

Privacy Policy

We – K.I.T. Group GmbH including our subsidiaries - are pleased that you are visiting our website. Protecting and securing your personal information while using our website is very important to us. Therefore, we would like to inform you here about which of your personal data we collect when you visit our website and for what purposes it is used. Personal data refers to individual details about the personal or factual circumstances of a specific or identifiable natural person (data subject), such as name, address, email addresses, and user behaviour. These are data that can be used to identify you. Additionally, you will also find occasional information here about data processing activities outside of this website (e.g., video conferences or newsletters).

A. Responsible for Data Processing

Data Controller

For the processing of personal data in accordance with the EU General Data Protection Regulation (GDPR)

K.I.T. Group GmbH

Kurfürstendamm 71

10709 Berlin

Phone: +49 30 24603 0

Email: info@kit-group.org

Data Protection Officer

exkulpa gmbh

Waldfeuchterstr. 266

52525 Heinsberg

Phone: +49 2452 99 33 11

Email: datenschutz@kit-group.org

B. General Information

In addition to the data you actively provide to us on this page (e.g., via our contact form), we collect some technical data. These so-called metadata are automatically transmitted from your computer to our servers as soon as you access our website (including browser, operating system, or timestamp). Such data help us ensure the error-free display of our website. Additionally, we may collect data through integrated third-party providers (e.g., for external media such as map services or analytics tools). We will inform you about the specific purposes and legal bases throughout this privacy policy.

(1) Retention Period

Unless a specific retention period is stated within this privacy policy, we retain your personal data for as long as the purpose of the data processing is applicable. If you submit a legitimate request for deletion or withdraw your consent, we will delete your data. Statutory retention obligations remain unaffected.

(2) Legal Bases for Data Processing

If you have consented to data processing, your personal data will be processed based on Art. 6(1)(a) GDPR or Art. 9(2)(a) GDPR if special categories of data are processed according to Art. 9(1) GDPR. If you have expressly consented to the transfer of personal data to third countries, the data will also be processed in accordance with Art. 49(1)(a) GDPR. If you have consented to the storage of cookies or access to information on your device (e.g., through device fingerprinting), data processing will also occur based on s. 25(1) TDDDG / applicable national law. Your consent can be withdrawn at any time. If your data are necessary for contract fulfilment or pre-contractual measures, we process your data according to Art. 6(1)(b) GDPR. Furthermore, we process your data if necessary to fulfil a legal obligation based on Art. 6(1)(c) GDPR. Data processing may also occur due to our legitimate interests in accordance with Art. 6(1)(f) GDPR. In the following sections of this privacy policy, you will be informed about the respective legal bases in individual cases.

(3) Notice on Data Transfer to Third Countries and US Companies without DPF Certification

Please note that we use tools from companies based in third countries or the USA that are not covered by the EU-US Data Privacy Framework (DPF). When using these tools, your personal data may be transferred to and processed in these countries. Please be aware that in these insecure third countries, a level of data protection comparable to that of the EU cannot be guaranteed.

We wish to clarify that the USA generally offers a level of data protection comparable to that of the EU. Data transfer to the USA is permitted if the recipient has DPF certification or provides appropriate additional guarantees. Information about data transfers to third countries, including data recipients, can be found in our privacy policy.

(4) Automated Decision-Making

Your personal data will not be processed for the purpose of automated decision-making.

(5) Your Rights

As a data subject under the General Data Protection Regulation (GDPR), you have the following rights:

- **Right of access:** You have the right to request confirmation from us as to whether your personal data are being processed and, if so, to obtain further information about the processing and copies of the processed data (Art. 15 GDPR).
- **Right to rectification:** You have the right to request the immediate correction of inaccurate personal data concerning you and, if necessary, the completion of incomplete personal data (Art. 16 GDPR).
- **Right to erasure:** You have the right to request the immediate deletion of personal data concerning you if the legal requirements are met, particularly if the data are no

longer necessary for the purposes pursued and the processing is unlawful (Art. 17 GDPR).

