

Privacy Policy

Preamble

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

The terms used are not gender-specific.

Last Update: 16. September 2024

Table of contents

- Preamble
- Controller
- Contact information of the Data Protection Officer
- Overview of processing operations
- Relevant legal bases
- Security Precautions
- Transmission of Personal Data
- International data transfers
- General Information on Data Retention and Deletion
- Rights of Data Subjects
- information about photographs during events
- Business services
- Business processes and operations
- Use of online platforms for listing and sales purposes
- Providers and services used in the course of business
- Payment Procedure

- Credit Assessment
- Provision of online services and web hosting
- Use of Cookies
- Registration, Login and User Account
- Contact and Inquiry Management
- Communication via Messenger
- Artificial Intelligence (AI)
- Video Conferences, Online Meetings, Webinars and Screen-Sharing
- Cloud Services
- Newsletter and Electronic Communications
- Commercial communication by E-Mail, Postal Mail, Fax or Telephone
- Sweepstakes and Contests
- Surveys and Questionnaires
- Web Analysis, Monitoring and Optimization
- Online Marketing
- Customer Reviews and Ratings
- Profiles in Social Networks (Social Media)
- Plugins and embedded functions and content
- Management, Organization and Utilities
- Processing of data in the context of employment relationships
- Job Application Process
- Privacy Information for Whistleblowers
- Whistleblower Systems
- Changes and Updates
- Terminology and Definitions

Controller

BMZ Germany GmbH
Zeche Gustav 1
63791 Karlstein
Germany

Authorised Representatives: Sven Bauer
E-mail address: mail@bmz-group.com
Phone: 06188 9956-0
Legal Notice: <https://bmz-group.com/index.php/impressum>

Contact information of the Data Protection Officer

Kompass Datenschutz GmbH
Jan Besold
Adresse: Bahnstr. 21 / 50858 Köln
E-Mail: besold (at) kompass-datenschutz.de
Telefon: 02233 / 6290596
Mobil: 01575/ 2623224

Overview of processing operations

The following table summarises the types of data processed, the purposes for which they are processed and the concerned data subjects.

Categories of Processed Data

- Inventory data.
- Employee Data.
- Payment Data.
- Location data.
- Contact data.
- Content data.
- Contract data.
- Usage data.
- Meta, communication and process data.
- Social data.
- Job applicant details.
- Images and/ or video recordings.
- Audio recordings.
- Contact Information (Facebook).
- Event Data (Facebook).

- Log data.
- Performance and behavioural data.
- Working hours data.
- Creditworthiness Data.
- Salary data.

Special Categories of Data

- Health Data.
- Religious or philosophical beliefs.
- Trade union membership.

Categories of Data Subjects

- Service recipients and clients.
- Employees.
- Prospective customers.
- Communication partner.
- Users.
- Job applicants.
- Participants in sweepstakes and competitions.
- Business and contractual partners.
- Education and course participants.
- Participants.
- Persons depicted.
- Third parties.
- Whistleblowers.
- Customers.

Purposes of Processing

- Provision of contractual services and fulfillment of contractual obligations.
- Communication.
- Security measures.
- Direct marketing.
- Web Analytics.
- Targeting.

- Office and organisational procedures.
- Remarketing.
- Conversion tracking.
- Affiliate Tracking.
- Organisational and Administrative Procedures.
- Job Application Process.
- Conducting sweepstakes and contests.
- Server monitoring and error detection.
- Feedback.
- Polls and Questionnaires.
- Marketing.
- Profiles with user-related information.
- Provision of our online services and usability.
- Assessment of creditworthiness.
- Establishment and execution of employment relationships.
- Information technology infrastructure.
- Whistleblower protection.
- Financial and Payment Management.
- Public relations.
- Sales promotion.
- Business processes and management procedures.
- Artificial Intelligence (AI).

Automated Individual Decision-Making

- Credit report.

Relevant legal bases

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

- **Consent (Article 6 (1) (a) GDPR)** - The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- **Performance of a contract and prior requests (Article 6 (1) (b) GDPR)** - Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- **Compliance with a legal obligation (Article 6 (1) (c) GDPR)** - Processing is necessary for compliance with a legal obligation to which the controller is subject.
- **Legitimate Interests (Article 6 (1) (f) GDPR)** - the processing is necessary for the protection of the legitimate interests of the controller or a third party, provided that the interests, fundamental rights, and freedoms of the data subject, which require the protection of personal data, do not prevail.
- **Job application process as a pre-contractual or contractual relationship (Article 6 (1) (b) GDPR)** - If special categories of personal data within the meaning of Article 9 (1) GDPR (e.g. health data, such as severely handicapped status or ethnic origin) are requested from applicants within the framework of the application procedure, so that the responsible person or the person concerned can carry out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, their processing shall be carried out in accordance with Article 9 (2)(b) GDPR , in the case of the protection of vital interests of applicants or other persons on the basis of Article 9 (2)(c) GDPR or for the purposes of preventive health care or occupational medicine, for the assessment of the employee's ability to work, for medical diagnostics, care or treatment in the health or social sector or for the administration of systems and services in the health or social sector in accordance with Article 9 (2)(d) GDPR. In the case of a communication of special categories of data based on voluntary consent, their processing is carried out on the basis of Article 9 (2)(a) GDPR.
- **Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR)** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the

management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.

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

National data protection regulations in France: In addition to the data protection regulations of the GDPR, national regulations on data protection apply in France. These include, in particular, the French Data Protection Act (Loi Informatique et Libertés).

National data protection regulations in Austria: In addition to the data protection regulations of the GDPR, national regulations apply to data protection in Austria. This includes in particular the Federal Act on the Protection of Individuals with regard to the Processing of Personal Data (Data Protection Act - DSG). In particular, the Data Protection Act contains special provisions on the right of access, rectification or cancellation, processing of special categories of personal data, processing for other purposes and transmission and automated decision making in individual cases.

National data protection regulations in Poland: In addition to the data protection regulations of the GDPR, national regulations on data protection apply in Poland. These include, in particular, the "Data Protection Act" (Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych).

Relevant legal basis according to the Swiss Data Protection Act: If you are located in Switzerland, we process your data based on the Federal Act on Data Protection (referred to as "Swiss DPA"). Unlike the GDPR, for instance, the Swiss DPA does not generally require that a legal basis for processing personal data be stated and that the processing of personal data is conducted in good faith, lawfully and proportionately (Art. 6 para. 1 and 2 of the Swiss DPA). Furthermore, we only collect personal data for a specific purpose recognizable to the data subject and process it only in a manner compatible with this purpose (Art. 6 para. 3 of the Swiss DPA).

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

Drittland (außerhalb der EU und der Schweiz): The data protection regulations in the country of the controller's registered office apply in addition to or alongside the GDPR. These regulations may contain specific provisions that go beyond or differ from the requirements of the GDPR. This includes, among other things, rules on protection against misuse of personal data, regulations on rights of access and erasure, rights to object, processing of special categories of personal data, processing for other purposes, transfer and automated decision-making including profiling. The respective national data protection laws and regulations of the corresponding third country must be observed and can influence the processing of personal data. It is important to be informed about the specific data protection regulations of the respective third country to ensure that all data protection requirements are met.

Security Precautions

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

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

Masking of the IP address: If IP addresses are processed by us or by the service providers and technologies used and the processing of a complete IP address is not necessary, the IP address is shortened (also referred to as "IP masking"). In this process, the last two digits or the last part of the IP address after a full stop are removed or replaced by wildcards. The masking of the IP address is intended to prevent the identification of a person by means of their IP address or to make such identification significantly more difficult.

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

indicated by the display of HTTPS in the URL. This serves as an indicator to users that their data is being securely and encryptedly transmitted.

Transmission of Personal Data

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

Data Transmission within the Group of Companies: Data transfer within the corporate group: We may transfer personal data to other companies within our corporate group or grant them access to it. This data sharing is based on our legitimate business and economic interests. By this, we mean, for example, the improvement of business processes, ensuring efficient and effective internal communication, the optimal use of our human and technological resources, as well as the ability to make informed business decisions. In certain cases, data sharing may also be necessary to fulfil our contractual obligations or may be based on the consent of the data subjects or a legal permission.

Data Transfer within the Organization: We may transfer personal data to other departments or units within our organisation or grant them access to it. If the data is shared for administrative purposes, it is based on our legitimate business and economic interests or occurs if it is necessary to fulfil our contractual obligations or if the data subjects have given their consent or a legal permission exists.

International data transfers

Data Processing in Third Countries: If we process data in a third country (i.e., outside the European Union (EU) or the European Economic Area (EEA)), or if the processing is done within the context of using third-party services or the disclosure or transfer of data to other individuals, entities, or companies, this is only done in accordance with legal requirements. If the data protection level in the third country has been recognized by an adequacy decision (Article 45 GDPR), this serves as the basis for data transfer. Otherwise, data transfers only occur if the data protection level is otherwise ensured, especially through standard contractual clauses (Article 46 (2)(c) GDPR), explicit consent, or in cases of contractual or legally required transfers (Article 49 (1) GDPR). Furthermore, we provide you with the basis of third-country transfers from individual third-country providers, with adequacy decisions primarily serving as the foundation. "Information regarding third-country transfers and existing adequacy decisions can be obtained from the information provided by the EU Commission:

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

EU-US Trans-Atlantic Data Privacy Framework: Within the context of the so-called "Data Privacy Framework" (DPF), the EU Commission has also recognized the data protection level for certain companies from the USA as secure within the adequacy decision of 10th July 2023. The list of certified companies as well as additional information about the DPF can be found on the website of the US Department of Commerce at <https://www.dataprivacyframework.gov/s/>. We will inform you which of our service providers are certified under the Data Privacy Framework as part of our data protection notices.

Disclosure of Personal Data Abroad: In accordance with the Swiss Data Protection Act (Swiss DPA), we only disclose personal data abroad when an appropriate level of protection for the affected persons is ensured (Art. 16 Swiss DPA). If the Federal Council does not determine that there is an adequate level of protection (list of states:

<https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales/anererkennung-staaten.html>), we implement alternative security measures. These measures may include international agreements, specific guarantees, data protection clauses in contracts, standard data protection clauses approved by the Federal Data Protection and Information Commissioner (FDPIC), or internal company data protection regulations previously recognised by the FDPIC or a competent data protection authority of another country.

Under Art. 16 of the Swiss DSG, exceptions can be made for the disclosure of data abroad if certain conditions are met, including the consent of the affected person, contract execution, public interest, protection of life or physical integrity, publicly made data or data from a legally provided register. Such disclosures always comply with the legal requirements.

General Information on Data Retention and Deletion

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

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

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

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

If a period does not expressly start on a specific date and lasts at least one year, it automatically begins at the end of the calendar year in which the event triggering the period occurred. In the

case of ongoing contractual relationships in the context of which data is stored, the event triggering the deadline is the time at which the termination or other termination of the legal relationship takes effect.

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

Further information on processing methods, procedures and services used:

- **Data Retention and Deletion:** The following general deadlines apply for the retention and archiving according to German law:
 - 10 Years - Fiscal Code/Commercial Code - Retention period for books and records, annual financial statements, inventories, management reports, opening balance sheet as well as the necessary work instructions and other organisational documents, booking receipts and invoices (Section 147 Paragraph 3 in conjunction with Paragraph 1 No. 1, 4 and 4a of the German General Tax Code (AO), Section 14b Paragraph 1 of the German VAT Act (UStG), Section 257 Paragraph 1 Numbers 1 and 4, Paragraph 4 of the German Commercial Code (HGB)).
 - 6 Years - Other business documents: received commercial or business letters, copies of dispatched commercial or business letters, and other documents to the extent that they are significant for taxation purposes, for example, hourly wage slips, operating accounting sheets, calculation documents, price tags, as well as payroll accounting documents, provided they are not already accounting vouchers and cash register tapes Section (Section 147 Paragraph 3 in conjunction with Paragraph 1 No. 2, 3, 5 of the German General Tax Code (AO), Section 257 Paragraph 1 No. 2 and 3, Paragraph 4 of the German Commercial Code (HGB)).
 - 3 Years - Data required to consider potential warranty and compensation claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experiences and common industry practices, will be stored for the duration of the regular statutory limitation period of three years. This period begins at the end of the year in which the relevant contractual transaction took place or the contractual relationship ended in the case of ongoing contracts (Sections 195, 199 of the German Civil Code).

- **Data Retention and Deletion:** The following general deadlines apply to retention and archiving according to Austrian law:
 - 10 Years - Retention period for books and records, annual financial statements, inventories, annual reports, opening balance sheets, booking receipts and invoices, as well as any necessary work instructions and other organisational documents (Austrian Federal Tax Code (BAO §132), Austrian Commercial Code (UGB §§190-212)).
 - 6 Years - Remaining business documents: Received business or trading letters, copies of sent business or trading letters, and other documents, if they are relevant for taxation. These could be hourly wage sheets, operational accounting sheets, calculation documents, price tags, and payroll documents, as long as they aren't already booking receipts and cash register strips (Austrian Federal Tax Code (BAO §132), Austrian Commercial Code (UGB §§190-212)).
 - 3 Years - Data required to consider potential warranty and compensation claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experiences and common industry practices, will be stored for the duration of the regular statutory limitation period of three years (Sections 1478, 1480 of the Austrian Civil Code).

- **Data Retention and Deletion:** The following general retention and archiving periods apply under Swiss law:
 - 10 years - Retention period for books and records, annual financial statements, inventories, management reports, opening balances, accounting vouchers and invoices, as well as all necessary working instructions and other organizational documents (Article 958f of the Swiss Code of Obligations (OR)).
 - 10 years - Data necessary to consider potential claims for damages or similar contractual claims and rights, as well as for the processing of related inquiries based on previous business experiences and usual industry practices, will be stored for the statutory limitation period of ten years, unless a shorter period of five years is applicable, which is relevant in certain cases (Articles 127, 130 OR). Claims for rent, lease, and interest on capital, as well as other periodic services,

for the delivery of food, for board and lodging, for innkeeper debts, as well as for craftsmanship, small-scale sales of goods, medical care, professional services by lawyers, legal agents, procurators, and notaries, and from the employment relationship of employees, expire after five years (Article 128 OR).

Rights of Data Subjects

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

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

- **Complaint to the supervisory authority:** In accordance with the law and without prejudice to any other administrative or judicial remedy, you also have the right to lodge a complaint with a data protection supervisory authority, in particular a supervisory authority in the Member State where you habitually reside, the supervisory authority of your place of work or the place of the alleged infringement, if you consider that the processing of personal data concerning you infringes the GDPR.

Rights of the data subjects under the Swiss DPA:

As the data subject, you have the following rights in accordance with the provisions of the Swiss DPA:

- **Right to information:** You have the right to request confirmation as to whether personal data concerning you are being processed, and to receive the information necessary for you to assert your rights under the Swiss DPA and to ensure transparent data processing.
- **Right to data release or transfer:** You have the right to request the release of your personal data, which you have provided to us, in a common electronic format, as well as its transfer to another data controller, provided this does not require disproportionate effort.
- **Right to rectification:** You have the right to request the rectification of inaccurate personal data concerning you.
- **Right to object, deletion, and destruction:** You have the right to object to the processing of your data, as well as to request that personal data concerning you be deleted or destroyed.

information about photographs during events

<https://www.bmz-group.com/index.php/informationspflicht-fotoaufnahmen-veranstaltungen>

Business services

We process data of our contractual and business partners, e.g. customers and interested parties (collectively referred to as "contractual partners") within the context of contractual and comparable legal relationships as well as associated actions and communication with the contractual partners or pre-contractually, e.g. to answer inquiries.

We process this data in order to fulfill our contractual obligations. These include, in particular, the obligations to provide the agreed services, any update obligations and remedies in the event of warranty and other service disruptions. In addition, we process the data to protect our rights and for the purpose of administrative tasks associated with these obligations and company organization. Furthermore, we process the data on the basis of our legitimate interests in proper and economical business management as well as security measures to protect our contractual partners and our business operations from misuse, endangerment of 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 applicable law, we only disclose the data of contractual partners to third parties to the extent that this is necessary for the aforementioned purposes or to fulfill legal obligations. Contractual partners will be informed about further forms of processing, e.g. for marketing purposes, within the scope of this privacy policy.

