

Privacy Policy

1. Introduction

With the following information, we would like to provide you as the "data subject" with an overview of how your personal data is processed by us and your rights under data protection laws. In general, the use of our website is possible without entering personal data. However, if you wish to make use of special services offered by our company via our website, the processing of personal data may become necessary. If the processing of personal data is required and there is no legal basis for such processing, we generally obtain your consent.

The processing of personal data, such as your name, address, or email address, is always carried out in accordance with the General Data Protection Regulation (GDPR) and in compliance with the country-specific data protection regulations applicable to "1cc GmbH". Through this privacy policy, we aim to inform you about the scope and purpose of the personal data we collect, use, and process.

As the data controller, we have implemented numerous technical and organizational measures to ensure the most complete protection of personal data processed through this website. Nevertheless, internet-based data transmissions can generally have security vulnerabilities, so absolute protection cannot be guaranteed. For this reason, you are free to transmit personal data to us via alternative means, such as by telephone or postal mail.

You can also take simple and easy-to-implement measures to protect yourself against unauthorized access to your data by third parties. Therefore, we would like to give you some tips on securely handling your data:

- Protect your account (login, user, or customer account) and your IT system (computer, laptop, tablet, or mobile device) with secure passwords.
- Only you should have access to your passwords.
- Ensure that you use your passwords only for one account (login, user, or customer account).
- Do not use the same password for different websites, applications, or online services.
- Especially when using publicly accessible or shared IT systems: Always log out after using a website, application, or online service.

Passwords should consist of at least 12 characters and be chosen so that they cannot be easily guessed. Therefore, they should not contain common words from everyday life, your own name, or the names of relatives, but should include upper and lower case letters, numbers, and special characters.

2. Data Controller

The controller within the meaning of the GDPR is:

1cc GmbH

Max-Eyth-Str. 35, 71088 Holzgerlingen, Deutschland

Telephone: +49 7031-4 39 38-0

E-mail: info@1cc-consulting.com

Representative of the controller: Meike Ruoff

3. Data Protection Officer

You can contact the data protection officer as follows:

Michael Weinmann

Telephone: +49 173 7632962

E-mail: michael.weinmann@dsb-office.de

If you have any questions or suggestions on the subject of data protection, you can contact our data protection officer directly at any time.

4. Definitions

This privacy policy is based on the terminology used by the European legislator for the adoption of the General Data Protection Regulation (GDPR). Our privacy policy should be easy to read and understand for both the public and our customers and business partners. To ensure this, we would like to first explain the terminology used.

In this privacy policy, we use, among others, the following terms:

1. Personal Data

Personal data refers to any information relating to an identified or identifiable natural person. 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, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

2. Data Subject

A data subject is any identified or identifiable natural person whose personal data is processed by the data controller (our company).

3. Processing

Processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

4. Restriction of Processing

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

5. Profiling

Profiling refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

6. Pseudonymization

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

7. Processor

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

8. Recipient

A recipient is a natural or legal person, public authority, agency, or another body, to which personal data are disclosed, whether a third party or not. However, public authorities that may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients.

9. Third Party

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

10. Consent

Consent of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

5. Legal Basis for Processing

Article 6(1)(a) GDPR (in conjunction with Section 25(1) TDDDGD (formerly TTDSGD)) serves as the 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 you are a party, as is the case, for example, with processing operations required for the delivery of goods or the provision of any other service or consideration, the processing is based on Article 6(1)(b) GDPR. The same applies to processing operations necessary to carry out pre-contractual measures, such as in the case of inquiries about our products or services.

If our company is subject to a legal obligation that requires the processing of personal data, such as for the fulfillment of tax obligations, the processing is based on Article 6(1)(c) GDPR.

In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or another natural person. This would be the case, for example, if a visitor were injured on our premises and their name, age, health insurance details, or other vital information had to be passed on to a doctor, hospital, or other third party. In such a case, the processing would be based on Article 6(1)(d) GDPR.

Ultimately, processing operations could be based on Article 6(1)(f) GDPR. This legal basis is used for processing operations that are not covered by any of the aforementioned legal grounds if the processing is necessary to protect the legitimate interests of our company or a third party, provided that the interests, fundamental rights, and freedoms of the data subject do not override these interests. Such processing operations are particularly permitted because they have been specifically mentioned by the European legislator. In this respect, the legislator took the view that a legitimate interest could be assumed if you are a customer of our company (Recital 47 Sentence 2 GDPR).

Our services are generally aimed at adults. Persons under the age of 16 may not transmit personal data to us without the consent of their parents or guardians. We do not request personal data from children and adolescents, do not collect it, and do not pass it on to third parties.

6. Transfer of Data to Third Parties

our personal data will not be transferred to third parties for purposes other than those listed below.

We only share your personal data with third parties if:

1. You have given your explicit consent in accordance with Article 6(1)(a) GDPR,
2. The transfer is permissible under Article 6(1)(f) GDPR to protect our legitimate interests, and there is no reason to assume that you have an overriding legitimate interest in not disclosing your data,
3. There is a legal obligation for the transfer under Article 6(1)(c) GDPR, and
4. It is legally permissible and necessary for the processing of contractual relationships with you under Article 6(1)(b) GDPR.

In the context of the processing operations described in this privacy policy, personal data may be transferred to the USA. Companies in the USA only have an adequate level of data protection if they are certified under the EU-US Data Privacy Framework, thus the EU Commission's adequacy decision under Article 45 GDPR applies. We have explicitly named the affected service providers in the privacy policy. To protect your data in all other cases, we have entered into data processing agreements based on the European Commission's Standard Contractual Clauses. If the Standard Contractual Clauses are not sufficient to ensure an adequate level of security, your consent under Article 49(1)(a) GDPR can serve as the legal basis for the transfer to third countries. This does not apply to data transfers to third countries for which the European Commission has issued an adequacy decision under Article 45 GDPR.

