

Privacy Policy

Preamble

With the following privacy policy we would like to inform you which types of your personal data (hereinafter also abbreviated as "data") we process for which purposes and in which scope. The privacy statement applies to all processing of personal data carried out by us, both in the context of providing our services and in particular on our websites, in mobile applications and within external online presences, such as our social media profiles (hereinafter collectively referred to as "online services").

The terms used are not gender-specific.

Last Update: 22. September 2025



Table of contents

- Preamble
- Controller
- Contact information of the Data Protection Officer
- Overview of processing operations
- Relevant legal bases
- Security Precautions
- Transmission of Personal Data

- International data transfers
- General Information on Data Retention and Deletion
- Rights of Data Subjects
- Provision of online services and web hosting
- Use of Cookies
- Blogs and publication media
- Contact and Inquiry Management
- Cloud Services
- Newsletter and Electronic Communications
- Web Analysis, Monitoring and Optimization
- Online Marketing
- Profiles in Social Networks (Social Media)
- Changes and Updates
- Terminology and Definitions

Controller

RACO-ELEKTRO-MASCHINEN GMBH
Data Protection Officer
Jesinghauser Str. 56-64
58332 Schwelm

E-mail address: datenschutz@raco.de

Legal Notice: <https://raco.de/en/impressum>

Contact information of the Data Protection Officer

datenschutz@raco.de

Overview of processing operations

The following table summarises the types of data processed, the purposes for which

they are processed and the concerned data subjects.

Categories of Processed Data

- Inventory data.
- Contact data.
- Content data.
- Usage data.
- Meta, communication and process data.
- Log data.

Categories of Data Subjects

- Prospective customers.
- Communication partner.
- Users.
- Business and contractual partners.

Purposes of Processing

- Communication.
- Security measures.
- Direct marketing.
- Web Analytics.
- Targeting.
- Office and organisational procedures.
- Remarketing.
- Conversion tracking.
- Affiliate Tracking.
- Organisational and Administrative Procedures.
- Feedback.
- Marketing.
- Profiles with user-related information.

- Provision of our online services and usability.
- Information technology infrastructure.
- Public relations.

Relevant legal bases

Relevant legal bases according to the GDPR: In the following, you will find an overview of the legal basis of the GDPR on which we base the processing of personal data. Please note that in addition to the provisions of the GDPR, national data protection provisions of your or our country of residence or domicile may apply. If, in addition, more specific legal bases are applicable in individual cases, we will inform you of these in the data protection declaration.

- **Consent (Article 6 (1) (a) GDPR)** - The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- **Performance of a contract and prior requests (Article 6 (1) (b) GDPR)** - Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- **Legitimate Interests (Article 6 (1) (f) GDPR)** - the processing is necessary for the protection of the legitimate interests of the controller or a third party, provided that the interests, fundamental rights, and freedoms of the data subject, which require the protection of personal data, do not prevail.

National data protection regulations in Germany: In addition to the data protection regulations of the GDPR, national regulations apply to data protection in Germany. This includes in particular the Law on Protection against Misuse of Personal Data in Data Processing (Federal Data Protection Act - BDSG). In particular, the BDSG contains special provisions on the right to access, the right to erase, the right to object, the processing of special categories of personal data, processing for other purposes and transmission as well as automated individual decision-making, including profiling. Furthermore, data protection laws of the individual federal states may apply.

Reference to the applicability of the GDPR and the Swiss DPA: These privacy policy serves both to provide information pursuant to the Swiss Federal Act on Data Protection (FADP) and the General Data Protection Regulation (GDPR). For this reason, we ask you to note that due to the broader spatial application and comprehensibility, the terms used in the GDPR are applied. In particular, instead of the terms used in the Swiss FADP such as "processing" of "personal data", "predominant interest", and "particularly sensitive personal data", the terms used in the GDPR, namely "processing" of "personal data", as well as "legitimate interest" and "special categories of data" are used. However, the legal meaning of these

terms will continue to be determined according to the Swiss FADP within its scope of application.

Security Precautions

We take appropriate technical and organisational measures in accordance with the legal requirements, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, in order to ensure a level of security appropriate to the risk.

The measures include, in particular, safeguarding the confidentiality, integrity and availability of data by controlling physical and electronic access to the data as well as access to, input, transmission, securing and separation of the data. In addition, we have established procedures to ensure that data subjects' rights are respected, that data is erased, and that we are prepared to respond to data threats rapidly. Furthermore, we take the protection of personal data into account as early as the development or selection of hardware, software and service providers, in accordance with the principle of privacy by design and privacy by default.

