YOUR DATA, OUR RESPONSIBILITY. THE 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: 9. September 2024

Table of contents

- Relevant legal bases
- Security Precautions
- Transmission of Personal Data
- General Information on Data Retention and Deletion
- Rights of Data Subjects
- Business processes and operations
- Providers and services used in the course of business
- Payment Procedure
- Provision of online services and web hosting
- Special Notes on Applications (Apps)
- Purchase of applications via Appstores
- Registration, Login and User Account
- Single Sign-on Authentication
- Contact and Inquiry Management
- Push notifications
- Cloud Services
- Newsletter and Electronic Communications
- Sweepstakes and Contests
- Surveys and Questionnaires
- Web Analysis, Monitoring and Optimization
- Online Marketing
- Profiles in Social Networks (Social Media)
- Processing of data in the context of employment relationships
- Job Application Process
- Changes and Updates
- Terminology and Definitions

Controller

TrustNXT GmbH
Bahrenfelder Chaussee 49a

22761 Hamburg
Germany

Authorised Representatives: Ariane Scheer-Danielsson, Andreas Reich, Sebastian Adank

E-mail address: info@trustnxt.com

Legal Notice: https://trustnxt.com/legal-notice/

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.
- Event Data (Facebook).
- Log data.
- Performance and behavioural data.
- Working hours data.
- Creditworthiness Data.

- Salary data.

Special Categories of Data

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

Categories of Data Subjects

- Service recipients and clients.
- Employees.
- Prospective customers.
- Communication partner.
- Users.
- Job applicants.
- Participants in sweepstakes and competitions.
- Business and contractual partners.
- Participants.
- 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.

- Remarketing.
- Conversion tracking.
- Affiliate Tracking.
- Organisational and Administrative Procedures.
- Job Application Process.
- Conducting sweepstakes and contests.
- Feedback.
- Polls and Questionnaires.
- Marketing.
- Profiles with user-related information.
- Authentication processes.
- Provision of our online services and usability.
- Assessment of creditworthiness.
- Establishment and execution of employment relationships.
- Information technology infrastructure.
- Financial and Payment Management.
- Public relations.
- Sales promotion.
- Business processes and management procedures.

Google user data will not be transferred to third parties for any of the following reasons:

- Targeted advertising
- Selling to data brokers
- Providing to information resellers
- Determining credit-worthiness
- Lending purposes
- User advertisements
- Personalized advertisements
- Retargeted advertisements
- Interest-based advertisements

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.

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

General Information on Data Retention and Deletion

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

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

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

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

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

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

Further information on processing methods, procedures and services used:

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

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

- **Data Retention and Deletion:** The following general 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 processes and operations

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

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

Personal data may be transferred to third parties if necessary for fulfilling the mentioned purposes or legal obligations. After legal retention periods expire or when the purpose of processing no longer applies, the data will be deleted. This also includes data that must be stored for longer periods due to tax law and legal obligations to provide evidence.

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

Further information on processing methods, procedures and services used:

- **Customer Management and Customer Relationship Management (CRM):** Processes required in the context of customer management and Customer Relationship Management (CRM) include customer acquisition in compliance with data protection regulations, measures to promote customer retention and loyalty, effective customer communication, complaint management and customer service with consideration of data protection, data management and analysis to support the customer relationship, management of CRM systems, secure account management, customer segmentation and targeting; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Contact management and contact maintenance:** Processes required in the context of organizing, maintaining, and securing contact information (e.g., setting up and maintaining a central contact database,