7. Technology

7.1 SSL/TLS Encryption

This site uses SSL or TLS encryption to ensure the security of data processing and to protect the transmission of confidential content, such as orders, login data, or contact requests that you send to us as the operator. You can recognize an encrypted connection by the change in the address line of your browser from "http://" to "https://" and by the lock symbol in your browser line.

We use this technology to protect your transmitted data.

7.2 Data Collection when visiting the website

When you use our website for informational purposes only, without registering, transmitting information to us, or consenting to processing that requires consent, we only collect the data that is technically necessary to provide the service. These are typically data that your browser transmits to our server ("in so-called server log files"). Each time you access a page on our website, either directly or via an automated system, a series of general data and information is collected and stored in the server log files. The data collected may include:

1. Browser types and versions used,
2. The operating system used by the accessing system,
3. The website from which an accessing system reaches our website (so-called referrer),
4. The subpages that are accessed on our website,
5. The date and time of access to the website,
6. A truncated Internet Protocol address (anonymized IP address), and
7. The Internet service provider of the accessing system.

When using this general data and information, we do not draw any conclusions about your person. This information is instead required to:

1. Deliver the content of our website correctly,
2. Optimize the content of our website as well as its advertising,
3. Ensure the long-term functionality of our IT systems and the technology of our website, and
4. Provide law enforcement authorities with the necessary information for prosecution in the event of a cyber attack.

Therefore, the collected data and information are evaluated statistically and with the aim of increasing data protection and data security in our company to ultimately ensure an optimal level of protection for the personal data we process. The anonymous data from the server log files are stored separately from any personal data provided by a data subject.

The legal basis for data processing is Article 6(1)(f) GDPR. Our legitimate interest follows from the purposes listed above for data collection.

7.3 Cloudflare (Content Delivery Network)

Our website uses functions provided by CloudFlare. The service provider is CloudFlare, Inc., located at 665 3rd St. #200, San Francisco, CA 94107, USA. CloudFlare offers a globally distributed Content Delivery Network (CDN) with DNS services. Technically, the information transfer between your browser and our website is routed through CloudFlare's network. This

allows CloudFlare to analyze the data traffic between users and our website to detect and defend against attacks on our services. Additionally, CloudFlare may store cookies on your computer to optimize and analyze its services.

You can configure your browser to inform you about the setting of cookies and allow cookies only in individual cases, exclude the acceptance of cookies for specific cases or generally, and activate the automatic deletion of cookies when closing the browser. However, disabling cookies may limit the functionality of this website.

We have entered into a data processing agreement with CloudFlare based on the GDPR and EU Standard Contractual Clauses. CloudFlare collects statistical data about visits to this website. The access data includes the name of the accessed webpage, file, date and time of access, transferred data volume, notification of successful retrieval, browser type and version, the user's operating system, referrer URL (the previously visited page), IP address, and the requesting provider. CloudFlare uses the log data for statistical evaluations for the purpose of operation, security, and optimization of the offering.

If you have consented to the use of CloudFlare, the legal basis for processing personal data is Article 6(1)(a) GDPR. Additionally, we have a legitimate interest in using CloudFlare to optimize and secure our online offering, which constitutes the legal basis under Article 6(1)(f) GDPR. Personal data will be retained as long as necessary to fulfill the processing purpose and will be deleted once it is no longer required for this purpose.

This US company is certified under the EU-US Data Privacy Framework. Therefore, an adequacy decision under Article 45 GDPR exists, allowing the transfer of personal data without additional guarantees or measures.

For more information about CloudFlare, please visit:

<https://www.cloudflare.com/privacypolicy/>.

7.4 Hosting by IONOS

We host our website with IONOS SE, Elgendorfer Str. 57, 56410 Montabaur (hereinafter referred to as IONOS). When you visit our website, your personal data (e.g., IP addresses in log files) is processed on IONOS servers.

The use of IONOS is based on Article 6(1)(f) GDPR. We have a legitimate interest in the most reliable possible presentation, provision, and security of our website.

We have entered into a Data Processing Agreement (DPA) with IONOS in accordance with Article 28 GDPR. This is a legally required contract that ensures IONOS processes the personal data of our website visitors only according to our instructions and in compliance with the GDPR.

For more information on IONOS's privacy policy, please visit:

<https://www.ionos.de/terms-gtc/terms-privacy>.

8. Cookies

8.1 General Information about Cookies

Cookies are small files that are automatically created by your browser and stored on your IT system (laptop, tablet, smartphone, etc.) when you visit our site. Information is stored in the

cookie that arises in each case in connection with the specific device used. However, this does not mean that we immediately become aware of your identity.

The use of cookies serves to make the use of our offer more pleasant for you. For example, we use so-called session cookies to recognize that you have already visited individual pages of our website. These are automatically deleted after you leave our site.

In addition, we also use temporary cookies to optimize user-friendliness, which are stored on your device for a specific, predefined period. If you visit our site again to use our services, it will automatically recognize that you have already been with us and what inputs and settings you have made so that you do not have to enter them again.

On the other hand, we use cookies to statistically record the use of our website and evaluate it for the purpose of optimizing our offer for you. These cookies enable us to recognize automatically that you have already visited our website when you visit it again. The cookies set in this way are automatically deleted after a defined period. The respective storage duration of the cookies can be found in the settings of the consent tool used.

8.2 Legal Basis for the Use of Cookies

The data processed by cookies, which are necessary for the proper functioning of the website, are required to safeguard our legitimate interests as well as those of third parties in accordance with Art. 6 para. 1 lit. f) DS-GVO.

For all other cookies, you have given your consent via our opt-in cookie banner pursuant to Art. 6 para. 1 lit. a) DS-GVO.