- **Right to restriction of processing:** You have the right to request the restriction of the processing of your personal data from us if the legal requirements are met, particularly if you contest the accuracy of the data, the processing is unlawful, and you oppose deletion (Art. 18 GDPR).
- **Right to data portability:** You have the right to receive the personal data concerning you, which you have provided to us, in a structured, commonly used, and machine-readable format, and you have the right to transmit those data to another controller without hindrance from us, where technically feasible (Art. 20 GDPR).
- **Right to object:** You have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data concerning you if the processing is based on Art. 6(1)(e) or (f) GDPR (Art. 21 GDPR).
- **Right to withdraw consent:** You have the right to withdraw your consent to the processing of personal data at any time with effect for the future. The withdrawal of your consent does not affect the lawfulness of processing based on consent before its withdrawal (Art. 7(3) GDPR).
- **Right to lodge a complaint with a supervisory authority:** You have the right to lodge a complaint with a data protection supervisory authority if you believe that the processing of your personal data violates the GDPR (Art. 77 GDPR).

C. Further Data Processing Procedures

(1) General Information Obligations

This information is directed at customers, prospective clients, suppliers, and employees. We process your personal data for the following purposes:

- To fulfil our contractual obligations to you (Art. 6(1)(b) GDPR).
- To carry out pre-contractual obligations (Art. 6(1)(b) GDPR).
- To respond to enquiries (Art. 6(1)(b) GDPR).
- If you have given us consent to process your personal data for specific purposes (such as receiving our newsletter), the data processing is based on your consent (Art. 6(1)(a) GDPR).
- To comply with legal obligations to which our company is subject (Art. 6(1)(c) GDPR).
- Where necessary, we also process your data to safeguard our legitimate interests, particularly for asserting legal claims and defending in legal disputes, ensuring IT security, consulting and exchanging data with credit agencies to determine credit and default risks, direct marketing and market research unless you have objected to the use of your data for this purpose, in measures for business management and development of services and products, in measures for product and sales

optimisation, in risk management measures, and for the prevention or investigation of criminal offences (Art. 6(1)(f) GDPR).

(2) Categories of Recipients of Personal Data

Within our company, only those employees who need access to the data to perform their tasks have access (need-to-know principle). Individual processes and services are carried out by carefully selected service providers who are commissioned in compliance with data protection regulations and are based within the EEA. If service providers commissioned by us gain access to personal data while performing their services, data processing agreements have been concluded with them in accordance with Art. 28(3) GDPR.

(3) Duration of Data Storage

The data we process is stored for the duration of the existence and execution of the contractual relationship and in compliance with statutory retention periods. These are particularly the commercial and tax retention obligations under the German Commercial Code (HGB) and the Fiscal Code (AO). The regular retention or documentation periods are up to ten years. If no contractual relationship is established, we process the data only as long as the specific purpose requires.

(4) Cookies

Cookies are small text files stored by your browser on your device to retain certain information during your use of the website. Cookies enable us to enhance various aspects of our website and make your visit more comfortable.

There are different types of cookies serving various purposes. Temporary cookies, also known as session cookies, are stored only for the duration of your website visit and are automatically deleted when you close your browser. Persistent cookies, on the other hand, remain on your device for a longer period, allowing us to recognise you and your preferences during repeated visits to the website.

Cookies can also be categorised into first-party cookies and third-party cookies. First-party cookies are set by our website, while third-party cookies are set by other websites or service providers whose content is integrated into our website, such as plugins or analytics tools.

The use of cookies serves various purposes, such as ensuring the website's functionality, saving user settings, creating anonymous statistics about user behaviour, or displaying personalised content and advertising. The legal basis for using cookies varies depending on their purpose. In some cases, the setting of cookies is based on your legitimate interest under Art. 6(1)(f) GDPR, to make our website functional and user-friendly. As website operators, we have a legitimate interest in storing necessary cookies for the technically error-free and optimised provision of our services. When we obtain your consent for the use of cookies, processing is based on Art. 6(1)(a) GDPR in conjunction with s. 25(1) TDDDG. Your consent can be withdrawn at any time.

