

Table of contents

- Preamble
- Controller
- How to contact the data protection officer
- Overview, data origin and purposes of processing
- Relevant legal basis
- Security measures
- Transfer of personal data
- Data deletion
- Rights of data subjects
- Use of cookies
- Commercial operations
- Use of online platforms for promotional and sales purposes
- Credit checks
- Provision of the online offering and web hosting
- Additional information about applications (apps)
- Purchase of applications through app stores
- Contact and request management
- Chatbots and chat functions
- Push notifications
- Video conferences, online meetings, webinars and screen sharing
- Application process
- Cloud services
- Newsletter and electronic messages
- Advertising communication via email, post, fax or telephone
- Prize draws and competitions
- Surveys and questionnaires
- Web analysis, monitoring and optimisation
- Online marketing
- Presence on social networks (social media)
- Plugins and embedded functions and content
- Management, organisation and auxiliary tools
- Changing and updating the privacy policy
- Exclusion of liability/disclaimer

Preamble

The following privacy policy will inform you about the different types of personal data (hereinafter also referred to as "data") that we process, for what purposes and to what extent. The privacy policy applies to all processing of personal data, both in the context of providing our services and in particular on our websites, in mobile applications and within third-party online platforms, such as our social media profiles (hereinafter collectively referred to as "online offering").

Die verwendeten Begriffe sind nicht geschlechtsspezifisch.

Please also refer to the following documents:

Privacy policy for business partners and interested parties

https://www.hahn-kolb.de/media/downloads/pdf/kundenservice/Datenschutzhinweise_fuer_Geschaeftpartner_und_Interessenten.pdf

Privacy policy for employees and applicants

https://www.hahn-kolb.de/media/downloads/pdf/kundenservice/Datenschutzhinweise_fuer_Mitarbeitende_und_Bewerbende.pdf

Privacy policy regarding video surveillance

https://www.hahn-kolb.de/media/downloads/pdf/kundenservice/Datenschutzhinweise_fuer_Mitarbeitende_und_Bewerbende.pdf

Version: 22 January 2024

Controller

HAHN+KOLB, a company with headquarters in Ludwigsburg, Germany, is the controller and is responsible for the collection, processing and use of your personal data within the meaning of the GDPR. This means that HAHN+KOLB decides the purpose and means of processing personal data.

HAHN+KOLB Werkzeuge GmbH
Schlieffenstraße 40, D-71636 Ludwigsburg, Germany
PO Box 06 60, D-71606 Ludwigsburg, Germany

Email address: info@hahn-kolb.de

Tel.: +49 (0) 7141 498-40

Publication details: https://www.hahn-kolb.de/de/hahn_kolb/rechtliches/impressum/impressum.php

How to contact the data protection officer

datenschutz@hahn-kolb.de

Overview, data origin and purposes of processing

Our aim is very simple: to make our customers' work easier by providing tailored services, practical system solutions and an extensive range of products. We collect, process and use personal data in order to meet this business purpose or support secondary purposes, such as customer service.

Within our website, some of the data is processed for security purposes and to ensure that the content can be provided without errors. Other data may be used to analyse your user behaviour, measure reach and for marketing purposes. Your data is also processed for the purpose of responding to contact requests and communicating with you.

Children are not a target group for our website content.

How do we obtain your personal data?

Your data is collected when you provide it to us. For example, this could be data that you enter in a contact form. Other data is automatically collected by our IT systems when you visit our website. This is mainly technical data (e.g. Internet browser, operating system or time of page access). This information is automatically collected as soon as you access our website.

When you visit our website, your browsing behaviour can be statistically evaluated. This is primarily done using cookies and analytics programs. Analysis of your browsing behaviour is usually anonymous, meaning that browsing behaviour cannot be traced back to you. If you have given your consent, your preferred products can be evaluated after you register as a customer. You can object to this analysis or avoid it by not using certain tools. This privacy policy provides information on how to object.

The following overview summarises the types of data processed and the purposes of processing, along with the data subjects.

Types of data processed

- Subscriber data
- Payment data
- Location data
- Contact data
- Content data
- Contract data
- Usage data
- Metadata, communication data and process data
- Applicant data
- Images and/or videos
- Event data (Facebook)

Categories of data subject

- Customers
- Employees
- Interested parties
- Communication partners
- Users
- Applicants
- Prize draw and competition entrants
- Business and contractual partners
- Participants
- Persons depicted

Purposes of processing

- Provision of contractual services and fulfilment of contractual obligations
- Contact requests and communication
- Security measures
- Direct marketing
- Reach measurement
- Tracking
- Office and organisational processes
- Remarketing
- Conversion measurement
- Click tracking
- Target group formation
- A/B tests
- Managing and answering requests
- Application process
- Implementation of prize draws and competitions
- Feedback
- Heat maps
- Marketing
- Profiles with user information
- Provision of our online offering and usability
- Determination of credit rating and creditworthiness
- Establishment and implementation of employment relationships
- IT infrastructure

Automated decisions in individual cases

- Credit check

Relevant legal basis

HAHN+KOLB processes your personal data to ensure proper fulfilment of the contractual obligations arising from the contractual relationship between you or your employer and HAHN+KOLB or prior to entering into a contract (Art. 6[1][b] GDPR), for compliance with legal obligations to which HAHN+KOLB is subject (Art. 6[1][c] GDPR), and to protect the legitimate interests of HAHN+KOLB in processing your data (Art. 6 [1][f] GDPR). HAHN+KOLB will only ask for your consent to process your personal data in exceptional cases when none of the other legal bases can be used (Art. 6[1][a] GDPR).

In normal cases, our legitimate interest is to guarantee proper business operation, to secure and implement contracts with you or your employer and to maintain contact with you, our customer, to improve the quality of our customer service and to contact you more easily in the event of queries.

Only in exceptional cases will HAHN+KOLB also process special categories of personal data, known as sensitive data (e.g. health data in the event of accidents on HAHN+KOLB premises). In this case, processing is based either on your consent (Art. 6[2][a] GDPR) or it is required for the establishment, exercise or defence of legal claims (Art. 6[2][f] GDPR).

Relevant legal basis according to the GDPR: The following is an overview of the legal basis of GDPR, which we use as the basis for processing your personal data. Please note that in addition to the provisions of GDPR, national data protection regulations may apply in your or our country of residence or domicile. If more specific legal bases also apply in individual cases, we will inform you of these in the privacy policy.

- **Consent (Art. 6[1][1][a] GDPR):** The data subject has given consent to the processing of their personal data for one or more specific purposes.
- **Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR):** Processing is necessary for the 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.
- **Legal obligation (Art. 6[1][1][c] GDPR):** Processing is necessary for compliance with a legal obligation to which the controller is subject.
- **Legitimate interests (Art. 6[1][1][f] GDPR):** Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
- **Application process as a pre-contractual or contractual relationship (Art. 6[1][1][b] GDPR):** Insofar as special categories of personal data within the meaning of Art. 9(1) GDPR are requested from applicants as part of the application process (e.g. health data, such as severe disability or ethnic origin) so that the controller or the data subject can exercise their rights under employment and social security and social protection law and fulfil their obligations in this regard, processing is carried out in accordance with Art. 9(2)(b) GDPR. In the case of the protection of vital interests of applicants or other persons in accordance with Art. 9(2)(c) GDPR or for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or treatment or the management of health or social care systems and services in accordance with Art. 9(2)(h) GDPR. In the case of communication of special categories of data based on voluntary consent, processing is carried out on the basis of Art. 9(2)(a) GDPR.

National data protection regulations in Germany: National regulations for data protection in Germany apply in addition to the data protection regulations of the GDPR. This includes, in particular, the act on the protection against misuse of personal data in data processing (Federal Data Protection Act [BDSG]). In particular, the BDSG contains special provisions on the right of access, the right to erasure, the right to object, the processing of special categories of personal data, processing for other purposes and transfer, as well as automated individual decision-making, including profiling. The data protection laws of the individual federal states may also apply.

Information on the validity of the GDPR and Swiss FADP: This privacy policy serves to provide information in accordance with both the Swiss Federal Act on Data Protection (FADP) and the General Data Protection Regulation (GDPR). For this reason, please note that the terms of the GDPR are used on account of their broader geographical application and comprehensibility. In particular, instead of the terms "editing" of "personal data", "overriding interest" and "sensitive personal data" used in the FADP, we have used the terms "processing" of "personal data", "legitimate interest" and "special categories of data" as used in the GDPR. However, the legal meaning of the terms will continue to be interpreted in accordance with the Swiss FADP within the scope of its application.

Security measures

We take appropriate technical and organisational measures in accordance with the legal requirements, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of processing as well as the different probabilities of occurrence and the extent of the threat to the rights and freedoms of natural persons, in order to ensure a level of protection appropriate to the risk.

In particular, the measures include ensuring the confidentiality, integrity and availability of data by controlling physical and electronic access to the data as well as access, input, disclosure, availability and segregation of the relevant data. We have also established procedures to ensure that the rights of data subjects are observed, that data is deleted and that action is taken in response to any data breaches. Furthermore, we take the protection of personal data into account early on in the development and selection of hardware, software and processes in accordance with the principle of data protection, namely through technology design and the use of default settings that protect data.

Truncation of IP addresses: Where IP addresses are processed by us or by the service providers and technologies used by us and the processing of a full IP address is not required, the IP address will be truncated (also known as IP masking). In this case, the last two digits or the last part of the IP address after a dot are removed or replaced by placeholders. The purpose of truncating the IP address is to prevent or significantly impede the identification of a person on the basis of their IP address.

TLS/SSL encryption (https): We use TLS/SSL encryption to protect user data that is transmitted via our online services. Secure Sockets Layer (SSL) is the standard technology to secure Internet connections by encrypting data transmitted between a website or app and a browser (or between two servers). Transport Layer Security (TLS) is an updated and more secure version of SSL. Hyper Text Transfer Protocol Secure (HTTPS) is displayed in the URL if a website is secured by SSL/TLS certification.

Transfer of personal data

As part of our processing of personal data, it may be necessary to transfer or disclose the data to other departments, companies, legally independent organisational units or persons. The recipients of this data may include, for example, service providers contracted to perform IT tasks or providers of services and content that are integrated into a website. In such cases, we observe the legal requirements and, in particular, conclude appropriate contracts or agreements with the recipients of your data that serve to protect your data.

Data transfer within our company

We may transfer personal data to other departments within our company or grant them access to this data. If this transfer takes place for administrative purposes, the transfer of the data is based on our legitimate business and commercial interests or takes place if it is necessary to fulfil our contractual obligations or if the consent of the data subjects or legal permission has been obtained.

Data transfer within the WÜRTH Group

Within the WÜRTH Group, your data will be transmitted to specific companies if these companies perform data processing tasks for the affiliated companies centrally (e.g. cloud services, planning and execution of events and business trips, data collection in purchasing and sales).

If we disclose, transfer or otherwise grant access to data to other companies in our Group, this is done in particular for administrative purposes as a legitimate interest and, in addition, on a basis that complies with legal requirements. For this purpose, a group data transfer agreement has been concluded with the respective WÜRTH companies. In this case, C2P transfers are carried out in accordance with to Art. 28 GDPR (contract processing) and C2C transfers in accordance with Art. 26 GDPR (common responsibilities).

Data processing in the international online shop (AFO)

For customers/users registered in the international online shop (www.hahn-kolb.net), we automatically forward the orders to our subsidiary and sister companies and partner companies (**AFO = Automatically Forwarded Orders**). The entire business relationship, including service, contact, support etc., is handled by the responsible subsidiary/sister company or the partner company. The ordered items are delivered by HAHN+KOLB Werkzeuge GmbH Germany or by the responsible subsidiary or sister company or the partner company.

We reserve the right to store your company and contact details that are necessary for registration, future orders and the entire processing of your interests at HAHN+KOLB Werkzeuge GmbH Germany. We also reserve the right to pass on this data to our respective subsidiaries/sister companies or partner companies in order to store the data for the purpose of the order process. For this purpose, a group data transfer agreement has been concluded with the respective WÜRTH Group companies. In this case, C2P transfers are carried out in accordance with to Art. 28 GDPR (contract processing) and C2C transfers in accordance with Art. 26 GDPR (common responsibilities).

If the relevant data has to be transferred to recipients outside of the EU/EEC in order to fulfil the purpose, the appropriate level of protection usually comes from the presence of an adequacy decision by the European Commission, the use of

inter-company or external agreements based on EU standard data protection clauses (in accordance with Art. 46(2)(c) and (d) GDPR) or the presence of an exception provided by the GDPR for the specific case (in accordance with Art. 49(1) GDPR, e.g. the transfer is required for the fulfilment of the contract between you and HAHN+KOLB).

