union. However, it cannot be ruled out that personal data may be transferred to the USA, although the European Commission has not generally determined a level of data protection for the

USA that is adequate for the EU. Your data may be subject to access by security authorities without adequate legal remedies. Here, the EU Standard Contractual Clauses with further implementation measures are applied as the basis for the transfer.

We have concluded data protection agreements and EU Standard Contractual Clauses with the provider Microsoft to guarantee a minimum level of data protection. Please note that we have no control over Microsoft's data processing operations. To the extent that 'Microsoft Teams' processes personal data in connection with Microsoft's legitimate business operations, Microsoft is the independent data controller for such use and, as such, is responsible for compliance with all applicable laws and obligations of a data controller.

For more information on the purpose and scope of data collection and its processing by Microsoft please refer to Microsoft's privacy policy:

<https://privacy.microsoft.com/en-US/privacystatement>

and Microsoft Teams:

<https://docs.microsoft.com/en-US/microsoftteams/teams-privacy>

18. Online presence in social media

We maintain online presences within social networks and platforms to be able to communicate with the customers, interested parties and users active there and to inform them about our services.

We point out that user data may be processed outside the European Union, especially in the USA. This can result in risks for the users because the enforcement of the users' rights could be made more difficult.

Furthermore, user data is generally processed for market research and advertising purposes. For example, user profiles can be created from the user behaviour and the resulting interests of the users. The user profiles can in turn be used, for example, to place advertisements inside and outside the platforms that presumably correspond to the interests of the users. For these purposes, cookies are usually stored on the users' computers, in which the usage behaviour and interests of the users are stored. Furthermore, data may also be stored in the user profiles regardless of the devices used by the users (especially if the users are members of the respective platforms and are logged in to them).

The processing of users' personal data is based on our legitimate interests in effective information of users and communication with users in accordance with Art. 6 para. 1 lit. f. DSGVO. If the users are asked by the respective providers of the platforms to give their consent to the afore-mentioned data processing, the legal basis for the processing is Art. 6 para. 1 lit. a., Art. 7 DSGVO.

For a detailed presentation of the respective processing and the possibilities of contradiction (opt-out), we refer to the providers listed below.

In the case of requests for information and the assertion of user rights, we would also like to point out that these can most effectively be asserted with the providers. Only the providers have access to the data of the users and can directly take appropriate measures and provide information.

Facebook

We have a profile on Facebook. The data protection officer of Facebook can be reached via this contact form:

<https://www.facebook.com/help/contact/540977946302970>

On this social media platform, we are jointly responsible with Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbor, Dublin 2, Ireland. The joint responsibility can be found in the form of an agreement at https://www.facebook.com/legal/terms/page_controller_addendum

Please note that despite the joint responsibility with the social media portal operators, we do not have full influence on the data processing operations of the social media portals. Our options are determined by the company policy of the respective provider.

You can customise your advertising settings independently in your user account. Click on the following link and log in: <https://www.facebook.com/settings?tab=ads>

You can find Facebook privacy policy at:

<https://www.facebook.com/about/privacy>

and information on the Insight data:

https://www.facebook.com/legal/terms/information_about_page_insights_data

It cannot be excluded that the processing by Facebook Ireland Ltd. will also take place in the United States by Facebook Inc., 1601 Willow Road, Menlo Park, California 94025.

Data transmission to the USA is based on the Standard Contractual Clauses (SCC) of the European Commission. Details can be found here:

https://www.facebook.com/legal/EU_data_transfer_addendum

Instagram

We have a profile on Instagram. The Instagram service is one of the Facebook products provided by Facebook Ireland Ltd. The data protection officer of Instagram can be reached via this contact form:

<https://www.facebook.com/help/contact/540977946302970>

On this social media platform, we are jointly responsible with Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbor, Dublin 2, Ireland. The joint responsibility can be found in the form of an agreement at https://www.facebook.com/legal/terms/page_controller_addendum

Please note that despite the joint responsibility with the social media portal operators, we do not have full influence on the data processing operations of the social media portals. Our options are determined by the company policy of the respective provider.

Details on the processing activities, their suppression, and the deletion of the data processed by Instagram can be found in its privacy policy:

<https://help.instagram.com/519522125107875>

It cannot be excluded that the processing by Facebook Ireland Ltd. will also take place in the United States by Facebook Inc., 1601 Willow Road, Menlo Park, California 94025.

Data transmission to the USA is based on the Standard Contractual Clauses (SCC) of the European Commission. Details can be found here:

https://www.facebook.com/legal/EU_data_transfer_addendum

Twitter

We have a profile on Twitter. The provider is Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland.