8.3 Instructions for Avoiding Cookies in Common Browsers

Through the settings of your browser, you have the option to delete cookies at any time, allow only selected cookies, or completely disable cookies. Further information can be found on the support pages of the respective providers:

- Chrome: <https://support.google.com/chrome/answer/95647?tid=311178978>.
- Safari: <https://support.apple.com/de-at/guide/safari/sfri11471/mac?tid=311178978>.
- Firefox: <https://support.mozilla.org/de/kb/cookies-und-website-daten-in-firefox-loschen?tid=311178978>.
- Microsoft Edge: <https://support.microsoft.com/de-de/microsoft-edge/cookies-in-microsoft-edge-l%C3%B6schen-63947406-40ac-c3b8-57b9-2a946a29ae09>.

8.4 Compliance GDPR/CCPA (Consent Management Tool)

We use the consent management tool "Compliance GDPR/CCPA Cookie Consent" (Compliance) provided by Compliance B.V., Kalmarweg 14-5, 9723 JG Groningen, Netherlands. This service enables us to obtain and manage the consent of website users for data processing.

Compliance collects data using cookies generated by end users who use our website. When an end user provides consent, Compliance automatically logs the following data:

- Browser information
- Date and time of access
- Device information
- URL of the visited page
- Banner language
- Consent ID

- The user's consent status, serving as proof of consent

The consent status is also stored in the user's browser so that the website can automatically read and comply with the user's consent on all subsequent page requests and future user sessions for up to 12 months. The consent data (consent and withdrawal of consent) is stored for three years, in accordance with the regular limitation period under § 195 BGB. The data is then immediately deleted.

The functionality of the website cannot be guaranteed without the described processing. Users do not have the option to object as long as there is a legal obligation to obtain user consent for certain data processing activities (Art. 7(1), 6(1) S. 1 lit. c) DS-GVO).

Complianz is a recipient of your personal data and acts as a processor for us. Data processing takes place exclusively within the European Union.

For detailed information on the use of Complianz, please visit: <https://complianz.io/legal/>.

9. Content of our Website

9.1 Contact / Contact Form

When contacting us, whether via a contact form or email, personal data is collected. The data collected when using a contact form can be seen in the respective form. This data is used solely for the purpose of responding to your inquiry or for contact and related technical administration.

The legal basis for processing your data is our legitimate interest in responding to your inquiry according to Art. 6(1)(f) GDPR. If your contact aims at entering into a contract, the additional legal basis for processing is Art. 6(1)(b) GDPR.

Your data will be deleted after your request has been fully processed, provided that it is clear from the circumstances that the issue has been resolved and that there are no legal obligations requiring retention.

9.2 Comment Functions (with Subscription)

For the comment function on this site, in addition to your comment, the timestamp of the comment, your email address, and, if you do not post anonymously, the username you selected, are also stored.

Our comment function stores the IP addresses of users who write comments. Since we do not review comments before they are published, we need this data to take action in case of legal violations, such as insults directed at the author. As a user of our website, you can subscribe to comments after registration. You will receive a confirmation email to verify whether you are the owner of the provided email address. You can unsubscribe from this function at any time via a link in the informational emails. The data entered when subscribing to comments will be deleted in this case; however, if you have provided this data for other purposes and elsewhere (e.g., for a newsletter subscription), it will remain with us. The comments and associated data (e.g., IP address) are stored and remain on our website until the commented content is completely deleted or the comments need to be removed for legal reasons (e.g., due to insults).

The storage of comments is based on your consent (Art. 6(1)(a) GDPR). You can withdraw any consent you have given at any time. A simple email to us is sufficient for this purpose. The legality of data processing activities already carried out remains unaffected by the withdrawal.

9.3 Comment Function on the Blog

We offer users the opportunity to leave individual comments on specific blog posts located on our website. A blog is an online platform, usually publicly accessible, where one or more individuals, known as bloggers or web bloggers, can post articles or write thoughts in so-called blog posts. Blog posts can typically be commented on by third parties.

When you leave a comment on the blog published on this website, in addition to the comment you leave, information such as the timestamp of the comment and the username you selected will also be stored and published. Furthermore, the IP address assigned by your Internet Service Provider (ISP) will be recorded. This storage of the IP address is for security reasons and in case you have infringed on the rights of third parties or posted illegal content in your comment. Therefore, the storage of this personal data is in our own interest to protect ourselves in case of legal violations. This constitutes a legitimate interest under Art. 6(1)(f) GDPR. The collected personal data will not be shared with third parties unless such sharing is legally required or serves our legal defense.

9.4 Application Management / Job Board

We collect and process the personal data of applicants for the purpose of managing the application process. This processing may also be carried out electronically, especially if an applicant submits application documents electronically, such as by email or via a web form on the website. If we enter into an employment or service contract with an applicant, the transmitted data will be stored for the purpose of managing the employment relationship, in compliance with legal requirements. If we do not enter into a contract with the applicant, the application documents will be automatically deleted two months after the notification of the rejection decision, unless there are other legitimate interests on our part that oppose deletion. Such a legitimate interest might be, for example, a duty of proof in a procedure under the General Equal Treatment Act (AGG).

The legal basis for the processing of your data is Art. 6(1)(b), 88 GDPR in conjunction with § 26(1) BDSG.

10. Newsletter Distribution

10.1 Marketing Newsletter

On our website, you are given the option to subscribe to our company's newsletter. The personal data transmitted to us when subscribing to the newsletter is determined by the input form used for this purpose.

We regularly inform our customers and business partners about our offers via a newsletter. You can generally receive our company's newsletter only if:

- You have a valid email address, and
- You have registered for the newsletter distribution.

A confirmation email will be sent to the email address you initially provided for the newsletter subscription for legal reasons. This confirmation email serves to verify that you, as the owner of the email address, have authorized the receipt of the newsletter.