The legal basis for the processing of your personal data is - if you are acting in your own name - Art. 6(1)(b) GDPR (data processing for contract initiation and execution). If you are acting on behalf of a company or third party, the legal basis for the processing of your personal data is Art. 6(1)(f) GDPR (data processing based on overriding legitimate interest).

Our legitimate interest is:

- To ensure smooth business operation and to sell goods and services, increase customer loyalty, promote sales and increase revenue.
- Customer service and sales: Processing for the purpose of initiating business with customers concerning the supply and service offer from HAHN+KOLB Werkzeuge GmbH. In addition, processing for route and travel planning during visits and on-site support.
- Supply chain management: Processing for the fulfilment and processing of supply contracts with customers and suppliers and for the implementation of the logistics processes along the supply chain (e.g. transfer of data for order processing to manufacturers and suppliers for direct delivery if the goods are not in stock at HAHN+KOLB).

Your data will not be passed on to recipients who are not directly involved in the processing of your orders or interests.

The subsidiary, sister company or partner company responsible for the customer is defined according to the country in which the customer is based. The complete list of subsidiaries and partner companies worldwide can be found here:

https://www.hahn-kolb.de/de/hahn_kolb/unternehmen/standorte/standorte.php.

All other countries that are not listed are supported by HAHN+KOLB Werkzeuge GmbH Germany.

Data transfer to business partners

Outside our company and the WÜRTH Group, regular recipients of data are business partners (business contact data to suppliers, service providers, interested parties, customers, consultants and experts); hotels, airlines and manufacturers of navigation systems (e.g. for business trips); training and education providers, external trainers and lecturers, conference hotels, caterers (e.g. for training courses, seminars and events); auditors, credit agencies, legal representatives, patent lawyers, tax consultants, banks, company doctors, external safety experts, classification societies, certification bodies and auditors, funding bodies, health, social and accident insurance providers and other insurance companies.

Data processors: Data processors engaged by us may receive data from us according to Art. 28 GDPR (e.g. data centre service providers, IT partners, document shredders, printers and advertising service providers, providers of online meeting tools). Data processors may be third parties or other companies within the WÜRTH Group.

Data transfer to public bodies and institutions

In certain cases, we also pass on data to public bodies and institutions (e.g. supervisory authorities, financial authorities, courts, registration offices, road traffic authorities, research institutions, universities, patent offices, embassies and consulates) as well as to creditors and representatives of creditors. As part of the containment of pandemics/epidemics, recipients can also be regulatory and health authorities.

International data transfers

Data processing in third countries: If we process data in a third country (i.e. outside the European Union [EU] and the European Economic Area [EEA]) or if the processing takes place in the context of the user of third-party services or the disclosure or transfer of data to other persons, bodies or companies, this will only take place in accordance with the legal requirements. If the level of data protection in the third country has been recognised by means of an adequacy decision (Art. 45 GDPR), this serves as the basis for the data transfer. Otherwise, data transfers only take place if the level of data protection is otherwise ensured, in particular through standard contractual clauses (Art. 46[2][c] GDPR), express consent or in the case of contractual or legally required transfers (Art. 49[1] GDPR). We will also provide you with the basis for the transfer of data to third countries for the individual providers from the third country, with the adequacy decisions taking precedence as the basis. Information about third-country transfers and existing adequacy decisions can be found in the information provided by the European Commission: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en?prefLang=de.

EU-U.S. Trans-Atlantic Data Privacy Framework: As part of the Data Privacy Framework (DPF), the European Commission has also recognised the level of data protection for certain companies from the U.S. as secure within the framework of the adequacy decision of 10 July 2023. The list of certified companies and further information about the DPF can be found on the U.S. Department of Commerce website at <https://www.dataprivacyframework.gov/>. As part of the privacy policy, we will inform you which of the service providers engaged by us are certified under the Data Privacy Framework.

Data deletion

The data we process will be deleted in accordance with the legal requirements as soon as the consent for processing it is revoked or other permissions cease to apply (e.g. if the purpose for processing this data no longer applies or if it is not required for the purpose). If the data is not deleted because it is required for other and legally permissible purposes, its processing shall be limited to these purposes. This means the data is restricted and not processed for other purposes. This applies, for example, to data that must be retained for commercial or tax law reasons or whose storage is necessary for the establishment, exercise or defence of legal claims or to protect the rights of another natural or legal person. As part of our privacy policy, we can provide users with further information on the deletion and retention of data that applies specifically to the respective processing operations.

Rights of data subjects

Rights of data subjects according to the GDPR: As a data subject, you are entitled to various rights under the GDPR, which arise in particular from Art. 15 to 21 GDPR:

- **Right to object:** You have the right to object at any time and for reasons relating to your particular situation to the processing of your personal data based on Art. 6(1)(e) or (f) GDPR. This also applies to profiling based on these provisions. Where your personal data is processed for direct marketing purposes, you have the right to object at any time to the processing of your personal data for such marketing, including profiling to the extent that it is related to such direct marketing.

- **Right of revocation of consent:** You have the right to revoke your consent at any time.
- **Right to disclosure:** You have the right to request confirmation as to whether your data is being processed and to request information about this data, as well as further information and a copy of the data in accordance with legal requirements.
- **Right to rectification:** In accordance with legal requirements, you have the right to request the completion of your personal data or the correction of incorrect data.
- **Right to erasure and restriction of processing:** In accordance with legal requirements, you have the right to request that your personal data be deleted immediately or, alternatively, to request a restriction on the processing of the data in accordance with legal requirements.
- **Right to data portability:** You have the right to receive the personal data concerning you, which you provided us, in a structured, commonly used and machine-readable format or request its transmission to another controller in accordance with legal requirements.
- **Complaints to a supervisory authority:** In accordance with legal requirements 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 in the member state of your habitual residence, place of work or place of the alleged infringement if you believe that the processing of your personal data is in violation of the GDPR.

Use of cookies

Cookies are small text files or other storage tags that store information on end devices and read information from end devices. For example, to store the login status in a user account, the contents of a shopping basket in an online shop, the content accessed or the functions used in the online offering. Cookies can also be used for different purposes, e.g. for the functionality, security and convenience of the online offering, as well as for analysing visitor flows.

Information on consent: We use cookies in accordance with legal requirements. We therefore obtain prior consent from users, except where it is not required by law. In particular, consent is not required if the storage and reading of information, including cookies, is absolutely necessary to provide users with a telemedia service that they have expressly requested (i.e. our online offering). Strictly necessary cookies typically include cookies with functionality that is essential for the display and operability of the online offering, load balancing, security, storage of user preferences and choices, or similar purposes related to the provision of the main and secondary functions of the online offering requested by users. The revocable consent is clearly communicated to users and contains information on the respective cookie usage.

Information on the legal basis for data protection: The legal basis under data protection law on which we process users' personal data with the help of cookies depends on whether we ask users for their consent. If the users consent, the legal basis for processing their data is the consent they have given. Otherwise, the data processed using cookies will be processed on the basis of our legitimate interests (e.g. in the commercial operation of our online offering and improving its usability) or, if this is done in the course of fulfilling our contractual obligations, when the use of cookies is necessary to fulfil our contractual obligations. We explain the purposes for which we process cookies in this privacy policy or as part of our consent and processing procedures.

Retention period: With regard to the retention period, a distinction is made between the following types of cookie:

- **Temporary cookies (also referred to as session cookies):** Temporary cookies are deleted at the latest after a user has exited the online content and closed their end device (e.g. browser or mobile app).
- **Permanent cookies:** Permanent cookies continue to be stored even after the end device is closed. For example, the login status can be saved or favourite content can be displayed as soon as the user visits a website again. The user data collected with the help of cookies can also be used for reach measurement. Unless we provide users with explicit information about the type and retention period of cookies (e.g. when obtaining consent), users should assume that cookies are permanent and may be stored for up to two years.

General information about revocation and objection (or "opt out"): Users can revoke their consent at any time and object to processing in accordance with the legal requirements. Among other things, users can restrict the use of cookies in their browser settings (although this may also restrict the functionality of our online offering). You can also declare your objection to the use of cookies for online marketing purposes via the websites <https://optout.aboutads.info> and <https://www.youonlinechoices.com/>.

- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR). Consent (Art. 6[1][1][a] GDPR).

Further information on processing procedures, processes and services:

- **Processing of cookie data on the basis of content:** We use a cookie consent management process to obtain users' consent to the use of cookies and the processing and providers specified in the cookie consent management process, and to enable users to manage and withdraw their consent. This involves storing the declaration of consent so that the request does not need to be repeated and so that the consent can be proven in accordance with the legal obligation. The data may be stored on the server and/or in a cookie (referred to as an opt-in cookie or using a comparable technology) in order to be able to assign the consent to a user or their device. Subject to individual information about the providers of cookie management services, the following information applies: Consent may be stored for up to two years. A pseudonymous user identifier is created and stored with the time of consent, information on the scope of consent (e.g. which categories of cookies and/or service providers) as well as the browser, system and end device used; **Legal basis:** Consent (Art. 6[1][1][a] GDPR)
- **Piwik Pro Consent Manager (cookie consent management):** An individual user ID, the domain, the types of consent and the time the consent was given are stored on the server and in the cookie on the user's device. The group's internal operator of the consent manager is Würth IT GmbH on its own servers. The system is maintained with the support of the software provider Piwik Pro, based in Berlin (<https://piwikpro.de/>); **Service provider:** Würth IT GmbH, Industriepark Würth, Drillberg 6, 97980 Bad Mergentheim, Germany; **Website:** <https://www.wuerth-it.com>. **Privacy policy:** <https://www.wuerth-it.com/de/it/datenschutz.php>.

Commercial operations

We process data from our contractual and business partners, e.g. customers and interested parties (collectively referred to as "contractual partners") in the context of contractual and comparable legal relationships and related measures and in the context of communication with contractual partners (or pre-contractual), e.g. to answer queries.

We process this data to fulfil our contractual obligations. These include, in particular, the obligations to provide the agreed services, any updating obligations and remedies in the event of breaches of warranty and other service disruptions. We also process data to protect our rights and for the purposes of the administrative tasks associated with these obligations and our company organisation. Furthermore, we process the data on the basis of our legitimate interests in proper and efficient business management and in security measures to protect our contractual partners and our business operations from misuse, risks to their data, secrets, information and rights (e.g. for the involvement of telecommunications, transport and other auxiliary services as well as subcontractors, banks, tax and legal advisors, payment service providers or tax authorities). Within the framework of the applicable law, we only pass on the data of contractual parties to third parties to the extent that this is necessary for the aforementioned purposes or to fulfil legal obligations. Contractual partners will be informed about other forms of processing, e.g. for marketing purposes, in this privacy policy.

We will inform our contractual partners of which data is required for the aforementioned purposes before or during data collection, e.g. in online forms, by means of special labelling (e.g. colours) or symbols (e.g. asterisks or similar), or in person.

We will delete the data after the expiry of legal warranty and comparable obligations, i.e. generally after four (4) years, unless the data is stored in a customer account, e.g. as long as it must be retained for legal archiving reasons. The statutory retention period for tax-related documents, as well as for account books, inventories, opening balance sheets and annual financial statements, the work instructions required to understand these documents, and other organisational documents and accounting records is ten (10) years, and six (6) years for commercial and business letters received and reproductions of commercial and business letters sent. The period begins at the end of the calendar year in which the last entry was made in the book; the inventory, opening balance sheet, annual financial statement or management report was prepared; the commercial or business letter was received or sent or the accounting record was created; the record was made or the other documents were created.

If we use third-party providers or platforms to provide our services, the terms and conditions and privacy policies of the respective third-party providers or platforms apply to the relationship between the users and the providers.

- **Data types processed:** Subscriber data (e.g. names, addresses); payment data (e.g. bank details, invoices, payment history); contact data (e.g. email, telephone numbers); contract data (e.g. subject matter of the contract, term, customer category); usage data (e.g. websites visited, interest in content, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Interested parties, business and contractual partners. Customers.
- **Purposes of processing:** Provision of contractual services and fulfilment of contractual obligations; contact requests and communication; office and organisational processes; managing and answering requests; conversion

measurement (measuring the effectiveness of marketing measures). Profiles with user information (creating user profiles).