Which data are necessary for the aforementioned purposes, we inform the contracting partners before or in the context of the data collection, e.g. in online forms by special marking (e.g. colors), and/or symbols (e.g. asterisks or the like), or personally.

We delete the data after expiry of statutory warranty and comparable obligations, i.e. in principle after expiry of 4 years, unless the data is stored in a customer account or must be kept for legal reasons of archiving. The statutory retention period for documents relevant under tax law as well as for commercial books, inventories, opening balance sheets, annual financial statements, the instructions required to understand these documents and other organizational documents and accounting records is ten years and for received commercial and business letters and reproductions of sent commercial and business letters six years. The period begins at the end of the calendar year in which the last entry was made in the book, the inventory, the opening balance sheet, the annual financial statements or the management report was prepared, the commercial or business letter was received or sent, or the accounting document was created, furthermore the record was made or the other documents were created.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties). Job applicant details (e.g. Personal data, postal and contact addresses and the documents pertaining to the application and the information contained therein, such as cover letter, curriculum vitae, certificates, etc., as well as

other information on the person or qualifications of applicants provided with regard to a specific job or voluntarily by applicants).

- **Data subjects:** Service recipients and clients; Prospective customers; Business and contractual partners; Education and course participants. Job applicants.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Security measures; Communication; Office and organisational procedures; Organisational and Administrative Procedures; Business processes and management procedures. Conversion tracking (Measurement of the effectiveness of marketing activities).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Compliance with a legal obligation (Article 6 (1) (c) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Online shop, order forms, e-commerce and delivery.:** We process the data of our customers in order to enable them to select, purchase or order the selected products, goods and related services, as well as their payment and delivery, or performance of other services. If necessary for the execution of an order, we use service providers, in particular postal, freight and shipping companies, in order to carry out the delivery or execution to our customers. For the processing of payment transactions we use the services of banks and payment service providers. The required details are identified as such in the course of the ordering or comparable purchasing process and include the details required for delivery, or other way of making the product available and invoicing as well as contact information in order to be able to hold any consultation; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).
- **Automotive Industry and Vehicle Technology:** We process the data of our customers and clients to enable them to develop, produce, and provide vehicles and vehicle technologies and related services. The required information includes that needed for project implementation and billing, as well as contact information for necessary coordination. To the extent that we have access to information from end customers, employees, or other persons, we process this in accordance with legal and contractual

requirements; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Education and Training Services:** We process the data of the participants of our education and training programmes (uniformly referred to as "students") in order to provide them with our educational and training services. The data processed, the type, scope and purpose of the processing and the necessity of its processing are determined by the underlying contractual and educational relationship. The processing also includes the performance evaluation and evaluation of our services and the teachers and instructors.

As part of our activities, we may also process special categories of data, in particular information on the health of persons undergoing training or further training and data revealing ethnic origin, political opinions, religious or philosophical convictions. To this end, we obtain, if necessary, the express consent of the students to be trained and further educated and process the special categories of data otherwise only if it is necessary for the provision of training services, for purposes of health care, social protection or protection of vital interests of the students to be trained and further educated; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

- **Coaching:** We process the data of our clients as well as prospects and other contractors or business partners (collectively referred to as "clients") in order to provide them with our services. The processes carried out within the framework and for the purposes of coaching include: initiating contact and communication with clients, needs analysis to determine suitable coaching measures, planning and conducting coaching sessions, documenting coaching progress, capturing and managing client-specific information and data, scheduling and organising appointments, providing coaching materials and resources, invoicing and payment management, post-processing and follow-up of coaching sessions, quality assurance and feedback processes.

The processed data, its nature, scope, purpose, and the necessity of its processing are determined by the underlying contractual relationship with the client.

Insofar as it is necessary for fulfilling our contract, protecting vital interests or legally

required, or if there is consent from the clients, we disclose or transfer the clients' data in compliance with professional legal requirements to third parties or agents such as authorities, billing centers as well as in the field of IT, office or comparable services;

Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

- **Data Analysis:** We process the data of our customers and clients to enable them to perform data analysis, evaluation, and consulting, as well as related services. The required information includes that needed for analysis, evaluation, and billing, as well as contact information for necessary coordination. To the extent that we have access to information from end customers, employees, or other persons, we process this in accordance with legal and contractual requirements; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Craft Services:** We process the data of our customers and clients (hereinafter uniformly referred to as "customers") in order to enable them to select, acquire or commission the selected services or works and related tasks, as well as their payment and delivery, or execution or provision.

The required details are identified as such within the framework of the conclusion of the order, order or comparable contract and include the details required for delivery and invoicing as well as contact information in order to be able to hold any consultations;

Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

- **IT Services:** We process the data of our clients as well as contractors to enable them to plan, implement, and support IT solutions and associated services. The required information is marked as such during the contract, project, or similar agreement phase and includes details necessary for service provision and billing, as well as contact information to facilitate any necessary consultations. Insofar as we gain access to information from end customers, employees, or other individuals, we process this in accordance with legal and contractual requirements.

Processing processes include project management and documentation, which cover all phases from initial requirement analysis to project completion. This involves creating and managing project timelines, budgets, and resource allocations. Data processing also supports change management, where changes in the project flow are documented and

tracked to ensure compliance and transparency.

Another process is customer relationship management (CRM), which involves recording and analyzing customer interactions and feedback to improve service quality and efficiently address individual customer needs. Additionally, the processing process encompasses technical support and trouble-shooting, which includes capturing and handling support requests, error resolutions, and regular maintenance.

Furthermore, reporting and performance analysis are conducted by capturing and evaluating performance metrics to assess the effectiveness of provided IT solutions continuously optimizing them. All these processes are aimed at ensuring high customer satisfaction and compliance with all relevant regulations; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Recruiting Services:** As part of our services, which include in particular the search for, contacting and placement of potential job candidates, we process the data of the job candidates and the personal data of potential employers or their employees.

We process the information and contact data provided by the job candidates for the purposes of establishing, implementing and, if necessary, terminating a job placement contract. In addition, we can ask interested parties questions about the success of our recruiting services at a later date, in accordance with legal requirements.

We process the data of the job candidates, as well as of the employers, in order to fulfil our contractual obligations, in order to process the requests we receive for the placement of jobs to the satisfaction of the parties involved.

We can record the recruiting processes in order to be able to prove the existence of the contractual relationship and the consent of the interested parties in accordance with the statutory accountability obligations (Article 5 (2) GDPR). This information will be stored for a period of three to four years if we need to prove the original request (e.g. to prove eligibility to contact the job candidates); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

- **Technical and Engineering services:** We process the data of our customers and clients (hereinafter uniformly referred to as "customers") in order to enable them to

select, acquire or commission the selected services or works as well as associated activities and to pay for and make available such services or works or to perform such services or works.

The required information is indicated as such within the framework of the conclusion of the agreement, order or equivalent contract and includes the information required for the provision of services and invoicing as well as contact information in order to be able to hold any consultations. Insofar as we gain access to the information of end customers, employees or other persons, we process it in accordance with the legal and contractual requirements; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

- **Event Management:** We process the data of the participants of the events, events and similar activities offered or organized by us (hereinafter uniformly referred to as "participants" and "events") in order to enable them to participate in the events and to make use of the services or actions associated with their participation.

Insofar as we process health-related data, religious, political or other special categories of data in this context, this is done within the framework of disclosure (e.g. for thematically oriented events or serves health care, security or is done with the consent of the data subjects).

The necessary information is identified as such in the context of the conclusion of the agreement, booking or comparable contract and includes the information required for the provision of services and billing as well as contact information in order to be able to hold any enquiries. Insofar as we gain access to information of end customers, employees or other persons, we process this in accordance with the legal and contractual requirements; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

- **Commission-based matching and agency services:** We process the information provided by interested parties as part of the request for agency for the purposes of establishing, implementing and, if necessary, terminating a contract for the brokerage of offers from providers of the requested products or services .

We use the contact data of the interested parties to specify their request by means of the agreed or otherwise permitted communication channel (e.g., telephone or e-mail) and to suggest suitable suppliers or offers based on the specified request. In addition, we can ask interested parties questions about the success of our agency services at a later point in time, in accordance with legal requirements.

We process the data of the interested parties, as well as the suppliers, to fulfil our contractual obligations, in order to link the enquiry of the interested parties submitted to us with the offers of the suppliers matching it and to forward it to the corresponding suppliers, or to recommend the suppliers.

We can record the entries in the online form sent by interested parties in order to be able to prove the existence of the contractual relationship and the consent of the interested parties in accordance with the statutory accountability obligations (Article 5 (2) GDPR). These details will be stored for a period of three to four years if we have to prove the original request (e.g. to be able to prove that we are entitled to contact the interested party); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Business processes and operations

Personal data of service recipients and clients - including customers, clients, or in specific cases, mandates, patients, or business partners as well as other third parties - are processed within the framework of contractual and comparable legal relationships and pre-contractual measures such as the initiation of business relations. This data processing supports and facilitates business processes in areas such as customer management, sales, payment transactions, accounting, and project management.

The collected data is used to fulfil contractual obligations and make business processes efficient. This includes the execution of business transactions, the management of customer relationships, the optimisation of sales strategies, and ensuring internal invoicing and financial processes. Additionally, the data supports the protection of the rights of the controller and promotes administrative tasks as well as the organisation of the company.

Personal data may be transferred to third parties if necessary for fulfilling the mentioned purposes or legal obligations. After legal retention periods expire or when the purpose of

processing no longer applies, the data will be deleted. This also includes data that must be stored for longer periods due to tax law and legal obligations to provide evidence.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Log data (e.g. log files concerning logins or data retrieval or access times.); Creditworthiness Data (e.g. received credit score, estimated default probability, risk classification based on this, historical payment behaviour). Employee Data (Information about employees and other individuals in an employment relationship).
- **Data subjects:** Service recipients and clients; Prospective customers; Communication partner (Recipients of e-mails, letters, etc.); Business and contractual partners; Customers; Third parties; Users (e.g. website visitors, users of online services). Employees (e.g. employees, job applicants, temporary workers, and other personnel.).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Business processes and management procedures; Security measures; Provision of our online services and usability; Communication; Marketing; Sales promotion; Public relations; Assessment of creditworthiness; Financial and Payment Management. Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR). Compliance with a legal obligation (Article 6 (1) (c) GDPR).

Further information on processing methods, procedures and services used:

- **Customer Management and Customer Relationship Management (CRM):** Processes required in the context of customer management and Customer Relationship Management (CRM) include customer acquisition in compliance with data protection regulations, measures to promote customer retention and loyalty, effective customer communication, complaint management and customer service with consideration of data protection, data management and analysis to support the customer relationship, management of CRM systems, secure account management, customer segmentation and targeting; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Contact management and contact maintenance:** Processes required in the context of organizing, maintaining, and securing contact information (e.g., setting up and maintaining a central contact database, regular updates of contact information, monitoring data integrity, implementing data protection measures, ensuring access controls, conducting backups and restorations of contact data, training employees in effective use of contact management software, regular review of communication history and adjustment of contact strategies); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Customer Account:** Customers can create an account within our online offer (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 of the details required for registration. The customer accounts are not public and cannot be indexed by search engines. In the course of registration and subsequent registration and use of the customer account, we store the IP addresses of the contractual partners along with the access times, in order to be able to prove the registration and prevent any misuse of the customer account. If the customer account has been terminated, the customer account data will be deleted after the termination date, unless it is retained for purposes other than provision in the customer account or must be retained for legal reasons (e.g. internal storage of customer data, order transactions or invoices). It is the customers' responsibility to back up their data when terminating the customer Account; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Product List/ Wishlist:** Customers can create a products/wish list In this case, the products are stored within the context of the fulfillment of our contractual obligations until the deletion of the account, unless the product list entries are removed by the customer or we expressly inform the customer of deviating storage periods; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).
- **General Payment Transactions:** Procedures required for carrying out payment transactions, monitoring bank accounts, and controlling payment flows (e.g., creation and verification of transfers, processing of direct debit transactions, checking of account statements, monitoring of incoming and outgoing payments, management of chargebacks, account reconciliation, cash management); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Accounting, accounts payable, accounts receivable:** Procedures required for the collection, processing, and control of business transactions in the area of accounts payable and receivable accounting (e.g., creation and verification of incoming and outgoing invoices, monitoring and management of outstanding items, execution of payment transactions, handling of dunning processes, account reconciliation within the scope of receivables and payables, accounts payable accounting, and accounts receivable accounting); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Financial Accounting and Taxes:** Procedures required for the collection, management, and control of finance-related business transactions as well as for the calculation, reporting, and payment of taxes (e.g., accounting and posting of business transactions, preparation of quarterly and annual financial statements, execution of payment transactions, handling of dunning processes, account reconciliation, tax consulting, preparation and submission of tax returns, management of tax affairs); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Purchasing:** Processes required in the procurement of goods, raw materials, or services (e.g., selection and evaluation of suppliers, price negotiations, placement and monitoring of orders, inspection and control of deliveries, invoice verification,

management of orders, inventory management, creation and maintenance of purchasing policies); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Sales:** Procedures required for the planning, implementation, and control of measures for marketing and selling products or services (e.g., customer acquisition, preparation and tracking of offers, order processing, customer consultation and support, sales promotion, product training, sales controlling and analysis, management of distribution channels); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Marketing, advertising, and sales promotion:** Processes required in the context of marketing, advertising, and sales promotion (e.g., market analysis and audience targeting, development of marketing strategies, planning and execution of advertising campaigns, design and production of advertising materials, online marketing including SEO and social media campaigns, event marketing and trade show participation, customer loyalty programs, sales promotion measures, performance measurement and optimisation of marketing activities, budget management and cost control); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Economic Analyses and Market Research:** To fulfill business management purposes and to identify market trends, desires of contractual partners, and users, the present data regarding business transactions, contracts, inquiries, etc., are analyzed. The group of affected individuals may include contractual partners, interested parties, customers, visitors, and users of the online service managed by the responsible entity. The execution of these analyses serves the purposes of business economic evaluations, marketing, and market research (e.g., to determine customer groups with different characteristics). Where available, profiles of registered users along with their information on services utilized are considered. The analyses are exclusively for the use of the responsible entity and are not disclosed externally unless they pertain to anonymous analyses with aggregated, thus anonymized values. Moreover, user privacy is accounted for; data is processed for analysis purposes in as pseudonymized a manner as possible and anonymized when feasible (e.g., as aggregated data); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

- **Public Relations:** Processes required in the context of public relations and public relations activities (e.g., development and implementation of communication strategies, planning and execution of PR campaigns, creation and distribution of press releases, maintenance of media contacts, monitoring and analysis of media response, organisation of press conferences and public events, crisis communication, creation of content for social media and corporate websites, management of corporate branding); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Guest Wi-Fi:** Procedures required for the setup, operation, maintenance, and monitoring of a wireless network for guests (e.g., installation and configuration of Wi-Fi access points, creation and management of guest access, monitoring of network connection, ensuring network security, resolving connection issues, updating network software, compliance with data protection regulations); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Use of online platforms for listing and sales purposes

We offer our services on online platforms operated by other service providers. In addition to our privacy policy, the privacy policies of the respective platforms apply. This is particularly true with regard to the payment process and the methods used on the platforms for performance measuring and behaviour-related marketing.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Service recipients and clients; Business and contractual partners. Prospective customers.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Marketing; Business processes and management procedures; Conversion

tracking (Measurement of the effectiveness of marketing activities). Provision of our online services and usability.

- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Shopware:** Platform for offering and performing e-commerce services. The services and processes carried out in connection with them include, in particular, online stores, websites, their offers and content, community elements, purchase and payment transactions, customer communication, as well as analysis and marketing; **Service provider:** shopware AG, Ebbinghoff 10, 48624 Schöppingen, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.shopware.com/en/>; **Privacy Policy:** <https://www.shopware.com/en/privacy/>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).

Providers and services used in the course of business

As part of our business activities, we use additional services, platforms, interfaces or plug-ins from third-party providers (in short, "services") in compliance with legal requirements. Their use is based on our interests in the proper, legal and economic management of our business operations and internal organization.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Contract data (e.g. contract object, duration, customer category). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Service recipients and clients; Prospective customers; Business and contractual partners; Employees (e.g. employees, job applicants, temporary workers, and other personnel.). Communication partner (Recipients of e-mails, letters, etc.).

- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Business processes and management procedures. Communication.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **DPD:** Logistics, shipping and delivery services. We share certain personal data with DPD to enable the shipment and delivery of packages, as well as parcel tracking and recipient notifications. This information may include the recipient's name, address, and contact details; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); **Service provider:** Wailandtstraße 1, PLZ/Ort: 63741 Aschaffenburg, Germany; **Website:** <https://www.dpd.com/>; **Privacy Policy:** <https://www.dpd.com/de/de/datenschutz/>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).
- **DHL Freight:** Logistics, shipping and delivery services. We share certain personal data with DHL to enable the shipment and delivery of packages, as well as parcel tracking and recipient notifications. This information may include the recipient's name, address, and contact details; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); **Service provider:** Freight GmbH DHL Freight GmbH, Gutenbergstraße 15, 63477 Maintal, Germany; **Website:** <https://www.dhl.com/de-en/>; **Privacy Policy:** <https://www.dhl.com/de-en/home/footer/privacy-notice.html>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).
- **Hermes:** Logistics, shipping and delivery services. We share certain personal data with Hermes to enable the shipment and delivery of packages, as well as parcel tracking and recipient notifications. This information may include the recipient's name, address, and contact details; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); **Service provider:** Hermes Germany GmbH, Essener Straße 89, D-22419 Hamburg, Germany; **Website:** <https://www.myhermes.de/>; **Privacy Policy:** <https://www.myhermes.de/datenschutz/>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).
- **GLS:** Logistics, shipping and delivery services. We share certain personal data with GLS to enable the shipment and delivery of packages, as well as parcel tracking and recipient

notifications. This information may include the recipient's name, address, and contact details; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); **Service provider:** General Logistics Systems Germany GmbH & Co. OHG, GLS Germany-Straße 1 – 7, DE-36286 Neuenstein, Germany; **Website:** <https://gls-group.eu/>; **Privacy Policy:** <https://gls-group.eu/DE/de/datenschutz-standard>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).

- **UPS:** Logistics, shipping and delivery services. We share certain personal data with UPS to enable the shipment and delivery of packages, as well as parcel tracking and recipient notifications. This information may include the recipient's name, address, and contact details; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); **Service provider:** UPS Europa SA, Ave Ariane 5, Brüssel, B-1200, Belgien; **Website:** <https://www.ups.com>; **Privacy Policy:** <https://www.ups.com/de/de/help-center/legal-terms-conditions/privacy-notice.page?>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Belgien).
- **Trans-o-flex Express:** Logistics, shipping and delivery services. We share certain personal data with Trans-o-flex Express to enable the shipment and delivery of packages, as well as parcel tracking and recipient notifications. This information may include the recipient's name, address, and contact details; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); **Service provider:** Zentrale Weinheim, Hertzstraße 10, 69469 Weinheim, Germany; **Website:** <https://www.trans-o-flex.com/>; **Privacy Policy:** <https://www.trans-o-flex.com/datenschutz/>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).
- **DATEV:** Software for accounting, communication with tax advisors as well as authorities and including document storage; **Service provider:** DATEV eG, Paumgartnerstr. 6 - 14, 90429 Nürnberg, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.datev.de/web/de/mydatev/online-anwendungen/>; **Privacy Policy:** <https://www.datev.de/web/de/m/ueber-datev/datenschutz/>; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).
- **DHL:** Logistics, shipping and delivery services. We share certain personal data with DHL to enable the shipment and delivery of packages, as well as parcel tracking and recipient notifications. This information may include the recipient's name, address, and contact

details; **Service provider:** Deutsche Post AG, Charles-de-Gaulle-Straße 20, 53113 Bonn, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.dhl.com/de-en/>; **Privacy Policy:** <https://www.dhl.com/de-en/home/footer/privacy-notice.html>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).

Payment Procedure

Within the framework of contractual and other legal relationships, due to legal obligations or otherwise on the basis of our legitimate interests, we offer data subjects efficient and secure payment options and use other service providers for this purpose in addition to banks and credit institutions (collectively referred to as "payment service providers").

The data processed by the payment service providers includes inventory data, such as the name and address, bank data, such as account numbers or credit card numbers, passwords, TANs and checksums, as well as the contract, total and recipient-related information. The information is required to carry out the transactions. However, the data entered is only processed by the payment service providers and stored with them. I.e. we do not receive any account or credit card related information, but only information with confirmation or negative information of the payment. Under certain circumstances, the data may be transmitted by the payment service providers to credit agencies. The purpose of this transmission is to check identity and creditworthiness. Please refer to the terms and conditions and data protection information of the payment service providers.

The terms and conditions and data protection information of the respective payment service providers apply to the payment transactions and can be accessed within the respective websites or transaction applications. We also refer to these for further information and the assertion of revocation, information and other data subject rights.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Service recipients and clients; Business and contractual partners. Prospective customers.

- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Business processes and management procedures; Office and organisational procedures. Assessment of creditworthiness.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Mastercard:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider:** Mastercard Europe SA, Chaussée de Tervuren 198A, B-1410 Waterloo, Belgium; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** <https://www.mastercard.co.uk>; **Privacy Policy:** <https://www.mastercard.co.uk/en-gb/vision/terms-of-use/commitment-to-privacy/privacy.html>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Belgium).
- **PayPal:** Payment-Service-Provider (technical integration of online-payment-methods) (e.g. PayPal, PayPal Plus, Braintree, Braintree); **Service provider:** PayPal (Europe) S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** <https://www.paypal.com>; **Privacy Policy:** <https://www.paypal.com/de/webapps/mpp/ua/privacy-full>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Luxembourg).
- **Visa:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider:** Visa Europe Services Inc., Zweigniederlassung London, 1 Sheldon Square, London W2 6TT, UK; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** <https://www.visa.de>; **Privacy Policy:** <https://www.visa.de/datenschutz>. **Basis for third-country transfers:** EEA - Adequacy decision (UK), Switzerland - Adequacy decision (UK).
- **CrefoPay:** Payment processing, receivables management and risk management; **Service provider:** Crefopayment GmbH & Co. KG, Schloßstr. 20, 12163 Berlin, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:**

<https://www.crefopay.de/>; **Privacy Policy:** <https://www.crefopay.de/datenschutz/>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).

Credit Assessment

Insofar as we make advance payments 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-statistical procedures in order to safeguard legitimate interests. We process the information received from credit agencies on the statistical probability of non-payment as part of an appropriate discretionary decision on the establishment, execution and termination of the contractual relationship. In the event of a negative result of the credit assessment, we reserve the right to refuse payment on account or any other advance payment. In accordance with the law, the decision as to whether we will provide goods or services prior to payment is made solely on the basis of an automated decision in the individual case, which our software makes on the basis of the information provided by the credit agency. If we obtain the express consent of contractual partners, the legal basis for the credit information and the transmission of the customer's data to the credit agencies is consent. If no consent is obtained, the credit rating will be based on our legitimate interests in the security of our payment claims.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Contract data (e.g. contract object, duration, customer category); Creditworthiness Data (e.g. received credit score, estimated default probability, risk classification based on this, historical payment behaviour). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Service recipients and clients; Prospective customers. Business and contractual partners.
- **Purposes of processing:** Assessment of creditworthiness.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

- **Automated individual decision-making:** Credit report (Decision based on a credit report).

Further information on processing methods, procedures and services used:

- **Credit check as a prerequisite for the provision of payment options:** The provision of payment options, e.g. payment on account or payment by installments, may be made dependent on the result of the customer's credit check. In this case, we ask customers to agree to the credit check procedure; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).
- **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 (Article 6 (1) (f) GDPR); **Website:** <https://www.creditreform.de/>; **Privacy Policy:** <https://www.creditreform.de/datenschutz>.
Basis for third-country transfers: Switzerland - Adequacy decision (Germany).

Provision of online services and web hosting

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

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Log data (e.g. log files concerning logins or data retrieval or access times.). Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of our online services and usability; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.); Security measures; Web Analytics (e.g. access statistics, recognition of returning visitors); Conversion tracking (Measurement of the effectiveness of marketing activities). Server monitoring and error detection.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

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

Further information on processing methods, procedures and services used:

- **Provision of online offer on rented hosting space:** For the provision of our online services, we use storage space, computing capacity and software that we rent or otherwise obtain from a corresponding server provider (also referred to as a "web hoster"); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Collection of Access Data and Log Files:** Access to our online service is logged in the form of so-called "server log files". Server log files may include the address and name of the accessed web pages and files, date and time of access, transferred data volumes, notification of successful retrieval, browser type along with version, the user's operating system, referrer URL (the previously visited page), and typically IP addresses and the requesting provider. The server log files can be used for security purposes, e.g., to prevent server overload (especially in the case of abusive attacks, known as DDoS attacks), and to ensure server load management and stability; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Retention period:** Log file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.
- **Content-Delivery-Network:** We use a so-called "Content Delivery Network" (CDN). A CDN is a service with whose help contents of our online services, in particular large media files, such as graphics or scripts, can be delivered faster and more securely with the help of regionally distributed servers connected via the Internet; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **ALL-INKL:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider:** ALL-INKL.COM - Neue Medien Münnich, Inhaber: René Münnich, Hauptstraße 68, 02742 Friedersdorf, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://all-inkl.com/>; **Privacy Policy:** <https://all-inkl.com/datenschutzinformationen/>; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).

- **Host Europe:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider:** Host Europe GmbH, Hansestrasse 111, 51149 Cologne, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <http://www.hosteurope.de/en/>; **Privacy Policy:** <http://www.hosteurope.de/en/terms-and-conditions/privacy/>; **Data Processing Agreement:** <https://www.hosteurope.de/Dokumente/>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).
- **Squarespace:** Squarespace offers Software as a Service for the creation and hosting of websites; **Service provider:** Squarespace Ireland Ltd., Le Pole House, Ship Street Great, Dublin 8, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.squarespace.com/>; **Privacy Policy:** <https://www.squarespace.com/privacy/>; **Data Processing Agreement:** <https://www.squarespace.com/dpa>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).
- **Google Cloud CDN:** Content-Delivery-Network (CDN) - service with whose help contents of our online services, in particular large media files, such as graphics or scripts, can be delivered faster and more securely with the help of regionally distributed servers connected via the Internet; **Service provider:** Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://cloud.google.com/cdn/>; **Privacy Policy:** <https://policies.google.com/privacy/>; **Data Processing Agreement:** <https://cloud.google.com/terms/data-processing-addendum/>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** <https://cloud.google.com/privacy/>.
- **Google Sites:** Creation of websites and web hosting (provision of storage space and computing capacity); **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://workspace.google.com/products/sites/>; **Privacy Policy:** <https://cloud.google.com/privacy/>; **Data Processing Agreement:** <https://cloud.google.com/terms/data-processing-addendum/>; **Basis for third-country**

transfers: EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** <https://cloud.google.com/privacy>.

Use of Cookies

Cookies are small text files or other types of storage markers that store information on end devices and read information from them. For example, to save the login status in a user account, the contents of a shopping cart in an e-shop, the content accessed, or the functions used of an online offer. Furthermore, cookies can be used for various concerns, such as for the functionality, security, and comfort of online offers as well as the creation of analyses of visitor flows.

Notes on Consent: We use cookies in accordance with legal regulations. Therefore, we obtain prior consent from users, unless it is not required by law. Permission is particularly not necessary if the storage and reading of information, including cookies, are absolutely necessary to provide a telemedia service (i.e., our online offer) expressly requested by the users. The revocable consent is clearly communicated to them and contains information on the respective cookie usage.

Notes on the legal basis for data protection: The legal basis on which we process users' personal data with the help of cookies depends on whether we ask them for consent. If users accept, the legal basis for processing their data is the declared consent. Otherwise, the data processed with the help of cookies are based on our legitimate interests (e.g., in a commercial operation of our online offer and its usability improvement) or, if this occurs within the fulfillment of our contractual obligations, when the use of cookies is necessary to fulfill our contractual obligations. We clarify the purposes for which the cookies are used by us in the course of this data protection declaration or within the scope of our consent and processing processes.

Storage Duration: Regarding the storage duration, the following types of cookies are distinguished:

- **Temporary cookies (also: session or session cookies):** Temporary cookies are deleted at the latest after a user has left an online offer and closed his end device (e.g., browser or mobile application).
- **Permanent cookies:** Permanent cookies remain stored even after closing the end device. For example, the login status can be saved and preferred content can be displayed directly when the user revisits a site. Similarly, user data collected via cookies can be used for reach measurement. Unless we provide users with explicit information about the nature and storage duration of cookies (e.g., when obtaining consent), they should assume that they are permanent and the storage duration can be up to two years.

General notes on revocation and objection (Opt-out): Users can revoke the consents they have given at any time and also declare an objection to the processing according to legal requirements, also via the privacy settings of their browser.

Cookie Settings/ Opt-Out:

Footer Symbol.

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

Further information on processing methods, procedures and services used:

- **Processing Cookie Data on the Basis of Consent:** We implement a consent management solution that obtains users' consent for the use of cookies or for the processes and providers mentioned within the consent management framework. This procedure is designed to solicit, log, manage, and revoke consents, particularly regarding the use of cookies and similar technologies employed to store, read from, and process information on users' devices. As part of this procedure, user consents are obtained for the use of cookies and the associated processing of information, including specific processing and providers named in the consent management process. Users also have the option to manage and withdraw their consents. Consent declarations are stored to avoid repeated queries and to provide proof of consent according to legal requirements. The storage is carried out server-side and/or in a cookie (so-called opt-in cookie) or by means of comparable technologies in order to associate the consent with a specific user or their device. If no specific details about the providers of consent management services are provided, the following general notes apply: The duration of consent storage is up to two years. A pseudonymous user identifier is created, which is stored along with the time of consent, details on the scope of consent (e.g., relevant categories of cookies and/or service providers), as well as information about the browser, system, and device used; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).
- **Cookiebot:** Cookie Consent Management: Procedures for obtaining, recording, managing, and revoking consents, particularly for the use of cookies and similar technologies for storing, accessing, and processing information on users' devices as well as their processing; **Service provider:** Usercentrics A/S, Havnegade 39, 1058

Kopenhagen, Dänemark; **Website:** <https://www.cookiebot.com>; **Privacy Policy:** <https://www.cookiebot.com/en/privacy-policy/>; **Data Processing Agreement:** Provided by the service provider; **Further Information:** Stored data (on the server of the service provider): The IP number of the user in anonymous form (the last three digits are set to 0), date and time of the consent, user agent of the user's browser, the URL from which the consent was sent, An anonymous, random and encrypted key value. the consent status of the user.

Registration, Login and User Account

Users can create a user account. Within the scope of registration, the required mandatory information is communicated to the users and processed for the purposes of providing the user account on the basis of contractual fulfilment of obligations. The processed data includes in particular the login information (name, password and an e-mail address).

Within the scope of using our registration and login functions as well as the use of the user account, we store the IP address and the time of the respective user action. The storage is based on our legitimate interests, as well as the user's protection against misuse and other unauthorized use. This data will not be passed on to third parties unless it is necessary to pursue our claims or there is a legal obligation to do so.

Users may be informed by e-mail of information relevant to their user account, such as technical changes.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Log data (e.g. log files concerning logins or data retrieval or access times.).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Security measures; Organisational and Administrative Procedures. Provision of our online services and usability.

- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Deletion after termination.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Registration with a real name:** Due to the nature of our community, we ask users to use our services only with their real names. This means that the use of pseudonyms is not permitted; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).
- **Users' profiles are public:** The users' profiles are not publicly visible or accessible.
- **Deletion of data after termination:** If users have terminated their user account, their data relating to the user account will be deleted, subject to any legal permission, obligation or consent of the users; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).
- **No obligation to retain data:** It is the responsibility of the users to secure their data before the end of the contract in the event of termination. We are entitled to irretrievably delete all user data stored during the term of the contract; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Contact and Inquiry Management

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).

- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Communication; Organisational and Administrative Procedures; Feedback (e.g. collecting feedback via online form). Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Further information on processing methods, procedures and services used:

- **Contact form:** Upon contacting us via our contact form, email, or other means of communication, we process the personal data transmitted to us for the purpose of responding to and handling the respective matter. This typically includes details such as name, contact information, and possibly additional information provided to us that is necessary for appropriate processing. We use this data exclusively for the stated purpose of contact and communication; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Communication via Messenger

We use messenger services for communication purposes and therefore ask you to observe the following information regarding the functionality of the messenger services, encryption, use of the metadata of the communication and your objection options.

You can also contact us by alternative means, e.g. telephone or e-mail. Please use the contact options provided to you or use the contact options provided within our online services.

In the case of encryption of content (i.e. the content of your message and attachments), we point out that the communication content (i.e. the content of the message and attachments) is encrypted end-to-end. This means that the content of the messages is not visible, not even by the messenger service providers themselves. You should always use a current version of the messenger service with activated encryption, so that the encryption of the message contents is guaranteed.

However, we would like to point out to our communication partners that although messenger service providers do not see the content, they can find out that and when communication partners communicate with us and process technical information on the communication partner's device used and, depending on the settings of their device, also location information (so-called metadata).

Information on Legal basis: If we ask communication partners for permission before communicating with them via messenger services, the legal basis of our processing of their data is their consent. Otherwise, if we do not request consent and you contact us, for example, voluntarily, we use messenger services in our dealings with our contractual partners and as part of the contract initiation process as a contractual measure and in the case of other interested parties and communication partners on the basis of our legitimate interests in fast and efficient communication and meeting the needs of our communication partners for communication via messenger services. We would also like to point out that we do not transmit the contact data provided to us to the messenger service providers for the first time without your consent.

Withdrawal, objection and deletion: You can withdraw your consent or object to communication with us via messenger services at any time. In the case of communication via messenger services, we delete the messages in accordance with our general data retention policy (i.e. as described above after the end of contractual relationships, archiving requirements, etc.) and otherwise as soon as we can assume that we have answered any information provided by the communication partners, if no reference to a previous conversation is to be expected and there are no legal obligations to store the messages to prevent their deletion.

Reservation of reference to other means of communication: For your security, we kindly ask for your understanding that we may not respond to enquiries via messenger for specific reasons. This applies in situations where contract details require heightened confidentiality or a response via messenger does not meet formal requirements. In such cases, we recommend using more appropriate communication channels.

- **Processed data types:** Contact data (e.g. postal and email addresses or phone numbers). Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Communication.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR); Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Instagram:** Messaging via the social network Instagram; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.instagram.com>; **Privacy Policy:** <https://privacycenter.instagram.com/policy/>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Ireland).

Artificial Intelligence (AI)

We use artificial intelligence (AI), which involves the processing of personal data. The specific purposes and our interest in using AI are mentioned below. According to the term "AI system" as defined in Article 3 No. 1 of the AI Regulation, we understand AI to be a machine-based system designed for varying degrees of autonomous operation, capable of adaptation after deployment, and producing outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Our AI systems are used in strict compliance with legal requirements. These include both specific regulations for artificial intelligence and data protection requirements. In particular, we adhere to the principles of lawfulness, transparency, fairness, human oversight, purpose limitation, data minimisation, integrity and confidentiality. We ensure that the processing of personal data is always based on a legal foundation. This may either be the consent of the data subjects or a statutory permission.

When using external AI systems, we carefully select their providers (hereinafter referred to as "AI providers"). In accordance with our legal obligations, we ensure that the AI providers comply with applicable provisions. We also observe our duties when using or operating the acquired AI services. The processing of personal data by us and the AI providers is carried out exclusively on the basis of consent or legal authorisation. We place particular emphasis on transparency, fairness and maintaining human oversight over AI-supported decision-making processes.

To protect processed data, we implement appropriate and robust technical as well as organisational measures. These ensure the integrity and confidentiality of processed data and minimise potential risks. Through regular reviews of AI providers and their services, we ensure ongoing compliance with current legal and ethical standards.

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

Further information on processing methods, procedures and services used:

- **ChatGPT:** AI-based service designed to understand and generate natural language and related input and data, analyze information, and make predictions ("AI", meaning

"Artificial Intelligence" shall be construed in the applicable legal sense of the term);

Service provider: OpenAI Ireland Ltd, 117-126 Sheriff Street Upper, D01 YC43 Dublin

1, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:**

<https://openai.com/product>; **Privacy Policy:** <https://openai.com/policies/privacy-policy/>;

Basis for third-country transfers: Switzerland - Adequacy decision (Ireland). **Opt-Out:**

<https://docs.google.com/forms/d/e/1FAIpQLSevgtKyiSWIOj6CV6XWBHI1daPZSOcIWzcUYUXQ1xttjBgDpA/viewform>.

Video Conferences, Online Meetings, Webinars and Screen-Sharing

We use platforms and applications of other providers (hereinafter referred to as "Conference Platforms") for the purpose of conducting video and audio conferences, webinars and other types of video and audio meetings (hereinafter collectively referred to as "Conference"). When using the Conference Platforms and their services, we comply with the legal requirements.

Data processed by Conference Platforms: In the course of participation in a Conference, the Data of the participants listed below are processed. The scope of the processing depends, on the one hand, on which data is requested in the context of a specific Conference (e.g., provision of access data or clear names) and which optional information is provided by the participants. In addition to processing for the purpose of conducting the conference, participants' Data may also be processed by the Conference Platforms for security purposes or service optimization. The processed Data includes personal information (first name, last name), contact information (e-mail 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 system, the browser and its technical and linguistic settings, information on the content-related communication processes, i.e. entries in chats and audio and video data, as well as the use of other available functions (e.g. surveys). The content of communications is encrypted to the extent technically provided by the conference providers. If participants are registered as users with the Conference Platforms, then further data may be processed in accordance with the agreement with the respective Conference Provider.

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

Data protection measures of the participants: Please refer to the data privacy information of the Conference Platforms for details on the processing of your data and select the optimum security and data privacy settings for you within the framework of the settings of the conference platforms. Furthermore, please ensure data and privacy protection in the background of your recording for the duration of a Conference (e.g., by notifying roommates, locking doors, and

using the background masking function, if technically possible). Links to the conference rooms as well as access data, should not be passed on to unauthorized third parties.

Notes on legal bases: Insofar as, in addition to the Conference Platforms, we also process users' data and ask users for their consent to use contents from the Conferences or certain functions (e.g. consent to a recording of Conferences), the legal basis of the processing is this consent. Furthermore, our processing may be necessary for the fulfillment of our contractual obligations (e.g. in participant lists, in the case of reprocessing of Conference results, etc.). Otherwise, user data is processed on the basis of our legitimate interests in efficient and secure communication with our communication partners.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Images and/ or video recordings (e.g. photographs or video recordings of a person); Audio recordings. Log data (e.g. log files concerning logins or data retrieval or access times.).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.); Users (e.g. website visitors, users of online services). Persons depicted.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Communication. Office and organisational procedures.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Microsoft Teams:** Audio and video conferencing, chat, file sharing, integration with Office 365 applications, real-time collaboration on documents, calendar functions, task management, screen sharing, optional recording; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.microsoft.com/microsoft-teams/>; **Privacy Policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security information:

<https://www.microsoft.com/de-de/trustcenter>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

- **TeamViewer:** Conference and communication software; **Service provider:** TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.teamviewer.com/en/>; **Privacy Policy:** <https://www.teamviewer.com/en/privacy-notice/>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).

Cloud Services

We use Internet-accessible software services (so-called "cloud services", also referred to as "Software as a Service") provided on the servers of its providers for the storage and management of content (e.g. document storage and management, exchange of documents, content and information with certain recipients or publication of content and information). Within this framework, personal data may be processed and stored on the provider's servers insofar as this data is part of communication processes with us or is otherwise processed by us in accordance with this privacy policy. This data may include in particular master data and contact data of data subjects, data on processes, contracts, other proceedings and their contents. Cloud service providers also process usage data and metadata that they use for security and service optimization purposes.

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Prospective customers; Communication partner (Recipients of e-mails, letters, etc.); Business and contractual partners. Users (e.g. website visitors, users of online services).

- **Purposes of processing:** Office and organisational procedures; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.). Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Apple iCloud:** Cloud storage service; **Service provider:** Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.apple.com>. **Privacy Policy:** <https://www.apple.com/legal/privacy/en-ww/>.
- **Google Cloud Storage:** Cloud storage, cloud infrastructure services and cloud-based application software; **Service provider:** Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://cloud.google.com/>; **Privacy Policy:** <https://policies.google.com/privacy>; **Data Processing Agreement:** <https://cloud.google.com/terms/data-processing-addendum>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** <https://cloud.google.com/privacy>.
- **Microsoft Cloud Services:** Cloud storage, cloud infrastructure services 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 (Article 6 (1) (f) GDPR); **Website:** <https://microsoft.com>; **Privacy Policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security information: <https://www.microsoft.com/de-de/trustcenter>; **Data Processing Agreement:** <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).
- **Microsoft Azure:** Cloud storage, cloud infrastructure services 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 (Article 6 (1) (f) GDPR); **Website:** <https://azure.microsoft.com>; **Privacy Policy:** <https://privacy.microsoft.com/en-us/privacystatement>; **Data Processing Agreement:** <https://azure.microsoft.com/en-us/support/legal/>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

Newsletter and Electronic Communications

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

Deletion and restriction of processing: We may store unsubscribed email addresses for up to three years based on our legitimate interests before deleting them to be able to demonstrate previously given consent. The processing of these data is limited to the purpose of potentially defending against claims. An individual request for deletion is possible at any time, provided that at the same time the former existence of consent is confirmed. In case of obligations to permanently observe objections, we reserve the right to store the email address solely for this purpose in a blocklist.

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

Contents:

Information about us, our services, promotions and offers.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.). Users (e.g. website visitors, users of online services).

- **Purposes of processing:** Direct marketing (e.g. by e-mail or postal); Web Analytics (e.g. access statistics, recognition of returning visitors). Provision of contractual services and fulfillment of contractual obligations.
- **Retention and deletion:** 3 years - Contractual claims (AT) (Data required to consider potential warranty and compensation claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experiences and common industry practices, will be stored for the duration of the regular statutory limitation period of three years (Sections 1478, 1480 of the Austrian Civil Code).). 10 years - Contractual claims (CH) (Data required to consider potential compensation claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experiences and common industry practices, will be stored for the duration of the statutory limitation period of ten years, unless a shorter period of 5 years is applicable, which is relevant in certain cases. This period begins at the end of the calendar year in which the claim arose (Articles 127 and 128 Swiss Code of Obligations (CO))).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).
- **Opt-Out:** You can cancel the receipt of our newsletter at any time, i.e. revoke your consent or object to further receipt. You will find a link to cancel the newsletter either at the end of each newsletter or you can otherwise use one of the contact options listed above, preferably e-mail.

Further information on processing methods, procedures and services used:

- **Measurement of opening rates and click rates:** The newsletters contain a so-called "web beacons", which is a pixel-sized file that is retrieved from our server, or the server of the dispatch service provider if one is used, when the newsletter is opened. In the course of this retrieval, technical information such as details about the browser and your system, as well as your IP address and the time of access are collected. This information is used to technically improve our newsletter based on technical data or target audiences and their reading behavior, which can be determined by their access locations (identifiable by IP address) or access times. This analysis also includes determining whether and when newsletters are opened and which links are clicked. The information is assigned to individual newsletter recipients and stored in their profiles until

deletion. The evaluations serve to recognize the reading habits of our users and adjust our content to them or send different content according to the interests of our users. The measurement of opening and click rates, as well as the storage of the measurement results in user profiles and their further processing, are based on user consent.

Unfortunately, it is not possible to revoke success measurement separately; in this case, the entire newsletter subscription must be cancelled or objected to. In that case, stored profile information will be deleted; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).

- **Prerequisite for the use of free services:** Consent to the sending of mailings can be made dependent on the use of free services (e.g. access to certain content or participation in certain campaigns) as a prerequisite. If the users would like to take advantage of the free service without registering for the newsletter, we offer them to contact us.
- **Brevo:** E-mail dispatch and automation services; **Service provider:** Sendinblue GmbH, Köpenicker Str. 126, 10179 Berlin, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.brevo.com/>; **Privacy Policy:** <https://www.brevo.com/de/legal/privacypolicy/>; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).

Commercial communication by E-Mail, Postal Mail, Fax or Telephone

We process personal data for the purposes of promotional communication, which may be carried out via various channels, such as e-mail, telephone, post or fax, in accordance with the legal requirements.

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

After revocation or objection, we store the data required to prove the past authorization to contact or send up to three years from 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 defense against claims. Based on the legitimate interest to permanently observe the revocation, respectively objection of the users, we further store the data necessary to avoid a renewed contact (e.g. depending on the communication channel, the e-mail address, telephone number, name).

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email

addresses or phone numbers). Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.).

- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Direct marketing (e.g. by e-mail or postal); Marketing. Sales promotion.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Sweepstakes and Contests

We process the personal data of participants in We process personal data of participants in competitions, contents, raffles, prize-draws or sweepstakes (hereinafter referred to as "competitions") only in compliance with the relevant data protection regulations and if the processing is contractually necessary for the provision, execution and handling of the competition, the participants 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 by possible recording of IP addresses when submitting entries to the competition).

In the event that entries are published as part of the competitions (e.g. as part of a vote or presentation of the competition entries, or the winner or reporting on the competition), we would like to point out that the names of participants may also be published in this context. The participants can object to this at any time.

If the competitions take place within an online platform or a social network (e.g. Facebook or Instagram, hereinafter referred to as "online platform"), the usage and data protection provisions of the respective online platforms also apply. In such cases, we would like to point out that we are responsible for the information provided by the participants as part of the competition and that we must be contacted with regard to the competitions.

The data of the participants will be deleted as soon as the competition has ended and the data is no longer required to inform the winners or because questions about the competition can be expected. In general, the data of the participants will be deleted at the latest 6 months after the end of the competition. Winners' data can be retained for a longer period of time, e.g. in order to answer questions about the prizes or to fulfil the prizes; in this case, the retention period depends on the type of prize and is up to three years for items or services, e.g. in order to be

able to process warranty claims. Furthermore, the participants' data may be stored for longer, e.g. in the form of coverage of the competition in online and offline media.

Insofar as data was collected for other purposes as part of the competition, its processing and storage period shall be governed by the privacy information for this use (e.g. in the case of registration for a newsletter as part of a competition).

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers). Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.).
- **Data subjects:** Participants in sweepstakes and competitions.
- **Purposes of processing:** Conducting sweepstakes and contests.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Surveys and Questionnaires

We conduct surveys and interviews to gather information for the survey purpose communicated in each case. The surveys and questionnaires ("surveys") carried out by us are evaluated anonymously. Personal data is only processed insofar as this is necessary for the provision and technical execution of the survey (e.g. processing the IP address to display the survey in the user's browser or to enable a resumption of the survey with the aid of a cookie).

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Participants; Users (e.g. website visitors, users of online services). Business and contractual partners.