(5) Consent with Borlabs Cookie

Our website uses the consent technology of Borlabs Cookie to obtain your consent for storing certain cookies in your browser or using certain technologies and to document this in compliance with data protection regulations. The provider is Borlabs - Benjamin A. Bornschein, Rübenkamp 32, 22305 Hamburg (hereinafter Borlabs).

To assign and document your consent or withdrawal, a cookie is set in your browser. This data is stored until you delete the cookie, request us to delete the data, or the purpose for data processing no longer applies. Statutory retention obligations remain unaffected. This data is not shared with the provider of Borlabs Cookie.

Details on data processing by Borlabs Cookie can be found at <https://de.borlabs.io/kb/welche-daten-speichert-borlabs-cookie/>.

The use of the Borlabs Cookie consent technology is to obtain the legally required consents for the use of cookies. The legal basis for this is Art. 6(1)(c) GDPR.

D. Data Processing in Detail

Below, we provide information on the individual processing operations, the scope and purpose of data processing, the legal basis, the obligation to provide your data, and the respective retention period. Automated decision-making, including profiling, does not take place.

(1) Provision of the Website

When you access and use our website, we collect personal data that your browser automatically transmits to our server. The following information is temporarily stored in a so-called log file:

- IP address of the requesting computer
- Date and time of access
- Name and URL of the retrieved file
- Website from which access is made (referrer URL)
- Browser used and, if applicable, the operating system of your computer, as well as the name of your access provider

Our website is not hosted by us directly but by a service provider who processes the aforementioned data on our behalf in accordance with Art. 28 GDPR for the purpose of providing the website.

The use of the hosting provider is for the purpose of fulfilling contracts with our potential and existing customers (Art. 6(1)(b) GDPR) and in the interest of a secure, fast, and efficient provision of our online offering by a professional provider (Art. 6(1)(f) GDPR).

We use the following hosting provider:

Host Europe GmbH

c/o WeWork

Friesenplatz 4

50672 Cologne

(2) Contact Form

Type and Scope of Processing

If you send us enquiries (e.g. via contact form, email, or telephone), we store all data arising from this (e.g. name, email address, subject of the enquiry, etc.). We require this data to process your enquiry and to respond to any follow-up questions. We do not share this data without your consent.

Purpose and Legal Basis

The processing of this data is based on Art. 6(1)(b) GDPR, provided your enquiry is related to the fulfilment of a contract or is necessary for pre-contractual measures. Otherwise, the processing is based on our legitimate interest in effectively handling enquiries directed to us (Art. 6(1)(f) GDPR) or on your consent (Art. 6(1)(a) GDPR) if you have given it previously.

Retention Period

The data you enter in the contact form remains with us until you request its deletion, withdraw your consent for storage, or the purpose for data storage no longer applies (e.g. after your enquiry has been processed). Mandatory legal provisions – especially retention periods – remain unaffected.

(3) Contact Form for Applicants

Nature and Scope of Processing

We collect and process personal data from applicants. Such data processing may also occur electronically, for example, when applicants submit application documents via email or through a web form available on our website. We offer you the option to submit applications for advertised job vacancies via email on our website.

Purpose and Legal Basis

We process applicants' personal data in accordance with legal requirements for the purpose of initiating an employment relationship (Art. 6(1)(b) GDPR). You are not obliged to provide us with this data. However, without this data, we cannot conduct an application process with you.

If the application is successful, the data you submitted will be stored in our data processing systems based on Art. 6(1)(b) GDPR, and if you provide us with special categories of personal data such as health information, based on Art. 9(2)(b) for the purpose of conducting the employment relationship.