- **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR); legal obligation (Art. 6[1][1][c] GDPR). Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Online shop, e-commerce and delivery:** We process our customers' data to enable them to select, purchase or order the selected products, goods and related services, as well as to pay for and deliver them. If necessary for the fulfilment of an order, we use service providers, in particular postal, freight and shipping companies, to carry out the delivery or fulfilment for our customers. We use the services of banks and payment service providers to process payment transactions. The required information is labelled as such in the ordering process or comparable purchasing process and includes the information required for delivery or provision and billing, as well as contact information to allow any necessary consultations; **Legal basis:** We process your personal data - if you are acting on your own behalf - in accordance with Art. 6(1)(b) GDPR for the performance of our services and implementation of contractual measures (e.g. execution of order processes) and to the extent required by law (e.g. legally required archiving of business transactions for trade and tax purposes) according to Art. 6(1)(c) GDPR. The data processed, as well as the nature, scope and purpose and the necessity of its processing, is determined according to the underlying contractual relationship. If you are acting on behalf of a company/third party, the legal basis for the processing of your personal data is Art. 6(1)(f) GDPR (data processing based on overriding legitimate interest). In normal cases, the legitimate interest is to ensure proper business operation, to secure and implement contracts with you or your employer and to have contact with you, our customer, to improve the quality of our advice and to contact you more easily in the event of queries. In addition, our legitimate interest is also to provide the necessary guarantee for the security and integrity of the processes and systems in the context of the use of our online content. **Order processing agreement:** Data Transfer Agreement of the Würth Group; **Service provider:** Würth IT GmbH, Industriepark Würth, Drillberg 6, 97980 Bad Mergentheim, Germany; **Website:** <https://www.wuerth-it.com>. **Privacy policy:** <https://www.wuerth-it.com/de/it/datenschutz.php>.
- **Customer account:** Customers can create an account within our online offering (e.g. customer or user account, "customer account" for short). If the registration of a customer account is required, customers will be informed of this as well as the information required for registration. Customer accounts are not public and cannot be indexed by search engines. As part of the registration process and subsequent logins and use of the customer account, we store the IP addresses of customers together with the access times in order to be able to verify registration and prevent any misuse of the customer account. If the customer account has been cancelled, the customer account data will be deleted after the date of cancellation, unless it is stored for purposes other than provision in the customer account or must be stored for legal reasons (e.g. internal storage of customer data, order processes or invoices). It is the customer's responsibility to back up their data when cancelling their customer account. **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).
- **Watchlist/wish list:** Customers can create a product/wish list. In this case, the products will be stored as part of the fulfilment of our contractual obligations until the account is deleted, unless the product list entries are

removed by the customer or we expressly inform the customer of different retention periods; **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).

- **Personal product recommendations:** If you have consented to the use of cookies for personal product recommendations on our website, we will use your browsing behaviour for product recommendations on this website after you have logged in. This includes, in particular, product pages and product categories that you have visited or searched for on our websites. You can revoke your consent to analyse browsing behaviour at any time. Please note that we will then no longer be able to offer you product recommendations tailored to your browsing behaviour. **Legal basis:** The storage of cookies for the creation of personal product recommendations takes place on the basis of Art. 6(1)(a) GDPR and Section 25(1) TTDSG (German Telecommunications Telemedia Data Protection Act), your consent. You can prevent the storage of cookies by not giving us your consent. However, we would advise you that doing so may prevent you from using all of the functions on this website to their full extent. If you do not give your consent, product recommendations will be shown on the basis of the currently displayed website content. The information generated by cookies for personal product recommendations will not be passed on to third parties. **Retention period:** If you do not or no longer agree to the storage and use of your data, you can adjust the storage and use here. In this case, your decision is stored in the form of a cookie. If you delete your cookies, this cookie will also be deleted. When you visit our site again, you will be asked again whether cookies may be used.
- **Shopping basket reminders:** When you add products to your shopping basket in our online shop, we give you the option of receiving shopping basket reminders. This function can be useful, for example, if the purchase process could not be continued due to a browser crash, oversight or forgetting. The processing of shopping basket reminders is based on your consent (Art. 6[1][a] GDPR and Section 25[1] TTDSG). You can revoke your consent to the processing of data for sending shopping basket reminders at any time, for example via the "unsubscribe" link in the email. The legality of data processing operations already carried out shall remain unaffected by this revocation. **Shopping basket reminders by email sent via Inxmail:** We use the Inxmail service to send shopping basket reminders by email. Inxmail is a service that can be used, among other things, to organise and analyse the dispatch of newsletters. The data processed for the purpose of subscribing to the newsletter is stored on Inxmail servers in Germany. **Data analysis by Inxmail:** To analyse the success of our shopping basket reminders, the emails sent with Inxmail contain a web beacon or tracking pixel, which is triggered by interactions with the email. This provides information such as whether a shopping basket reminder has been opened, whether links have been clicked or at what time the email was read.

The following data is processed by Inxmail as part of the success analysis:

- Master data (e.g. name, address)
- Contact data (e.g. email address, telephone number)
- Metadata and communication data (e.g. device information, IP address)
- Usage data (e.g. interests, access times)

Revocation of consent to the success analysis can also be declared separately. If you want to prevent analysis by Inxmail, you can disable the analysis in the corresponding newsletter. We provide a corresponding link in each shopping basket reminder for this purpose.

Legal basis: The data processing is based on your consent (Art. 6[1][a] GDPR and Section 25[1] TTDSG). You may revoke this consent at any time. The legality of data processing operations already carried out shall remain unaffected by this revocation. **Retention period:** The data processed by us for the purpose of receiving

shopping basket reminders from us will be stored by us until you unsubscribe from the recipient list for shopping basket reminders and will be deleted after cancellation. Data stored by us for other purposes (e.g. email addresses for registration in the online shop) shall remain unaffected by this. **Order processing agreement:** We have concluded an order processing agreement with email service provider Inxmail in accordance with Art. 28 GDPR; **Service provider:** Inxmail GmbH, Wentzingerstr. 17, 79106 Freiburg, Germany; **Website:** <https://www.inxmail.de>. **Privacy policy:** <https://www.inxmail.de/datenschutz>.

- **Transaction emails:** We use Inxmail to send transaction emails related to your orders. Transaction emails are emails that are automatically sent after certain business transactions, such as order confirmations or delivery notifications.

The following data is processed by Inxmail as part of the sending of transaction emails:

- Technical information about the recipient's end device: Operating system, information about the browser used, recipient's IP address, other information about the end device and the Internet connection;
- Recipient's contact data: Email address, name if necessary
- Data about user interaction: Information about opened newsletter, links clicked, date and time of the interaction

Legal basis: Data processing for the dispatch of transaction emails related to your orders is carried out for contractual purposes. Data processing for the purposes of documenting the fulfilment of information obligations is carried out on the basis of Art. 6(1)(f) GDPR (processing for the purposes of legitimate interests of the controller).

Retention period: The data you provide us for the purpose of receiving transaction emails will be deleted both from our servers and the Inxmail servers as part of the regular deletion routine after dispatch. The data stored by us for the purpose of documenting the fulfilment of information obligations will be deleted both from our servers and the Inxmail servers as part of the regular deletion routine after a period of six (6) months after the email has been sent. **Order processing agreement:** We have concluded an order processing agreement with email service provider Inxmail in accordance with Art. 28 GDPR; **Service provider:** Inxmail GmbH, Wentzingerstr. 17, 79106 Freiburg, Germany; **Website:** <https://www.inxmail.de>. **Privacy policy:** <https://www.inxmail.de/datenschutz>.

- **Online courses and online training:** We process the data of the participants of our online courses and online training (collectively referred to as "participants") in order to provide them with our course and training services. The data processed, as well as the nature, scope, purpose and the necessity of its processing, is determined according to the underlying contractual relationship. The data generally includes information on the courses taken and services used and, to the extent that they are part of our range of services, personal specifications and results of the participants. The forms of processing also include the performance assessment and evaluation of our services and those of the course and training instructors; **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).
- **Software and platform service offering:** We process the data of our users, registered users and any test users (hereinafter collectively referred to as "users") in order to provide them with our contractual services and, on the basis of legitimate interests, to ensure the security of our offering and to be able to develop it further. The required information is labelled as such as in the order, purchase order or comparable contract and includes the information required for provision of services and billing, as well as contact information to allow any necessary consultations; **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).

- **Technical services:** We process the data of our customers and clients (hereinafter collectively referred to as "customers") to enable them to select, purchase or commission the selected services or works and related activities, as well as to pay for and provide or execute or perform them. The required information is labelled as such as in the order, purchase order or comparable contract and includes the information required for provision of services and billing, as well as contact information to allow any necessary consultations. Provided we obtain access to information from end customers, employees or other persons, we process this in accordance with the legal and contractual requirements; **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).
- **Administration, accounting, office organisation and contact management:** We process data in the context of administrative tasks and the organisation of our operations, financial accounting and compliance with legal obligations, such as archiving. In doing so, we process the same data that we process in the course of providing our contractual services. Customers, interested parties, business partners and website visitors are affected by the processing. The purpose of and our interest in the processing lies in the administration, financial accounting, office organisation, archiving of data, that is tasks that serve to maintain our business activities, perform our tasks and provide our services. The deletion of data in relation to contractual services and communication corresponds to the information specified for these processing activities. We disclose or transmit data to the tax authorities, consultants, such as tax advisors or auditors, as well as other fee agencies and payment service providers. Furthermore, we store information about suppliers, event organisers and other business partners on the basis of our business interests, for example for the purpose of contacting them at a later date. We generally store this data, which is mostly company-related, permanently. **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR), legitimate interests (Art. 6[1][1][f] GDPR).
- **Economic analyses and market research:** For business reasons and to identify market trends and the wishes of contractual partners and users, we analyse the data we have on business transactions, contracts, enquiries etc. The group of data subjects may include contractual partners, interested parties, customers, visitors and users of our online offering. The analyses are carried out for the purpose of business evaluations, marketing and market research (e.g. to determine customer groups with different characteristics). In doing so, we may take into account the profiles of registered users, if available, together with their details, such as the services used. The analyses are for our use only and will not be disclosed externally, unless they are anonymous analyses with summarised, i.e. anonymised, values. Furthermore, we respect the privacy of users and process the data for analysis purposes as pseudonymously and, if feasible, anonymously (e.g. as summarised data) as possible; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).

Use of online platforms for promotional and sales purposes

We offer our services on online platforms that are operated by other service providers. In this context, the privacy policies of the respective platforms apply in addition to our privacy policy. This applies in particular with regard to the execution of the payment process and the procedures used on the platforms for reach measurement and interest-based marketing.

- **Data types processed:** Subscriber data (e.g. names, addresses); payment data (e.g. bank details, invoices, payment history); contact data (e.g. email, telephone numbers); contract data (e.g. subject matter of the contract, term, customer category); usage data (e.g. websites visited, interest in content, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Customers.
- **Purposes of processing:** Provision of contractual services and fulfilment of contractual obligations. Marketing.
- **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).

Further information on processing procedures, processes and services:

- **Mercateo:** Online procurement platform for business customers; Legal basis: Legitimate interests (Art. 6[1][1][f] GDPR); **Service provider:** Mercateo Deutschland AG, Museumsgasse 4-5, 06366 Köthen, Germany; **Website:** <https://www.mercateo.com/>. **Privacy policy:** <https://www.mercateo.com/procure/datenschutz/>.
- **Wucato:** Online procurement platform for business customers; Legal basis: Legitimate interests (Art. 6[1][1][f] GDPR); **Service provider:** WUCATO Marketplace GmbH, Feuerseeplatz 14, 70176 Stuttgart, Germany; **Website:** <https://www.wucato.de/>. **Privacy policy:** <https://www.wucato.de/de/wucato/datenschutz/datenschutz.php>.

Credit checks

If we provide advance services or enter into comparable economic risks (e.g. when ordering on account), we reserve the right to obtain identity and credit information from specialised service providers (credit agencies) for the purpose of assessing the credit risk on the basis of mathematical and statistical procedures in order to safeguard legitimate interests.

We process the information obtained from the credit agencies on the statistical probability of a payment default as part of an appropriate discretionary decision on the establishment, execution and termination of the contractual relationship. We reserve the right to refuse payment on account or any other advance service in the event the credit check returns a negative result.

In accordance with the legal requirements, the decision as to whether we provide advance services is made solely on the basis of an automated decision in individual cases, which is carried out by our software based on the information provided by the credit agency.

If we obtain the express consent of contractual partners, this consent serves as the legal basis for the credit check and the transmission of the customer's data to the credit agencies. If consent is not obtained, the credit check is carried out on the basis of our legitimate interests in the reliability of our payment claims.

- **Data types processed:** Subscriber data (e.g. names, addresses); payment data (e.g. bank details, invoices, payment history); contact data (e.g. email, telephone numbers); contract data (e.g. subject matter of the contract, term, customer category); usage data (e.g. websites visited, interest in content, access times).
- **Data subjects:** Customers; interested parties. Business and contractual partners.
- **Purposes of processing:** Determination of credit rating and creditworthiness.
- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).
- **Automated decisions in individual cases:** Credit report (decision on the basis of a credit check).

Further information on processing procedures, processes and services:

- **CRIF Bürgel GmbH:** Credit agency; **Service provider:** CRIF Bürgel GmbH, Radlkoferstraße 2, 81373 Munich, Germany; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.crifbuergel.de/>. **Privacy policy:** <https://www.crifbuergel.de/datenschutz>.
- **Verband der Vereine Creditreform e.V.:** Credit agency; **Service provider:** Verband der Vereine Creditreform e.V., Hellersbergstraße 12, D-41460 Neuss, Germany; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.creditreform.de/>. **Privacy policy:** <https://www.creditreform.de/datenschutz>.