- **Purposes of processing:** Feedback (e.g. collecting feedback via online form); Polls and Questionnaires (e.g. surveys with input options, multiple choice questions); Office and organisational procedures; Provision of our online services and usability. Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Microsoft Azure:** Cloud storage, cloud infrastructure services 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 (Article 6 (1) (f) GDPR); **Website:** <https://azure.microsoft.com>; **Privacy Policy:** <https://privacy.microsoft.com/en-us/privacystatement>; **Data Processing Agreement:** <https://azure.microsoft.com/en-us/support/legal/>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).
- **Microsoft Cloud Services:** Cloud storage, cloud infrastructure services 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 (Article 6 (1) (f) GDPR); **Website:** <https://microsoft.com>; **Privacy Policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security information: <https://www.microsoft.com/de-de/trustcenter>; **Data Processing Agreement:** <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

Web Analysis, Monitoring and Optimization

Web analysis is used to evaluate the visitor traffic on our website and may include the behaviour, interests or demographic information of users, such as age or gender, as

pseudonymous values. With the help of web analysis we can e.g. recognize, at which time our online services or their functions or contents are most frequently used or requested for repeatedly, as well as which areas require optimization.

In addition to web analysis, we can also use test procedures, e.g. to test and optimize different versions of our online services or their components.

Unless otherwise stated below, profiles, i.e. data aggregated for a usage process, can be created for these purposes and information can be stored in a browser or in a terminal device and read from it. The information collected includes, in particular, websites visited and 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 agreed to the collection of their location data from us or from the providers of the services we use, location data may also be processed. Unless otherwise stated below, profiles, that is data summarized for a usage process or user, may be created for these purposes and stored in a browser or terminal device (so-called "cookies") or similar processes may be used for the same purpose. The information collected includes, in particular, websites visited and 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 or profiles to us or to the providers of the services we use, these may also be processed, depending on the provider.

The IP addresses of the users are also stored. However, we use any existing IP masking procedure (i.e. pseudonymisation by shortening the IP address) to protect the user. In general, within the framework of web analysis, A/B testing and optimisation, no user data (such as e-mail addresses or names) is stored, but pseudonyms. This means that we, as well as the providers of the software used, do not know the actual identity of the users, but only the information stored in their profiles for the purposes of the respective processes.

Notes on legal bases: If we ask users for their consent to use third-party providers, the legal basis for data processing is consent. Otherwise, user data will be processed on the basis of our legitimate interests (i.e. interest in efficient, economical and recipient-friendly services). In this context, we would also like to draw your attention to the information on the use of cookies in this privacy policy.

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Remarketing; Affiliate Tracking; Web Analytics (e.g. access statistics, recognition of returning visitors); Profiles with user-related information (Creating user profiles). Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Storage of cookies for up

to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.).

- **Security measures:** IP Masking (Pseudonymization of the IP address).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Google Analytics:** We use Google Analytics to perform measurement and analysis of the use of our online services by users based on 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 recognize which content users have accessed within one or various usage processes, which search terms they have used, have accessed again or have interacted with our online services. Likewise, the time of use and its duration are stored, as well as the sources of users referring to our online services and technical aspects of their end devices and browsers.

In the process, pseudonymous profiles of users are created with information from the use of various devices, and cookies may be used. Google Analytics does not log or store individual IP addresses. Analytics does provide coarse geo-location data by deriving the following metadata from IP addresses: City (and the derived latitude, and longitude of the city), Continent, Country, Region, Subcontinent (and ID-based counterparts). For EU-based traffic, IP-address data is used solely for geo-location data derivation before being immediately discarded. It is not logged, accessible, or used for any additional use cases. When Analytics collects measurement data, all IP lookups are performed on EU-based servers before forwarding traffic to Analytics servers for processing; **Service**

provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland;

Legal Basis: Consent (Article 6 (1) (a) GDPR); **Website:**

<https://marketingplatform.google.com/intl/en/about/analytics/>; **Security measures:** IP

Masking (Pseudonymization of the IP address); **Privacy Policy:**

<https://policies.google.com/privacy>; **Data Processing Agreement:**

<https://business.safety.google/adsprocessor/terms/>; **Basis for third-country transfers:**

EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Opt-**

Out: Opt-Out-Plugin: <https://tools.google.com/dlpage/gaoptout?hl=en>, Settings for the

Display of Advertisements: <https://myadcenter.google.com/personalizationoff>. **Further Information:** <https://business.safety.google/adsservices/> (Types of processing and data processed).

- **Google as a recipient of consent:** The consent given by users in the context of a consent dialogue (also known as "Cookie Opt-In/Consent", "Cookie Banner", etc.) serves multiple purposes. Firstly, it helps us to fulfil our obligation to obtain consent for the storage and reading of information on and from the end-user's device (in accordance with ePrivacy Directives). Secondly, it covers the processing of users' personal data in accordance with data protection requirements. Additionally, this consent is also applicable to Google, as the company is required by the Digital Markets Act to obtain consent for personalised services. Therefore, we share the status of consents given by users with Google. Our consent management software informs Google about whether consents have been given or not. The aim is to ensure that user consents—or their absence—are taken into account when using Google Analytics and integrating features and external services. Thus, user consents and their revocation can be dynamically adjusted within our online offerings through Google Analytics and other Google services, depending on user selection; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://support.google.com/analytics/answer/9976101?hl=en>; **Privacy Policy:** <https://policies.google.com/privacy>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Ireland).
- **Google Signals (Google Analytics function):** Google signals are session data from sites and apps that Google associates with users who have signed in to their Google accounts, and who have turned on Ads Personalization. This association of data with these signed-in users is used to enable cross-device reporting, cross-device remarketing, and cross-device conversion export to Ads. These are the areas where more information is gathered when Google Signals is activated (but only for users with Ads Personalization enabled): Cross Platform reporting - Connection of data about devices and activities from different sessions using your User-ID or Google-signals data providing an understanding of user behavior at each step of the conversion process, from initial contact to conversion and beyond; Remarketing with Google Analytics - Creation of remarketing audiences from Google Analytics data, and sharing of those

audiences with linked advertising accounts; Demographics & Interests: Google Analytics collects additional information about demographics and interests from users who are signed in to their Google accounts and who have turned on Ads Personalization;

Service provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:**

<https://support.google.com/analytics/answer/7532985?hl=en>; **Privacy Policy:**

<https://policies.google.com/privacy>; **Data Processing Agreement:**

<https://business.safety.google/adsprocessorterms>; **Basis for third-country transfers:**

EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

Further Information: <https://business.safety.google/adsservices/> (Types of processing and data processed).

- **Google Analytics Audiences:** We use Google Analytics to specifically present ads, placed through Google's advertising services and those of its partners, to users who have already shown interest in our online offering or exhibit certain characteristics (e.g., interests in specific topics or products determined based on the websites they have visited). We transmit this data to Google as part of what is known as "Remarketing" or "Google Analytics Audiences". The purpose of using Remarketing Audiences is to ensure that our ads align as closely as possible with the potential interests of the users; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://marketingplatform.google.com>; **Legal Basis:** <https://business.safety.google/adsprocessorterms/>; **Privacy Policy:** <https://policies.google.com/privacy>; **Data Processing Agreement:** <https://business.safety.google/adsprocessorterms/>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further Information:** Types of processing and data processed: <https://business.safety.google/adsservices/>. Data Processing Conditions for Google Advertising Products and standard contractual clauses for data transfers to third countries: <https://business.safety.google/adsprocessorterms> .
- **Google Tag Manager:** We use Google Tag Manager, a software provided by Google, which enables us to manage so-called website tags centrally via a user interface. Tags are small code elements on our website that serve to record and analyse visitor

activities. This technology assists us in improving our website and the content offered on it. Google Tag Manager itself does not create user profiles, store cookies with user profiles, or perform any independent analyses. Its function is limited to simplifying and making the integration and management of tools and services we use on our website more efficient. Nevertheless, when using Google Tag Manager, users' IP addresses are transmitted to Google, which is technically necessary to implement the services we use. Cookies may also be set in this process. However, this data processing only occurs if services are integrated via the Tag Manager. For more detailed information about these services and their data processing, please refer to the further sections of this privacy policy; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://marketingplatform.google.com>; **Privacy Policy:** <https://policies.google.com/privacy>; **Data Processing Agreement:** <https://business.safety.google/adsprocessorterms>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

Online Marketing

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

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

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

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

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

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

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

Notes on revocation and objection:

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

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

- **Processed data types:** Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Event Data (Facebook) ("Event Data" is data that can be transmitted from us to Facebook, e.g. via Facebook pixels (via apps or other means) and relates to persons or their actions; the data includes, for example, information about visits to websites, interactions with content, functions, installations of apps, purchases of products, etc.; 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 written comments),

login information, and Contact Information (such as names, email addresses, and phone numbers). Event Data is deleted by Facebook after a maximum of two years, the Custom Audiences created from them with the deletion of our Facebook account); Contact Information (Facebook) ("Contact Information" is data that (clearly) identifies data subjects, such as names, email addresses and phone numbers, that can be transmitted to Facebook, e.g. via Facebook pixels or uploads for matching purposes to form Custom Audiences; After the matching to create target groups, the Contact Information is deleted). 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:** Web Analytics (e.g. access statistics, recognition of returning visitors); Targeting (e.g. profiling based on interests and behaviour, use of cookies); Conversion tracking (Measurement of the effectiveness of marketing activities); Affiliate Tracking; Marketing; Profiles with user-related information (Creating user profiles); Provision of our online services and usability. Remarketing.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.).
- **Security measures:** IP Masking (Pseudonymization of the IP address).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Meta Pixel and Custom Audiences (Custom Audiences):** With the help of the Meta-Pixel (or equivalent functions, to transfer Event-Data or Contact Information via interfaces or other software in apps), Meta is on the one hand able to determine the visitors of our online services as a target group for the presentation of ads (so-called "Meta ads"). Accordingly, we use Meta-Pixels to display Meta ads placed by us only to Meta users and within the services of partners cooperating with Meta (so-called "audience network" <https://www.facebook.com/audiencenetwork/>) who have shown an interest in our online services or who have certain characteristics (e.g. interests in certain topics or products that are determined on the basis of the websites visited) that

we transmit to Meta (so-called "custom audiences"). With the help of Meta-Pixels, we also want to ensure that our Meta ads correspond to the potential interest of users and do not appear annoying. The Meta-Pixel also enables us to track the effectiveness of Meta ads for statistical and market research purposes by showing whether users were referred to our website after clicking on a Meta ad (known as "conversion tracking");

Service provider: Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:**

<https://www.facebook.com>; **Privacy Policy:** <https://www.facebook.com/privacy/policy/>;

Data Processing Agreement: <https://www.facebook.com/legal/terms/dataprocessing>;

Basis for third-country transfers: EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** User event data, i.e. behavioral and interest data, is processed for the purposes of targeted advertising and audience building on the basis of the joint controllership agreement ("Controller Addendum", https://www.facebook.com/legal/controller_addendum). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).

- **Advanced matching for the Meta-Pixel:** In addition to the processing of Event Data in the context of the use of the Meta-Pixel (or equivalent functions, e.g. in apps), Contact Information (data identifying individual persons, names, email addresses and telephone numbers) is also collected by Meta within our online offer or transmitted to Meta. The processing of contact information serves to form target groups (so-called "Custom Audiences") for the display of content and advertising information based on the presumed interests of users. The collection, or transmission and matching with data available on Meta is not in plain text, but as so-called "hash values", i.e. mathematical representations of the data (this method is used, for example, in the storage of passwords). After the matching to create target groups, the Contact Information is deleted; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Privacy Policy:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Data Processing Agreement:** <https://www.facebook.com/legal/terms/dataprocessing>; **Basis for third-**

country transfers: EEA - Data Privacy Framework (DPF), Switzerland - Standard Contractual Clauses (https://www.facebook.com/legal/EU_data_transfer_addendum).

Further Information: https://www.facebook.com/legal/terms/data_security_terms.

- **Facebook Ads:** Placement of ads within the Facebook platform and analysis of ad results; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://www.facebook.com>; **Privacy Policy:** <https://www.facebook.com/privacy/policy/>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **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 access and other data subject rights, as described in Facebook's privacy policy. **Further Information:** User event data, i.e. behavioral and interest data, is processed for the purposes of targeted advertising and audience building on the basis of the joint controllership agreement ("Controller Addendum", https://www.facebook.com/legal/controller_addendum). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).
- **Google Ad Manager:** We use the service "Google Ad Manager" to place ads in the Google advertising network (e.g. in search results, videos, websites, etc.). The Google Ad Manager stands out because ads are displayed in real time based on users' presumed interests. This allows us to display ads for our online offering to users who may have a potential interest in our offering or who have previously shown interest, and measure the success of the ads; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://marketingplatform.google.com>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further Information:** Types of processing and data processed:

<https://business.safety.google/adsservices/>; Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: <https://business.safety.google/adscontrollerterms>. where Google acts as processor, Data Processing Conditions for Google Advertising Products and standard contractual clauses for data transfers to third countries: <https://business.safety.google/adsprocesorterms> apply.

- **AdMob:** Platform for displaying advertising content within mobile apps; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://admob.google.com/home/>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** Processing by Google as controller: <https://business.safety.google/adscontrollerterms/>.
- **Google Ads and Conversion Tracking:** Online marketing process for purposes of placing content and advertisements within the provider's advertising network (e.g., in search results, in videos, on web pages, etc.) so that they are displayed to users who have a presumed interest in the ads. Furthermore, we measure the conversion of the ads, i.e. whether the users took them as a reason to interact with the ads and make use of the advertised offers (so-called 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 (Article 6 (1) (a) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://marketingplatform.google.com>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further Information:** Types of processing and data processed: <https://business.safety.google/adsservices/>. Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: <https://business.safety.google/adscontrollerterms>.
- **Google Ads Remarketing:** Google Remarketing, also known as retargeting, is a technology that adds users who use an online service to a pseudonymous remarketing list so that users can be shown ads on other online services based on their visit to the

online service

; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:**

<https://marketingplatform.google.com>; **Privacy Policy:**

<https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further**

Information: Types of processing and data processed:

<https://business.safety.google/adsservices/>. Google Ads Controller-Controller Data

Protection Terms and standard contractual clauses for data transfers to third countries:

<https://business.safety.google/adscontrollerterms>.

- **Enhanced Conversions for Google Ads:** When users click on our Google ads and subsequently use the advertised service (so-called "conversion"), the data entered by the user, such as email address, name, residential address or telephone number, may be transmitted to Google. The hash values are then matched with existing Google accounts of the users to better evaluate and improve their interaction with the ads (e.g., clicks or views) and thus their performance; **Legal Basis:** Consent (Article 6 (1) (a) GDPR). **Website:** <https://support.google.com/google-ads/answer/9888656>.
- **Google AdSense with personalized ads:** We integrate the service Google AdSense, which enables the placement of personalized advertisements within our online offering. Google AdSense analyzes user behavior and uses this data to deliver targeted advertising that is aligned with the interests of our visitors. We receive financial compensation for each advertisement placement or other types of usage of these ads; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://marketingplatform.google.com>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further Information:** Types of processing and data processed: <https://business.safety.google/adsservices/>. Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: <https://business.safety.google/adscontrollerterms>.

- **Google Adsense with non-personalized ads:** We use the service Google Adsense to display non-personalised advertisements in our online offering. These advertisements are not based on individual user behaviour but are selected based on general characteristics such as the content of the page or your approximate geographical location. We receive a fee for the display or other use of these advertisements; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://marketingplatform.google.com>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further Information:** Types of processing and data processed: <https://business.safety.google/adsservices/>. Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: <https://business.safety.google/adscontrollerterms>.
- **Instagram Ads:** Placement of ads within the Instagram platform and analysis of ad results; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://www.instagram.com>; **Privacy Policy:** <https://privacycenter.instagram.com/policy/>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Opt-Out:** We refer to the data protection and advertising settings in the user's profile on the Instagram platform as well as Instagram's consent procedure and Instagram's contact options for exercising information and other data subject rights in Instagram's privacy policy. **Further Information:** User event data, i.e. behavioral and interest data, is processed for the purposes of targeted advertising and audience building on the basis of the joint controllership agreement ("Controller Addendum", https://www.facebook.com/legal/controller_addendum). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).

