

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: 10. July 2025



Table of contents

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

- International data transfers
- General Information on Data Retention and Deletion
- Rights of Data Subjects
- Business services
- Business processes and operations
- Providers and services used in the course of business
- Provision of online services and web hosting
- Use of Cookies
- Contact and Inquiry Management
- 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
- Surveys and Questionnaires
- Web Analysis, Monitoring and Optimization
- 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
- Changes and Updates

Controller

Iscador AG
 Data protection officer
 Kirschweg 9
 4144 Arlesheim

Iscador AG
 Data protection officer

Spitalstr. 22
79539 Lörrach

E-mail address: dsb@iscador.com

Legal Notice: <https://iscador.com/en/imprint/>

Contact information of the Data Protection Officer

dsb@iscador.com

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.
- Log data.
- Performance and behavioural data.
- Working hours data.

- Salary data.

Categories of Data Subjects

- Service recipients and clients.
- Employees.
- Prospective customers.
- Communication partner.
- Users.
- Job applicants.
- Business and contractual partners.
- Participants.
- Persons depicted.
- Third parties.
- 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.
- Clicktracking.
- Affiliate Tracking.
- A/B Tests.
- Organisational and Administrative Procedures.
- Job Application Process.
- Firewall.
- Feedback.

- Heatmaps.
- Polls and Questionnaires.
- Marketing.
- Profiles with user-related information.
- Provision of our online services and usability.
- Establishment and execution of employment relationships.
- Information technology infrastructure.
- Financial and Payment Management.
- Public relations.
- Sales promotion.
- Business processes and management procedures.
- Artificial Intelligence (AI).

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.

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.

Security Precautions

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

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

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

Transmission of Personal Data

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

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.

International data transfers

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

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

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

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

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

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

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

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 has not determined an adequate level of protection (list of states:

<https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales/anerkennung-staaten.html>), we implement alternative security measures.

For data transfers to the USA, we primarily rely on the Data Privacy Framework (DPF), which has been recognized as a secure legal framework by Switzerland's adequacy decision of June 7, 2024. Additionally, we have concluded Standard Data Protection Clauses with the respective providers, which have been approved by the Federal Data Protection and Information Commissioner (FDPIC) and establish contractual obligations to protect your data.

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

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

For data transfers to other third countries, appropriate safeguards apply, including international agreements, specific guarantees, FDPIC-approved Standard Data Protection Clauses, or internal company data protection regulations previously recognized by the FDPIC or a competent data protection authority of another country.

Under Art. 16 of the Swiss DPA, 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.

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

General Information on Data Retention and Deletion

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

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

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

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

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

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

- 10 Years - Fiscal Code/Commercial Code - Retention period for books and records, annual financial statements, inventories, management reports, opening balance sheet as well as the necessary work instructions and other organisational documents (Section 147 Paragraph 1 No. 1 in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 14b Paragraph 1 of the German VAT Act (UStG), Section 257 Paragraph 1 No. 1 in conjunction with Paragraph 4 of the German Commercial Code (HGB)).

- 8 years - Accounting documents, such as invoices, booking and expense receipts (Section 147 Paragraph 1 No. 4 and 4a in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 257 Paragraph 1 No. 4 in conjunction with Paragraph 4 of the German Commercial Code (HGB))
- 6 Years - Other business documents: received commercial or business letters, copies of dispatched commercial or business letters, and other documents to the extent that they are significant for taxation purposes, for example, hourly wage slips, operating accounting sheets, calculation documents, price tags, as well as payroll accounting documents, provided they are not already accounting vouchers and cash register tapes Section (Section 147 Paragraph 1 No. 2, 3, 5 in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 257 Paragraph 1 No. 2 and 3 in conjunction with Paragraph 4 of the German Commercial Code (HGB)).
- 3 Years - Data required to consider potential warranty and compensation claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experiences and common industry practices, will be stored for the duration of the regular statutory limitation period of three years. This period begins at the end of the year in which the relevant contractual transaction took place or the contractual relationship ended in the case of ongoing contracts (Sections 195, 199 of the German Civil Code).

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.

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).
- **Data subjects:** Service recipients and clients; Prospective customers. Business and contractual partners.
- **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.
- **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).