When signing up for the newsletter, we also store the IP address assigned to you by your Internet Service Provider (ISP) and the date and time of registration. This data is collected to track any possible misuse of your email address at a later date and thus serves our legal protection.

The personal data collected during the newsletter registration will be used exclusively for sending our newsletter. Additionally, newsletter subscribers may be informed by email if necessary for the operation of the newsletter service or related registrations, such as changes to the newsletter offering or technical modifications. No personal data collected during the newsletter service will be shared with third parties. You can cancel your newsletter subscription at any time. The consent to the storage of personal data you provided for newsletter distribution can be withdrawn at any time. Each newsletter contains a link for withdrawing consent. You also have the option to unsubscribe directly on our website or inform us of your cancellation through other means.

The legal basis for processing data for the purpose of newsletter distribution is Art. 6(1)(a) GDPR.

10.2 Newsletter Tracking

Our newsletters contain so-called tracking pixels. A tracking pixel is a tiny graphic embedded in HTML-formatted emails that enables log file recording and analysis. This allows for a statistical evaluation of the success or failure of online marketing campaigns. Through the embedded tracking pixel, we can determine whether and when you opened an email and which links contained in the email you clicked on.

The personal data collected through the tracking pixels in the newsletters are stored and analyzed by us to optimize the newsletter distribution and better tailor the content of future newsletters to your interests. This personal data is not shared with third parties. Affected individuals have the right to withdraw their separate consent given through the Double-Opt-in process at any time. After a withdrawal, this personal data will be deleted by us. Unsubscribing from the newsletter will be automatically interpreted as a withdrawal.

Such evaluation is conducted based on our legitimate interests in displaying personalized advertising, market research, and/or tailoring our website to meet needs, as outlined in Art. 6(1)(f) GDPR.

10.3 Management and Distribution with Technical Service Provider

To manage recipients, interests, consents, and objections, as well as to send newsletters, we use the services of HubSpot, Inc.; Address: 25 First Street, Cambridge, MA 02141, USA. We have a data processing agreement with HubSpot, which requires HubSpot to meet the necessary data protection guarantees through the Standard Contractual Clauses of the EU Commission. For more information on data processing by HubSpot, Inc., please visit <https://legal.hubspot.com/de/privacy-policy>

11. Our Activities on Social Networks

To communicate with you and inform you about our services, we are present on social networks with our own pages. When you visit one of our social media pages, we are jointly responsible for the processing of data triggered by your visit, in accordance with Art. 26 GDPR, with the provider of the respective social media platform.

We are not the original provider of these pages but utilize them within the framework provided by the respective providers. Therefore, please be aware that your data may also be processed outside of the European Union or the European Economic Area. This usage may involve data protection risks for you, as safeguarding your rights such as access, deletion, objection, etc., could be more difficult, and processing on social networks often occurs directly for advertising purposes or for analyzing user behavior by the providers, without our influence. Providers may create usage profiles and often use cookies or assign usage behavior to your own member profile on the social networks.

The described processing of personal data is carried out based on our legitimate interest and the legitimate interest of the respective provider, as outlined in Art. 6(1)(f) GDPR, to communicate with you in a modern manner or to inform you about our services. If you need to give consent to data processing as a user with the respective providers, the legal basis is Art. 6(1)(a) GDPR in conjunction with Art. 7 GDPR.

Since we do not have access to the providers' data repositories, we recommend that you assert your rights (e.g., access, correction, deletion, etc.) directly with the respective provider. Further information on the processing of your data on the social networks we use is provided below for each of the social network providers:

11.1 Facebook

(Co-)Controller for Data Processing in Europe:

Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland

Privacy Policy (Data Policy): You can find detailed information about the data processing and privacy practices of Facebook on their privacy policy page:

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

11.2 LinkedIn

(Co-)Controller for Data Processing in Europe:

LinkedIn Ireland Unlimited Company Wilton Place, Dublin 2, Ireland

Privacy Policy (Data Policy): You can find detailed information about the data processing and privacy practices of LinkedIn on their privacy policy page:

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

11.3 X (Twitter)

(Co-)Controller for Data Processing in Europe:

Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland

Privacy Policy (Data Policy): You can find detailed information about the data processing and privacy practices of X (Twitter) on their privacy policy page:

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

Information about your data:

https://twitter.com/settings/your_twitter_data

11.4 XING (New Work SE)

(Co-)Controller for Data Processing in Germany:

New Work SE, Am Strandkai 1, 20457 Hamburg, Deutschland

Privacy Policy (Data Policy): You can find detailed information about the data processing and privacy practices of XING on their privacy policy page:

<https://privacy.xing.com/de/datenschutzerklaerung>

Information requests for XING members:

<https://www.xing.com/settings/privacy/data/disclosure>

12. Web Analysis

12.1 Google Analytics 4 (GA4)

On our websites, we use Google Analytics 4 (GA4), a web analysis service provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland ("Google").

In this context, pseudonymized usage profiles are created and cookies (see "Cookies") are used. The information generated by the cookie about your use of this website may include:

- A brief recording of the IP address without permanent storage
- Location data
- Browser type/version
- Operating system used
- Referrer URL (previously visited page)
- Time of the server request

The pseudonymized data may be transmitted by Google to a server in the USA and stored there.

The information is used to evaluate the use of the website, compile reports on website activities, and provide other services related to website usage and internet usage for market research and needs-based design of these websites. This information may also be shared with third parties if required by law or if third parties process this data on behalf of Google.

These processing operations are carried out solely with explicit consent in accordance with Art. 6 (1) lit. a) GDPR.

Google's default data retention period is 14 months. Additionally, personal data is retained as long as necessary to fulfill the processing purpose. Data is deleted as soon as it is no longer required for the purpose.