Provision of the online offering and web hosting

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

- **Data types processed:** Usage data (e.g. websites visited, interest in content, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status); content data (e.g. entries in online forms).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of our online offering and usability; IT infrastructure (operation and provision of information systems and technical devices [computers, servers etc.]); security measures.
- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Provision of our online offering:** Services in the area of provision of IT infrastructure and related services (e.g. storage space and/or computing capacity); **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Order processing agreement:** Data Transfer Agreement of the Würth Group; **Service provider:** Würth IT GmbH, Industriepark Würth, Drillberg 6, 97980 Bad Mergentheim, Germany; **Website:** <https://www.wuerth-it.com/>. **Privacy policy:** <https://www.wuerth-it.com/de/it/datenschutz.php>.
- **Collection of access data and log files:** Accessing of our online offering is logged in the form of server log files. The server log files may include the address and name of the websites and files accessed, the date and time of access, the amount of data transferred, notification of successful access, browser type and 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, for example to avoid overloading the servers (especially in the case of abusive attacks, referred to as DDoS attacks), and to ensure the utilisation and stability of the servers; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR). **Data deletion:** Log file information is stored for a duration of up to thirty (30) days and is then deleted or anonymised. Data that must be retained longer for evidence purposes will be excluded from deletion until the incident in question has been definitively clarified.
- **Email dispatch and hosting:** The web hosting services we use also include sending, receiving and storing emails. For these purposes, the addresses of the recipients and senders as well as other information relating to the sending of emails (e.g. the providers involved) and the content of the respective emails are processed. The aforementioned data may also be processed for the purpose of detecting spam. Please note that emails on the Internet are generally not sent in encrypted form. As a rule, emails are encrypted in transit, but not on the servers from which they are sent and received (unless an end-to-end encryption method is used). We therefore accept no responsibility for the transmission of emails from the sender to our server; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).

- **Akamai Content Delivery Network (CDN):** Service that can be used to deliver the content of an online offering, in particular large media files such as graphics or program scripts, faster and more securely with the help of regionally distributed servers connected via the Internet. The group's internal operator of the service is Würth IT GmbH on its own servers. Maintenance of the system is carried out with the support of the software provider, Akamai Technologies Belgium SRL (<https://www.akamai.com>); **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Order processing agreement:** Data Transfer Agreement of the Würth Group; **Service provider:** Würth IT GmbH, Industriepark Würth, Drillberg 6, 97980 Bad Mergentheim, Germany; **Website:** <https://www.wuerth-it.com>. **Privacy policy:** <https://www.wuerth-it.com/de/it/datenschutz.php>.

Additional information about applications (apps)

We process the data of the users of our application to the extent necessary to provide the users with the application and its functionalities, to monitor its security and to develop it further. We may also contact users in compliance with legal requirements if communication is necessary for the administration or use of the application. The processing of user data is detailed in the data protection information in this privacy policy.

Legal basis: The processing of data required for the provision of the application's functionalities serves to fulfil contractual obligations. This also applies if user authorisation is required to provide the functions (e.g. enabling device functions). If the processing of data is not necessary for the provision of the application's functionalities, but serves the security of the application or our business interests (e.g. collection of data for the purpose of optimising the application or security purposes), it is carried out on the basis of our legitimate interests. If users are expressly asked to consent to the processing of their data, the data covered by the consent is processed on the basis of the consent.

- **Data types processed:** Subscriber data (e.g. names, addresses); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status); payment data (e.g. bank details, invoices, payment history); contract data (e.g. subject matter of the contract, term, customer category). Location data (information on the geographical position of a device or person).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of contractual services and fulfilment of contractual obligations.
- **Legal basis:** Consent (Art. 6[1][1][a] GDPR); performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR). Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Commercial use:** We process the data of the users of our application, registered users and any test users (hereinafter collectively referred to as "users") in order to provide them with our contractual services and, on the basis of legitimate interests, to ensure the security of our application and to be able to develop it further. The required information is labelled as such as part of the usage, order, purchase order or comparable contract and may include the information required for provision of services and billing, as well as contact information to allow any necessary consultations; **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).
- **Storage of a universally unique identifier (UUID):** The application stores a universally unique identifier (UUID) for the purposes of analysing the use and functionality of the application and for storing user settings. This identifier is generated when this application is installed (but is not linked to the device, so it is not a device identifier in that sense), remains stored between launches of the application and its updates, and is deleted when users remove the application from their device.
- **Device authorisations for accessing functions and data:** The use of our application or its functionalities may require user authorisation to allow access to certain functions of the devices used or to the data stored on the devices or data that can be accessed using the devices. By default, these authorisations must be granted by

users and can be revoked at any time in the settings of the respective devices. The exact procedure for managing app authorisations may vary depending on the device and the user's software. Users can contact us if they require further clarification. We would advise you that the denial or revocation of the respective authorisations can affect the functionality of our application.

- **Processing of location data:** As part of the use of our application, location data collected from the device used or location data otherwise entered by the user is processed. The use of location data requires user authorisation, which may be revoked at any time. The use of location data is only for the purpose of providing the respective functionality of our application, in accordance with its description to users, or its typical and expected functionality.

Purchase of applications through app stores

Our application can be obtained from special online platforms operated by other service providers, known as app stores. In this context, the privacy policies of the respective app stores apply in addition to our privacy policy. This applies in particular with regard to the procedures used on the platforms for reach measurement and interest-related marketing as well as any fees that may be charged.

- **Data types processed:** Subscriber data (e.g. names, addresses); payment data (e.g. bank details, invoices, payment history); contact data (e.g. email, telephone numbers); contract data (e.g. subject matter of the contract, term, customer category); usage data (e.g. websites visited, interest in content, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status); content data (e.g. entries in online forms).
- **Data subjects:** Customers; users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of contractual services and fulfilment of contractual obligations. Marketing.
- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Apple App Store:** App and software sales platform; **Service provider:** Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.apple.com/de/app-store/>. **Privacy policy:** <https://www.apple.com/legal/privacy/de-ww/>.
- **Google Play:** App and software sales platform; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://play.google.com/store/apps?hl=de>. **Privacy policy:** <https://policies.google.com/privacy>.

Contact and request management

When contacting us (e.g. by post, contact form, email, telephone or via social media) as well as in the context of existing user and business relationships, the details of the person enquiring are processed, provided this is necessary to answer the contact enquiries and any actions requested.

- **Data types processed:** Contact data (e.g. email, telephone numbers); content data (e.g. entries in online forms); usage data (e.g. websites visited, interest in contents, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status); subscriber data (e.g. names, addresses); contract data (e.g. subject matter of the contract, term, customer category).
- **Data subjects:** Communication partners; customers; interested parties. Business and contractual partners.
- **Purposes of processing:** Contact requests and communication; managing and answering requests; feedback (e.g. collecting feedback via online form); provision of our online offering and usability; provision of contractual services and fulfilment of contractual obligations. Office and organisational processes.
- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR). Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).

Further information on processing procedures, processes and services:

- **SAP Cloud Services for sales and marketing:** CRM system; customer management and process and sales support with personalised customer care with multi-channel communication, i.e. management of customer requests from different channels and with analysis and feedback functions; Legal basis: Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR), legitimate interests (Art. 6[1][1][f] GDPR); order processing agreement: <https://www.sap.com/germany/docs/download/agreements/product-use-and-support-terms/dpa/data-processing-agreement-for-cloud-services-german-v8-2021.pdf>; **Service provider:** SAP Deutschland SE & Co. KG, Hasso-Plattner-Ring 7, 69190 Walldorf, Germany; **Website:** www.sap.com. **Privacy policy:** www.sap.com/germany/about/trust-center/data-privacy.html.
- **Contact form:** When users contact us via our contact form, email or other communication channels, we process the data provided to us in this context in order to deal with the matter in question; **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR), legitimate interests (Art. 6[1][1][f] GDPR).
- **SnapAddy:** Collection, supplementation and management of contact information from individual and public sources; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Service provider:** SnapAddy GmbH, Haugerkirchgasse 7, 97070 Würzburg, Germany; **Order processing agreement:** <https://www.snapaddy.com/de/privacy-security-hub/datenschutz.html>; **Website:** <https://www.snapaddy.com/de/>; **Privacy policy:** <https://www.snapaddy.com/de/privacy-security-hub/datenschutz.html>.

Chatbots and chat functions

We offer online chats and chatbot functions as an option for communication (collectively referred to as "chat services"). A chat is an online conversation that takes place within a certain amount of time. A chatbot is a piece of software that answers the users' questions or informs them about messages. When you use our chat functions, we may process your personal data.

If you use our chat services within an online platform, your identification number will also be stored within the respective platform. In addition, we may collect information about which users interacted with our chat services and when. Furthermore, we store the content of your conversations via the chat services and log registration and consent processes in order to provide evidence of these in accordance with legal requirements.

We would advise users that the respective platform provider can find out whether and when users communicate with our chat services and can collect technical information about the user's device used and, depending on the settings of their device, also location information (known as metadata) for the purposes of optimising the respective services and for security purposes. Likewise, the metadata from communication via chat services (i.e. information such as who has communicated with whom) may be used by the respective platform providers in accordance with their terms and conditions (please refer to these for further information) for marketing purposes or to display targeted advertising.

If users give their consent to a chatbot to enable information with regular messages, they have the option to unsubscribe from the information in the future at any time. The chatbot tells users how and with which terms they can unsubscribe from the messages. When unsubscribing from the chatbot messages, the user's data will be deleted from the directory of message recipients.

We use the aforementioned information to operate our chat services, such as to address users personally, to respond their queries, to provide any requested content and also to improve our chat services (e.g. to 'teach' chatbots answers to frequently asked questions or to detect unanswered queries).

Information on legal basis: We use the chat services on the basis of consent if we have previously obtained the users' consent to the processing of their data in the context of our chat services (this applies to cases in which users are asked for consent, e.g. so that a chatbot can send them regular messages). If we use chat services to answer users' enquiries about our services or our company, this is done for the purposes of contractual and pre-contractual communication. We also use chat services on the basis of our legitimate interests in optimising chat services, their operational efficiency and improving the user experience.

Revocation, objection and deletion: You can revoke consent given at any time or object to the processing of your data in the context of our chat services.

- **Data types processed:** Contact data (e.g. email, telephone numbers); content data (e.g. entries in online forms); usage data (e.g. websites visited, interest in contents, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partners.
- **Purposes of processing:** Contact requests and communication; direct marketing (e.g. by email or post).

- **Legal basis:** Consent (Art. 6[1][1][a] GDPR); performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR). Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Luware Chat:** Chat and assistance software and associated services. The data is processed on the chat system and displayed for the customer and agent. No data is stored on the server. The group's internal operator of the service is Würth IT GmbH on its own servers. Maintenance of the system is carried out with the support of the software provider, Luware AG, Zurich (<https://luware.com>); **Legal basis:** Contract or contract initiation (Art. 6[1][1][b] GDPR), legitimate interests (Art. 6[1][1][f] GDPR); **Order processing agreement:** Data Transfer Agreement of the Würth Group; **Service provider:** Würth IT GmbH, Industriepark Würth, Drillberg 6, 97980 Bad Mergentheim, Germany; **Website:** www.wuerth-it.com. **Privacy policy:** www.wuerth-it.com/de/it/datenschutz.php.

Push notifications

With user's consent, we can send users push notifications. These are messages that are displayed on users' screens, end devices or browsers, even when our online service is not actively being used.

To register for push notifications, users must confirm the request from their browser or end device to receive push notifications. This agreement process is documented and stored. The storage is necessary to verify whether users have consented to receive push notifications and to be able to provide evidence of this consent. For these purposes, a pseudonymous browser identifier (known as a "push token") or the device ID of an end device is stored.

The push notifications may be necessary for the fulfilment of contractual obligations (e.g. technical and organisational information relevant to the use of our online services) and are otherwise sent on the basis of the user's consent, unless specifically mentioned below. Users can change their push notification settings at any time under the notification settings of their respective browsers or end devices.

- **Data types processed:** Usage data (e.g. websites visited, interest in content, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partners.
- **Purposes of processing:** Provision of our online offering and usability; reach measurement (e.g. access statistics, recognising returning visitors).
- **Legal basis:** Consent (Art. 6[1][1][a] GDPR). Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).