Securing online connections through TLS/SSL encryption technology (HTTPS): To protect the data of users transmitted via our online services from unauthorized access, we employ TLS/SSL encryption technology. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are the cornerstones of secure data transmission on the internet. These technologies encrypt the information that is transferred between the website or app and the user's browser (or between two servers), thereby safeguarding the data from unauthorized access. TLS, as the more advanced and secure version of SSL, ensures that all data transmissions conform to the highest security standards. When a website is secured with an SSL/TLS certificate, this is indicated by the display of HTTPS in the URL. This serves as an indicator to users that their data is being securely and encryptedly transmitted.

Transmission of Personal Data

In the course of processing personal data, it may happen that this data is transmitted to or disclosed to other entities, companies, legally independent organizational units, or individuals. Recipients of this data may include service providers tasked with IT duties or providers of services and content that are integrated into a website. In such cases, we observe the legal requirements and particularly conclude relevant contracts or agreements that serve to protect your data with the recipients of your data.

International data transfers

Data Processing in Third Countries: If we transfer data to a third country (i.e., outside the European Union (EU) or the European Economic Area (EEA)), or if this occurs in the context of using third-party services or the disclosure or transfer of data to other individuals, entities, or companies (which becomes apparent either from the postal address of the respective provider or when explicitly mentioned in the privacy policy regarding data transfer to third countries), this is always done in accordance with legal requirements.

For data transfers to the USA, we primarily rely on the Data Privacy Framework (DPF), which has been recognized as a secure legal framework by the EU Commission's adequacy decision of July 10, 2023. Additionally, we have concluded Standard Contractual Clauses with the respective providers, which comply with the EU Commission's requirements and establish contractual obligations to protect your data.

This dual safeguard ensures comprehensive protection of your data: The DPF serves as the primary level of protection, while the Standard Contractual Clauses act as an additional security measure. Should any changes occur within the DPF framework, the Standard Contractual Clauses will serve as a reliable fallback option. This ensures that your data remains adequately protected even in the event of political or legal changes.

For individual service providers, we will inform you whether they are certified under the DPF and if Standard Contractual Clauses are in place. The list of certified companies and further information about the DPF can be found on the U.S. Department of Commerce's website at <https://www.dataprivacyframework.gov/>.

For data transfers to other third countries, appropriate safeguards apply, particularly Standard Contractual Clauses, explicit consent, or legally required transfers. Information on third-country transfers and applicable adequacy decisions can be found in the information provided by the EU Commission:

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en.

We will inform you which of our service providers are certified under the Data Privacy Framework as part of our data protection notices.

General Information on Data Retention and Deletion

We delete personal data that we process in accordance with legal regulations as

soon as the underlying consents are revoked or no further legal bases for processing exist. This applies to cases where the original purpose of processing is no longer applicable or the data is no longer needed. Exceptions to this rule exist if statutory obligations or special interests require a longer retention or archiving of the data.

In particular, data that must be retained for commercial or tax law reasons, or whose storage is necessary for legal prosecution or protection of the rights of other natural or legal persons, must be archived accordingly.

Our privacy notices contain additional information on the retention and deletion of data specifically applicable to certain processing processes.

In cases where multiple retention periods or deletion deadlines for a date are specified, the longest period always prevails.

Data that is no longer stored for its originally intended purpose but due to legal requirements or other reasons are processed exclusively for the reasons justifying their retention.

Data Retention and Deletion: The following general deadlines apply for the retention and archiving according to German law:

- 10 Years - Fiscal Code/Commercial Code - Retention period for books and records, annual financial statements, inventories, management reports, opening balance sheet as well as the necessary work instructions and other organisational documents (Section 147 Paragraph 1 No. 1 in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 14b Paragraph 1 of the German VAT Act (UStG), Section 257 Paragraph 1 No. 1 in conjunction with Paragraph 4 of the German Commercial Code (HGB)).
- 8 years - Accounting documents, such as invoices, booking and expense receipts (Section 147 Paragraph 1 No. 4 and 4a in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 257 Paragraph 1 No. 4 in conjunction with Paragraph 4 of the German Commercial Code (HGB))
- 6 Years - Other business documents: received commercial or business letters, copies of dispatched commercial or business letters, and other documents to the extent that they are significant for taxation purposes, for example, hourly wage slips, operating accounting sheets, calculation documents, price tags, as well as payroll accounting documents, provided they are not already accounting vouchers and cash register tapes (Section 147 Paragraph 1 No. 2, 3, 5 in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 257 Paragraph 1 No. 2 and 3 in conjunction with Paragraph 4 of the German Commercial Code (HGB)).