Google LLC, the parent company, is certified under the EU-US Data Privacy Framework. This provides an adequacy decision under Art. 45 GDPR, allowing the transfer of personal data without further guarantees or additional measures.

For more information on data protection when using GA4, visit: <https://support.google.com/analytics/answer/12017362?hl=de>.

12.2 Google Analytics 4 (GA4) - Additional Information on Google Signals

Google Signals is a feature in Google Analytics that captures session data from websites and apps where users are logged in with their Google account and have enabled personalized advertising. It allows for enhanced analysis by linking user behavior across different devices and providing additional information such as demographic characteristics and interests. Your consent to use Google Analytics (as described above) also includes consent to the Google Signals feature.

12.3 Google Analytics 4 (GA4) - Additional Information on Consent Mode, Simple Implementation

Under the Digital Markets Act (DMA), Google is required to obtain user consent before processing user data for personalized advertising. Google complies with this requirement through its "Consent Mode." Users are required to implement this mode and thus demonstrate the collection of consent from website visitors.

Google offers two implementation modes: the simple and the advanced implementation.

We use the simple implementation method of Google Consent Mode. Only if you give your consent for the use of Google Analytics (as described above), a connection to Google will be established, a Google code will be executed, and the processing described above will occur. If you refuse consent, Google will only receive information that consent was not given. The Google code will not be executed, and no Google Analytics cookies will be set.

12.4 HubSpot

On this website, we use HubSpot functionalities. The provider is HubSpot, Inc., 25 First Street, Cambridge, MA 02141, USA.

HubSpot tracks visitors to our website using browser cookies. Each time you access our website, HubSpot checks if a HubSpot tracking cookie is set. If no such cookie is set on your browser, and provided you consent, a HubSpot cookie will be placed on your browser, which records all the pages you access on our website later.

Regarding HubSpot's handling of tracking cookies, please note the following:

- Your visit to our website is only tracked using the HubSpot cookie if you have consented to the placement of HubSpot cookies or all tracking cookies.
- If you fill out and submit one of the forms on our website (e.g., a contact form) and have consented to the placement of HubSpot cookies, HubSpot will associate your previous page views, as derived from the tracking cookie, with the form you submitted.
- If you have previously been in contact with us, the email address you submit through the form will be matched with the information we already have stored.
- If you delete all your cookies or specifically HubSpot cookies, you will be considered a new visitor to our website, and a new cookie will be set. However, HubSpot automatically duplicates all form submissions coming from the same email address, even if these submissions are associated with different browser cookies.
- Since cookies are set only once per browser, submissions from two people sharing a single computer will be assigned to the same contact entry. This deduplication by cookie ensures that if a contact sends forms to your website from different email addresses, all submissions will be associated with a single contact entry in HubSpot.

- HubSpot assigns page views to a contact if the contact clicks a link in a tracked marketing email that leads to a page where the HubSpot tracking code is installed.

These processing activities occur only with explicit consent according to Art. 6 (1) lit. a) GDPR. Your data will be stored until you withdraw your consent.

You can configure your browser to be informed about the setting of cookies and allow cookies only on a case-by-case basis, exclude the acceptance of cookies for certain cases or generally, and activate the automatic deletion of cookies when closing the browser. Disabling cookies may affect the functionality of this website.

The transfer of your personal data to the USA is based on standard contractual clauses.

For more information about HubSpot, please visit:

<https://legal.hubspot.com/privacy-policy>.

12.5 LinkedIn Analytics

On this website, we use LinkedIn's retargeting tool and conversion tracking provided by LinkedIn Ireland, Wilton Plaza, Wilton Place, Dublin 2, Ireland (LinkedIn).

To this end, the LinkedIn Insight Tag is integrated on our website, which allows LinkedIn to collect statistical data about your visit and use of our website and to provide us with corresponding aggregated statistics. Additionally, this service is used to show you interest-specific and relevant offers and recommendations after you have visited certain services, information, and offers on our website. This information is stored in a cookie.

The following data is typically collected and processed:

- IP address
- Device information
- Browser information
- Referrer URL
- Timestamp

These processing activities occur only with explicit consent according to Art. 6 (1) lit. a) GDPR. Your data will be stored until you withdraw your consent.

As part of the processing via LinkedIn, data may be transmitted to the USA and Singapore. This US company is certified under the EU-US Data Privacy Framework. This constitutes an adequacy decision pursuant to Art. 45 GDPR, allowing the transfer of personal data without additional guarantees or measures. Additionally, the security of the transfer is regularly ensured through so-called Standard Contractual Clauses, which guarantee that the processing of personal data is subject to a level of security comparable to that of the GDPR. If the Standard Contractual Clauses are insufficient to ensure an adequate level of security, consent pursuant to Art. 49 (1) lit. a) GDPR will be obtained from you.

For more information on LinkedIn's data protection policies, please visit:

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

13. Advertising

13.1 Google AdSense

We have integrated Google AdSense on this website. The operator of the Google AdSense component is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Google AdSense is an online service that enables the placement of advertisements on third-party sites. Google AdSense is based on an algorithm that selects advertisements displayed on third-party sites according to the content of those sites. Google AdSense allows for interest-based targeting of internet users, which is implemented by generating individual user profiles.

The purpose of the Google AdSense component is to integrate advertisements on our website. Google AdSense sets a cookie on your IT system. By setting this cookie, Alphabet Inc., 1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, USA, is able to analyze the use of our website. Each time a page on our website, which includes a Google AdSense component, is accessed, the web browser on your IT system is automatically prompted by the respective Google AdSense component to transmit data for the purpose of online advertising and commission billing to Alphabet Inc. In the course of this technical process, Alphabet Inc. gains knowledge of personal data such as your IP address, which Alphabet Inc. uses, among other things, to track the origin of visitors and clicks and subsequently to facilitate commission settlements.