- **Online Courses and Online Training:** We process the data of participants in our online courses and training sessions (collectively referred to as "participants") in order to be able to provide them with our course and training services. The data processed, the type, scope, purpose, and necessity of their processing are determined by the underlying contractual relationship. The data generally includes information on the courses and services utilized, as well as personal preferences and results of the participants, insofar as they are part of our service offering. Processing forms also include performance evaluation and the evaluation of our services as well as those of the course and training instructors. Additionally, depending on the equipment and structure of the respective courses or learning content, further processing operations may be implemented, such as attendance tracking for documenting participation, progress monitoring for measuring and analyzing learning progress by collecting exam and test results, and analyzing interactions on learning platforms, such as forum posts and assignment submissions; **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).

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); Log data (e.g. log files concerning logins or data retrieval or access times.); 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); Employee Data (Information about employees and other individuals in an employment relationship). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Service recipients and clients; Prospective customers; Communication partner (Recipients of e-mails, letters, etc.); Business and contractual partners; Third parties; Users (e.g. website visitors, users of

online services). Customers.

- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Business processes and management procedures; Communication; Marketing; Sales promotion. Financial and Payment Management.
- **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).
- **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).

- **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).

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); Location data (Information on the geographical position of a device or 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).

- **Data subjects:** Service recipients and clients; Prospective customers; Business and contractual partners; 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; Business processes and management procedures; Communication; Provision of our online services and usability. Marketing.
- **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:

- **WP Store Locator:** Helps customers to find nearby retailers; **Service provider:** Executed on servers and/or computers under our controllership; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Website:** <https://wpstorelocator.co>.
- **Gravity Forms:** Creation and evaluation of online forms, surveys, feedback forms as well as acceptance of payments and implementation of automated workflows; **Service provider:** Executed on servers and/or computers under our controllership; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Website:** <https://www.gravityforms.com/>.

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. Firewall.
- **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.
- **E-mail Sending and Hosting:** The web hosting services we use also include sending, receiving and storing e-mails. For these purposes, the addresses of the recipients and senders, as well as other information relating to the sending of e-mails (e.g. the providers involved) and the contents of the respective e-mails are processed. The above data may also be processed for SPAM detection purposes. Please note that e-mails on the Internet are generally not sent in encrypted form. As a rule, e-mails are encrypted during transport, but not on the servers from which they are sent and received (unless a so-called end-to-end encryption method is used). We can therefore accept no responsibility for the transmission path of e-mails between the sender and reception on our server; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

- **Wordpress.com:** Hosting and software for the creation, provision and operation of websites, blogs and other online services; **Service provider:** Aut O'Mattic A8C Ireland Ltd., Grand Canal Dock, 25 Herbert Pl, Dublin, D02 AY86, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://wordpress.com>; **Privacy Policy:** <https://automattic.com/privacy/>; **Data Processing Agreement:** <https://wordpress.com/support/data-processing-agreements/>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider).
- **Wordfence:** firewall and security and error detection functions to detect and prevent unauthorized access attempts as well as technical vulnerabilities that could enable such access. For these purposes, cookies and similar storage procedures required for this purpose may be used and security logs may be created during testing and, in particular, in the event of unauthorized access. In this context, the IP addresses of the users, a user identification number and their activities, including the time of access, are processed and stored and compared with the data provided by the provider of the firewall and security function and transmitted to the latter; **Service provider:** Defiant, Inc., 800 5th Ave Ste 4100, Seattle, WA 98104, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.wordfence.com>; **Privacy Policy:** <https://www.wordfence.com/privacy-policy/>; **Basis for third-country transfers:** EEA - Standard Contractual Clauses (<https://www.wordfence.com/standard-contractual-clauses/>), Switzerland - Standard Contractual Clauses (<https://www.wordfence.com/standard-contractual-clauses/>). **Further Information:** <https://www.wordfence.com/help/general-data-protection-regulation/>.
- **Cyon:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider:** cyon GmbH, Brunngässlein 12, CH - 4052 Basel, Switzerland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.cyon.ch>. **Privacy Policy:** <https://www.cyon.ch/legal/datenschutzerklaerung>.

Use of Cookies

The term "cookies" refers to functions that store information on users' devices and read it from them. Cookies can also be used for different purposes, such as ensuring the functionality, security, and convenience of online services, as well as analyzing visitor traffic. We use cookies in accordance with legal regulations. If necessary, we obtain users' consent in advance. If consent is not required, we rely

on our legitimate interests. This applies when storing and reading information is essential to provide explicitly requested content and functions. This includes, for example, saving settings and ensuring the functionality and security of our online services. Consent can be withdrawn at any time. We clearly inform users about the scope of the consent and which cookies are used.