- 3 Years - Data required to consider potential warranty and compensation claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experiences and common industry practices, will be stored for the duration of the regular statutory limitation period of three years. This period begins at the end of the year in which the relevant contractual transaction took place or the contractual relationship ended in the case of ongoing contracts (Sections 195, 199 of the German Civil Code).

Start of the period at the end of the year: If a period does not expressly start on a specific date and lasts at least one year, it automatically begins at the end of the calendar year in which the event triggering the period occurred. In the case of ongoing contractual relationships in the context of which data is stored, the event triggering the deadline is the time at which the termination or other termination of the legal relationship takes effect.

Rights of Data Subjects

Rights of the Data Subjects under the GDPR: As data subject, you are entitled to various rights under the GDPR, which arise in particular from Articles 15 to 21 of the GDPR:

- **Right to Object:** You have the right, on grounds arising from your particular situation, to object at any time to the processing of your personal data which is based on letter (e) or (f) of Article 6(1) GDPR, including profiling based on those provisions. Where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of the personal data concerning you for the purpose of such marketing, which includes profiling to the extent that it is related to such direct marketing.
- **Right of withdrawal for consents:** You have the right to revoke consents at any time.
- **Right of access:** You have the right to request confirmation as to whether the data in question will be processed and to be informed of this data and to receive further information and a copy of the data in accordance with the provisions of the law.
- **Right to rectification:** You have the right, in accordance with the law, to request the completion of the data concerning you or the rectification of the incorrect data concerning you.
- **Right to Erasure and Right to Restriction of Processing:** In accordance with the statutory provisions, you have the right to demand that the relevant

data be erased immediately or, alternatively, to demand that the processing of the data be restricted in accordance with the statutory provisions.

- **Right to data portability:** You have the right to receive data concerning you which you have provided to us in a structured, common and machine-readable format in accordance with the legal requirements, or to request its transmission to another controller.
- **Complaint to the supervisory authority:** In accordance with the law and without prejudice to any other administrative or judicial remedy, you also have the right to lodge a complaint with a data protection supervisory authority, in particular a supervisory authority in the Member State where you habitually reside, the supervisory authority of your place of work or the place of the alleged infringement, if you consider that the processing of personal data concerning you infringes the GDPR.

Provision of online services and web hosting

We process user data in order to be able to provide them with our online services. For this purpose, we process the IP address of the user, which is necessary to transmit the content and functions of our online services to the user's browser or terminal device.

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties). Log data (e.g. log files concerning logins or data retrieval or access times.).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of our online services and usability; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)). Security measures.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Provision of online offer on rented hosting space:** For the provision of our online services, we use storage space, computing capacity and software

that we rent or otherwise obtain from a corresponding server provider (also referred to as a "web hoster"); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

- **Collection of Access Data and Log Files:** Access to our online service is logged in the form of so-called "server log files". Server log files may include the address and name of the accessed web pages and files, date and time of access, transferred data volumes, notification of successful retrieval, browser type along with version, the user's operating system, referrer URL (the previously visited page), and typically IP addresses and the requesting provider. The server log files can be used for security purposes, e.g., to prevent server overload (especially in the case of abusive attacks, known as DDoS attacks), and to ensure server load management and stability; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Retention period:** Log file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.
- **Hetzner:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider:** Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.hetzner.com>; **Privacy Policy:** <https://www.hetzner.com/de/rechtliches/datenschutz>. **Data Processing Agreement:** <https://docs.hetzner.com/de/general/general-terms-and-conditions/data-privacy-faq/>.
- **United Domains:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider:** united-domains AG, Gautinger Straße 10, 82319 Starnberg, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.united-domains.de>; **Privacy Policy:** <https://www.united-domains.de/unternehmen/datenschutz/>. **Data Processing Agreement:** <https://www.united-domains.de/help/faq-article/wie-erhalte-ich-den-auftragsverarbeitungs-vertrag-avv-nach-dsgvo>.

Use of Cookies

The term "cookies" refers to functions that store information on users' devices and read it from them. Cookies can also be used for different purposes, such as ensuring the functionality, security, and convenience of online services, as well as analyzing visitor traffic. We use cookies in accordance with legal regulations. If

necessary, we obtain users' consent in advance. If consent is not required, we rely on our legitimate interests. This applies when storing and reading information is essential to provide explicitly requested content and functions. This includes, for example, saving settings and ensuring the functionality and security of our online services. Consent can be withdrawn at any time. We clearly inform users about the scope of the consent and which cookies are used.