regular updates of contact information, monitoring data integrity, implementing data protection measures, ensuring access controls, conducting backups and restorations of contact data, training employees in effective use of contact management software, regular review of communication history and adjustment of contact strategies); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Customer Account:** Customers can create an account within our online offer (e.g. customer or user account, "customer account" for short). If the registration of a customer account is required, customers will be informed of this as well as of the details required for registration. The customer accounts are not public and cannot be indexed by search engines. In the course of registration and subsequent registration and use of the customer account, we store the IP addresses of the contractual partners along with the access times, in order to be able to prove the registration and prevent any misuse of the customer account. If the customer account has been terminated, the customer account data will be deleted after the termination date, unless it is retained for purposes other than provision in the customer account or must be retained for legal reasons (e.g. internal storage of customer data, order transactions or invoices). It is the customers' responsibility to back up their data when terminating the customer Account; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **General Payment Transactions:** Procedures required for carrying out payment transactions, monitoring bank accounts, and controlling payment flows (e.g., creation and verification of transfers, processing of direct debit transactions, checking of account statements, monitoring of incoming and outgoing payments, management of chargebacks, account reconciliation, cash management); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Accounting, accounts payable, accounts receivable:** Procedures required for the collection, processing, and control of business transactions in the area of accounts payable and receivable accounting (e.g., creation and verification of incoming and outgoing invoices, monitoring and management of outstanding items, execution of payment transactions, handling of dunning processes, account reconciliation within the scope of receivables and payables, accounts payable accounting, and accounts receivable accounting); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Financial Accounting and Taxes:** Procedures required for the collection, management, and control of finance-related business transactions as well as for the calculation, reporting, and payment of taxes (e.g., accounting and posting of business transactions, preparation of quarterly and annual financial statements, execution of payment transactions, handling of dunning processes, account reconciliation, tax consulting, preparation and submission of tax returns, management of tax affairs); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Sales:** Procedures required for the planning, implementation, and control of measures for marketing and selling products or services (e.g., customer acquisition, preparation and tracking of offers, order processing, customer consultation and support, sales promotion, product training, sales controlling and

analysis, management of distribution channels); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Marketing, advertising, and sales promotion:** Processes required in the context of marketing, advertising, and sales promotion (e.g., market analysis and audience targeting, development of marketing strategies, planning and execution of advertising campaigns, design and production of advertising materials, online marketing including SEO and social media campaigns, event marketing and trade show participation, customer loyalty programs, sales promotion measures, performance measurement and optimisation of marketing activities, budget management and cost control); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Economic Analyses and Market Research:** To fulfill business management purposes and to identify market trends, desires of contractual partners, and users, the present data regarding business transactions, contracts, inquiries, etc., are analyzed. The group of affected individuals may include contractual partners, interested parties, customers, visitors, and users of the online service managed by the responsible entity. The execution of these analyses serves the purposes of business economic evaluations, marketing, and market research (e.g., to determine customer groups with different characteristics). Where available, profiles of registered users along with their information on services utilized are considered. The analyses are exclusively for the use of the responsible entity and are not disclosed externally unless they pertain to anonymous analyses with aggregated, thus anonymized values. Moreover, user privacy is accounted for; data is processed for analysis purposes in as pseudonymized a manner as possible and anonymized when feasible (e.g., as aggregated data); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Public Relations:** Processes required in the context of public relations and public relations activities (e.g., development and implementation of communication strategies, planning and execution of PR campaigns, creation and distribution of press releases, maintenance of media contacts, monitoring and analysis of media response, organisation of press conferences and public events, crisis communication, creation of content for social media and corporate websites, management of corporate branding); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

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).

- **Data subjects:** Service recipients and clients; Prospective customers; Business and contractual partners. Employees (e.g. employees, job applicants, temporary workers, and other personnel.).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures. Business processes and management procedures.
- **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:

- **DATEV:** Software for accounting, communication with tax advisors as well as authorities and including document storage; **Service provider**: DATEV eG, Paumgartnerstr. 6 – 14, 90429 Nürnberg, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.datev.de/web/de/mydatev/online-anwendungen/; **Privacy Policy:** https://www.datev.de/web/de/m/ueber-datev/datenschutz/; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** Switzerland – Adequacy decision (Germany).