Further information on processing procedures, processes and services:

- **Analysis and success measurement:** We statistically evaluate push notifications in order to determine whether and when push notifications have been displayed and clicked on. This information is used for the technical improvement of our push notifications using the technical data or the target groups and their access behaviour or the access times. This analysis also includes determining whether the push notifications are opened, when they are opened and whether users interact with their content or buttons. For technical reasons, this information can be linked to the individual push notification recipients. However, it is neither our aim nor that of the push notification service provider, if used, to monitor individual users. Rather, the analyses help us to recognise the usage habits of our users and to adapt our push notifications to them or to send different push notifications according to the interests of our users. The analysis of push notifications and the success measurement are carried out on the basis of express consent of the user, which is given with the agreement to receive push notifications. Users can object to the analysis and success measurement by unsubscribing from push notifications. Unfortunately, it is not possible to revoke consent for analysis and success measurement separately;
Legal basis: Consent (Art. 6[1][1][a] GDPR).

Video conferences, online meetings, webinars and screen sharing

We use platforms and applications from other providers (hereinafter referred to as "conference platforms") for the purposes of conducting video and audio conferences, webinars and other types of video and audio meetings (hereinafter collectively referred to as "conference"). We comply with the legal requirements when selecting conference platforms and their services.

Data processed by conference platforms: When participating in a conference, the conference platforms process the following personal data of the participants. The scope of the processing depends on what data is required for a specific conference (e.g. access data or real names) and what optional information is provided by the participants. In addition to the processing required in order to hold the conference, the participants' data may also be processed by the conference platforms for security purposes or service optimisation. The processed data includes personal data (first name, last name), contact information (email address, telephone number), access data (access codes or passwords), profile pictures, information on professional position/function, the IP address of the Internet access, information on the participants' end devices, their operating systems, the browser and its technical and language settings, information on the content of communication processes, i.e. entries in chats as well as audio and video data, and the use of other available functions (e.g. surveys). The content of the communications is encrypted to the extent technically provided by the conference providers. If the participants are registered as users with the conference platforms, further data may be processed in accordance with the agreement with the respective conference provider.

Logging and recordings: If text entries, participation results (e.g. from surveys) and video or audio recordings are logged, this will be transparently communicated to the participants in advance and, if necessary, they will be asked to provide their consent.

Data protection measures of the participants: Please refer to the privacy policies of the conference platforms for details of how they process your data and select the security and privacy settings that are best for you when you adjust the settings of the conference platforms. Please also ensure that data and privacy protection is implemented in the background for the duration of your video conference (e.g. by notifying housemates, locking doors and, as far as technically possible, using the background blurring function). Links to the conference rooms and access data must not be passed on to unauthorised third parties.

Information on legal basis: If, in addition to the conference platforms, we also process users' data and ask users for their consent to use the conference platforms or certain functions (e.g. consent to the recording of conferences), this consent will serve as the legal basis for processing. Furthermore, our processing may be necessary to fulfil our contractual obligations (e.g. in participant lists, in the case of processing the results of discussions etc.). Otherwise, user data is processed on the basis of our legitimate interests in efficient and secure communication with our communication partners.

- **Data types processed:** Subscriber data (e.g. names, addresses); contact data (e.g. email, telephone numbers); content data (e.g. entries in online forms); usage data (e.g. websites visited, interest in contents, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partners; users (e.g. website visitors, users of online services). Persons depicted.

- **Purposes of processing:** Provision of contractual services and fulfilment of contractual obligations; contact requests and communication. Office and organisational processes.
- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Microsoft Teams:** Conferencing and communication software; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.microsoft.com/de-de/microsoft-365>; **Privacy policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security notice: <https://www.microsoft.com/de-de/trustcenter>. **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF), standard contractual clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>).
- **TeamViewer:** Conferencing and communication software; **Service provider:** TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen, Germany; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.teamviewer.com/de/>. **Privacy policy:** <https://www.teamviewer.com/de/legal/privacy-and-cookies/>.

Application process

The application process requires that applicants provide us with the data necessary for their assessment and selection. The information required can be found in the job description or, in the case of online forms, in the information provided there.

The required information generally includes personal details such as your name, address and contact details, as well as proof of the qualifications required for the position. We will be happy to provide additional information on what details are required on request.

If provided, applicants can send us their applications using an online form. The data will be encrypted and transmitted to us using the latest technology. Applicants can also send us their applications by email. However, please note that emails on the Internet are generally not sent in encrypted form. As a rule, emails are encrypted in transit, but not on the servers from which they are sent and received. We therefore accept no responsibility for the transmission of the application from the sender to our server.

For the purposes of searching for applicants, submitting applications and selecting applicants, we may use applicant management or recruitment software and platforms and services from third-party providers in compliance with legal requirements.

Applicants are welcome to contact us about how to submit their application or send us their application by post.

Processing of special categories of data: Insofar as special categories of personal data (Art. 9[1] GDPR, e.g. health data, such as severe disability or ethnic origin) are requested from applicants or communicated by them as part of the application process, processing is carried out so that the controller or the data subject can exercise their rights under employment and social security and social protection law and fulfil their obligations in this regard. In the case of the protection of vital interests of applicants or other persons or for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or treatment or the management of health or social care systems and services.

Data deletion: In the event of a successful application, the data provided by applicants may be further processed by us for the purposes of the employment relationship. Otherwise, if the application is unsuccessful, the applicants' data will be deleted. Applicants' data will also be deleted if an application is withdrawn, which applicants are entitled to do at any time. Subject to a justified revocation by the applicant, the deletion will take place at the latest after a period of six (6) months, so that we can answer any follow-up questions regarding the application and fulfil our obligations to provide evidence under the regulations on equal treatment of applicants. Invoices for any reimbursement of travel expenses will be archived in accordance with tax regulations.

Inclusion in an applicant pool: Inclusion in an applicant pool, if offered, is based on consent. Applicants are informed that their consent to inclusion in the talent pool is voluntary, has no influence on the current application process and that they can revoke their consent at any time in the future.

- **Data types processed:** Subscriber data (e.g. names, addresses); contact data (e.g. emails, telephone numbers); content data (e.g. entries in online forms); applicant data (e.g. personal information, postal and contact addresses, the documents belonging to the application and the information contained therein, such as cover letter, CV, certificates and other personal and qualification information provided by applicants for a specific position or voluntarily).

- **Data subjects:** Applicants
- **Purposes of processing:** Application process (justification and possible subsequent implementation and possible subsequent termination of the employment relationship).
- **Legal basis:** Application process as pre-contractual or contractual relationship (Art. 6[1][1][b] GDPR). Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Privacy policy for employees and applicants:** Please also note our detailed privacy policy for employees and applicants: https://www.hahn-kolb.de/media/downloads/pdf/kundenservice/Datenschutzhinweise_fuer_Mitarbeitende_und_Bewerbende.pdf.
- **Recruitment on LinkedIn:** Job search and application-related services within the LinkedIn platform (searching for employees, communication, application process, contract negotiations); **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Order processing agreement:** <https://legal.linkedin.com/dpa>; **Service provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Website:** <https://www.linkedin.com>. **Privacy policy:** <https://www.linkedin.com/legal/privacy-policy>.
- **Ausbildung.de:** Services in connection with the recruitment of trainees and students (searching for trainees and students, communication, application process, contract negotiations); **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Service provider:** Ausbildung.de GmbH, Wittener Str. 87, 44789 Bochum, Germany; **Website:** <https://www.ausbildung.de/>. **Privacy policy:** <https://www.ausbildung.de/datenschutz/>.
- **StepStone:** Services in connection with employee acquisition/recruitment (searching for employees, communication, application process, contract negotiations); **Service provider:** StepStone Deutschland GmbH, Völklinger Straße 1, 40219 Düsseldorf, Germany; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.stepstone.de>. **Privacy policy:** <https://www.stepstone.de/Ueber-StepStone/Rechtliche-Hinweise/datenschutzerklaerung/>.

Cloud services

We use software services that are accessible via the Internet and run on their providers' servers (known as "cloud services" or "software as a service") for the storage and management of content (e.g. document storage and management, document sharing, sharing content and information with specific recipients or publishing content and information).

In this context, personal data may be processed and stored on the providers' servers, insofar as these are part of communication processes with us or are otherwise processed by us, as set out in this privacy policy. This data may include, in particular, master data and contact data of users, data on transactions, contracts, other processes and their content. Cloud service providers also process usage data and metadata for security purposes and service optimisation.

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

- **Data types processed:** Subscriber data (e.g. names, addresses); contact data (e.g. email, telephone numbers); content data (e.g. entries in online forms); usage data (e.g. websites visited, interest in contents, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status); images and/or videos (e.g. photographs or videos of a person).
- **Data subjects:** Customers; employees (e.g. staff, applicants, former employees); interested parties. Communication partners.
- **Purposes of processing:** Office and organisational processes; IT infrastructure (operation and provision of information systems and technical devices [computers, servers etc.]). Provision of contractual services and fulfilment of contractual obligations.
- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Adobe Creative Cloud:** Cloud storage, cloud infrastructure services and cloud-based application software, e.g. for photo editing, video editing, graphic design, web development; **Service provider:** Adobe Systems Software Ireland, 4-6, Riverwalk Drive, Citywest Business Campus, Brownsbarn, Dublin 24, D24 DCW0, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).; **Website:** <https://www.adobe.com/de/creativecloud.html>; **Privacy policy:** <https://www.adobe.com/de/privacy.html>, **Order processing agreement:** Provided by the service provider. **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF), standard contractual clauses (provided by the service provider).
- **Microsoft cloud services:** Cloud storage, cloud infrastructure and cloud-based application software; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).; **Website:** <https://www.microsoft.com/de-de>; **Privacy policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security notice: <https://www.microsoft.com/de-de/trustcenter>; **Order processing agreement:**

<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>.

Basis for transfer to third countries: EU-U.S. 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 messages

We send newsletters, emails and other electronic notifications (hereinafter "newsletters") only with the consent of the recipient or where legally permitted to do so. If the contents of a newsletter are specifically described in the registration process, this information is decisive for the user's consent. Our newsletters also contain information about our services and us.

To subscribe to our newsletters, you will usually only need to provide your email address. However, we may ask you to provide a name so that we can address you personally in the newsletter, or other information necessary for the purposes of the newsletter.

Double opt-in process: Registration for our newsletter is always carried out using a double opt-in process. This means that after registering, you will receive an email asking you to confirm your registration. This confirmation is necessary to prevent someone from registering with another person's email addresses. Newsletter registrations are logged in order to prove the registration in accordance with legal requirements. This includes storing the time of registration and confirmation as well as the IP address. Changes to your data stored by the email service provider are also logged.

Deletion and restriction of processing: We may store unsubscribed email addresses for up to three (3) years on the basis of our legitimate interests before deleting them to allow us to prove that consent was previously given. The processing of this data is limited to the purpose of a possible defence against claims. An individual request for deletion is possible at any time, provided that the prior existence of consent is confirmed at the same time. In the event of obligations to permanently observe objections, we reserve the right to store the email address in a block list solely for this purpose.

The registration process is logged on the basis of our legitimate interests for the purpose of proving that it has been carried out properly. If we commission a service provider to send emails, this is done on the basis of our legitimate interests in an efficient and secure dispatch system.

Content: Information about us, our products and services, promotions and offers.

- **Data types processed:** Subscriber data (e.g. names, addresses); contact data (e.g. email, telephone numbers); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partners.
- **Purposes of processing:** Direct marketing (e.g. by email or post).
- **Legal basis:** Consent (Art. 6[1][1][a] GDPR).
- **Option to object (opt out):** You can cancel 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 at the bottom of every newsletter, or you can use one of the contact options listed above, preferably email.

Further information on processing procedures, processes and services:

- **Email service provider Inxmail:** The newsletter is sent using email dispatch and automation service Inxmail. Inxmail is a service that can be used, among other things, to organise and analyse the dispatch of newsletters.

The data you enter for the purpose of subscribing to the newsletter is stored on Inxmail servers in Germany. The mailing service provider may use the recipients' data in pseudonymous form, i.e. without assigning it to a user, to optimise or improve its own services, for example for technical optimisation of the dispatch and presentation of the newsletter or for statistical purposes. However, the mailing service provider does not use the data of our newsletter recipients to contact them directly or to pass the data on to third parties. If you want to prevent analysis by Inxmail, you will need to unsubscribe from the corresponding newsletter. We provide a link in each newsletter email for this purpose. **Order processing agreement:** We have concluded an order processing agreement with email service provider Inxmail in accordance with Art. 28 GDPR.

Legal basis: Legitimate interests (Art. 6[1][1][f] GDPR); **Service provider:** Inxmail GmbH, Wentzingerstr. 17, 79106 Freiburg, Germany; **Website:** <https://www.inxmail.de>. **Privacy policy:** <https://www.inxmail.de/datenschutz>.