Information on legal data protection bases: Whether we process personal data using cookies depends on users' consent. If consent is given, it serves as the legal basis. Without consent, we rely on our legitimate interests, as outlined in this section and in the context of the respective services and procedures.

Storage duration: The following types of cookies are distinguished based on their storage duration:

- **Temporary cookies (also: session cookies):** Temporary cookies are deleted at the latest after a user leaves an online service and closes their device (e.g., browser or mobile application).
- **Permanent cookies:** Permanent cookies remain stored even after the device is closed. For example, the login status can be saved, and preferred content can be displayed directly when the user revisits a website. Additionally, the user data collected with cookies may be used for audience measurement. Unless we provide explicit information to users about the type and storage duration of cookies (e.g., when obtaining consent), users should assume that these are permanent and may have a storage duration of up to two years.

General information on withdrawal and objection (opt-out): Users can withdraw their consent at any time and also object to the processing according to legal regulations, including through the privacy settings of their browser.

- **Processed data types:** Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). Consent (Article 6 (1) (a) GDPR).

Further information on processing methods, procedures and services used:

- **Processing Cookie Data on the Basis of Consent:** We implement a consent management solution that obtains users' consent for the use of cookies or for the processes and providers mentioned within the consent management framework. This procedure is designed to solicit, log, manage, and revoke consents, particularly regarding the use of cookies and similar technologies employed to store, read from, and process information on users'

devices. As part of this procedure, user consents are obtained for the use of cookies and the associated processing of information, including specific processing and providers named in the consent management process. Users also have the option to manage and withdraw their consents. Consent declarations are stored to avoid repeated queries and to provide proof of consent according to legal requirements. The storage is carried out server-side and/or in a cookie (so-called opt-in cookie) or by means of comparable technologies in order to associate the consent with a specific user or their device. If no specific details about the providers of consent management services are provided, the following general notes apply: The duration of consent storage is up to two years. A pseudonymous user identifier is created, which is stored along with the time of consent, details on the scope of consent (e.g., relevant categories of cookies and/or service providers), as well as information about the browser, system, and device used; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).

- **Cookiebot:** Cookie Consent Management: Procedures for obtaining, recording, managing, and revoking consents, particularly for the use of cookies and similar technologies for storing, accessing, and processing information on users' devices as well as their processing; **Service provider:** Usercentrics A/S, Havnegade 39, 1058 Copenhagen, Denmark; **Website:** <https://www.cookiebot.com>; **Privacy Policy:** <https://www.cookiebot.com/en/privacy-policy/>; **Data Processing Agreement:** Provided by the service provider; **Further Information:** Stored data (on the server of the service provider): The IP number of the user in anonymous form (the last three digits are set to 0), date and time of the consent, user agent of the user's browser, the URL from which the consent was sent, An anonymous, random and encrypted key value. the consent status of the user.

Blogs and publication media

We use blogs or comparable means of online communication and publication (hereinafter "publication medium"). Readers' data will only be processed for the purposes of the publication medium to the extent necessary for its presentation and communication between authors and readers or for security reasons. For the rest, we refer to the information on the processing of visitors to our publication medium within the scope of this privacy policy.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and

frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).

- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Feedback (e.g. collecting feedback via online form). Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Contact and Inquiry Management

When contacting us (e.g. via mail, contact form, e-mail, telephone or via social media) as well as in the context of existing user and business relationships, the information of the inquiring persons is processed to the extent necessary to respond to the contact requests and any requested measures.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Communication; Organisational and Administrative Procedures; Feedback (e.g. collecting feedback via online form). Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Further information on processing methods, procedures and services used:

- **Contact form:** Upon contacting us via our contact form, email, or other means of communication, we process the personal data transmitted to us for the purpose of responding to and handling the respective matter. This

typically includes details such as name, contact information, and possibly additional information provided to us that is necessary for appropriate processing. We use this data exclusively for the stated purpose of contact and communication; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Cloud Services

We use Internet-accessible software services (so-called "cloud services", also referred to as "Software as a Service") provided on the servers of its providers for the storage and management of content (e.g. document storage and management, exchange of documents, content and information with certain recipients or publication of content and information).

Within this framework, personal data may be processed and stored on the provider's servers insofar as this data is part of communication processes with us or is otherwise processed by us in accordance with this privacy policy. This data may include in particular master data and contact data of data subjects, data on processes, contracts, other proceedings and their contents. Cloud service providers also process usage data and metadata that they use for security and service optimization purposes.

If we use cloud services to provide documents and content to other users or publicly accessible websites, forms, etc., providers may store cookies on users' devices for web analysis or to remember user settings (e.g. in the case of media control).