For the purpose of contacting potential applicants, we also use services from professional networks LinkedIn and XING. The operators of these networks act as processors on our behalf according to our instructions. The legal basis for data processing when contacting potential applicants on our behalf is Art. 6(1)(f) GDPR (our legitimate interests). If you send us your application following such contact, we process your data for the purpose of initiating an employment relationship as described above based on Art. 6(1)(b) GDPR.

Retention Period

In the event of a rejection, your data will be stored for a period of 6 months beyond the conclusion of the application process. This is to protect our legitimate interests, to assess

whether we need the data to defend against any claims related to the application process. Subsequently, we are obliged to delete or anonymise your data. In this case, the data will only be available to us as so-called metadata without direct personal reference for statistical evaluations (e.g., proportion of female or male applicants, number of applications per period, etc.).

If it becomes apparent that further storage of the data beyond the 6-month period is necessary to protect our legitimate interests (e.g., due to a pending or threatened legal dispute), deletion will only occur when the purpose for further retention ceases. The legal basis for this further data storage is our legitimate interests in asserting, exercising, or defending civil law claims (Art. 6(1)(f) GDPR in conjunction with s. 24(1)(2) BDSG or, where special categories of personal data are stored, Art. 9(2)(f) GDPR in conjunction with s. 24(2) BDSG).

Inclusion in the Applicant Pool

As part of the application process, we offer applicants the opportunity to be included in our "Talent Pool" for a period of 24 months based on consent in accordance with Art. 6(1)(a), Art. 9(2)(a) GDPR. If you have provided special categories of personal data in your application, such as health information, your consent also extends to this data. You are not obliged to provide us with your application data for our Talent Pool. However, without this data, we cannot consider you for future advertised positions unless you submit a new application.

Consent to the inclusion of application data in the Talent Pool is voluntary and can be withdrawn at any time with effect for the future. Withdrawal of consent does not affect the lawfulness of data processing carried out based on consent before its withdrawal.

Your application documents in the Talent Pool will be deleted at the latest after the storage period expires, or in the event of a withdrawal or acceptance of a job offer with one of the companies responsible for the Talent Pool.

If you receive and accept an offer of employment with us during the application process, we or the respective company will store the personal data collected during the application process for the purpose of conducting the employment relationship. The legal basis for this data processing is Art. 6(1)(b) GDPR or, if you provide us with special categories of personal data such as health information, Art. 9(2)(b).

E. Presence on Social Media Platforms

We operate public profiles on various social networks through our website. More detailed information about the social networks we use can be found in the relevant sections of our privacy policy.

Social networks like Facebook, X (formerly Twitter), and others can comprehensively analyse your user behaviour when you visit their websites or a website with integrated social media content (e.g., like buttons or advertising banners). Visiting our social media presences triggers numerous data protection-related processing operations:

If you are logged into your social media account and visit our social media presence, the operator of the social media portal can associate this visit with your user account. However, your personal data may also be collected even if you are not logged in or do not have an

account with the respective social media portal. This data collection occurs, for example, through cookies stored on your device or by capturing your IP address.

With the data collected in this way, the operators of the social media portals can create user profiles in which your preferences and interests are stored. This allows interest-based advertising to be displayed to you both within and outside the respective social media presence. If you have an account with the respective social network, interest-based advertising can be displayed on all devices on which you are or were logged in.

Please note that we cannot track all processing activities on social media portals. Depending on the provider, additional processing operations may be carried out by the operators of the social media portals. For details, please refer to the terms of use and privacy policies of the respective social media portals.

Legal Basis for Data Processing

Our social media appearances aim to ensure the broadest possible presence on the internet. This constitutes a legitimate interest within the meaning of Art. 6(1)(f) GDPR. The analysis processes initiated by the social networks may be based on different legal grounds, which must be specified by the operators of the social networks (e.g., consent within the meaning of Art. 6(1)(a) GDPR).