Google AdSense also uses so-called counting pixels. A counting pixel is a miniature graphic embedded in web pages that enables log file recording and analysis, allowing for statistical evaluation. By means of the embedded counting pixel, Alphabet Inc. can determine whether and when a web page was opened from your IT system and which links were clicked. Counting pixels are used, among other things, to analyze the flow of visitors on a website.

Through Google AdSense, personal data and information, including IP addresses necessary for capturing and billing the displayed advertisements, is transferred to Alphabet Inc. in the United States of America. This personal data is stored and processed in the United States. Alphabet Inc. may disclose the personal data collected through this technical process to third parties.

These processing activities occur only with explicit consent in accordance with Art. 6 (1) lit. a) GDPR.

The parent company, Google LLC, is certified under the EU-US Data Privacy Framework. This constitutes an adequacy decision pursuant to Art. 45 GDPR, allowing the transfer of personal data without additional guarantees or measures.

For more information on Google AdSense's privacy policies and additional information, please visit: <https://www.google.de/intl/de/adsense/start/> and <https://www.google.com/policies/technologies/ads/>.

14. Plugins and other Services

14.1 Google Tag Manager

On this website, we use the Google Tag Manager service. The operator of Google Tag Manager is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Google Ireland Limited is part of the Google group of companies headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

This tool allows for the implementation and management of "website tags" (i.e., keywords embedded in HTML elements) via a unified interface. By using Google Tag Manager, we can automatically track which button, link, or personalized image you have clicked and determine which content on our website is of particular interest to you.

The tool also triggers other tags that may collect data. Google Tag Manager does not access this data. If you have opted out at the domain or cookie level, this opt-out remains effective for all tracking tags implemented with Google Tag Manager.

These processing activities occur only with explicit consent in accordance with Art. 6 (1) lit. a) GDPR.

The parent company, Google LLC, is certified under the EU-US Data Privacy Framework. This constitutes an adequacy decision pursuant to Art. 45 GDPR, allowing the transfer of personal data without additional guarantees or measures.

For more information on Google Tag Manager and Google's privacy policy, please visit: <https://www.google.com/intl/de/policies/privacy/>.

14.2 Microsoft Teams

We use the tool "Microsoft Teams" ("MS-Teams") for conducting our communication, including written communication (chat), telephone conferences, online meetings, and video conferences. The service provider is Microsoft Ireland Operations ("Microsoft"), Ltd., 70 Sir John Rogerson's Quay, Dublin, Ireland. Microsoft Ireland Operations, Ltd. is part of the Microsoft group of companies headquartered at One Microsoft Way, Redmond, Washington, USA.

When using MS-Teams, the following personal data is processed:

- Meetings, chats, voicemails, shared files, recordings, and transcriptions.
- Data you share, such as your email address, profile picture, and phone number.
- A detailed history of the phone calls you make.
- Data related to call quality.
- Support/Feedback data, including information related to troubleshooting tickets or feedback sent to Microsoft.
- Diagnostic and service data related to the use of the service.

To enable video display and audio playback, data from your device's microphone and camera are processed during the meeting. You can turn off the camera or mute the microphone at any time using the "Microsoft Teams" applications.

If consent has been requested, processing occurs solely based on Art. 6 (1) lit. a) GDPR. For employment relationships, data processing is based on § 26 BDSG (German Federal Data Protection Act). The legal basis for using "MS Teams" in the context of contractual

relationships is Art. 6 (1) lit. b) GDPR. In all other cases, the legal basis for processing your personal data is Art. 6 (1) lit. f) GDPR, which pertains to our interest in effectively conducting online meetings.

If we record online meetings, we will inform you before starting and, if necessary, ask for your consent to the recording. If you do not wish to be recorded, you can leave the online meeting.

As a cloud-based service, "MS-Teams" processes the mentioned data in the course of providing the service. To the extent that "MS-Teams" processes personal data in connection with Microsoft's legitimate business operations, Microsoft acts as an independent data controller for this use and is responsible for complying with applicable data protection laws and obligations of a data controller. When you visit the MS-Teams website, Microsoft is responsible for the data processing. Accessing the website is necessary to download the MS-Teams software.

This US company is certified under the EU-US Data Privacy Framework. An adequacy decision pursuant to Art. 45 GDPR is in place, allowing the transfer of personal data without additional guarantees or measures.

For detailed information on data protection related to Microsoft and "MS-Teams," please visit: <https://docs.microsoft.com/de-de/microsoftteams/teams-privacy>.

14.3 Zoom - Videoconferences

We use the "Zoom" software for conducting our communication in the form of telephone conferences, online meetings, video conferences, and webinars (hereinafter referred to as "Online Meetings"). The provider of the software is Zoom Video Communications, Inc., 55 Almaden Blvd, Suite 600, San Jose, USA.

During the use of "Zoom," various types of data are processed. The extent of the data depends on the information you provide before or during participation in an "Online Meeting." The following personal data may be processed:

- User information such as first name, last name, phone number (optional), email address (optional), password (if "Single Sign-On" is not used), profile picture (optional).
- Meeting metadata such as topic, description (optional), participant IP addresses, device/hardware information.
- In case of recordings (optional), all video, audio, and presentation recordings, and text files from the online meeting chat may be processed.
- For telephone dial-ins, information such as the incoming and outgoing phone numbers, country name, start and end time is processed. Additional connection data such as the IP address of the device may also be stored.
- You may also have the option (optional) to use chat, question, or polling functions during an "Online Meeting." Your text inputs will be processed to display them in the "Online Meeting" and, if necessary, to log them. To enable video display and audio playback, data from your device's microphone and camera are processed during the meeting. You can turn off the camera or mute the microphone at any time using the "Zoom" applications.