- **Measurement of opening and click rates:** The newsletters contain a web beacon, which is a pixel-sized file that is retrieved from our server when the newsletter is opened or, if we use a mailing service provider, from their server. As part of this retrieval, technical information, such as information about the browser and your system, as well as your IP address and the time of retrieval, is initially collected. This information is used for the technical improvement of our newsletter based on the technical data or the target groups and their reading behaviour based on their retrieval locations (which can be determined using the IP address) or the access times. This analysis also includes determining whether the newsletters are opened, when they are opened and which links are clicked. This information is assigned to the individual newsletter recipients and stored in their profiles until they are deleted. The analyses help us to recognise the reading habits of our users and to adapt our content to them or to send different content according to the interests of our users. The measurement of opening rates and click rates and the storage of the measurement results in the user profiles and their further processing are carried out on the basis of the user's consent. Unfortunately, it is not possible to cancel the performance measurement separately - you will need to cancel or object to the entire newsletter subscription. In this case, the stored profile information will be deleted. Legal basis: Consent (Art. 6[1][1][a] GDPR).

Advertising communication via email, post, fax or telephone

We process personal data for the purpose of advertising communication, which may take place through various channels, such as email, telephone, post or fax, in accordance with legal requirements.

Recipients have the right to withdraw their consent at any time or to object to advertising communication at any time.

After revocation or objection, we store the data required to prove the previous authorisation for contacting or sending for up to three (3) years after the end of the year of revocation or objection on the basis of our legitimate interests. The processing of this data is limited to the purpose of a possible defence against claims. On the basis of the legitimate interest in permanently observing revocation or objection by users, we also store the data required to prevent further contact (e.g. depending on the communication channel, email address, telephone number, name).

- **Data types processed:** Subscriber data (e.g. names, addresses); contact data (e.g. email, telephone numbers).
- **Data subjects:** Communication partners.
- **Purposes of processing:** Direct marketing (e.g. by email or post).
- **Legal basis:** Consent (Art. 6[1][1][a] GDPR). Legitimate interests (Art. 6[1][1][f] GDPR).

Prize draws and competitions

We process the personal data of entrants in prize draws and competitions only in compliance with the relevant data protection regulations, insofar as the processing is contractually required for the provision, implementation and organisation of the competition, the entrants have consented to the processing or the processing serves our legitimate interests (e.g. in the security of the competition or the protection of our interests against misuse through the possible collection of IP addresses when submitting competition entries).

If entrants' entries are published as part of the competitions (e.g. as part of a vote or presentation of the competition entries or the winners or reporting on the competition), we would advise you that the names of the entrants may also be published in this context. Entrants can object to this at any time.

If the competition takes place within an online platform or a social network (e.g. Facebook or Instagram, hereinafter referred to as "online platform"), the terms of use and data protection provisions of the respective platforms also apply. In these cases, we would advise that we are responsible for the information provided by the entrants as part of the competition and that enquiries regarding the competition should be addressed to us.

Entrants' data will be erased as soon as the competition has ended and the data is no longer required to inform the winners, or because queries about the competition are no longer expected. Generally, entrants' data will be erased no later than six (6) months after the end of the competition. Winners' data may be retained for longer, for example in order to answer queries about the prizes or to fulfil the prize. In this case, the retention period depends on the type of prize and is up to three (3) years, for example in the case of items or services, in order to be able to process warranty claims. Furthermore, entrants' data may be stored for longer, for example as part of reporting on the competition in online and offline media.

If data has also been collected for other purposes as part of the competition, its processing and the retention period are based on the privacy policy for this use (e.g. in the case of registration for the newsletter as part of a competition).

- **Data types processed:** Subscriber data (e.g. names, addresses); content data (e.g. entries in online forms); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Prize draw and competition entrants.
- **Purposes of processing:** Implementation of prize draws and competitions.
- **Legal basis:** Performance of a contract and steps prior to entering into a contract (Art. 6[1][1][b] GDPR).

Surveys and questionnaires

We conduct surveys and questionnaires in order to collect information for the communicated purpose of the survey and questionnaire. The surveys and questionnaires (hereinafter referred to as "surveys") we conduct are analysed anonymously. Personal data is only processed to the extent that this is necessary for the provision and technical implementation of the surveys (e.g. processing of the IP address to display the survey in the user's browser or to enable the survey to be resumed with the help of a cookie).

- **Data types processed:** Contact data (e.g. email, telephone numbers); content data (e.g. entries in online forms); usage data (e.g. websites visited, interest in contents, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partners. Participants.
- **Purposes of processing:** Feedback (e.g. collecting feedback via online forms).
- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Microsoft Forms:** Creation and evaluation of online forms, surveys, feedback forms etc.; Legal basis: Legitimate interests (Art. 6[1][1][f] GDPR); **Standard contractual clauses:** <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>; **Order processing agreement:** <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Website:** <https://microsoft.com/de-de>. **Privacy policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security notice: <https://www.microsoft.com/de-de/trustcenter>.

Web analysis, monitoring and optimisation

Web analysis (also referred to as "reach measurement") is used to evaluate the flow of visitors to our online offering and may include behaviour, interests or demographic information about visitors, such as age or gender, as pseudonymous values. With the help of reach analysis, we can, for example, identify the time at which our online offering or its functions or content are most frequently used or prompt users to revisit. We can also understand which areas require optimisation.

In addition to web analysis, we may also use test procedures, for example to test and optimise different versions of our online offering or its components.

Unless otherwise stated below, profiles, i.e. data summarised for a usage process, can be created for these purposes and information can be stored in a browser or end device and read out from it. The information collected includes, in particular, websites visited and the elements used there as well as technical information such as the browser used, the computer system used and information on usage times. If users have consented to the collection of their location data by us or by the providers of the services we use, location data may also be processed.

The IP addresses of users are also stored. However, we use an IP masking process (i.e. pseudonymisation by truncating the IP address) to protect users. Generally, no plain user data (such as email addresses or names) is stored for web analysis, A/B testing and optimisation purposes; instead, pseudonyms are used. This means that neither we nor the providers of the software used know the actual identity of users, but only the information stored in their profiles for the purposes of the respective processes.

- **Data types processed:** Usage data (e.g. websites visited, interest in content, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Remarketing; target group formation; reach measurement (e.g. access statistics, detection of returning visitors); profiles with user-related information (creating user profiles); provision of our online offering and usability; tracking (e.g. interest/behaviour-related profiling, use of cookies); click tracking; A/B tests. Heat maps (mouse movements by the user, which are summarised to form an overall picture).
- **Security measures:** IP masking (pseudonymisation of the IP address).
- **Legal basis:** Consent (Art. 6[1][1][a] GDPR).

Further information on processing procedures, processes and services:

- **Web analysis on the basis of Matomo:** Our website uses functions of our own web analysis service, which is based on open source software Matomo (formerly Piwik). The group's internal operator of the web analysis service is Würth IT GmbH on its own servers. The system is maintained with the support of the software provider Piwik Pro, based in Berlin (<https://piwikpro.de/>).

Data types processed: The browser type and version you are using, the operating system you are using, your country of origin, the date and time of the server request, the number of visits, the time you spend on the website and the external links you click on. The IP address of the user is anonymised before storage.

Cookies: Our web analysis uses cookies. These are text files that are stored on your computer and enable analysis of how you use the website. The processed data can be used to create pseudonymised user profiles. For this purpose, the information generated by the cookies about the use of our website is stored on our server. The information generated by the cookie about the use of our website will not be passed on to third parties. You can refuse the storage of cookies using the appropriate setting in your browser software; however, we would advise you that doing so may prevent you from using all of the functions of our online offering to their full extent.

IP anonymisation: We use IP anonymisation. This means we truncate your IP address before storage. We use this information to analyse your use of our online offering, to compile reports on website activity and to provide other services relating to website activity and Internet usage.

Legal basis: Consent (Art. 6[1][a] GDPR), legitimate interests (Art. 6[1][f] GDPR); **Order processing agreement:** Data Transfer Agreement of the Würth Group. **Service provider:** Würth IT GmbH, Industriepark Würth, Drillberg 6, 97980 Bad Mergentheim, Germany; **Website:** <https://www.wuerth-it.com/>. **Privacy policy:** <https://www.wuerth-it.com/de/it/datenschutz.php>

Option to object (opt out): You can object to the anonymised collection of data by the Matomo program at any time with effect for the future by clicking on the link below. In this case, an opt-out cookie is stored in your browser, which means that Matomo no longer collects any session data and thus no information about your personal browsing behaviour is stored. The opt-out cookie has a retention period of two (2) years. However, if you delete your cookies, the opt-out cookies will also be deleted and must therefore be reactivated by you.

[Hier bitte den Link zum Consent-Banner einfügen!]

[Please insert the link to the consent banner here!]

- **Google Analytics 4:** We use Google Analytics to measure and analyse the use of our online offering on the basis of a pseudonymous user identification number. This identification number does not contain any unique data, such as names or email addresses. It is used to assign analysis information to an end device in order to recognise what content users have accessed within one or more usage processes, what search terms they have used, what content they have accessed again or how they have interacted with our online offering. The time and duration of use are also stored, as well as the sources of the users who provide links to our online offering and technical aspects of their end devices and browsers. Pseudonymised user profiles are created with information from the use of various devices, for which cookies may be used. Google Analytics does not log or store any individual IP addresses for EU users. However, Analytics provides rough geographic location data by deriving the following metadata from IP addresses: City (and the city's derived latitude and longitude), continent, country, region, subcontinent (and ID-based counterparts). For EU traffic, the IP address data is used exclusively for this derivation of geolocation data before it is immediately deleted. It is not logged, is not accessible and is not used for any other purpose. When Google Analytics collects measurement data, all IP queries are performed on EU-based servers before the traffic is forwarded to Analytics servers for processing; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal basis:** Consent (Art. 6[1][1][a] GDPR); **Website:** <https://marketingplatform.google.com/intl/de/about/analytics/>; **Privacy policy:** <https://policies.google.com/privacy>; **Data processing agreement:** <https://business.safety.google/adsprocessorterms/>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF), standard contractual clauses (<https://business.safety.google/adsprocessorterms/>); **Option to object (opt out):** Opt-out plugin: <https://tools.google.com/dlpage/gaoptout?hl=de>, Settings for the

display of adverts: <https://myadcenter.google.com/personalizationoff>. **Further information:** <https://business.safety.google/adsservices/> (types of processing and the data processed).

- **Google Analytics in consent mode:** In consent mode, Google processes users' personal data for measurement and advertising purposes according to the users' consent. Consent is obtained from users as part of our online services. If users do not give their consent at all, the data is only processed at an aggregated level (i.e. not assigned to individual users and summarised). If the consent only includes statistical measurement, no personal data of the users will be processed for the display of adverts or the measurement of advertising success (known as "conversion"); **Legal basis:** Consent (Art. 6[1][1][a] GDPR). **Website:** <https://support.google.com/analytics/answer/9976101?hl=de>.
- **Target group formation with Google Analytics:** We use Google Analytics to display the adverts placed by Google and its partners within advertising services only to those users who have also shown an interest in our online offering or who have certain characteristics (e.g. interests in certain topics or products determined on the basis of the websites visited), which we transmit to Google (known as "remarketing audiences" or "Google Analytics audiences"). With the help of remarketing audiences, we also want to ensure that our adverts are relevant to the potential interests of users; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal basis:** Consent (Art. 6[1][1][a] GDPR); **Website:** <https://marketingplatform.google.com>; **Legal basis:** <https://business.safety.google/adsprocessorterms/>; **Privacy policy:** <https://policies.google.com/privacy>; **Order processing agreement:** <https://business.safety.google/adsprocessorterms/>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF); **Further information:** Types of processing and the data processed: <https://business.safety.google/adsservices/>. Data processing conditions for Google advertising products and standard contractual clauses for data transfer to third countries: <https://business.safety.google/adsprocessorterms>.
- **Google Tag Manager:** Google Tag Manager is a solution that allows us to manage website tags via an interface and thus integrate other services into our online offering (further information can be found in this privacy policy). Tag Manager itself (which implements the tags) therefore does not create user profiles or store cookies, for example. Google only learns the IP address of the user, which is necessary to run Google Tag Manager; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal basis:** Consent (Art. 6[1][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 transfer to third countries:** EU-U.S. Data Privacy Framework (DPF), standard contractual clauses (<https://business.safety.google/adsprocessorterms>).
- **Hotjar Observe:** Software for analysis and optimisation of online offers on the basis of pseudonymised measurements and analyses of user behaviour, which may include, in particular, A/B tests (measurement of the popularity and usability of different content and functions), measurement of click paths and interaction with content and functions of the online offering (heat maps and recordings); **Legal basis:** Consent (Art. 6[1][1][a] GDPR); **Option to object (opt out):** <https://www.hotjar.com/policies/do-not-track/>; **Data deletion:** The cookies that Hotjar uses have different "lifespans"; some remain valid for up to 365 days, some only during the current visit; **Cookie guidelines:** <https://help.hotjar.com/hc/de/articles/115011789248-Cookies-auf-hotjar-com>; **Service provider:** Hotjar Ltd., 3 Lyons Range, 20 Bisazza Street, Sliema SLM 1640, Malta; **Website:**

<https://www.hotjar.com>; **Privacy policy:** <https://www.hotjar.com/legal/policies/privacy/de/>; **Order processing agreement:** <https://www.hotjar.com/de/legal/support/dpa/>

- **Kameleoon:** Web analysis, reach measurement, A/B testing and analysis of user behaviour in terms of usage and interests regarding functions and content as well as their duration of use on the basis of a pseudonymous user identification number and profile creation; **Service provider:** Kameleoon SAS, 12, rue de la Chaussée d'Antin 75009 Paris, France; **Legal basis:** Consent (Art. 6[1][1][a] GDPR); **Website:** <https://www.kameleoon.com/>; **Privacy policy:** <https://www.kameleoon.com/de/datenschutz>.