Controller and Assertion of Rights

When visiting our social media presences (e.g., Facebook), we are jointly responsible with the operator of the social media platform for the data processing operations triggered during this visit. You can generally assert your rights (access, rectification, deletion, restriction of processing, data portability, and complaint) both against us and against the operator of the respective social media portal (e.g., against Facebook).

Despite the joint responsibility with the social media portal operators, we do not have full influence over the data processing operations of the social media portals. Our options are largely determined by the corporate policy of the respective provider.

Retention Period

The data directly collected by us via the social media presence will be deleted from our systems as soon as you request us to delete it, withdraw your consent for storage, or the purpose for data storage no longer applies. Stored cookies remain on your device until you delete them. Mandatory legal provisions – especially retention periods – remain unaffected.

We have no influence on the retention period of your data, which is stored by the operators of the social networks for their own purposes. For details, please refer directly to the operators of the social networks (e.g., via their privacy policy, see below).

(1) Facebook Page

Our company maintains a profile on Facebook. The service provider is Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland (hereinafter Meta). According to Meta, the collected data is also transferred to the USA and other third countries.

We have entered into a joint processing agreement (Controller Addendum) with Meta. This agreement specifies which data processing operations we or Meta are responsible for when

you visit our Facebook page. You can view the agreement at the following link:
https://www.facebook.com/legal/terms/page_controller_addendum.

You can independently adjust your advertising settings in your user account. To do this, click on the following link and log in: <https://www.facebook.com/settings?tab=ads>.

The company is certified under the "EU-US Data Privacy Framework" (DPF), an agreement between the European Union and the USA aimed at ensuring compliance with European data protection standards in data processing in the USA. Certification under the DPF obliges companies to adhere to these data protection standards.

The data transfer to the USA is based on the EU Commission's Standard Contractual Clauses. Details can be found here: https://www.facebook.com/legal/EU_data_transfer_addendum and <https://de-de.facebook.com/help/566994660333381>.

For further information, please refer to Facebook's privacy policy:
<https://www.facebook.com/about/privacy/>.

(2) Instagram Page

Our company maintains a profile on Instagram. The service provider is Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

The company is certified under the "EU-US Data Privacy Framework" (DPF), an agreement between the European Union and the USA aimed at ensuring compliance with European data protection standards when processing data in the USA. Certification under the DPF obliges companies to adhere to these data protection standards.

Data transfer to the USA is based on the EU Commission's Standard Contractual Clauses. Details can be found here: https://www.facebook.com/legal/EU_data_transfer_addendum, <https://help.instagram.com/519522125107875> and <https://de-de.facebook.com/help/566994660333381>.

For further information on how your personal data is handled, please refer to Instagram's privacy policy: <https://help.instagram.com/519522125107875>.

(3) X (formerly Twitter Page)

Our company uses the microblogging service X (formerly Twitter). The provider is Twitter International Unlimited Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland.

You can independently adjust your X privacy settings in your user account; to do so, log in at the following link: <https://x.com/settings/account/personalization>.

The company is certified under the "EU-US Data Privacy Framework" (DPF), an agreement between the European Union and the USA aimed at ensuring compliance with European data protection standards when processing data in the USA. Certification under the DPF obliges companies to adhere to these data protection standards.

Data transfer to the USA is based on the EU Commission's standard contractual clauses. Details can be found here: <https://gdpr.x.com/en/controller-to-controller-transfers.html>.

For further information, please refer to X's privacy policy: <https://x.com/de/privacy>.

(4) LinkedIn Page

Our company has a profile on LinkedIn. The provider is LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Ireland. LinkedIn uses advertising cookies.

If you wish to disable LinkedIn advertising cookies, please use the following link:
<https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>.

The company is certified under the "EU-US Data Privacy Framework" (DPF), an agreement between the European Union and the USA aimed at ensuring compliance with European data protection standards when processing data in the USA. Certification under the DPF obliges companies to adhere to these data protection standards.