If consent has been requested, processing occurs solely based on Art. 6 (1) lit. a) GDPR. For employment relationships, data processing is based on § 26 BDSG (German Federal Data Protection Act). The legal basis for using "Zoom" in the context of existing or prospective contractual relationships is Art. 6 (1) lit. b) GDPR. In all other cases, the legal basis for processing your personal data is Art. 6 (1) lit. f) GDPR, which pertains to our interest in effectively conducting "Online Meetings."

If we record "Online Meetings," we will inform you before starting and, if necessary, request your consent for the recording. If you do not wish to be recorded, you can leave the "Online Meeting."

The provider of "Zoom" necessarily becomes aware of the aforementioned data as part of our data processing agreement (Art. 28 GDPR) with "Zoom." This includes the purpose of providing, optimizing, and securing the service. The participation information you provide is used to identify you in the "Online Meeting." "Zoom" is a service provided by a US-based provider. As such, the processing of personal data also takes place in a third country (outside the EU and EEA). As safeguards, we have entered into EU Standard Contractual Clauses (Art. 46 (2) and (3) GDPR) and configured our Zoom settings to use only data centers within the EU or other secure third countries (e.g., by adequacy decision pursuant to Art. 45 GDPR) for conducting "Online Meetings." However, we cannot exclude the possibility that data routing may occur through internet servers located outside the EU/EEA, especially if participants in "Online Meetings" are located in a third country. The data is encrypted during transmission over the internet and thus protected from unauthorized access by third parties.

To the extent that "Zoom" processes personal data in connection with the legitimate business operations of "Zoom," "Zoom" acts as an independent data controller for this use and is responsible for complying with applicable laws and obligations of a data controller. When you visit other websites of the provider or install the provider's application on your device, the processing of personal data is governed solely by the provider's privacy policy.

For more information on "Zoom," please visit: <https://explore.zoom.us/de/privacy/>.

15. Processing of Customer and Supplier Data

Type and Purpose of Processing:

To manage customer orders and procurement processes, we process personal data of our customers and suppliers, as well as their contacts. This data is stored in our CRM/ERP system and used in all processes related to performance fulfillment or procurement. Additionally, we use this data for active customer engagement and supplier management, including internal supplier evaluations.

Legal Basis:

The processing is carried out to fulfill contractual obligations under Art. 6(1)(b) GDPR. Data processing may also be necessary due to legal requirements, such as:

- Tax laws and statutory bookkeeping
- Compliance with requests from supervisory or law enforcement authorities
- Fulfillment of tax-related reporting and monitoring obligations

Furthermore, the disclosure of personal data may be necessary in the context of legal or court proceedings for evidence collection, criminal prosecution, or enforcement of civil claims. Under the legitimate interests balancing test according to Art. 6(1)(f) GDPR, we may process your data beyond contract fulfillment to protect legitimate interests, such as:

- Processing in the CRM system for active customer engagement
- Supplier evaluation
- Assertion of legal claims and defense in legal disputes

Recipients:

Your data may be shared with employees responsible for contacting you and managing contractual relationships, including fulfilling pre-contractual measures. Additionally, data may be disclosed to service providers who act as data processors for us, such as those providing support or maintenance for IT systems, data destruction services, or SaaS solutions for process management and CRM/ERP systems. All service providers are contractually bound to handle your data confidentially. Data may be disclosed to external recipients only in compliance with applicable data protection regulations. Potential recipients of personal data may include:

- Public Authorities and Institutions (e.g., financial or law enforcement authorities) where required by legal or regulatory obligations.
- Credit and Financial Service Providers (for payment processing).
- Tax Consultants or Auditors (for statutory audit purposes).

To manage our sales activities, we use the service of HubSpot, Inc.; Address: 25 First Street, Cambridge, MA 02141, USA. We have entered into a data processing agreement with HubSpot, which obliges HubSpot to provide the necessary safeguards for data protection through EU Standard Contractual Clauses. Further information on data processing by HubSpot, Inc. can be found at <https://legal.hubspot.com/de/privacy-policy>

For creating quotes and processing related to order fulfillment, we use the service of Odoo S.A., Chaussée de Namur, 40, 1367 Grand Rosière, Belgium. We have a data processing agreement with Odoo S.A., which requires them to process data according to our instructions. More information on data processing by Odoo S.A. can be found at https://www.odoo.com/de_DE/privacy.

Storage Duration:

We process and store your personal data for as long as necessary to fulfill our contractual and legal obligations. Once the data is no longer required for the fulfillment of contractual or legal obligations, it will be regularly deleted. Exceptions include:

- Legal Retention Obligations: For compliance with statutory retention requirements, such as those set out in the Commercial Code (HGB) and the Fiscal Code (AO), which typically require data retention for six to ten years.
- Preservation of Evidence: To retain evidence in accordance with statutory limitation periods. According to Sections 195 et seq. of the German Civil Code (BGB), these limitation periods can be up to 30 years, with the regular limitation period being 3 years.
- Other Exceptions: As applicable.

If data processing is carried out in our or a third party's legitimate interest, the personal data will be deleted once this interest no longer exists, subject to the mentioned exceptions.

Transfer to Third Countries:

Your data will also be processed in the USA as part of the use of HubSpot, Inc. Please refer to the section on recipients for details about HubSpot, Inc.

Withdrawal of Consent:

You have the right to object at any time, on grounds related to your particular situation, to the processing of your personal data based on Article 6(1)(f) GDPR (processing based on legitimate interests), including profiling based on this provision. If you object, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or the processing is necessary for the establishment, exercise, or defense of legal claims.

Provision Required or Necessary:

In the context of the contractual relationship, you must provide those personal data that are necessary for the initiation, performance, and termination of the contractual relationship and to fulfill the associated contractual obligations or which we are legally obligated to collect. Without this data, we will generally not be able to enter into or perform the contract with you.