Payment Procedure

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

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

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties). Contact data (e.g. postal and email addresses or phone numbers).
- **Data subjects:** Service recipients and clients; Business and contractual partners. Prospective customers.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations. Business processes and management procedures.
- **Retention and deletion:** Deletion in accordance with the information provided in the section “General Information on Data Retention and Deletion”.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Apple Pay:** Payment services provider; **Service provider**: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.apple.com/apple-pay/. **Privacy Policy:** https://www.apple.com/legal/privacy/en-ww/.
- **Google Pay:** Payment services provider; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://pay.google.com/intl/en_uk/about/; **Privacy Policy:** https://policies.google.com/privacy. **Basis for third-country transfers:** Switzerland – Adequacy decision (Ireland).
- **Mastercard:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider**: Mastercard Europe SA, Chaussée de Tervuren 198A, B-1410 Waterloo, Belgium; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.mastercard.co.uk; **Privacy Policy:** https://www.mastercard.co.uk/en-gb/vision/terms-of-use/commitment-to-privacy/privacy.html. **Basis for third-country transfers:** Switzerland – Adequacy decision (Belgium).
- **PayPal:** Payment-Service-Provider (technical integration of online-payment-methods) (e.g. PayPal, PayPal Plus, Braintree, Braintree); **Service provider**: PayPal (Europe) S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.paypal.com; **Privacy Policy:** https://www.paypal.com/de/webapps/mpp/ua/privacy-full. **Basis for third-country transfers:** Switzerland – Adequacy decision (Luxembourg).

- **Visa:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider**: Visa Europe Services Inc., Zweigniederlassung London, 1 Sheldon Square, London W2 6TT, UK; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.visa.de; **Privacy Policy:** https://www.visa.de/datenschutz. **Basis for third-country transfers:** EEA – Adequacy decision (UK), Switzerland – Adequacy decision (UK).

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

Further information on processing methods, procedures and services used:

- **Provision of online offer on rented hosting space:** For the provision of our online services, we use storage space, computing capacity and software that we rent or otherwise obtain from a corresponding server provider (also referred to as a "web hoster"); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Collection of Access Data and Log Files:** Access to our online service is logged in the form of so-called "server log files". Server log files may include the address and name of the accessed web pages and files, date and time of access, transferred data volumes, notification of successful retrieval, browser type along with version, the user's operating system, referrer URL (the previously visited page), and typically IP addresses and the requesting provider. The server log files can be used for security purposes, e.g., to

prevent server overload (especially in the case of abusive attacks, known as DDoS attacks), and to ensure server load management and stability; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Retention period:** Log file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.

- **Content-Delivery-Network:** We use a so-called "Content Delivery Network" (CDN). A CDN is a service with whose help contents of our online services, in particular large media files, such as graphics or scripts, can be delivered faster and more securely with the help of regionally distributed servers connected via the Internet; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **ALL-INKL:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider**: ALL-INKL.COM – Neue Medien Münnich, Inhaber: René Münnich, Hauptstraße 68, 02742 Friedersdorf, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://all-inkl.com/; **Privacy Policy:** https://all-inkl.com/datenschutzinformationen/; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** Switzerland – Adequacy decision (Germany).
- **Amazon Web Services (AWS):** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider**: Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, 1855, Luxembourg; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://aws.amazon.com/; **Privacy Policy:** https://aws.amazon.com/privacy/; **Data Processing Agreement:** https://aws.amazon.com/compliance/gdpr-center/. **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF), Switzerland – Adequacy decision (Luxembourg).
- **United Domains:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider**: united-domains AG, Gautinger Straße 10, 82319 Starnberg, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.united-domains.de; **Privacy Policy:** https://www.united-domains.de/unternehmen/datenschutz/; **Data Processing Agreement:** https://www.united-domains.de/help/faq-article/wie-erhalte-ich-den-auftragsverarbeitungs-vertrag-avv-nach-dsgvo. **Basis for third-country transfers:** Switzerland – Adequacy decision (Germany).
- **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), Switzerland – Adequacy decision (Ireland).
- **Amazon CloudFront:** Content-Delivery-Network (CDN) – service with whose help contents of our online services, in particular large media files, such as graphics or scripts, can be delivered faster and more securely with the help of regionally distributed servers connected via the Internet; **Service provider**:

Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, 1855, Luxembourg; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://aws.amazon.com/cloudfront/; **Privacy Policy:** https://aws.amazon.com/privacy/; **Data Processing Agreement:** https://aws.amazon.com/compliance/gdpr-center/. **Basis for third-country transfers:** EEA – Standard Contractual Clauses (Provided by the service provider), Switzerland – Adequacy decision (Luxembourg).