Data transfer to the USA is based on the EU Commission's Standard Contractual Clauses. Details can be found here: <https://www.linkedin.com/legal/l/dpa> and <https://www.linkedin.com/legal/l/eu-sccs>.

For more information on how your personal data is handled, please refer to LinkedIn's privacy policy: <https://www.linkedin.com/legal/privacy-policy>.

(5) YouTube

We have a profile on YouTube. The provider is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. You can find details on how they handle your personal data in YouTube's privacy policy: <https://policies.google.com/privacy?hl=en>.

The company is certified under the "EU-US Data Privacy Framework" (DPF), an agreement between the European Union and the USA aimed at ensuring compliance with European data protection standards when processing data in the USA. Certification under the DPF obliges companies to adhere to these data protection standards.

F. Video Conferences

Data Processing

We use online conferencing tools to communicate with our clients. The specific tools we use are listed below. When you communicate with us via video or audio conference, your personal data is collected and processed by us and the provider of the respective tool.

The tools collect the data you provide, including your email address and telephone number. They also process the duration of the conference, when you participated, the number of participants, and other metadata.

Additionally, the provider of the tool processes all technical data necessary for conducting the conference. This includes, in particular, IP addresses, MAC addresses, device IDs, device type, operating system type and version, client version, camera type, microphone or speaker, and the type of connection.

If you share content using this service, it will be stored on the providers' servers. This includes cloud recordings, chat messages, voice messages, as well as photos and videos you have shared during the use of this service.

Please note that we do not have full control over the data processing operations of the tools used. For more detailed information on data processing by the conferencing tools, please refer to the privacy policies of the respective tools used.

Purpose and Legal Basis

The conferencing tools are used to communicate with prospective or existing contractual partners or to offer certain services to our clients (Art. 6(1)(b) GDPR). Furthermore, the use of the tools serves the general simplification and acceleration of communication with us or our company (legitimate interest within the meaning of Art. 6(1)(f) GDPR). If you have previously given consent for data processing, your data will be processed solely on the basis of Art. 6(1)(a) GDPR; consent can be withdrawn at any time.

Retention Period

The data directly collected by us via the video and conferencing tools will be deleted from our systems as soon as you request us to delete it, withdraw your consent for storage, or the purpose for data storage 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 retention period of your data stored by the operators of the conferencing tools for their own purposes. For details, please consult the operators of the conferencing tools directly.

G. Third-Party Services and Tools

(1) Google Tag Manager

We use services and features from Google Tag Manager on this website, offered by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

Google Tag Manager is a tool that allows us to deploy other tools on our website. It does not create user profiles, store cookies, or conduct independent analyses. However, your IP address is collected and may be transferred to the United States. Google Tag Manager itself is only used for managing these tools that are integrated through it.

Purpose & Legal Basis

When using Google Tag Manager on this website, we rely on Art. 6(1)(f) GDPR as the legal basis, as we have a legitimate interest in implementing and managing tracking tools on this website easily and quickly. If you have previously given consent for data processing on this website via Google Tag Manager, your data will be processed solely on the legal basis of Art. 6(1)(a) GDPR in conjunction with s. 25(1) TDDDG / applicable national law. You can withdraw your consent at any time.

The company is certified under the "EU-US Data Privacy Framework" (DPF), an agreement between the European Union and the United States aimed at ensuring compliance with European data protection standards when processing data in the United States. Certification under the DPF obliges companies to adhere to these data protection standards. For more information, please visit: <https://www.dataprivacyframework.gov/s/participant-search/participant-detail?contact=true&id=a2zt000000001L5AAI&status=Active>

(2) Google reCAPTCHA

This website uses Google reCAPTCHA. The provider is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

Nature and Scope of Data Processing

reCAPTCHA is used to check whether data entered on this website (e.g., in a contact form) is done by a human or an automated program. Google reCAPTCHA analyses the behaviour of the website visitor based on various characteristics. The analysis starts automatically as soon as the visitor accesses the website. Data collected during the analysis, such as the IP address, the duration of the website visit, or mouse movements, are forwarded to Google.