Use of the 1cc Reporting Tool/Compliance Data

To enable you to use the 1cc Reporting Tool/Compliance Data, we need to process not only the information about the reportable company but also the login credentials of the respective user. Additionally, your sales figures will also be stored. This processing is based on the contractual agreement made for this purpose. When using the reporting tool, the collected data is transmitted to the relevant National Reporting Authority to fulfill your reporting obligations.

16. Data Protection for Applications and the Application Process

Type and Purpose of Processing:

We collect and process the personal data of applicants for the purpose of managing the application process. Processing may also occur electronically, particularly when an applicant submits application materials electronically, for example, via email or through a web form on the website.

Legal Basis:

The processing of data is carried out for the preparation of an employment contract with the applicant. The legal basis for the data processing is the execution of pre-contractual measures to which the data subject is a party (Art. 6(1)(b) GDPR).

Recipients:

Recipients of your information include HR staff responsible for contacting you and managing contractual relationships (including pre-contractual measures), as well as decision-makers involved in the hiring process. Your data may be shared with service providers acting as data

processors on our behalf, such as those providing support or maintenance for IT systems and data destruction. All service providers are contractually bound and specifically obligated to treat your data confidentially. Data is only shared with recipients outside our organization in compliance with applicable data protection regulations.

Storage Duration:

If we enter into an employment contract with you as an applicant, the transmitted data will be stored for the purpose of managing the employment relationship, in accordance with legal requirements. If no employment contract is concluded, the application materials will be automatically deleted six months after the notification of the rejection decision, unless there are other legitimate interests of the data controller that prevent deletion. Such legitimate interests may include, for example, the need to provide evidence in a procedure under the General Equal Treatment Act (AGG).

Transfer to Third Countries:

Your data will only be processed within the European Union and countries within the European Economic Area (EEA).

Provision Required or Necessary:

In the context of the application process, you must provide the personal data required for the initiation, execution, and termination of the contractual relationship and for fulfilling the related contractual obligations or for which we are legally obligated to collect. Without this data, we will generally be unable to properly consider you in the decision-making process for the position.

17. Your Rights as a Data Subject

17.1 Right to Confirmation

You have the right to request confirmation from us as to whether personal data concerning you is being processed.

17.2 Right to Access (Art. 15 GDPR)

You have the right to obtain from us, free of charge, information about the personal data stored about you and a copy of this data, in accordance with legal provisions.

17.3 Right to Rectification (Art. 16 GDPR)

You have the right to request the rectification of inaccurate personal data concerning you. Furthermore, you have the right to request the completion of incomplete personal data, taking into account the purposes of the processing.

17.4 Right to Deletion (Art. 17 GDPR)

You have the right to request the immediate deletion of personal data concerning you, provided that one of the legally prescribed reasons applies and the processing or storage is not necessary.

17.5 Right to Restriction of Processing (Art. 18 GDPR)

You have the right to request the restriction of processing from us if one of the legal requirements is met.

17.6 Right to Data Portability (Art. 20 GDPR)

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. You also have the right to transmit this data to another controller without hindrance from us, provided that the processing is based on consent according to Art. 6(1)(a) GDPR or Art. 9(2)(a) GDPR, or on a contract according to Art. 6(1)(b) GDPR, and the processing is carried out by automated means, 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 us.

Additionally, when exercising your right to data portability according to Art. 20(1) GDPR, you have the right to have the personal data transmitted directly from one controller to another, where technically feasible, and provided that this does not adversely affect the rights and freedoms of others.

17.7 Right to Object (Art. 21 GDPR)

You have the right to object, at any time and on grounds relating to your particular situation, to the processing of personal data concerning you, which is carried out based on Art. 6(1)(e) (processing in the public interest) or (f) (processing based on balancing of interests) GDPR. This also applies to profiling based on these provisions according to Art. 4(4) GDPR.

If you object, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or if the processing is necessary for the establishment, exercise, or defense of legal claims.

In certain cases, we process personal data for the purpose of direct marketing. You may object to the processing of personal data for such marketing purposes at any time. This also applies to profiling to the extent that it is related to such direct marketing. If you object to the processing for direct marketing purposes, we will no longer process the personal data for those purposes.

Additionally, you have the right to object, on grounds relating to your particular situation, to the processing of personal data concerning you for scientific or historical research purposes or statistical purposes under Art. 89(1) GDPR, unless such processing is necessary for the performance of a task carried out for reasons of public interest.

You are free to exercise your right to object in the context of the use of information society services, notwithstanding Directive 2002/58/EC, using automated procedures, including technical specifications.

17.8 Withdrawal of Consent

You have the right to withdraw your consent to the processing of personal data at any time with effect for the future.

17.9 Complaint to a Supervisory Authority

You have the right to lodge a complaint with a data protection supervisory authority regarding our processing of personal data.

18. Routine Storage, Deletion, and Blocking of Personal Data

We process and store your personal data only for the period necessary to achieve the storage purpose or as required by the legal regulations applicable to our company. If the storage purpose ceases or a prescribed storage period expires, the personal data will be routinely blocked or deleted in accordance with legal requirements.

19. Duration of Storage of Personal Data

The criterion for the duration of storage of personal data is the respective legal retention period. After the expiration of this period, the corresponding data will be routinely deleted, unless it is still required for the fulfillment of a contract or the initiation of a contract.

20. Currency and Modification of the Privacy Policy

This privacy policy is currently valid and is dated September 2024. Due to the ongoing development of our websites and offers or due to changed legal or regulatory requirements, it may be necessary to amend this privacy policy. The current version of the privacy policy can be accessed and printed at any time on our website at https://1cc-consulting.com/wp-content/uploads/datenschutz_en.pdf.

This privacy policy was created with the support of the data protection software: audatis MANAGER.