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Prospective customers; Communication partner (Recipients of e-mails, letters, etc.). Business and contractual partners.
- **Purposes of processing:** Office and organisational procedures. Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Microsoft 365 and Microsoft Cloud Services:** Provision of applications, protection of data and IT systems, as well as the use of system-generated log, diagnostic, and metadata for contract execution by Microsoft. The data processed includes contact details (name, email address), content data (files, comments, profiles), software setup and inventory data, device connectivity and configuration data, work interactions (badge swipe), as well as log and metadata. The processing is carried out for purposes of improving efficiency and productivity, cost efficiency, flexibility, mobility, enhanced communication, integration of Microsoft services, IT security and business operations of Microsoft. Data retention is determined by the respective document and company policies: up to 12 months for Defender (protection of data and IT systems) and 10 days for print management. Additionally, diagnostic data is collected for product stability and improvement; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://microsoft.com>; **Privacy Policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security information: <https://www.microsoft.com/de-de/trustcenter>; **Data Processing Agreement:** <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>. **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>).

Newsletter and Electronic Communications

We send newsletters, emails, and other electronic notifications (hereinafter "newsletters") exclusively with the consent of the recipients or based on a legal basis. If the contents of the newsletter are specified during registration for the newsletter, these contents are decisive for the users' consent. Normally, providing your email address is sufficient to sign up for our newsletter. However, to offer you a personalised service, we may ask for your name for personal salutation in the newsletter or for additional information if necessary for the purpose of the newsletter.

Deletion and restriction of processing: We may store unsubscribed email addresses for up to three years based on our legitimate interests before deleting them to be able to demonstrate previously given consent. The processing of these data is

limited to the purpose of potentially defending against claims. An individual request for deletion is possible at any time, provided that at the same time the former existence of consent is confirmed. In case of obligations to permanently observe objections, we reserve the right to store the email address solely for this purpose in a blocklist.

The logging of the registration process is based on our legitimate interests for the purpose of proving its proper execution. If we commission a service provider to send emails, this is done based on our legitimate interests in an efficient and secure mailing system.

Contents:

Information about us, our services, promotions and offers.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Direct marketing (e.g. by e-mail or postal).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR).
- **Opt-Out:** You can cancel the receipt of our newsletter at any time, i.e. revoke your consent or object to further receipt. You will find a link to cancel the newsletter either at the end of each newsletter or you can otherwise use one of the contact options listed above, preferably e-mail.

Web Analysis, Monitoring and Optimization

Web analytics (also referred to as "reach measurement") is used to evaluate the visitor flows of our online services and may include pseudonymous values related to visitor behavior, interests, or demographic information such as age or gender. Through reach analysis, we can, for example, identify when our online services or their functions and content are most frequently used or likely to encourage repeat visits. It also enables us to determine which areas need optimization.

In addition to web analytics, we may also use testing procedures to test and optimize different versions of our online services or their components.

Unless otherwise specified below, profiles (i.e., data combined from a usage process) may be created for these purposes, and information can be stored in and later retrieved from a browser or device. The data collected includes, in particular,

visited websites and elements used on them, as well as technical information such as the browser used, the computer system, and information about usage times. If users have given consent to the collection of their location data to us or to the providers of the services we use, the processing of location data is also possible.

Additionally, users' IP addresses are stored. However, we use an IP masking process (i.e., pseudonymization by shortening the IP address) to protect users. In general, no clear user data (such as email addresses or names) is stored as part of web analytics, A/B testing, or optimization. Instead, pseudonyms are used. This means that neither we nor the providers of the software used know the actual identity of the users, only the information stored in their profiles for the respective procedures.

Legal basis information: If we ask users for their consent to use third-party providers, the legal basis for data processing is consent. Otherwise, user data is processed based on our legitimate interests (i.e., our interest in efficient, economic, and user-friendly services). In this context, we would also like to point out the information on the use of cookies in this privacy policy.

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Web Analytics (e.g. access statistics, recognition of returning visitors); Profiles with user-related information (Creating user profiles); Remarketing. Targeting (e.g. profiling based on interests and behaviour, use of cookies).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.).
- **Security measures:** IP Masking (Pseudonymization of the IP address).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Matomo:** Matomo is software that is used for the purposes of web analysis and reach measurement. As part of the use of Matomo, cookies are generated and stored on the user's terminal device. User data collected through the use

of Matomo is processed only by us and is not shared with third parties. The cookies are stored for a maximum period of 13 months:

https://matomo.org/faq/general/faq_146/; **Legal Basis:** Consent (Article 6 (1) (a) GDPR). **Retention period:** The cookies have a maximum storage period of 13 months.