- **LinkedIn Insight Tag:** Code that is loaded when a user visits our online offering and tracks the user's behavior and conversions, as well as stores it in a profile (possible use cases: measuring campaign performance, optimizing ad delivery, building custom and similar target groups); **Service provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://www.linkedin.com>; **Privacy Policy:** <https://www.linkedin.com/legal/privacy-policy>, cookie policy: https://www.linkedin.com/legal/cookie_policy; **Data Processing Agreement:** <https://www.linkedin.com/legal/dpa>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Opt-Out:** <https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>.
- **Microsoft Advertising:** Online marketing process for purposes of placing content and advertisements within the provider's advertising network (e.g., in search results, in videos, on web pages, etc.) so that they are displayed to users who have a presumed interest in the ads. Furthermore, we measure the conversion of the ads, i.e. whether the users took them as a reason to interact with the ads and make use of the advertised offers (so-called 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 (Article 6 (1) (a) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://about.ads.microsoft.com/de-de>; **Privacy Policy:** <https://privacy.microsoft.com/en-us/privacystatement>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Opt-Out:** <https://account.microsoft.com/privacy/ad-settings/>.
- **Google Search Ads 360:** Search management platform that enables agencies and advertisers to manage and target search marketing campaigns across multiple search engines and media channels; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://marketingplatform.google.com/intl/en/about/search-ads-360/>; **Privacy Policy:** <https://policies.google.com/privacy>; **Data Processing Agreement:** <https://business.safety.google/adsprocessor/terms/>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

Further Information: <https://business.safety.google/adsservices/> (Types of processing and data processed).

- **LinkedIn Ads:** Placement of ads within the LinkedIn platform and analysis of ad results; **Service provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://business.linkedin.com/de-de/marketing-solutions/ads>; **Privacy Policy:** <https://www.linkedin.com/legal/privacy-policy>; **Data Processing Agreement:** <https://www.linkedin.com/legal/l/dpa>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Opt-Out:** <https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>.
- **Facebook Conversions API:** We use the "Conversions API" provided by Facebook. The Conversions API is an interface with which event data is sent directly from our servers to Facebook. The functionality and processing of data within the framework of the Conversions API corresponds to the functionality and processing within the framework of the use of the Facebook Pixel, and therefore we refer to the data protection information on the Facebook Pixel and Custom Audiences in this respect; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).

Customer Reviews and Ratings

We participate in review and rating procedures to evaluate, optimise and advertise our performance. If users rate us via the participating rating platforms or methods or otherwise provide feedback, the General Terms and Conditions of Business or Use and the data protection information of the providers also apply. As a rule, the rating also requires registration with the respective provider.

In order to ensure that the evaluators have actually made use of our services, we transmit, with the consent of the customer, the necessary data relating to the customer and the service or products used to the respective rating platform (this includes the name, e-mail address, order number or article number). This data is used solely to verify the authenticity of the user.

- **Processed data types:** Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).

- **Data subjects:** Service recipients and clients. Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Feedback (e.g. collecting feedback via online form). Marketing.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Google Customer Reviews:** Service for obtaining and/or displaying customer satisfaction and customer opinions; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.google.com/>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further Information:** In the context of obtaining customer reviews, an identification number and time for the business transaction to be evaluated, in the case of review requests sent directly to customers, the customer's e-mail address and its country of residence information as well as the review information itself are processed; Further information on types of processing and data processed: <https://business.safety.google/adsservices/>. Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: <https://business.safety.google/adscontrollerterms>.

Profiles in Social Networks (Social Media)

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

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

In addition, user data is usually processed within social networks for market research and advertising purposes. For example, user profiles can be created on the basis of user behaviour and the associated interests of users. The user profiles can then be used, for example, to place advertisements within and outside the networks which are presumed to correspond to the interests of the users. For these purposes, cookies are usually stored on the user's computer, in which the user's usage behaviour and interests are stored. Furthermore, data can be stored in the user profiles independently of the devices used by the users (especially if the users are members of the respective networks or will become members later on).

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

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

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

Further information on processing methods, procedures and services used:

- **Instagram:** Social network, allows the sharing of photos and videos, commenting on and favouriting posts, messaging, subscribing to profiles and pages; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.instagram.com>; **Privacy Policy:** <https://privacycenter.instagram.com/policy/>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).
- **Facebook Pages:** Profiles within the social network Facebook - We are jointly responsible (so called "joint controller") with Meta Platforms Ireland Limited for the collection (but not the further processing) of data of visitors to our Facebook page. This data includes information about the types of content users view or interact with, or the actions they take (see "Things that you and others do and provide" in the Facebook Data

Policy: <https://www.facebook.com/privacy/policy/>), and information about the devices used by users (e.g., IP addresses, operating system, browser type, language settings, cookie information; see "Device Information" in the Facebook Data Policy: <https://www.facebook.com/privacy/policy/>). As explained in the Facebook Data Policy under "How we use this information?" Facebook also collects and uses information to provide analytics services, known as "page insights," to site operators to help them understand how people interact with their pages and with 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 the security measures that Facebook must observe and in which Facebook has agreed to fulfill the rights of the persons concerned (i.e. users can send information access or deletion requests directly to Facebook). The rights of users (in particular to access to information, erasure, objection and complaint to the competent supervisory authority) are not restricted by the agreements with Facebook. Further information can be found in the "Information about Page Insights" (https://www.facebook.com/legal/terms/information_about_page_insights_data). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.facebook.com>; **Privacy Policy:** <https://www.facebook.com/privacy/policy/>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

- **Facebook-Groups:** We use the "Groups" function of the Facebook platform to create interest groups within which Facebook users can contact each other or us and exchange information. In doing so, we process personal data of the users of our groups as far as this is necessary for the purpose of the group use as well as its moderation. These data include information on first and last names, as well as published or privately shared content, as well as values on the status of group membership or group-related activities, such as entry or exit, as well as the time information on the aforementioned data. Our guidelines within the groups may contain further specifications and information on the use of the respective group. Furthermore, we would like to point out the processing of

data of the users by Facebook itself. This data includes information about the types of content users view or interact with, or the actions they take (see under "Things You and Others Do and Provide" in the Facebook Data Policy:

<https://www.facebook.com/privacy/policy/>), as well as information about the devices users use (e.g., IP addresses, operating system, browser type, language settings, cookie data; see under "Device Information" in the Facebook Data Policy:

<https://www.facebook.com/privacy/policy/>). As explained in the Facebook Data Policy under "How do we use this information?", Facebook also collects and uses information to provide analytics services, called "Insights," to group operators to provide them with insights about how people interact with their groups and with content associated with them; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:**

<https://www.facebook.com/>; **Privacy Policy:** <https://www.facebook.com/privacy/policy/>.

Basis for third-country transfers: EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

- **Facebook events:** Event profiles within the social network Facebook - We use the "Events" function of the Facebook platform to refer to events and dates as well as to get in touch with users (participants and interested parties) and to exchange information. In doing so, we process personal data of the users of our event pages, as far as this is necessary for the purpose of the event page as well as its moderation. These data include information on first and last names, as well as published or privately communicated content, as well as values on the status of participation and the time information on the aforementioned data. Furthermore, we refer to the processing of data of users by Facebook itself. This data includes information about the types of content users view or interact with, or the actions they take (see under "Things You and Others Do and Provide" in the Facebook Data Policy: <https://www.facebook.com/privacy/policy/>), as well as information about the devices users use (e.g., IP addresses, operating system, browser type, language settings, cookie data; see under "Device Information" in the Facebook Data Policy: <https://www.facebook.com/privacy/policy/>). As explained in the Facebook Data Policy under "How do we use this information?", Facebook also collects and uses information to provide analytics services, known as "insights," to event providers to provide them

with insights about how people interact with their event pages and with content associated with them; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.facebook.com>; **Privacy Policy:** <https://www.facebook.com/privacy/policy/>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

- **LinkedIn:** Social network - We are jointly responsible with LinkedIn Ireland Unlimited Company for the collection (but not the further processing) of data from visitors for the purposes of creating „Page-Insights" (statistics) for our LinkedIn profiles. This data includes information about the types of content that users view or interact with, or the actions they take, as well as information about the devices used by the users (e.g., IP addresses, operating system, browser type, language settings, cookie data) and details from the users' profiles, such as job function, country, industry, seniority, company size, and employment status. Privacy information regarding the processing of user data by LinkedIn can be found in LinkedIn's privacy notices:

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

We have concluded a special agreement with LinkedIn Ireland, the 'Page Insights Joint Controller Addendum (the 'Addendum')' (<https://legal.linkedin.com/pages-joint-controller-addendum>), which specifically regulates the security measures that LinkedIn must observe and wherein LinkedIn has agreed to fulfill the rights of the affected parties (i.e., users can, for example, direct requests for information or deletion directly to LinkedIn).

The rights of the users (in particular to access to information, erasure, objection, and complaint to the competent supervisory authority) are not restricted by the agreements with LinkedIn. The joint responsibility is limited to the collection of data by and transmission to Ireland Unlimited Company, a company based in the EU. The further processing of the data is the sole responsibility of Ireland Unlimited Company, particularly regarding the transmission of data to the parent company LinkedIn

Corporation in the USA; **Service provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR);

Website: <https://www.linkedin.com>; **Privacy Policy:**

<https://www.linkedin.com/legal/privacy-policy>; **Basis for third-country transfers:** EEA -

Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Opt-Out:** <https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>.

- **TikTok:** Social network, allows the sharing of photos and videos, commenting on and favouriting posts, messaging, subscribing to accounts; **Service provider:** TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Ireland and TikTok Information Technologies UK Limited, Kaleidoscope, 4 Lindsey Street, London, United Kingdom, EC1A 9HP; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://www.tiktok.com>; **Privacy Policy:** <https://www.tiktok.com/de/privacy-policy>. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (<https://ads.tiktok.com/i18n/official/policy/jurisdiction-specific-terms>), Switzerland - Standard Contractual Clauses (<https://ads.tiktok.com/i18n/official/policy/jurisdiction-specific-terms>).
- **X:** Social network; **Service provider:** Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2 D02 AX07, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://x.com>; **Privacy Policy:** <https://x.com/privacy>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Ireland).
- **YouTube:** Social network and video platform; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Opt-Out:** <https://myadcenter.google.com/personalizationoff>.

Plugins and embedded functions and content

Within our online services, we integrate functional and content elements that are obtained from the servers of their respective providers (hereinafter referred to as "third-party providers"). These may, for example, be graphics, videos or city maps (hereinafter uniformly referred to as "Content").

The integration always presupposes that the third-party providers of this content process the IP address of the user, since they could not send the content to their browser without the IP address. The IP address is therefore required for the presentation of these contents or functions. We strive to use only those contents, whose respective offerers use the IP address only for the distribution of the contents. Third parties may also use so-called pixel tags (invisible graphics, also known as "web beacons") for statistical or marketing purposes. The "pixel tags"

can be used to evaluate 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 include technical information about the browser and operating system, referring websites, visit times and other information about the use of our website, as well as may be linked to such information from other sources.

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers). Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of our online services and usability; Provision of contractual services and fulfillment of contractual obligations; Marketing. Profiles with user-related information (Creating user profiles).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Google Fonts (from Google Server):** Obtaining fonts (and symbols) for the purpose of a technically secure, maintenance-free and efficient use of fonts and symbols with regard to timeliness and loading times, their uniform presentation and consideration of possible restrictions under licensing law. The provider of the fonts is informed of the user's IP address so that the fonts can be made available in the user's browser. In addition, technical data (language settings, screen resolution, operating system, hardware used) are transmitted which are necessary for the provision of the fonts depending on the devices used and the technical environment. This data may be processed on a server of the provider of the fonts in the USA - When visiting our online

services, users' browsers send their browser HTTP requests to the Google Fonts Web API. The Google Fonts Web API provides users with Google Fonts' cascading style sheets (CSS) and then with the fonts specified in the CCS. These HTTP requests include (1) the IP address used by each user to access the Internet, (2) the requested URL on the Google server, and (3) the HTTP headers, including the user agent describing the browser and operating system versions of the website visitors, as well as the referral URL (i.e., the web page where the Google font is to be displayed). IP addresses are not logged or stored on Google servers and they are not analyzed. The Google Fonts Web API logs details of HTTP requests (requested URL, user agent, and referring URL). Access to this data is restricted and strictly controlled. The requested URL identifies the font families for which the user wants to load fonts. This data is logged so that Google can determine how often a particular font family is requested. With the Google Fonts Web API, the user agent must match the font that is generated for the particular browser type. The user agent is logged primarily for debugging purposes and is used to generate aggregate usage statistics that measure the popularity of font families. These aggregate usage statistics are published on Google Fonts' Analytics page. Finally, the referral URL is logged so that the data can be used for production maintenance and to generate an aggregate report on top integrations based on the number of font requests. Google says it does not use any of the information collected by Google Fonts to profile end users or serve targeted ads; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://fonts.google.com/>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** <https://developers.google.com/fonts/faq/privacy?hl=en>.

- **Google Maps APIs and SDKs:** Interfaces to the map and location services provided by Google, which, for example, allow the addition of address entries, location determinations, distance calculations or the provision of supplementary information on locations and other places; **Service provider:** Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://mapsplatform.google.com/>; **Privacy Policy:**

<https://policies.google.com/privacy>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

- **Instagram plugins and contents:** Instagram plugins and contents - This can include content such as images, videos or text and buttons with which users can share content from this online service within Instagram . - We are jointly responsible (so-called "joint-controllership") with Meta Platforms Ireland Limited for the collection or transmission (but not further processing) of "Event Data" that Facebook collects or receives as part of a transmission using Instagram functions that run on our website for the following purposes: a) displaying content advertising information that matches users' presumed interests; b) delivering commercial and transactional messages (e.g. b) delivering commercial and transactional messages (e.g., addressing users via Facebook Messenger); c) improving ad delivery and personalizing features and content (e.g., improving recognition of which content or advertising information is believed to be of interest to users). We have entered into a special agreement with Facebook ("Controller Addendum", https://www.facebook.com/legal/controller_addendum), which specifically addresses the security measures that Facebook must take (https://www.facebook.com/legal/terms/data_security_terms) and in which Facebook has agreed to comply with the rights of data subjects (i.e., users can, for example, submit information access or deletion requests directly to Facebook). Note: If Facebook provides us with measurements, analyses and reports (which are aggregated, i.e. do not contain information on individual users and are anonymous to us), then this processing is not carried out within the scope of joint responsibility, but on the basis of a DPA ("Data Processing Terms", <https://www.facebook.com/legal/terms/dataprocessing/update>), the "Data Security Conditions" (https://www.facebook.com/legal/terms/data_security_terms) and, with regard to processing in the USA, on the basis of Standard Contractual Clauses ("Facebook EU Data Transfer Addendum", https://www.facebook.com/legal/EU_data_transfer_addendum). The rights of users (in particular to access to information, erasure, objection and complaint to the competent supervisory authority) are not restricted by the agreements with Facebook; **Service provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:**

<https://www.instagram.com>; **Privacy Policy:** <https://privacycenter.instagram.com/policy/>.

Basis for third-country transfers: Switzerland - Adequacy decision (Ireland).