Online marketing

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

For these purposes, user profiles are created and stored in a file (known as a "cookie"), or similar methods are used to store user information relevant to the presentation of the aforementioned content. This information may include, for example, content viewed, websites visited, online networks used, as well as communication partners and technical information such as the browser used, the computer system used and information on usage times and functions used. If users have consented to the collection of their location data, this can also be processed.

The IP addresses of users are also stored. However, we use available IP masking processes (i.e. pseudonymisation by truncating the IP address) to protect users. Generally, no plain user data (such as email addresses or names) is stored as part of the online marketing process; instead, pseudonyms are used. This means that neither we nor the providers of the online marketing process used know the actual identity of users, but only the information stored in their profiles.

The information in the profiles are generally stored in the cookies or using a similar process. These cookies can generally also be read later on other websites that use the same online marketing process and analysed for the purpose of displaying content as well as supplemented with further data and stored on the server of the online marketing process provider.

In exceptional cases, plain 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 process we use and the network links the user profiles with the aforementioned data. Please note that users can make additional agreements with the providers, e.g. by giving their consent when registering.

We only receive access to summarised information about the success of our adverts. However, as part of conversion measurements, we can check which of our online marketing processes have led to a conversion, for example, to the conclusion of a contract with us. The conversion measurement is used solely to analyse the success of our marketing measures.

Unless otherwise stated, you should assume that the cookies used are stored for a period of two (2) years.

- **Data types processed:** Usage data (e.g. websites visited, interest in content, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status); event data (Facebook) ("event data" is data that can be transmitted by us to Facebook via Facebook pixels [via apps or in other ways], for example, and relates to people or their actions; the data includes, for example, information about visits to websites, interactions with content, functions, app installations, product purchases etc.; the event data is processed for the purpose of creating target groups for content and advertising information [custom audiences]; event data does not include the actual content [such as comments written], no login information and no contact information [i.e. no names, email addresses or telephone numbers]. Event data will be deleted by Facebook after a maximum of two [2] years, and the target groups formed from it will be deleted when our Facebook account is deleted).
- **Data subjects:** Users (e.g. website visitors, users of online services).

- **Purposes of processing:** Reach measurement (e.g. access statistics, detection of returning visitors); tracking (e.g. interest/behaviour-related profiling, use of cookies); marketing; profiles with user information (creating user profiles); conversion measurement (measurement of the effectiveness of marketing measures); target group formation; provision of our online offering and usability. Remarketing.
- **Security measures:** IP masking (pseudonymisation of the IP address).
- **Legal basis:** Consent (Art. 6[1][1][a] GDPR). Legitimate interests (Art. 6[1][1][f] GDPR).
- **Option to object (opt out):** We refer to the privacy policies of the respective providers and the opt-out options provided by the providers. If no explicit opt-out option has been specified, you have the option of disabling cookies in your browser settings. However, this may restrict the functions of our online offering. We therefore recommend the following additional opt-out options, which are summarised for the respective regions:
 - a) Europe: <https://www.youronlinechoices.eu>.
 - b) Canada: <https://www.youradchoices.ca/choices>.
 - c) USA: <https://www.aboutads.info/choices>.
 - d) All regions: <https://optout.aboutads.info>.

Further information on processing procedures, processes and services:

- **Google Ads and conversion measurement:** Online marketing methods for the purpose of displaying content and adverts within the service provider's advertising network (e.g. in search results, in videos, on websites etc.) so that they are displayed to users who are presumed to have an interest in the adverts. We also measure the conversion of the adverts, i.e. whether users have chosen to interact with the adverts and take advantage of the advertised offers (known as "conversion"). However, we only receive anonymous information and no personal information about individual users; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal basis:** Consent (Art. 6[1][1][a] GDPR), legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://marketingplatform.google.com>; **Privacy policy:** <https://policies.google.com/privacy>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF); **Further information:** Types of processing and the data processed: <https://business.safety.google/adsservices/>. Data processing conditions between the controller and standard contractual clauses for data transfer to third countries: <https://business.safety.google/adscontrollerterms>.
- **Google Ads remarketing:** Google remarketing, also known as retargeting, is a technology whereby users who use an online service are included in a pseudonymous remarketing list so that users can be shown adverts on other online offerings based on their visit to the online service; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal basis:** Consent (Art. 6[1][1][a] GDPR); **Website:** <https://marketingplatform.google.com>; **Privacy policy:** <https://policies.google.com/privacy>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF); **Further information:** Types of processing and the data processed: <https://business.safety.google/adsservices/>. Data processing conditions between the controller and standard contractual clauses for data transfer to third countries: <https://business.safety.google/adscontrollerterms>.
- **Microsoft Advertising:** Online marketing methods for the purpose of displaying content and adverts within the service provider's advertising network (e.g. in search results, in videos, on websites etc.) so that they are

displayed to users who are presumed to have an interest in the adverts. We also measure the conversion of the adverts, i.e. whether users have chosen to interact with the adverts and take advantage of the advertised offers (known as "conversion"). However, we only receive anonymous information and no personal information about individual users; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal basis:** Consent (Art. 6[1][1][a] GDPR), legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://about.ads.microsoft.com/en-us>; **Privacy policy:** <https://privacy.microsoft.com/de-de/privacystatement>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF); **Option to object (opt out):** <https://account.microsoft.com/privacy/ad-settings/>. **Further information:** <https://about.ads.microsoft.com/de-de/policies/legal-privacy-and-security>.

- **Facebook adverts:** Display of adverts within the Facebook platform and evaluation of the advertising results; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal basis:** Consent (Art. 6[1][1][a] GDPR); **Website:** <https://www.facebook.com>; **Privacy policy:** <https://www.facebook.com/about/privacy>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF); **Option to object (opt out):** We refer to the privacy and advertising settings in the users' profiles on the Facebook platforms as well as to Facebook's consent procedures and contact options for exercising disclosure and other data subject rights, as described in Facebook's privacy policy; **Further information:** Event user data, i.e. behavioural and interest data, is processed for the purposes of targeted advertising and target group formation on the basis of the agreement on joint controllership ("Addendum for Controllers", https://www.facebook.com/legal/controller_addendum). Joint controllership is limited to the collection by and transfer of data to Meta Platforms Ireland Limited, a company based in the EU. The further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which in particular concerns the transfer of the data to parent company Meta Platforms, Inc. in the USA (on the basis of the standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).
- **Instagram adverts:** Display of adverts within the Instagram platform and evaluation of the advertising results; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal basis:** Consent (Art. 6[1][1][a] GDPR); **Website:** <https://www.instagram.com>; **Privacy policy:** <https://instagram.com/about/legal/privacy>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF); **Option to object (opt out):** We refer to the privacy and advertising settings in the users' profiles on the Instagram platform as well as part of Instagram's consent procedures and Instagram's contact options for exercising disclosure and other data subject rights in Instagram's privacy policy; **Further information:** Event user data, i.e. behavioural and interest data, is processed for the purposes of targeted advertising and target group formation on the basis of the agreement on joint controllership ("Addendum for Controllers", https://www.facebook.com/legal/controller_addendum). Joint controllership is limited to the collection by and transfer of data to Meta Platforms Ireland Limited, a company based in the EU. The further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which in particular concerns the transfer of the data to parent company Meta Platforms, Inc. in the USA (on the basis of the standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).

Presence on social networks (social media)

We maintain an online presence on social networks and process user data in this context in order to communicate with the users active there or to provide information about us.

We would advise that user data may be processed outside the European Union. This may result in risks for users because, for example, it could make it more difficult to enforce users' rights.

Furthermore, user data is generally processed within social networks for market research and advertising purposes. For example, user profiles can be created based on user behaviour and the resulting interests of users. The user profiles can in turn be used, for example, to place adverts within and outside the networks that are likely to align with the interests of the users. For these purposes, cookies are usually stored on the user's computer, which contain the user's usage behaviour and interests. Furthermore, data can also be stored in the user profiles independently of the devices used by the users (especially if the users are members of the respective platforms and are logged in to them).

For a detailed description of the respective forms of processing and the opt-out options, please refer to the privacy policies and information provided by the operators of the respective networks.

In the case of disclosure requests and the assertion of data subject rights, we would also advise that these can be asserted most effectively with the providers. Only the providers have access to the users' data and can take appropriate measures and provide information directly. If you still need help, you can contact us.

- **Data types processed:** Contact data (e.g. email, telephone numbers); content data (e.g. entries in online forms); usage data (e.g. websites visited, interest in contents, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Contact requests and communication; feedback (e.g. collecting feedback via online forms). Marketing.
- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Instagram:** Social network; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.instagram.com>. **Privacy policy:** <https://instagram.com/about/legal/privacy>.
- **Facebook pages:** Profiles within the Facebook social network; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.facebook.com>; **Privacy policy:** <https://www.facebook.com/about/privacy>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF), standard contractual clauses (https://www.facebook.com/legal/EU_data_transfer_addendum); **Further information:** We are jointly responsible with Meta Platforms Ireland Limited for the collection (but not the further processing) of data of visitors to our Facebook page ("fan page"). This data includes information about the types of content users view

or interact with, or the actions they take (see also "Activities and information provided by you and others" in the Facebook privacy policy: <https://www.facebook.com/policy>), and information about the devices used by users (e.g. IP addresses, operating system, browser type, language settings, cookie data; see also "Device information" in the Facebook privacy policy: <https://www.facebook.com/policy>). As explained in the Facebook privacy policy under "How do we use your information?", Facebook also collects and uses information to provide analytics services, known as "Page Insights", to page administrators to help them understand how people interact with their pages and the content associated with them. We have concluded a special agreement with Facebook ("Information about Page Insights", https://www.facebook.com/legal/terms/page_controller_addendum), which regulates in particular which security measures Facebook must observe, and in which Facebook has agreed to fulfil the rights of data subjects (i.e. users can, for example, send disclosure or deletion requests directly to Facebook). The rights of users (in particular to disclosure, deletion, objection and appeal to the competent supervisory authority) are not restricted by the agreements with Facebook. Further information can be found in "Information about Page Insights" (https://www.facebook.com/legal/terms/information_about_page_insights_data). Joint controllership is limited to the collection by and transfer of data to Meta Platforms Ireland Limited, a company based in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which in particular concerns the transmission of the data to parent company Meta Platforms, Inc. in the USA.

- **LinkedIn:** Social network; **Service provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.linkedin.com>; **Privacy policy:** <https://www.linkedin.com/legal/privacy-policy>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF), standard contractual clauses (<https://legal.linkedin.com/dpa>); **Option to object (opt out):** <https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>; **Further information:** We are jointly responsible with LinkedIn Ireland Unlimited Company for the collection (but not further processing) of visitors' data for the purpose of creating the "page insights" (statistics) of our LinkedIn profiles. This data includes information about the types of content users view or interact with, or the actions they take, as well as information about the devices used by users (e.g. IP addresses, operating system, browser type, language settings, cookies data) and information from the user's profile, such as job role, country, industry, hierarchy level, company size and employment status. Data protection information on the processing of user data by LinkedIn can be found in LinkedIn's privacy policy: <https://www.linkedin.com/legal/privacy-policy>
We have concluded a special agreement with LinkedIn Ireland ("Page Insights Joint Controller Addendum (the "Addendum")", <https://legal.linkedin.com/pages-joint-controller-addendum>), which regulates in particular which security measures LinkedIn must observe, and in which LinkedIn has agreed to fulfil the rights of data subjects (i.e. users can, for example, send disclosure or deletion requests directly to LinkedIn). The rights of users (in particular to disclosure, deletion, objection and appeal to the competent supervisory authority) are not restricted by the agreements with LinkedIn. Joint responsibility is limited to the collection of data by and transmission to the Ireland Unlimited Company, a company based in the EU. Further processing of the data is the sole responsibility of Ireland Unlimited Company, in particular the transmission of data to parent company LinkedIn Corporation in the USA.
- **YouTube:** Social network and video platform; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Privacy policy:**

<https://policies.google.com/privacy>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF). **Option to object (opt out):** <https://myadcenter.google.com/personalizationoff>.