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

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

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

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

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

Further information on processing methods, procedures and services used:

- **DocCheck:** DocCheck uses cookies to facilitate the use of the services. The information generated by these cookies is only transmitted to DocCheck servers and is not shared with the website operator or other third parties. Data transfer to countries outside the EU does not take place.

Cookie 1 'Doccheck_user_id'

Enables single sign-on for all DocCheck logins. Lifetime = 1 session

Cookie 2 'Doccheck_scu_data'

Serves to provide suitable content using pseudonymised identification data (e.g. occupation, country, language). Lifetime = 1 year

Log information

When using DocCheck password protection, DocCheck collects the so-called protocol data (IP address, access date, access time, referrer URL, information about used hardware and software such as browser features, device information such as resolution) of the user,

starting from the website of the information provider who integrates the login into the website via "embed" or iFrame. This data is not used to draw conclusions about the person, but serves to ensure the correct presentation of the page or iFrame contents and/or the security of the DocCheck services;

Service provider: DocCheck Community GmbH

Vogelsanger Str. 66

50823 Köln. **Privacy Policy:** <https://more.doccheck.com/de/privacy/>.

- **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).
- **BorlabsCookie:** 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:** Executed on servers and/or computers under our controllership; **Website:** <https://borlabs.io/borlabs-cookie/>. **Further Information:** An individual user

ID, language as well as types of consent and the time of their submission are stored on the server and in the cookie on the user's device.

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.); Service recipients and clients. Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Communication; Organisational and Administrative Procedures; Feedback (e.g. collecting feedback via online form); Provision of our online services and usability. Marketing.
- **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).
- **Elementor:** Creation of online forms, collection and storage of related user

entries; **Service provider:** Elementor Ltd., Tuval St 40, Ramat Gan, Israel; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://elementor.com/features/form-builder/>; **Privacy Policy:** <https://elementor.com/about/privacy/>; **Data Processing Agreement:** <https://elementor.com/terms/cloud-toc/elementor-data-processing-agreement/>; **Basis for third-country transfers:** EEA - Standard Contractual Clauses (<https://elementor.com/terms/cloud-toc/elementor-data-processing-agreement/>), Switzerland - Standard Contractual Clauses (<https://elementor.com/terms/cloud-toc/elementor-data-processing-agreement/>). **Further Information:** <https://elementor.com/trust/>.

- **Gravity Forms:** Creation and evaluation of online forms, surveys, feedback forms as well as acceptance of payments and implementation of automated workflows; **Service provider:** Executed on servers and/or computers under our controllership; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Website:** <https://www.gravityforms.com/>.

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/chatgpt/overview/>; **Privacy Policy:** <https://openai.com/privacy-policy/>. **Opt-Out:** <https://privacy.openai.com/policies?modal=select-subject>.
- **DeepL:** Translation of texts into various languages and provision of synonyms as well as context examples. Support with the correction and improvement of texts in different languages; **Service provider:** DeepL SE, Maarweg 165, 50825 Köln, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.deepl.com>; **Privacy Policy:** <https://www.deepl.com/en/privacy>. **Data Processing Agreement:** Provided by the service provider.

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), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>).
- **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/>.

- **Zoom:** Video conferences, online meetings, webinars, screen sharing, optional recording of sessions, chat function, integration with calendars and other apps; **Service provider:** Zoom Video Communications, Inc., 55 Almaden Blvd., Suite 600, San Jose, CA 95113, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://zoom.us>; **Privacy Policy:** <https://explore.zoom.us/en/privacy/>; **Data Processing Agreement:** https://explore.zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://explore.zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://explore.zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf).

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). Images and/ or video recordings (e.g. photographs or video recordings of a person).

- **Data subjects:** Prospective customers; Communication partner (Recipients of e-mails, letters, etc.). Business and contractual partners.
- **Purposes of processing:** Office and organisational procedures; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)). Provision of contractual services and fulfillment of contractual obligations.
- **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:

- **Adobe Creative Cloud:** Cloud storage, cloud infrastructure services, and cloud-based application software, among others for photo editing, video editing, graphic design, web development; **Service provider:** Adobe Systems Software Ireland, 4-6, Riverwalk Drive, Citywest Business Campus, Brownsbarn, Dublin 24, D24 DCW0, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.adobe.com/creativecloud.html>; **Privacy Policy:** <https://www.adobe.com/privacy.html>; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider).
- **Dropbox:** Cloud storage service; **Service provider:** Dropbox, Inc., 333 Brannan Street, San Francisco, California 94107, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.dropbox.com>; **Privacy Policy:** <https://www.dropbox.com/privacy>; **Data Processing Agreement:** <https://assets.dropbox.com/documents/en/legal/dfb-data-processing-agreement.pdf>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (<https://assets.dropbox.com/documents/en/legal/dfb-data-processing-agreement.pdf>), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (<https://assets.dropbox.com/documents/en/legal/dfb-data-processing-agreement.pdf>).
- **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), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>).