Website visitors are not informed that an analysis is taking place; it runs entirely in the background.

Legal Basis

The storage and analysis of data are based on our legitimate interest in protecting our web offerings from abusive automated surveillance and SPAM (Art. 6(1)(f) GDPR). If consent has been requested, data processing is carried out exclusively on the basis of your consent according to Art. 6(1)(a) GDPR and s. 25(1) TDDDG / applicable national law. This consent can be withdrawn at any time.

You can find Google's privacy policy and terms of use at the following links:

<https://policies.google.com/privacy?hl=en> and <https://policies.google.com/terms?hl=en>.

The company is certified under the "EU-US Data Privacy Framework" (DPF), an agreement between the European Union and the United States aimed at ensuring compliance with European data protection standards when processing data in the USA. Certification under the DPF obliges companies to adhere to these data protection standards. Further information is available at: <https://www.dataprivacyframework.gov/s/participant-search/participant-detail?contact=true&id=a2zt000000001L5AAI&status=Active>

(3) AWS S3

Type and Scope of Processing

We use AWS S3 to properly provide the content of our website. AWS S3 is a service by Amazon Web Services, Inc., which functions as a Content Delivery Network (CDN) on our website.

A CDN helps to deliver content from our online offering, particularly files such as graphics or scripts, more quickly using regionally or internationally distributed servers. When you access this content, you connect to servers of Amazon Web Services, Inc., during which your IP address and possibly browser data such as your user agent are transmitted. These data are processed solely for the aforementioned purposes and to maintain the security and functionality of AWS S3.

Purpose and Legal Basis

The use of the Content Delivery Network is based on our legitimate interests, i.e., interest in a secure and efficient provision as well as the optimisation of our online offering in accordance with Art. 6(1)(f) GDPR.

We intend to transfer personal data to third countries outside the European Economic Area, particularly the USA. Data transfers to the USA are carried out under Art. 45(1) GDPR based on the European Commission's adequacy decision. The involved US companies and/or their US subcontractors are certified under the EU-U.S. Data Privacy Framework (EU-U.S. DPF).

In cases where no adequacy decision by the European Commission exists (including US companies not certified under the EU-U.S. DPF), we have agreed on other appropriate safeguards with the data recipients in accordance with Art. 44 et seq. GDPR. These are, unless otherwise specified, the EU Commission's standard contractual clauses pursuant to Implementing Decision (EU) 2021/914 of 4 June 2021. You can view a copy of these standard contractual clauses at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN>.

Additionally, we obtain your consent for such third-country transfers under Art. 49(1)(a) GDPR, which you provide via the consent manager (or other forms, registrations, etc.). We inform you that third-country transfers may involve unknown risks in detail (e.g., data processing by the third country's security authorities, the exact scope and consequences of which we do not know, cannot influence, and of which you may not be aware).

Retention Period

The specific retention period of the processed data is not within our control but is determined by Amazon Web Services, Inc. Further information can be found in the privacy policy for AWS S3: <https://aws.amazon.com/privacy/>.

(4) Adobe Typekit

To design our website according to uniform design standards, we use Web Fonts from Adobe Typekit. This service is provided by Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA (Adobe).

Nature and Scope of Data Processing

When you access our website, the required fonts are loaded directly into your browser from Adobe Typekit to ensure correct display on your device. During this process, your browser connects to Adobe's servers in the USA, allowing Adobe to know that our website was accessed via your IP address. According to Adobe, no cookies are stored in this process.

Legal Basis

The storage and processing of data are based on Art. 6(1)(f) GDPR, as we, as website operators, have a legitimate interest in the uniform presentation of fonts on our website. If consent for the processing of personal data (e.g., for the storage of cookies) has been given, data processing is carried out exclusively on the basis of Art. 6(1)(a) GDPR; this consent can be withdrawn at any time.