- **Google Tag Manager:** We use Google Tag Manager, a software provided by Google, which enables us to manage so-called website tags centrally via a user interface. Tags are small code elements on our website that serve to record and analyse visitor activities. This technology assists us in improving our website and the content offered on it. Google Tag Manager itself does not create user profiles, store cookies with user profiles, or perform any independent analyses. Its function is limited to simplifying and making the integration and management of tools and services we use on our website more efficient. Nevertheless, when using Google Tag Manager, users' IP addresses are transmitted to Google, which is technically necessary to implement the services we use. Cookies may also be set in this process. However, this data processing only occurs if services are integrated via the Tag Manager. For more detailed information about these services and their data processing, please refer to the further sections of this privacy policy; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://marketingplatform.google.com/>; **Privacy Policy:** <https://policies.google.com/privacy>; **Data Processing Agreement:** <https://business.safety.google/adsprocessorterms>. **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (<https://business.safety.google/adsprocessorterms>).
- **Microsoft Clarity:** Web analysis, measuring reach and analyzing user behavior in relation to the use and interests regarding functions and content as well as their duration of use based on a pseudonymous user identification number and profile creation; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://clarity.microsoft.com/>; **Privacy Policy:** <https://privacy.microsoft.com/en-us/privacystatement>; **Data Processing Agreement:** <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>. **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (<https://privacy.microsoft.com/en-us/privacystatement>).

Online Marketing

We process personal data for the purposes of online marketing, which may include in particular the marketing of advertising space or the display of advertising and other content (collectively referred to as "Content") based on the potential interests of users and the measurement of their effectiveness.

For these purposes, so-called user profiles are created and stored in a file (so-called "cookie") or similar procedure is used by which the relevant user information for the display of the aforementioned content is stored. This information may include, for example, content viewed, websites visited, online networks used, communication partners and technical information such as the browser used, computer system used and information on usage times and used functions. If users have consented to the collection of their sideline data, these can also be processed.

The IP addresses of the users are also stored. However, we use provided IP masking procedures (i.e. pseudonymisation by shortening the IP address) to ensure the protection of the user's by using a pseudonym. In general, within the framework of the online marketing process, no clear user data (such as e-mail addresses or names) is secured, but pseudonyms. This means that we, as well as the providers of online marketing procedures, do not know the actual identity of the users, but only the information stored in their profiles.

The information in the profiles is usually stored in the cookies or similar memorizing procedures. These cookies can later, generally also on other websites that use the same online marketing technology, be read and analyzed for purposes of content display, as well as supplemented with other data and stored on the server of the online marketing technology provider.

Exceptionally, clear data can be assigned to the profiles. This is the case, for example, if the users are members of a social network whose online marketing technology we use and the network links the profiles of the users in the aforementioned data. Please note that users may enter into additional agreements with the social network providers or other service providers, e.g. by consenting as part of a registration process.

As a matter of principle, we only gain access to summarised information about the performance of our advertisements. However, within the framework of so-called conversion measurement, we can check which of our online marketing processes have led to a so-called conversion, i.e. to the conclusion of a contract with us. The conversion measurement is used alone for the performance analysis of our marketing activities.

Unless otherwise stated, we kindly ask you to consider that cookies used will be stored for a period of two years.

Notes on revocation and objection:

We refer to the privacy policies of the respective service providers and the possibilities for objection (so-called "opt-out"). If no explicit opt-out option has been specified, it is possible to deactivate cookies in the settings of your browser. However, this may restrict the functions of our online offer. We therefore recommend the following additional opt-out options, which are offered collectively for each area:

- a) Europe: <https://www.youronlinechoices.eu>.
- b) Canada: <https://www.youradchoices.ca/choices>.
- c) USA: <https://www.aboutads.info/choices>.
- d) Cross-regional: <https://optout.aboutads.info>.

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Web Analytics (e.g. access statistics, recognition of returning visitors); Targeting (e.g. profiling based on interests and behaviour, use of cookies); Affiliate Tracking; Marketing; Profiles with user-related information (Creating user profiles); Conversion tracking (Measurement of the effectiveness of marketing activities); Provision of our online services and usability. Remarketing.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.).
- **Security measures:** IP Masking (Pseudonymization of the IP address).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **LinkedIn Ads:** Placement of ads within the LinkedIn platform and analysis of ad results; **Service provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR),

Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://business.linkedin.com/de-de/marketing-solutions/ads>; **Privacy Policy:** <https://www.linkedin.com/legal/privacy-policy>; **Data Processing Agreement:** <https://www.linkedin.com/legal/l/dpa>; **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (<https://legal.linkedin.com/dpa>). **Opt-Out:** <https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>.