Newsletter and Electronic Communications

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

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

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

Contents:

Information about us, our services, promotions and offers.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Meta, communication and process data (e.g. IP addresses, timestamps,

identification numbers, involved parties). 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.).
- **Purposes of processing:** Direct marketing (e.g. by e-mail or postal).
- **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).
- **Mailchimp:** Email marketing, automation of marketing processes, collection, storage and management of contact information, measurement of campaign performance, recording and analysis of recipient interaction with content, personalisation of content; **Service provider:** Rocket Science Group, LLC, 675 Ponce De Leon Ave NE #5000, Atlanta, GA 30308, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://mailchimp.com>; **Privacy Policy:** <https://mailchimp.com/legal/>; **Data Processing Agreement:** <https://mailchimp.com/legal/data-processing-addendum/>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard

Contractual Clauses (Provided by the service provider), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider). **Further Information:** Special safety measures: <https://mailchimp.com/help/Mailchimp-european-data-transfers/>.

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).

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. Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Feedback (e.g. collecting feedback via online form); Polls and Questionnaires (e.g. surveys with input options, multiple choice questions). Direct marketing (e.g. by e-mail or postal).
- **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:

- **Mailchimp:** Email marketing, automation of marketing processes, collection, storage and management of contact information, measurement of campaign performance, recording and analysis of recipient interaction with content, personalisation of content; **Service provider:** Rocket Science Group, LLC, 675 Ponce De Leon Ave NE #5000, Atlanta, GA 30308, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://mailchimp.com>; **Privacy Policy:** <https://mailchimp.com/legal/>; **Data Processing Agreement:** <https://mailchimp.com/legal/data-processing-addendum/>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider). **Further Information:** Special safety measures: <https://mailchimp.com/help/Mailchimp-european-data-transfers/>.

- **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), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>).

Web Analysis, Monitoring and Optimization

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

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

Unless otherwise specified below, profiles (i.e., data combined from a usage process) may be created for these purposes, and information can be stored in and later retrieved from a browser or device. The data collected includes, in particular, visited websites and elements used on them, as well as technical information such as the browser used, the computer system, and information about usage times. If users have given consent to the collection of their location data to us or to the providers of the services we use, the processing of location data is also possible.

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

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

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Web Analytics (e.g. access statistics, recognition of returning visitors); Profiles with user-related information (Creating user profiles); Provision of our online services and usability; Targeting (e.g. profiling based on interests and behaviour, use of cookies); Clicktracking; A/B Tests. Heatmaps ("Heatmaps" are mouse movements of the users, which are combined to an overall picture.).
- **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/adsprocessorterms/>; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (<https://business.safety.google/adsprocessorterms>), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (<https://business.safety.google/adsprocessorterms>); **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 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), Standard Contractual Clauses (<https://business.safety.google/adsprocessorterms>), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (<https://business.safety.google/adsprocessorterms>).

- **Hotjar Observe:** Software for the analysis and optimization of online services based on pseudonymously performed measurements and analyses of user behavior, which may include in particular A/B tests (measurement of the popularity and user-friendliness of different content and functions), measurement of click paths and interaction with content and functions of the online service (as so-called heat maps and recordings); **Service provider:** Hotjar Ltd., 3 Lyons Range, 20 Bisazza Street, Sliema SLM 1640, Malta; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://www.hotjar.com>; **Privacy Policy:** <https://www.hotjar.com/legal/policies/privacy>; **Retention period:** The cookies that Hotjar uses have a different "lifetime"; some last up to 365 days, some only last during the current visit; cookie policy: <https://www.hotjar.com/legal/policies/cookie-information>. **Opt-Out:** <https://www.hotjar.com/legal/compliance/opt-out>.
- **SISTRIX:** Service for evaluating publicly available information from search engines and comparable services, such as Google, Amazon, Facebook and public websites, with the purpose of improving the findability of an online offering in search engines and generally on the Internet (so-called search engine optimisation) and also improving the user-friendliness of the online services; **Service provider:** SISTRIX GmbH, Thomas-Mann-Str. 37, 53111 Bonn, Germany; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** <https://www.sistrix.com/>; **Privacy Policy:** <https://www.sistrix.com/sistrix/datenschutz/>. **Further Information:** When evaluating the publicly available information, personal data contained in the information may also be processed (e.g. names or content). This data is not used for personal processing nor for profiling purposes, but is used solely for the technical and business analysis of the publicly available content by SYSTRIX as the data controller.