- **LinkedIn plugins and contents:** LinkedIn plugins and contents - This can include content such as images, videos or text and buttons with which users can share content from this online service within LinkedIn; **Service provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.linkedin.com>; **Privacy Policy:** <https://www.linkedin.com/legal/privacy-policy>; **Data Processing Agreement:** <https://legal.linkedin.com/dpa>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Opt-Out:** <https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out>.
- **reCAPTCHA:** We integrate the "reCAPTCHA" function to be able to recognise whether entries (e.g. in online forms) are made by humans and not by automatically operating machines (so-called "bots"). The data processed may include IP addresses, information on operating systems, devices or browsers used, language settings, location, mouse movements, keystrokes, time spent on websites, previously visited websites, interactions with ReCaptcha on other websites, possibly cookies and results of manual recognition processes (e.g. answering questions asked or selecting objects in images). The data processing is based on our legitimate interest to protect our online services from abusive automated crawling and spam; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, , parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.google.com/recaptcha/>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF). **Opt-Out:** Opt-Out-Plugin: <https://tools.google.com/dlpage/gaoptout?hl=en>, Settings for the Display of Advertisements: <https://myadcenter.google.com/personalizationoff>.
- **X plugins and contents:** Plugins and buttons of the platform "X" - This may include, for example, content such as images, videos or texts and buttons with which users can share content of this online offer within X; **Service provider:** Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2 D02 AX07, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://x.com>; **Privacy**

Policy: <https://x.com/privacy>, (Settings: <https://x.com/personalization>); **Data Processing Agreement:** <https://privacy.x.com/en/for-our-partners/global-dpa>. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (<https://privacy.x.com/en/for-our-partners/global-dpa>), Switzerland - Adequacy decision (Ireland).

- **YouTube videos:** Video contents; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, , parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://www.youtube.com>; **Privacy Policy:** <https://policies.google.com/privacy>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF). **Opt-Out:** Opt-Out-Plugin: <https://tools.google.com/dlpage/gaoptout?hl=en>, Settings for the Display of Advertisements: <https://myadcenter.google.com/personalizationoff>.
- **Google Hosted Libraries:** Google Hosted Libraries is a globally available Content Delivery Network (CDN) for the most commonly used open-source JavaScript libraries. These are provided to supply web libraries that optimise website loading times, reduce bandwidth usage, and enhance performance through the use of shared, public resources; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://developers.google.com/speed/libraries/>; **Privacy Policy:** <https://policies.google.com/privacy>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Ireland).
- **Adobe Typekit fonts:** We integrate the fonts ("Typekit fonts") of the provider Adobe, whereby the data of the users are used solely for purposes of the representation of the fonts in the browser of the users. The integration takes place on the basis of our legitimate interests in a technically secure, maintenance-free and efficient use of fonts, their uniform presentation and consideration of possible licensing restrictions for their integration; **Service provider:** Adobe Systems Software Ireland, 4-6, Riverwalk Drive, Citywest Business Campus, Brownsbarn, Dublin 24, D24 DCW0, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.adobe.com>; **Privacy Policy:** <https://www.adobe.com/de/privacy.html>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

Management, Organization and Utilities

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

Within this context, personal data may be processed and stored on the servers of third-party providers. This may include 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 processes, contracts, other processes and their contents.

If users are referred to the third-party providers or their software or platforms in the context of communication, business or other relationships with us, the third-party provider processing may process usage data and metadata that can be processed by them for security purposes, service optimisation or marketing purposes. We therefore ask you to read the data protection notices of the respective third party providers.

- **Processed data types:** Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.). Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations. Office and organisational procedures.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **swoogo:** Event management platform that helps event organisers to organise virtual, face-to-face and hybrid events and offers features for attendee communication, event registration, networking, agenda management and live streaming; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Data Processing Agreement: <https://swoogo.events/legal/data-processing-addendum/>; **Service provider:** Swoogo

LLC , 1925 Century Park E Ste 1700 Los Angeles, CA 90067, USA; **Website:**
<https://swoogo.events>. **Privacy Policy:** <https://swoogo.events/legal/privacy/>.

Processing of data in the context of employment relationships

In the context of employment relationships, the processing of personal data aims to effectively manage the establishment, execution, and termination of such relationships. This data processing supports various operational and administrative functions necessary for managing employee relations.

The data processing covers various aspects ranging from contract initiation to termination. Included are the organization and management of daily working hours, management of access rights and permissions, as well as handling personnel development measures and staff appraisals. The processing also serves payroll accounting and management of wage and salary payments, which represent critical aspects of contract execution.

Additionally, the data processing considers legitimate interests of the responsible employer, such as ensuring workplace safety or capturing performance data for evaluating and optimizing operational processes. Moreover, the data processing includes disclosing employee data in external communication and publication processes where necessary for operational or legal purposes.

The processing of this data always takes place with due regard for the applicable legal frameworks, aiming always to create and maintain a fair and efficient working environment. This also includes considering the privacy of affected employees, anonymizing or deleting data after fulfilling the processing purpose or according to legal retention periods.

- **Processed data types:** Employee Data (Information about employees and other individuals in an employment relationship); Payment Data (e.g. bank details, invoices, payment history); Contract data (e.g. contract object, duration, customer category); Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Social data (Data subject to a special social confidentiality obligation and processed, for example, by social insurance institutions, social welfare institutions or pension authorities.); Log data (e.g. log files concerning logins or data retrieval or access times.); Performance and behavioural data (For example, performance and behavioural data aspects such as performance evaluations, feedback from supervisors, training attendance, compliance with company policies, self-assessments, and behavioural

assessments.); Working hours data (e.g. start of work time, end of work time, actual working hours, target working hours, break times, overtime, vacation days, special leave days, sick days, absences, home office days, business trips); Salary data (e.g. basic salary, bonus payments, premiums, tax class information, surcharges for night work/overtime, tax deductions, social security contributions, net payout amount); Images and/ or video recordings (e.g. photographs or video recordings of a person); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).

- **Special categories of personal data:** Health Data; Religious or philosophical beliefs. Trade union membership.
- **Data subjects:** Employees (e.g. employees, job applicants, temporary workers, and other personnel.).
- **Purposes of processing:** Establishment and execution of employment relationships (Processing of employee data in the context of the establishment and execution of employment relationships); Business processes and management procedures; Provision of contractual services and fulfillment of contractual obligations; Public relations; Security measures. Office and organisational procedures.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Compliance with a legal obligation (Article 6 (1) (c) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR); Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR). Consent (Article 6 (1) (a) GDPR).

Further information on processing methods, procedures and services used:

- **Time Recording:** Processes for recording employees' working hours include both manual and automated methods, such as the use of punch clocks, time tracking software, or mobile apps. Activities involved include entering clock-in and clock-out times, break times, overtime, and absences. To verify and validate the recorded working hours, they are compared with deployment or shift schedules, checked for absences, and approved for overtime by supervisors. Reports and analyses are generated based on the recorded working hours to provide work time records, overtime reports, and absence statistics for management and the human resources department; **Legal Basis:**

Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Authorization Management:** Procedures required for the definition, management, and control of access rights and user roles within a system or an organisation (e.g., creation of authorisation profiles, role- and access-based control, review and approval of access requests, regular review of access rights, tracking and auditing of user activities, creation of security policies and procedures); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Special categories of personal data:** Special categories of personal data are processed in the context of employment relationships or to fulfil legal obligations. The processed special categories of personal data include information concerning the health, trade union membership, or religious affiliation of employees. This data may be transferred to health insurance companies or processed for assessing the employees' work capacity, for corporate health management, or for declarations to the tax authorities; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Sources of Processed Data:** Personal data received during the application process and/or employment relationship will be processed. Furthermore, where required by law, personal data will be collected from other sources. These may include financial authorities for tax-related information, the respective health insurance company for information on work incapacity, third parties such as employment agencies, or publicly accessible sources like professional social networks in the context of application procedures; **Legal Basis:** Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Purposes of Data Processing:** The personal data of employees are primarily processed for the establishment, execution, and termination of the employment relationship. Furthermore, the processing of this data is necessary to fulfil legal obligations in the field of tax and social security law. In addition to these primary purposes, the data of employees are also used to meet regulatory and supervisory requirements, to optimise processes of electronic data processing, and to compile

company-internal or cross-company data, possibly including statistical data. Moreover, the data of employees may be processed for the assertion of legal claims and defense in legal disputes; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Transmission to the works council:** The processes for transmitting information to the works council include compiling relevant data and information and transmitting it to the works council. This includes sharing information on personnel matters, working conditions, working hours, remuneration, and other topics of interest to the works council in the specific case, in accordance with legal provisions and the regulations of the works agreements. The collected data includes information about employees, working hours, remuneration, and other work-related aspects that are relevant to the works council; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).
- **Transmission of Employee Data to Third Countries:** The transfer of employee data to third countries, meaning countries outside the European Union (EU) and the European Economic Area (EEA), occurs only if it is necessary for the fulfilment of the employment relationship, legally required, or if employees have given their consent. Employees will be informed about the details separately, as far as legally required; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Transmission of Employee Data:** The data of employees is processed internally only by those departments that require it to fulfil operational, contractual, and legal obligations. The transfer of data to external recipients only occurs if it is legally required, or if the affected employees have given their consent. Possible scenarios for this can include requests for information from authorities or in the case of asset formation benefits. Furthermore, the controller may transfer personal data to further recipients as far as this is necessary for fulfilling his contractual and legal obligations as an employer. These recipients can include: a) banks b) health insurance companies, pension insurance institutions, providers of old-age provisions and other social insurance carriers c) authorities, courts (e.g., tax authorities, labour courts, further supervisory authorities

within the framework of fulfilling reporting and information obligations) d) tax and legal advisors e) third-party debtors in the case of wage and salary garnishments f) other entities to which legally obligatory declarations must be made.

In addition, data can be transferred to third parties if this is necessary for communication with business partners, suppliers or other service providers. Examples include details in the sender area of emails or letterheads as well as creating profiles on external platforms; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Business Travel and Travel Expense Settlement:** Procedures required for planning, executing, and accounting for business trips (e.g., booking of travel, organizing accommodations and transportation, managing travel expense advances, submitting and reviewing travel expense reports, controlling and recording incurred costs, compliance with travel policies, handling of the travel expense management); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).
- **Payroll and wage accounting:** Procedures required for calculating, disbursing, and documenting wages, salaries, and other remuneration for employees (e.g., recording of working hours, calculation of deductions and surcharges, remittance of taxes and social security contributions, preparation of payroll statements, management of wage accounts, reporting to the tax authorities and social security institutions); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR).
- **Deletion of Employee Data:** Employment data will be deleted under German law when it is no longer required for the purpose for which it was collected, unless there is a legal obligation to retain or archive it, or it needs to be kept for the interests of the employer. The following retention and archiving obligations are observed:**Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).

- General personnel records - General personnel records (such as employment contracts, references, supplementary agreements) are retained for up to three years after the termination of the employment relationship (§ 195 German Civil Code (BGB)).
Tax-relevant documents - Tax-relevant documents in the personnel file are kept for six years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
Information on wages and working hours - Information on wages and working hours for (accident) insured with wage proof are kept for five years (§ 165 I 1, IV 2 Social Code Book VII (SGB VII)).
- Payrolls including lists for special payments - Payrolls including lists for special payments, if a booking receipt is available, are kept for ten years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
- Wage lists for interim, final, and special payments - Wage lists for interim, final, and special payments are kept for six years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
- Documents on employee insurance - Documents on employee insurance, if booking receipts are available, are kept for ten years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
- Contribution statements to social security institutions - Contribution statements to social security institutions are kept for ten years (§ 165 Social Code Book VII (SGB VII)).
Wage accounts - Wage accounts are kept for six years (§ 41 I 9 Income Tax Act (EStG)).
- Applicant data - Kept for a maximum of six months from the receipt of rejection.
- Working time records (for more than 8 hours on workdays) - Kept for two years (§ 16 II Working Time Act (ArbZG)).
- Application documents (following online job advertisement) - Kept for three to a maximum of six months from the receipt of rejection (§ 26 Federal Data Protection Act (BDSG) n.F., § 15 IV General Act on Equal Treatment (AGG)).
- Certificates of incapacity for work (AU) - Kept for up to five years (§ 6 I Act on the Compensation of Expenses (AAG)).

- Documents on company pension schemes - Kept for 30 years (§ 18a Act to Improve Occupational Pensions (BetrAVG)).
 - Sickness data of employees - Kept for twelve months from the start of the illness, if the absence in a year does not exceed six weeks.
 - Documents on maternity protection - Kept for two years (§ 27 para. 5 Maternity Protection Act (MuSchG)).
- **Personnel file management:** Procedures required for the organisation, updating, and management of employee data and records (e.g., recording of basic personnel data, retention of employment contracts, certificates and attestations, updating data upon changes, compilation of documents for employee discussions, archiving of personnel files, compliance with data protection regulations); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).
 - **Personnel development, performance evaluation, and staff appraisals:** Procedures required in the area of employee promotion and development, as well as in assessing their performance and during employee discussions (e.g., needs analysis for further training, planning and implementation of training measures, creation of performance evaluations, conducting goal-setting and feedback discussions, career planning and talent management, succession planning); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).
 - **Obligation to Provide Data:** The person in charge informs the employees that the provision of their data is required. This is generally the case when the data are necessary for the establishment and execution of the employment relationship, or when their collection is mandated by law. The provision of data may also be required when employees assert claims or are entitled to claims. The implementation of these measures or fulfilment of services depends on the provision of such data (for example, providing data for the receipt of wages); **Legal Basis:** Performance of a contract and

prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Publication and Disclosure of Employee Data:** The data of employees will only be published or disclosed to third parties if it is necessary for the performance of work tasks according to the employment contract. This applies, for example, when employees are named as contact persons in correspondences, on the website, or in public registers following an agreement or specified job description, or if their field of work includes representative functions. Similarly, this may occur if representation or communication with the public takes place as part of performing these tasks, such as image recordings during public relations activities. Otherwise, employee data is published only with their consent or based on the legitimate interests of the employer, for example, in the case of stage or group photographs taken during a public event; **Legal Basis:** Consent (Article 6 (1) (a) GDPR), Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Job Application Process

The application process requires applicants to 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 contained therein.

In principle, the required information includes personal information such as name, address, a contact option and proof of the qualifications required for a particular employment. Upon request, we will be happy to provide you with additional information.

Where available, applicants are welcome to submit their applications via our online form, which is securely encrypted to the latest standards. Alternatively, applications can also be sent to us by email. However, we kindly remind you that emails are not inherently encrypted over the Internet. While emails are usually encrypted in transit, they are not encrypted on the servers from which they are sent and received. Therefore, we cannot assume responsibility for the security of the application during its transmission from the sender to our server.

Processing of special categories of data: To the extent that special categories of personal data (Article 9(1) GDPR, e.g., health data, such as disability status or ethnic origin) are requested from applicants or communicated by them during the application process, their processing is carried out so that the controller or the data subject can exercise rights arising from employment law and the law of social security and social protection, in the case of protection of vital interests of the applicants or other persons, or for purposes of preventive or occupational medicine, for the assessment of the employee's work ability, for medical diagnosis,

for the provision or treatment in the health or social sector, or for the management of systems and services in the health or social sector.

Ereasure of data: In the event of a successful application, the data provided by the applicants may be further processed by us for the purposes of the employment relationship. Otherwise, if the application for a job offer is not successful, the applicant's data will be deleted. Applicants' data will also be deleted if an application is withdrawn, to which applicants are entitled at any time. Subject to a justified revocation by the applicant, the deletion will take place at the latest after the expiry of a period of six months, so that we can answer any follow-up questions regarding the application and comply with our duty of proof under the regulations on equal treatment of applicants. Invoices for any reimbursement of travel expenses are archived in accordance with tax regulations.

Admission to a talent pool - Admission to a talent pool, if offered, is based on consent. Applicants are informed that their consent to be included in the talent pool is voluntary, has no influence on the current application process and that they can revoke their consent at any time for the future.

Duration of data retention in the applicant pool in months: 12

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Job applicant details (e.g. Personal data, postal and contact addresses and the documents pertaining to the application and the information contained therein, such as cover letter, curriculum vitae, certificates, etc., as well as other information on the person or qualifications of applicants provided with regard to a specific job or voluntarily by applicants).
- **Data subjects:** Job applicants.
- **Purposes of processing:** Job Application Process (Establishment and possible later execution as well as possible later termination of the employment relationship).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Job application process as a pre-contractual or contractual relationship (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Umantis:** Management of application processes, collection and analysis of applicant data, creation of job advertisements, management of employee data, conducting employee interviews, performance assessments and target agreements, training

management, succession planning and talent management; **Service provider:** Abacus Umantis AG, Unterstrasse 11, CH 9001 St. Gallen, Switzerland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.umantis.com/>; **Privacy Policy:** <https://www.umantis.com/datenschutz/>. **Basis for third-country transfers:** EEA - Adequacy decision (Switzerland).