- **Google Ads Remarketing:** Google Remarketing, also known as retargeting, is a technology that adds users who use an online service to a pseudonymous remarketing list so that users can be shown ads on other online services based on their visit to the online service
; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://marketingplatform.google.com>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** Data Privacy Framework (DPF); **Further Information:** Types of processing and data processed: <https://business.safety.google/adsservices/>. Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: <https://business.safety.google/adscontrollerterms>.
- **Enhanced Conversions for Google Ads:** When users click on our Google ads and subsequently use the advertised service (so-called "conversion"), the data entered by the user, such as email address, name, residential address or telephone number, may be transmitted to Google. The hash values are then matched with existing Google accounts of the users to better evaluate and improve their interaction with the ads (e.g., clicks or views) and thus their performance; **Legal Basis:** Consent (Article 6 (1) (a) GDPR). **Website:** <https://support.google.com/google-ads/answer/9888656>.

Profiles in Social Networks (Social Media)

We maintain online presences within social networks and process user data in this context in order to communicate with the users active there or to offer information about us.

We would like to point out that user data may be processed outside the European Union. This may entail risks for users, e.g. by making it more difficult to enforce users' rights.

In addition, user data is usually processed within social networks for market research and advertising purposes. For example, user profiles can be created on the basis of user behaviour and the associated interests of users. The user profiles can then be used, for example, to place advertisements within and outside the

networks which are presumed to correspond to the interests of the users. For these purposes, cookies are usually stored on the user's computer, in which the user's usage behaviour and interests are stored. Furthermore, data can be stored in the user profiles independently of the devices used by the users (especially if the users are members of the respective networks or will become members later on).

For a detailed description of the respective processing operations and the opt-out options, please refer to the respective data protection declarations and information provided by the providers of the respective networks.

Also in the case of requests for information and the exercise of rights of data subjects, we point out that these can be most effectively pursued with the providers. Only the providers have access to the data of the users and can directly take appropriate measures and provide information. If you still need help, please do not hesitate to contact us.

- **Processed data types:** Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Communication; Feedback (e.g. collecting feedback via online form). Public relations.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **LinkedIn:** Social network - We are jointly responsible with LinkedIn Ireland Unlimited Company for the collection (but not the further processing) of visitor data, which is used to create "Page Insights" (statistics) for our LinkedIn profiles. This data includes information about the types of content users view or interact with, as well as the actions they take. It also includes details about the devices used, such as IP addresses, operating systems, browser types, language settings, and cookie data, as well as profile details of users, such as job function, country, industry, seniority, company size, and employment status. Privacy information regarding the processing of user data by LinkedIn can be found in LinkedIn's privacy policy:
<https://www.linkedin.com/legal/privacy-policy>.
We have entered into a special agreement with LinkedIn Ireland ("Page Insights Joint Controller Addendum,"

<https://legal.linkedin.com/pages-joint-controller-addendum>), which specifically regulates the security measures LinkedIn must comply with and in which LinkedIn has agreed to fulfill the rights of data subjects (i.e., users can, for example, direct requests for information or deletion directly to LinkedIn). The rights of users (particularly the right to information, deletion, objection, and to lodge a complaint with the competent supervisory authority) are not restricted by our agreements with LinkedIn. The joint responsibility is limited to the collection of data and its transmission to LinkedIn Ireland Unlimited Company, a company based in the EU. Further processing of the data is the sole responsibility of LinkedIn Ireland Unlimited Company, particularly concerning the transfer of data to the parent company LinkedIn Corporation in the USA; **Service provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.linkedin.com>; **Privacy Policy:** <https://www.linkedin.com/legal/privacy-policy>; **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (<https://legal.linkedin.com/dpa>). **Opt-Out:** <https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>.

- **Xing:** Social network; **Service provider:** New Work SE, Am Strandkai 1, 20457 Hamburg, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.xing.com>. **Privacy Policy:** <https://privacy.xing.com/en>.

Changes and Updates

We kindly ask you to inform yourself regularly about the contents of our data protection declaration. We will adjust the privacy policy as changes in our data processing practices make this necessary. We will inform you as soon as the changes require your cooperation (e.g. consent) or other individual notification.

If we provide addresses and contact information of companies and organizations in this privacy policy, we ask you to note that addresses may change over time and to verify the information before contacting us.

Terminology and Definitions

In this section, you will find an overview of the terminology used in this privacy policy. Where the terminology is legally defined, their legal definitions apply. The following explanations, however, are primarily intended to aid understanding.