Your personal data is transferred to the USA and relies on the EU Commission's standard contractual clauses. Further information can be found at:

<https://www.adobe.com/de/privacy/eudatatransfers.html>.

To ensure that personal data is processed according to our instructions and in compliance with the GDPR, we have concluded a data processing agreement with the provider.

Further information about Adobe Typekit and its privacy policies can be found at:

<https://www.adobe.com/de/privacy/policies/adobe-fonts.html> and

<https://www.adobe.com/de/privacy/policy.html>.

(5) MailChimp

We use the services of Mailchimp on our website, provided by The Rocket Science Group LLC, 675 Ponce De Leon Ave NE, Suite 5000, Atlanta, GA 30308, USA, for organising and analysing the dispatch of newsletters. The data you enter for subscribing to the newsletter, such as your email address, is stored on Mailchimp's servers in the USA.

Mailchimp enables us to analyse the effectiveness of newsletter campaigns. When you open an email sent by Mailchimp, a file contained in the email (known as a web beacon) connects to Mailchimp's servers in the USA. This allows us to determine whether the newsletter message was opened and which links in the email were clicked. Additionally, technical information such as the time of retrieval, IP address, browser type, and operating system is collected. This data cannot be attributed to individual newsletter recipients and is used solely for statistical evaluations. These evaluations help us tailor future newsletters to the interests of the recipients.

If you do not wish for Mailchimp to conduct this analysis, you must unsubscribe from our newsletter. We provide an unsubscribe link in every newsletter for this purpose. Data processing is based on your consent in accordance with Art. 6(1)(a) GDPR. You can withdraw this consent at any time by unsubscribing from the newsletter. The legality of data processing operations already carried out remains unaffected by this withdrawal.

Your data will be retained by us for the purpose of newsletter subscription and will be deleted both by us and the newsletter service provider once you unsubscribe from the newsletter. Data stored for other purposes remains unaffected.

Upon unsubscribing from the newsletter distribution list, your email address may be stored by us or the newsletter service provider in a so-called blacklist to prevent future mailings. The data from the blacklist is used solely for this purpose and is not combined with other data. This serves both your interest and our interest in complying with legal requirements for sending newsletters, in accordance with the legitimate interest under Art. 6(1)(f) GDPR. Storage in the blacklist is indefinite. You may object to this storage if your interests outweigh our legitimate interest. For more information on Mailchimp's privacy practices, please visit: <https://mailchimp.com/legal/terms/>.

The company is certified under the "EU-US Data Privacy Framework" (DPF), an agreement between the European Union and the USA aimed at ensuring compliance with European data protection standards when processing data in the USA. Certification under the DPF obliges companies to adhere to these data protection standards.

Data transfer to the USA is based on the EU Commission's standard contractual clauses. Details can be found at <https://mailchimp.com/eu-us-data-transfer-statement/> and https://mailchimp.com/legal/data-processing-addendum/#Annex_C_-_Standard_Contractual_Clauses.

To ensure that personal data is processed according to our instructions and in compliance with the GDPR, we have concluded a data processing agreement with the provider.

(6) accessWidget

Type and Scope of Processing

We use accessWidget to properly provide our website. accessWidget enables us to offer an accessible web presence through features such as a screen reader, keyboard navigation, or simple design adjustments from the user's side.

When you access these contents, you establish a connection to the servers of accessiBe Inc., during which your IP address and possibly browser data such as your user agent are transmitted. These data are processed solely for the aforementioned purposes and to maintain the security and functionality of accessWidget.

Purpose and Legal Basis

The use of accessWidget is based on our legitimate interests, i.e., the interest in optimising and providing our online offering in an accessible manner in accordance with Art. 6(1)(f) GDPR.

Retention Period

The specific retention period of the processed data is not within our control but is determined by accessiBe Inc. Further information can be found in the privacy policy for accessWidget: <https://accessibe.com/privacy-policy>.