You can adjust your Twitter privacy settings independently in your user account. To do so, click on the following link and log in: <https://twitter.com/personalization>

Data transmission to the USA is based on the Standard Contractual Clauses (SCC) of the European Commission. Details can be found here: <https://gdpr.twitter.com/en/controller-to-controller-transfers.html>

The privacy policy of Twitter can be found at:

<https://twitter.com/de/privacy>

YouTube

We have a profile on YouTube. YouTube is a service of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, a subsidiary of Google LLC, 1600 Amphitheater Parkway, Mountain View, CA 94043 USA.

Data transmission to the USA is based on the Standard Contractual Clauses (SCC) of the European Commission. Details can be found here:

<https://privacy.google.com/businesses/controllerterms/mccs/>

The privacy policy of YouTube can be found at:

<https://policies.google.com/privacy>

LinkedIn

We have a LinkedIn profile. The provider is the LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Ireland, a subsidiary of LinkedIn Corporation, 1000 W. Maude Avenue, Sunnyvale, CA 94085, USA. LinkedIn uses advertising cookies.

If you want to disable LinkedIn advertising cookies, please use the following link:

<https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>

Data transmission to the US is based on the Standard Contractual Clauses (SCC) of the European Commission. Details can be found here: <https://www.linkedin.com/legal/l/dpa>

and <https://www.linkedin.com/legal/l/eu-sccs>

The privacy policy of LinkedIn can be found at:

<https://www.linkedin.com/legal/privacy-policy>

XING

We have a profile on XING. The provider is New Work SE, Dammtorstraße 30, 20354 Hamburg, Germany.

The privacy policy of XING can be found at:

<https://privacy.xing.com/en/privacy-policy>

19. Legal basis of the processing

Art. 6 I lit. a GDPR serves our company as a legal basis for processing operations for which we obtain consent for a specific processing purpose.

If the processing of personal data is necessary for the performance of a contract to which the data subject is a party, as is the case, for example, with processing operations necessary for the supply of goods or provision of other services or consideration, the processing is based on Art. 6 I lit. b GDPR. The same applies to such processing operations that are necessary for the performance of pre-contractual measures, for example in cases of enquiries about our products or services.

If our company is subject to a legal obligation which makes the processing of personal data necessary, for example to fulfil tax obligations, the processing is based on Art. 6 I lit. c GDPR.

In rare cases, the processing of personal data might be necessary to protect vital interests of the data subject or another natural person. This would be the case, for example, if a visitor to our company were to be injured and his or her name, age, health insurance details or other vital information had to be passed on to a doctor, hospital or other third party. Then the processing would be based on Art. 6 I lit. d GDPR.

Ultimately, processing operations could be based on Art. 6 I lit. f GDPR. Processing operations not covered by any of the aforementioned legal bases are based on this legal basis if the processing is necessary to safeguard a legitimate interest of our company or of a third party, unless the interests, fundamental rights and freedoms of the data subject prevail. Such processing operations are permitted to us in particular because they have been specifically mentioned by the European legislator. In this respect, it took the view that a legitimate interest could be assumed if the data subject is a customer of the controller (recital 47 sentence 2 GDPR).

20. Legitimate interests in the processing pursued by the controller or a third party

If the processing of personal data is based on Article 6 I lit. f of the GDPR, our legitimate interest is to carry out our business activities in all their forms.

Your personal data is also available to the employees of FIR Aachen GmbH, since the staff of the FIR Aachen GmbH consists of employees of FIR e. V. and FIR Aachen GmbH uses the infrastructure of FIR e. V.

According to Art. 21 para. 4 GDPR you have a right of objection against this legitimate interest. Address your objection directly to us or to our data protection officer. You can find the contact details above.

21. Duration for which the personal data are stored

The criterion for the duration of storage of personal data is the respective legal retention period. After the expiry of this period, the corresponding data is routinely deleted if it is no longer required for the fulfilment or initiation of the contract.

22. Legal or contractual provisions on the provision of personal data

We would like to inform you that the provision of personal data is partly required by law (e.g. tax regulations) or may also result from contractual regulations (e.g. information on the contractual partner). Sometimes it may be necessary for the conclusion of a contract that a data subject provides us with personal data, which must subsequently be processed by us. For example, the data subject is obliged to provide us with personal data if our company concludes a contract with him/her. Failure to provide the personal data would mean that the contract with the data subject could not be concluded.

Before the data subject provides personal data, he or she can contact our data protection officer. Our data protection officer will then inform the data subject on a case-by-case basis whether the provision of the personal data is required by law or contract or necessary for the conclusion of the contract, whether there is an obligation to provide the personal data and what the consequences would be if the personal data were not provided.

23. Existence of an automated decision making process

As a responsible company, we avoid automatic decision making or profiling.

Last update: June 2021