- **Affiliate Tracking:** Custom Audiences refers to the process of determining

target groups for advertising purposes, e.g. the display of advertisements. For example, a user's interest in certain products or topics on the Internet may be used to conclude that the user is interested in advertisements for similar products or the online store in which the user viewed the products.

"Lookalike Audiences" is the term used to describe content that is viewed as suitable by users whose profiles or interests presumably correspond to the users for whom the profiles were created. For the purposes of creating custom audiences and lookalike audiences, cookies and web beacons are typically used.

- **Contact data:** Contact details are essential information that enables communication with individuals or organizations. They include, among others, phone numbers, postal addresses, and email addresses, as well as means of communication like social media handles and instant messaging identifiers.
- **Content data:** Content data comprise information generated in the process of creating, editing, and publishing content of all types. This category of data may include texts, images, videos, audio files, and other multimedia content published across various platforms and media. Content data are not limited to the content itself but also include metadata providing information about the content, such as tags, descriptions, authorship details, and publication dates.
- **Controller:** "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Conversion tracking:** Conversion tracking is a method used to evaluate the effectiveness of marketing measures. For this purpose, a cookie is usually stored on the devices of the users within the websites on which the marketing measures take place and then called up again on the target website (e.g. we can thus trace whether the advertisements placed by us on other websites were successful).
- **Inventory data:** Inventory data encompass essential information required for the identification and management of contractual partners, user accounts, profiles, and similar assignments. These data may include, among others, personal and demographic details such as names, contact information (addresses, phone numbers, email addresses), birth dates, and specific identifiers (user IDs). Inventory data form the foundation for any formal interaction between individuals and services, facilities, or systems, by enabling unique assignment and communication.
- **Log data:** Protocol data, or log data, refer to information regarding events or activities that have been logged within a system or network. These data typically include details such as timestamps, IP addresses, user actions, error messages, and other specifics about the usage or operation of a system. Protocol data is often used for analyzing system issues, monitoring security, or generating performance reports.

- **Meta, communication and process data:** Meta-, communication, and procedural data are categories that contain information about how data is processed, transmitted, and managed. Meta-data, also known as data about data, include information that describes the context, origin, and structure of other data. They can include details about file size, creation date, the author of a document, and modification histories. Communication data capture the exchange of information between users across various channels, such as email traffic, call logs, messages in social networks, and chat histories, including the involved parties, timestamps, and transmission paths. Procedural data describe the processes and operations within systems or organisations, including workflow documentations, logs of transactions and activities, and audit logs used for tracking and verifying procedures.
- **Personal Data:** "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, 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.
- **Processing:** The term "processing" covers a wide range and practically every handling of data, be it collection, evaluation, storage, transmission or erasure.
- **Profiles with user-related information:** The processing of "profiles with user-related information", or "profiles" for short, includes any kind of automated processing of personal data that consists of using these personal data to analyse, evaluate or predict certain personal aspects relating to a natural person (depending on the type of profiling, this may include different information concerning demographics, behaviour and interests, such as interaction with websites and their content, etc.) (e.g. interests in certain content or products, click behaviour on a website or location). Cookies and web beacons are often used for profiling purposes.
- **Remarketing:** Remarketing" or "retargeting" is the term used, for example, to indicate for advertising purposes which products a user is interested in on a website in order to remind the user of these products on other websites, e.g. in advertisements.
- **Targeting:** "Tracking" is the term used when the behaviour of users can be traced across several websites. As a rule, behavior and interest information with regard to the websites used is stored in cookies or on the servers of the tracking technology providers (so-called profiling). This information can then be used, for example, to display advertisements to users presumably corresponding to their interests.
- **Usage data:** Usage data refer to information that captures how users interact with digital products, services, or platforms. These data encompass a wide

range of information that demonstrates how users utilise applications, which features they prefer, how long they spend on specific pages, and through what paths they navigate an application. Usage data can also include the frequency of use, timestamps of activities, IP addresses, device information, and location data. They are particularly valuable for analysing user behaviour, optimising user experiences, personalising content, and improving products or services. Furthermore, usage data play a crucial role in identifying trends, preferences, and potential problem areas within digital offerings

- **Web Analytics:** Web Analytics serves the evaluation of visitor traffic of online services and can determine their behavior or interests in certain information, such as content of websites. With the help of web analytics, website owners, for example, can recognize at what time visitors visit their website and what content they are interested in. This enables them, for example, to better adapt the content of their websites to the needs of their visitors. For the purposes of web analytics , pseudonymous cookies and web beacons are often used to recognize returning visitors and thus obtain more precise analyses of the use of an online service.