- **Indeed:** Recruitment-related services (search for employees, communication, application process, contract negotiations); **Service provider:** Indeed Ireland Operations Limited, 124 St. Stephen's Green, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://de.indeed.com/>; **Privacy Policy:** <https://www.indeed.com/legal?hl=en#privacypolicy>. **Basis for third-country transfers:** Switzerland - Adequacy decision (Ireland).

Privacy Information for Whistleblowers

In this section, you will find information on how we handle data from individuals who provide tips (whistleblowers), as well as from affected and involved parties within the framework of our whistleblower procedure. Our aim is to offer a straightforward and secure means of reporting potential misconduct by us, our employees, or service providers, especially for actions that violate laws or ethical guidelines. Furthermore, we ensure appropriate processing and handling of the reports.

Legal Bases (Germany): To the extent that we process data to fulfil our legal obligations in accordance with the Whistleblower Protection Act (HinSchG), the legal basis for processing is Article 6(1)(c) GDPR and, in the case of special categories of personal data, Article 9(2)(g) GDPR, § 22 BDSG, in conjunction with § 10 HinSchG. This relates to the obligation to establish and operate an internal whistleblower reporting office, the fulfilment of its legal duties, and, in the case of using data collected in the reporting process, the initiation of further investigations or employment-related steps against individuals found to have committed a violation.

To the extent that we process data (especially in cases of identified misconduct) for the purpose of or in preparation for legal defence, this is done on the basis of our legitimate interests in lawful and ethical conduct in accordance with Article 6(1)(f) GDPR.

To the extent that consent has been given for processing personal data for specific purposes, processing is based on this consent according to Article 6(1)(a) of the GDPR and in case of special categories of personal data Article 9(2)(a) of the GDPR. An example would be disclosing a whistleblower's identity or creating a verbatim report during a personal meeting. Given consent can be revoked at any time with effect for the future.

Legal Bases: To the extent that we process data to fulfill our legal obligations in accordance with the applicable whistleblower protection law, the legal basis for processing is Article 6(1)(c)

of the GDPR, and in the case of special categories of personal data, Article 9(2)(g) of the GDPR, each in conjunction with the relevant law. This relates to the obligation to set up and operate an internal whistleblower reporting office, the fulfillment of its legal tasks, and in the case of using data collected during the reporting process, taking further investigations or employment-related steps against individuals who have been found guilty of a violation. To the extent that we process data (particularly in cases of identified misconduct) as part of or in preparation for legal defense, this is based on our legitimate interests in lawful and ethical behavior according to Article 6(1)(f) of the GDPR. To the extent that consent has been given for processing personal data for specific purposes, processing is based on this consent according to Article 6(1)(a) of the GDPR and in case of special categories of personal data Article 9(2)(a) of the GDPR. An example would be disclosing a whistleblower's identity or creating a verbatim report during a personal meeting. Given consent can be revoked at any time with effect for the future.

Processed types of data:

In the course of receiving and processing reports, as well as in the subsequent whistleblower procedure, we may collect various data. These particularly include information provided by a whistleblower, such as:

- Name, contact details, and location of the person making the report,
- Names and information about potential witnesses or individuals affected by the report,
- Names and information about the individuals who are the subject of the report,
- Data concerning the alleged misconduct,
- Other relevant details if communicated by the whistleblower.

For the purposes of fact-finding and further proceedings, we also process the following personal data:

- Unique identification of the report,
- Contact details of the reporting individual, if provided,
- Personal data of individuals mentioned in the report, if provided,
- Personal data of individuals indirectly affected by fact-finding, if applicable,
- Personal data from individuals in other involved companies (e.g., within legal counsel), if relevant,
- Additional data related to the circumstances.

Special categories of personal data:

It may occur that we collect special categories of personal data in the course of our activities, especially when they are provided by a whistleblower. These include:

- Health-related data of a person,
- Data on a person's racial or ethnic origin,
- Information about a person's religious or philosophical beliefs,
- Details about a person's sexual orientation.

These data are only processed if they are relevant to the handling of the respective report and have been explicitly provided by the whistleblower.

Use of our online forms: Please note that you have the option to submit tips anonymously. To ensure the security of your data when using our online forms, we recommend accessing them in the so-called 'Incognito Mode' of your browser. Here's how you can open an Incognito window: a) On a Windows PC: Open your browser and press Ctrl+Shift+N; b) On a Mac: Open your browser and press Command+Shift+N; c) On mobile devices: Switch to private mode via the tab menu.

When accessing our website in normal mode, your browser automatically sends certain information to our server, such as browser type and version, date and time of your access. This also includes the IP address of your device. These data are temporarily stored in a log file and automatically deleted after no more than 30 days.

The processing of the IP address serves technical and administrative purposes for establishing a connection to our website. It ensures the security, stability, and functionality of the whistleblower form and is an essential part of our measures to ensure the confidential submission of reports.

The processing of logged data is based on Article 6 (1)(f) GDPR. Our legitimate interest lies in the need for security and the necessity to ensure the technical conditions for a smooth and uninterrupted submission of reports.

Disclosure of names: You have the option to submit reports anonymously. However, unless prohibited by national legislation, we recommend that you provide your name and contact details. This enables us to follow up on the report more effectively and, if necessary, to contact you directly. Should you choose to provide your name and contact information, your identity will be treated with strict confidentiality. Exceptions to this confidentiality exist only if we are legally obliged to disclose your identity. This may be necessary in order to protect or defend our rights or the rights of our employees, customers, suppliers, or business partners. Another exception is if it is determined that the allegations were made with malicious intent.

Disclosure of data to third parties: Data related to the report provided will only be disclosed to third parties under certain circumstances. This occurs either a) if you have given us your explicit

consent according to Art. 6 (1)(a) of the GDPR, or b) if there is a legal obligation to disclose the data pursuant to Art. 6 (1)(c) of the GDPR. Possible third parties include public authorities, government, regulatory or tax agencies, if disclosure is necessary for compliance with a legal or regulatory obligation. Furthermore, within the scope of legal provisions, we may engage lawyers and other professional advisers who are authorised to investigate suspected misconduct and take necessary actions following an investigation, such as initiating disciplinary or legal proceedings. Additionally, carefully selected and supervised service providers whom we employ may also receive data for these purposes (such as operators of a web-based reporting tool). However, these providers are contractually bound to comply with the prevailing data protection regulations under a so-called data processing agreement.

Data retention and deletion: Personal data will be processed only for as long as necessary to fulfil the purposes of processing described above. If the data are no longer needed for these purposes, they will be deleted. However, in certain situations, the data may be retained for longer periods to meet legal requirements, provided this is necessary and proportionate. In such cases, the data will be deleted as soon as they are no longer required for these purposes.

Technical and organisational measures: We have implemented the necessary contractual, technical, and organisational measures to ensure the security of all data processed by us. This data is processed exclusively for the purposes set out. The incoming hints are handled by authorised individuals who gain access to the respective reports and carry out the subsequent examination of the facts. Our employees are specifically trained, educated, and bound to strict confidentiality in the proper execution of these examinations of facts.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Employee Data (Information about employees and other individuals in an employment relationship); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Employees (e.g. employees, job applicants, temporary workers, and other personnel.); Third parties. Whistleblowers.
- **Purposes of processing:** Whistleblower protection. Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR); Compliance with a legal obligation (Article 6 (1) (c) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Whistleblower Systems

As part of our whistleblower procedure, we employ external service providers. In doing so, we operate within the framework of legal requirements and ensure that the technical and organizational demands for security measures that we adhere to are also met by the external providers.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Employee Data (Information about employees and other individuals in an employment relationship); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Employees (e.g. employees, job applicants, temporary workers, and other personnel.); Third parties. Whistleblowers.
- **Purposes of processing:** Whistleblower protection.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR); Compliance with a legal obligation (Article 6 (1) (c) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Changes and Updates

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

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

Terminology and Definitions

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

- **Affiliate Tracking:** Custom Audiences refers to the process of determining target groups for advertising purposes, e.g. the display of advertisements. For example, a user's interest in certain products or topics on the Internet may be used to conclude that the user is interested in advertisements for similar products or the online store in which the user viewed the products. "Lookalike Audiences" is the term used to describe content that is viewed as suitable by users whose profiles or interests presumably correspond to the users for whom the profiles were created. For the purposes of creating custom audiences and lookalike audiences, cookies and web beacons are typically used.
- **Artificial Intelligence (AI):** The purpose of processing data through Artificial Intelligence (AI) includes the automated analysis and processing of user data to identify patterns, make predictions, and improve the efficiency and quality of our services. This involves the collection, cleansing, and structuring of data, training and applying AI models, as well as the continuous review and optimisation of results, and is carried out exclusively with users' consent or based on legal authorisation grounds.
- **Contact data:** Contact details are essential information that enables communication with individuals or organizations. They include, among others, phone numbers, postal addresses, and email addresses, as well as means of communication like social media handles and instant messaging identifiers.
- **Content data:** Content data comprise information generated in the process of creating, editing, and publishing content of all types. This category of data may include texts, images, videos, audio files, and other multimedia content published across various platforms and media. Content data are not limited to the content itself but also include metadata providing information about the content, such as tags, descriptions, authorship details, and publication dates.
- **Contract data:** Contract data are specific details pertaining to the formalisation of an agreement between two or more parties. They document the terms under which services

or products are provided, exchanged, or sold. This category of data is essential for managing and fulfilling contractual obligations and includes both the identification of the contracting parties and the specific terms and conditions of the agreement. Contract data may encompass the start and end dates of the contract, the nature of the agreed-upon services or products, pricing arrangements, payment terms, termination rights, extension options, and special conditions or clauses. They serve as the legal foundation for the relationship between the parties and are crucial for clarifying rights and duties, enforcing claims, and resolving disputes.

- **Controller:** "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Conversion tracking:** Conversion tracking is a method used to evaluate the effectiveness of marketing measures. For this purpose, a cookie is usually stored on the devices of the users within the websites on which the marketing measures take place and then called up again on the target website (e.g. we can thus trace whether the advertisements placed by us on other websites were successful).
- **Credit report:** Automated decisions are based on automatic data processing without human intervention (e.g. in the case of an automatic rejection of a purchase on account, an online credit application or an online application procedure without any human intervention). Such automated decisions are only allowed under Article 22 GDPR if data subjects consent, if they are necessary for the performance of a contract or if national laws allow such decisions.
- **Employees:** As employees, individuals are those who are engaged in an employment relationship, whether as staff, employees, or in similar positions. Employment refers to a legal relationship between an employer and an employee, established through an employment contract or agreement. It entails the obligation of the employer to pay the employee remuneration while the employee performs their work. The employment relationship encompasses various stages, including establishment, where the employment contract is concluded, execution, where the employee carries out their work activities, and termination, when the employment relationship ends, whether through termination, mutual agreement, or otherwise. Employee data encompasses all information pertaining to these individuals within the context of their employment. This

includes aspects such as personal identification details, identification numbers, salary and banking information, working hours, holiday entitlements, health data, and performance assessments.

- **Inventory data:** Inventory data encompass essential information required for the identification and management of contractual partners, user accounts, profiles, and similar assignments. These data may include, among others, personal and demographic details such as names, contact information (addresses, phone numbers, email addresses), birth dates, and specific identifiers (user IDs). Inventory data form the foundation for any formal interaction between individuals and services, facilities, or systems, by enabling unique assignment and communication.
- **Location data:** Location data is created when a mobile device (or another device with the technical requirements for a location determination) connects to a radio cell, a WLAN or similar technical means and functions of location determination. Location data serve to indicate the geographically determinable position of the earth at which the respective device is located. Location data can be used, for example, to display map functions or other information dependent on a location.
- **Log data:** Protocol data, or log data, refer to information regarding events or activities that have been logged within a system or network. These data typically include details such as timestamps, IP addresses, user actions, error messages, and other specifics about the usage or operation of a system. Protocol data is often used for analyzing system issues, monitoring security, or generating performance reports.
- **Meta, communication and process data:** Meta-, communication, and procedural data are categories that contain information about how data is processed, transmitted, and managed. Meta-data, also known as data about data, include information that describes the context, origin, and structure of other data. They can include details about file size, creation date, the author of a document, and modification histories. Communication data capture the exchange of information between users across various channels, such as email traffic, call logs, messages in social networks, and chat histories, including the involved parties, timestamps, and transmission paths. Procedural data describe the processes and operations within systems or organisations, including workflow documentations, logs of transactions and activities, and audit logs used for tracking and verifying procedures.

- **Payment Data:** Payment data comprise all information necessary for processing payment transactions between buyers and sellers. This data is crucial for e-commerce, online banking, and any other form of financial transaction. It includes details such as credit card numbers, bank account information, payment amounts, transaction dates, verification numbers, and billing information. Payment data may also contain information on payment status, chargebacks, authorizations, and fees.
- **Performance and behavioural data:** Performance and behavioral data refer to information related to how individuals perform tasks or behave within a certain context, such as in an educational, work, or social setting. This data may include metrics such as productivity, efficiency, quality of work, attendance, and adherence to policies or procedures. Behavioral data could encompass interactions with colleagues, communication styles, decision-making processes, and responses to various situations. These types of data are often used for performance evaluations, training and development purposes, and decision-making within organizations.
- **Personal Data:** "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processing:** The term "processing" covers a wide range and practically every handling of data, be it collection, evaluation, storage, transmission or erasure.
- **Profiles with user-related information:** The processing of "profiles with user-related information", or "profiles" for short, includes any kind of automated processing of personal data that consists of using these personal data to analyse, evaluate or predict certain personal aspects relating to a natural person (depending on the type of profiling, this may include different information concerning demographics, behaviour and interests, such as interaction with websites and their content, etc.) (e.g. interests in certain content or products, click behaviour on a website or location). Cookies and web beacons are often used for profiling purposes.

- **Remarketing:** Remarketing" or "retargeting" is the term used, for example, to indicate for advertising purposes which products a user is interested in on a website in order to remind the user of these products on other websites, e.g. in advertisements.
- **Server monitoring and error detection:** With the help of server monitoring and error detection, we ensure the availability and integrity of our online service and use the data processed in this process to technically optimise our online services. For this purpose, performance, utilization and comparable technical values, which provide information about the stability and any conspicuous features of our online offer, are processed. In the event of errors and irregularities, individual requests from users of our online services are recorded in order to identify and eliminate sources of problems.
- **Targeting:** "Tracking" is the term used when the behaviour of users can be traced across several websites. As a rule, behavior and interest information with regard to the websites used is stored in cookies or on the servers of the tracking technology providers (so-called profiling). This information can then be used, for example, to display advertisements to users presumably corresponding to their interests.
- **Usage data:** Usage data refer to information that captures how users interact with digital products, services, or platforms. These data encompass a wide range of information that demonstrates how users utilise applications, which features they prefer, how long they spend on specific pages, and through what paths they navigate an application. Usage data can also include the frequency of use, timestamps of activities, IP addresses, device information, and location data. They are particularly valuable for analysing user behaviour, optimising user experiences, personalising content, and improving products or services. Furthermore, usage data play a crucial role in identifying trends, preferences, and potential problem areas within digital offerings
- **Web Analytics:** Web Analytics serves the evaluation of visitor traffic of online services and can determine their behavior or interests in certain information, such as content of websites. With the help of web analytics, website owners, for example, can recognize at what time visitors visit their website and what content they are interested in. This enables them, for example, to better adapt the content of their websites to the needs of their visitors. For the purposes of web analytics , pseudonymous cookies and web beacons are often used to recognize returning visitors and thus obtain more precise analyses of the use of an online service.