- **Xing:** Social network; **Service provider:** New Work SE, Am Strandkai 1, 20457 Hamburg, Germany; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.xing.com/>. **Privacy policy:** <https://privacy.xing.com/de/datenschutzerklaerung>.

Plugins and embedded functions and content

We incorporate functional and content elements into our online offering that are obtained from the servers of their respective providers (hereinafter referred to as "third-party providers"). These may be, for example, graphics, videos or maps (hereinafter collectively referred to as "content").

Integration always requires that the third-party providers of this content process the IP address of the user, as they would not be able to send the content to their browser without the IP address. The IP address is therefore required to display this content or function. We endeavour to use only content from providers who use IP addresses solely for the purpose of delivering content. Third-party providers may also use pixel tags (invisible graphics, also known as "web beacons") for statistical or marketing purposes. Pixel tags can be used to analyse information such as visitor traffic on the pages of this website. The pseudonymous information may also be stored in cookies on the user's device and may contain, among other things, technical information about the browser and operating system, referring websites, time of visit and other information about the use of our online offering, and may also be linked to such information from other sources.

- **Data types processed:** Usage data (e.g. websites visited, interest in content, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status); subscriber data (e.g. names, addresses); contact data (e.g. email, telephone numbers); content data (e.g. entries in online forms). Location data (information on the geographical position of a device or person).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of our online offering and usability; feedback (e.g. collecting feedback via online forms). Security measures.
- **Legal basis:** Consent (Art. 6[1][1][a] GDPR). Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **Google Maps:** We integrate maps from the Google Maps service provided by Google. The processed data may include, in particular, IP addresses and user location data; **Service provider:** Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland; **Legal basis:** Consent (Art. 6[1][1][a] GDPR); **Website:** <https://mapsplatform.google.com/>; **Privacy policy:** <https://policies.google.com/privacy>. **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF).
- **Google Fonts (provision on our own servers):** Provision of font files for the purpose of a user-friendly presentation of our online offering; **Service provider:** Google Fonts are hosted on our server, and no data is transmitted to Google; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).
- **YouTube videos:** Video content; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal basis:** Consent (Art. 6[1][1][a] GDPR); **Website:** <https://www.youtube.com>; **Privacy policy:** <https://policies.google.com/privacy>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF). **Option to object (opt out):** Opt-out plugin: <https://tools.google.com/dlpage/gaoptout?hl=de>, Settings for the display of adverts: <https://myadcenter.google.com/personalizationoff>.

- **Catalogue browser:** The platform and application for digitising print media enable the conversion or alternative presentation of physical catalogues, brochures and magazines into digital flip page catalogues and offer the integration of multimedia elements, links and analysis functions; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Service provider:** COMINTO GmbH, Klosterstraße 49, 40210 Düsseldorf, Germany; **Website:** <https://www.blaetterkatalog.de/>. **Privacy policy:** <https://www.blaetterkatalog.de/de/datenschutz/>.
- **QR codes:** When using QR codes, we do not use any tracking cookies. There is only one cookie set on your device, which shows which codes you have previously accessed, in order to display a list of the accessed codes. No personal data is stored or passed on in this process. No tracking or advertising cookies from Facebook, Google Analytics or similar are used. As the operator of the QR code platform and our service provider, we only see when and how often a code was accessed, but not by whom. No conclusion can be drawn from the data. The aim is for us to analyse the effectiveness of QR code advertising. However, this technology is not designed to track individuals or profile natural persons. We attach great importance to the protection of personal data, which is why only anonymised IP addresses of QR code users are stored. By default, the last three digits of your IP address are replaced with 'x' (i.e. one byte is masked) - instead of the visitor's actual IP address (e.g. 123.123.123.123), an anonymous IP address (123.123.123.xxx) is stored. This means that it is no longer possible to identify individuals. The statistics are therefore completely anonymous to us and our service provider and do not allow any conclusions to be drawn about a natural person.

The server log files are completely disabled at web server level. **Download link to be sent:** For linked PDF documents, it is possible to have the link sent to an email address provided by you. Your email address will only be processed for this purpose and only for the duration of the sending process. We therefore only process your email address temporarily in order to send you the link. Your email address will not be saved, will not be used for other advertising purposes and will not be passed on to third parties. The email address you enter is transmitted to the web server in encrypted form. TLS encryption ensures that it cannot be read by third parties. We also support TLS encryption for outgoing emails with PDF download links if this is also supported by the other party.

Purpose and legal basis for processing: The legal basis for processing is Art. 6(1)(f) GDPR. Our legitimate interest is corporate communication - informing and advertising to customers and interested parties about HAHN+KOLB and its products and services. **Retention period:** Anonymous analysis data is stored for the lifetime of the QR codes. As soon as a QR code is deleted from the system, the associated analysis data is also deleted; **Service provider:** IANEO Solutions GmbH, Eisenbahnstraße 28, 66299 Friedrichsthal, Germany; **Website:** <https://www.ianeo.de/>. **Privacy policy:** <https://www.ianeo.de/datenschutzerklaerung/>.
- **Friendly Captcha:** CAPTCHA service, which is used to check whether the data entered within our online offering (e.g. on a login page or a contact form) has been entered by a human or an automated program. For this purpose, the service analyses the behaviour of users of our online offering based on various characteristics. This analysis begins automatically as soon as a user uses our online offering. Various information is evaluated for the analysis (IP address, time spent by the visitor on the website or app or mouse movements by the user as well as technical information on the end device and browser used by the user); **Service provider:** Friendly Captcha GmbH, Am Anger 3-5, 82237 Wörthsee, Germany; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).; **Website:** <https://friendlycaptcha.com/de/>; **Privacy policy:** <https://friendlycaptcha.com/de/legal/privacy-end-users/>. **Order processing agreement:** <https://friendlycaptcha.com/de/legal/>.
- **Shariff:** We use Shariff buttons, which ensure data privacy. Shariff was developed to enable more privacy on the Internet and to replace the typical "Share" buttons on social networks. In this case, instead of the user's browser,

the server on which this online service is located connects to the server of the respective social media platforms and queries the number of likes, for example. The user remains anonymous. You can find more information about the Shariff project from the developers at c't magazine: <https://www.heise.de/hintergrund/Ein-Shariff-fuer-mehr-Datenschutz-2467514.html>; **Service provider:** Heise Medien GmbH & Co. KG, Karl-Wiechert-Allee 10, 30625 Hanover, Germany; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.heise.de/ct/artikel/Shariff-Social-Media-Buttons-mit-Datenschutz-2467514.html>. **Privacy policy:** <https://www.heise.de/Datenschutzerklaerung-der-Heise-Medien-GmbH-Co-KG-4860.html>.

Management, organisation and auxiliary tools

We use services, platforms and software from other providers (hereinafter referred to as "third-party providers") for the purposes of organising, managing, planning and providing our services. We comply with the legal requirements when selecting the third-party provider and their services.

In this context, personal data may be processed and stored on the servers of third-party providers. This may affect various data that we process in accordance with this privacy policy. This data may include, in particular, master data and contact data of users, data on transactions, contracts, other processes and their content.

If users are referred to the third-party providers or their software or platforms in the course of communication, business or other relationships with us, the third-party providers may process usage data and metadata for security, service optimisation or marketing purposes. We therefore advise you to refer to the privacy policies of the respective third-party providers.

- **Data types processed:** Content data (e.g. entries in online forms); usage data (e.g. websites visited, interest in contents, access times); metadata, communication data and process data (e.g. IP addresses, time information, identification numbers, consent status); contract data (e.g. subject matter of the contract, term, customer category); subscriber data (e.g. names, addresses).
- **Data subjects:** Communication partners; users (e.g. website visitors, users of online services); employees (e.g. staff, applicants, former employees). Business and contractual partners.
- **Purposes of processing:** Provision of contractual services and fulfilment of contractual obligations; office and organisational processes; establishment and implementation of employment relationships (processing of employee data as part of the establishment and implementation of employment relationships); reach measurement (e.g. access statistics, detection of returning visitors); click tracking; provision of our online offering and usability. IT infrastructure (operation and provision of information systems and technical devices [computers, servers etc.]).
- **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).

Further information on processing procedures, processes and services:

- **FP Sign:** Electronic signing of documents, sending documents for signing, tracking the status of documents, storing signed documents; **Service provider:** FP Digital Business Solutions GmbH, Griesbergstr. 8, D-31162 Bad Salzdetfurth, Germany; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.fp-sign.com/de/>. **Privacy policy:** <https://www.fp-sign.com/de/datenschutzerklaerung>.
- **Confluence:** Software for the creation and administration of wiki and knowledge platforms; **Service provider:** Atlassian Inc. (San Francisco, Harrison Street Location), 1098 Harrison Street, San Francisco, California 94103, USA; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.atlassian.com/software/confluence>; **Privacy policy:** <https://www.atlassian.com/legal/privacy-policy>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF), standard contractual clauses

(provided by the service provider). **Further information:** Data transfer impact assessment: <https://www.atlassian.com/legal/data-transfer-impact-assessment>.

- **Jira:** Web application for error management, troubleshooting and operational project management; **Service provider:** Atlassian Inc. (San Francisco, Harrison Street Location), 1098 Harrison Street, San Francisco, California 94103, USA; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.atlassian.com/software/jira>; **Privacy policy:** <https://www.atlassian.com/legal/privacy-policy>; **Order processing agreement:** <https://www.atlassian.com/legal/data-processing-addendum>; **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF), standard contractual clauses (provided by the service provider). **Further information:** Data transfer impact assessment: <https://www.atlassian.com/legal/data-transfer-impact-assessment>.
- **Doxis:** Document management system: Contract management, invoice processing, digitisation and analysis of documents, legally compliant archiving; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Service provider:** SER Solutions Deutschland GmbH, Joseph-Schumpeter-Allee 19, 53227 Bonn, Germany; **Website:** <https://www.sergroup.com/>. **Privacy policy:** <https://www.sergroup.com/de/datenschutzerklaerung.html>.
- **Twixl:** Creation and management of digital content, publication of apps on various platforms, analysis of user behaviour, personalisation of content for the end user; **Service provider:** Twixl media bvba, Kortrijksesteenweg 1144 N, 9051 Ghent, Belgium; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://twixlmedia.com>. **Privacy policy:** <https://twixlmedia.com/twixl-legal-notice>.
- **Adobe AI:** AI-based image editing service designed to understand and generate natural language and related inputs and data, analyse information and make predictions ("AI", artificial intelligence, is to be understood in the applicable legal sense of the term); **Service provider:** Adobe Systems Software Ireland, 4-6, Riverwalk Drive, Citywest Business Campus, Brownsbarn, Dublin 24, D24 DCW0, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR).; **Website:** <https://www.adobe.com/de/>; **Privacy policy:** <https://www.adobe.com/de/privacy.html>, **Order processing agreement:** Provided by the service provider. **Basis for transfer to third countries:** EU-U.S. Data Privacy Framework (DPF), standard contractual clauses (provided by the service provider).
- **Bing AI:** AI-based service designed to understand and generate natural language and related inputs and data, analyse information and make predictions ("AI", artificial intelligence, is to be understood in the applicable legal sense of the term); **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.bing.com/>. **Privacy policy:** <https://privacy.microsoft.com/de-de/privacystatement>.
- **Corporate Benefits:** Provision of employee benefits and additional services for employees (known as corporate benefits); **Service provider:** Corporate Benefits Deutschland GmbH, Schiffbauerdamm 40, 10117 Berlin, Germany; **Legal basis:** Legitimate interests (Art. 6[1][1][f] GDPR); **Website:** <https://www.corporate-benefits.de/>. **Privacy policy:** <https://www.corporate-benefits.de/datenschutz>.

Changing and updating the privacy policy

We encourage you to regularly review the contents of our privacy policy. We will amend the data protection declaration as soon as any changes to the data processing we carry out make this necessary. We will notify you in the event that your action (e.g. consent) or other individual notification is required as a result of the changes.

Please note that any addresses and contact information for companies and organisations that we provide in this privacy policy may change over time. We therefore advise you to check the information before contacting us.

Exclusion of liability/disclaimer

HAHN+KOLB Werkzeuge GmbH's privacy policy does not apply to applications, products, services, websites or social media functions of third-party providers that can be accessed via links provided by us for information purposes. When you click on these links, you leave the HAHN+KOLB website, so there is a possibility that information about you may be collected or passed on by third parties. We have no influence over third-party websites and do not make any recommendations or assurances about these websites or their data privacy practices. We therefore strongly encourage you to carefully read and review the privacy policies of any websites you interact with before authorising them to collect, process and use your personal data.