Profiles in Social Networks (Social Media)

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

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

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

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

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

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

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

Further information on processing methods, procedures and services used:

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

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

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

We have entered into a special agreement with LinkedIn Ireland ("Page Insights Joint Controller Addendum,"

<https://legal.linkedin.com/pages-joint-controller-addendum>), which specifically

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

- **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 - Data Privacy Framework (DPF). **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). Location data (Information on the geographical position of a device or person).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of our online services and usability; Web Analytics (e.g. access statistics, recognition of returning visitors); Targeting (e.g. profiling based on interests and behaviour, use of cookies); Affiliate Tracking; Marketing. Provision of contractual services and fulfillment of contractual obligations.
- **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 Maps:** We integrate the maps of the service "Google Maps" from the provider Google. The data processed may include, in particular, IP addresses and location data of users; **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 - Data Privacy Framework (DPF).
- **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 - Data Privacy Framework (DPF).

- **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), Switzerland - 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>.
- **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), Switzerland - 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>.
- **Monotype:** Provision of font files for the purpose of a user-friendly presentation of our online services; **Service provider:** Monotype Imaging Holdings Inc., 600 Unicorn Park Drive, 01801 Woburn, Massachusetts, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.monotype.com/>. **Privacy Policy:** <https://www.monotype.com/legal/privacy-policy>.

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:** Communication; Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Web Analytics (e.g. access statistics, recognition of returning visitors). 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".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Bitly:** URL shortening service and link management platform; **Service provider:** Bitly, Inc., 139 Fifth Avenue, 5th Floor, New York, NY 10010, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://bitly.com>; **Privacy Policy:** <https://bitly.com/pages/privacy>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Data Privacy Framework (DPF).
- **Trello:** Project management tool; **Service provider:** Atlassian Pty Ltd, 350 Bush Street, Floor 13, San Francisco, CA 94104, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://trello.com/>; **Privacy Policy:** <https://trello.com/privacy>; **Data Processing Agreement:** <https://www.atlassian.com/legal/data-processing-addendum>. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses

(<https://www.atlassian.com/legal/data-processing-addendum#europe-uk-switzerland>), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses
(<https://www.atlassian.com/legal/data-processing-addendum#europe-uk-switzerland>).

- **WeTransfer:** Transferring files over the Internet; **Service provider:** WeTransfer BV, Oostelijke Handelskade 751, Amsterdam, 1019 BW, Netherlands; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://wetransfer.com>. **Privacy Policy:** <https://wetransfer.com/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); 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:** 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; 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).

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).
- **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 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).
- **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:** Employee data in Switzerland is deleted when it is no longer required for the purpose for which it was collected, unless it must be retained or archived due to legal obligations or due to the interests of the employer. The following retention and archiving obligations are observed:
 - 10 years - Retention period for ledgers and records, annual accounts, inventories, management reports, opening balances, accounting vouchers, and invoices, as well as all required work instructions and other organisational documents (Art. 958f of the Swiss Code of Obligations (OR)).
 - 10 years - Data necessary for considering potential claims for damages or similar contractual claims and rights, as well as for processing associated inquiries, based on past business experiences and usual industry practices, are stored for the statutory limitation period of ten years, unless a shorter period of five years is applicable, which is relevant in certain cases (Art. 127, 130 OR). Claims expire after five years for rental, lease and capital interest payments, and other periodic services, from the supply of food, for catering and innkeeper debts, as well as from craftsmanship, retail sale of goods, medical care, professional work of lawyers, legal agents, solicitors, and notaries, and from the employment relationship of employees (Art. 128 OR).
 - 10 years - Mandatory retention period for finance-related accounting documents and corresponding business correspondence as per the Business Recordkeeping Ordinance (GeBüV), specifically pertaining to financial documents of employees (e.g., payroll, social insurance) and clients (e.g., accounts receivable management, pension contracts).

- 5 years - Mandatory retention period for employment-related documents as per Art. 73 of Ordinance 1 on the Labour Law (ArGV1), specifically for documents relating to personal details, type of employment, entry/exit, work/break/rest periods, salary supplements, and medical evaluations.
- **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).

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.

- **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).

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.