- **Vercel:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities) as well as development environment; **Service provider**: Vercel Inc., 340 S Lemon Ave #4133, Walnut, CA 91789, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://vercel.com; **Privacy Policy:** https://vercel.com/legal/privacy-policy; **Data Processing Agreement:** https://vercel.com/legal/dpa. **Basis for third-country transfers:** EEA – Standard Contractual Clauses (https://vercel.com/legal/dpa), Switzerland – Standard Contractual Clauses (https://vercel.com/legal/dpa).

Special Notes on Applications (Apps)

We process the data of the users of our application to the extent necessary to provide the users with the application and its functionalities, to monitor its security and to develop it further. Furthermore, we may contact users in compliance with the statutory provisions if communication is necessary for the purposes of administration or use of the application. In addition, we refer to the data protection information in this privacy policy with regard to the processing of user data.

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

Information on the functions of the application:

Camera function: To take and protect photos with the camera

Location data: To protect photos and insert location data

Access to media library: To access photos and protect them.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); 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); Payment Data (e.g. bank details, invoices, payment history); Contract data (e.g. contract object, duration, customer category); Images and/ or video recordings (e.g. photographs or video recordings of a person). Location data (Information on the geographical position of a device or person).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Security measures. Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section “General Information on Data Retention and Deletion”.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Commercial use:** We process the data of the users of our application, registered and any test users (hereinafter uniformly referred to as “users”) in order to provide them with our contractual services and on the basis of legitimate interests to ensure the security of our application and to develop it further. The required details are identified as such within the scope of the conclusion of a contract for the use of the application, the conclusion of an order, an order or a comparable contract and may include the details required for the provision of services and any invoicing as well as contact information in order to be able to hold any consultations; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).
- **Device authorizations for access to functions and data:** The use of certain functions of our application may require access to the camera and the stored recordings of the users. By default, these authorizations must be granted by the user and can be revoked at any time in the settings of the respective devices. The exact procedure for controlling app permissions may depend on the user’s device and software. Users can contact us if they require further explanation. We would like to point out that the refusal or revocation of the respective authorizations can affect the functionality of our application.
- **Accessing the camera and stored recordings:** In the course of using our application, image and/or video recordings (whereby audio recordings are also included) of the users (and of other persons captured by the recordings) are processed by accessing the camera functions or stored recordings. Access to the camera functions or stored recordings requires an authorization by the user that can be withdrawn at any time. The processing of the image and/or video recordings serves only to provide the respective functionality of our application, according to its description to the users or the typical and expectable functionality of the application.

- **Processing of location data:** Within the course of using our application, the location data collected by the device used or otherwise entered by the user are processed. The use of the location data requires an authorization of the users, which can be revoked at any time. The use of the location data serves only to provide the respective functionality of our application, according to its description to the users or its typical and expectable functionality.
- **Location history and movement profiles:** The location data is only used selectively and is not processed to create a location history or a movement profile of the devices used or of their users.

Purchase of applications via Appstores

The purchase of our apps is done via special online platforms operated by other service providers (so-called "appstores"). In this context, the data protection notices of the respective appstores apply in addition to our data protection notices. This applies in particular with regard to the methods used on the platforms for webanalytics and for interest-related marketing as well as possible costs.

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

Further information on processing methods, procedures and services used:

- **Apple App Store:** App and software distribution platform; **Service provider**: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.apple.com/app-store/. **Privacy Policy:** https://www.apple.com/privacy/privacy-policy/.

Registration, Login and User Account

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

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

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Log data (e.g. log files concerning logins or data retrieval or access times.).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Security measures; Organisational and Administrative Procedures. Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Deletion after termination.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

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

Single Sign-on Authentication

Single Sign-On" or "Single Sign-On Authentication or Logon" are procedures that allow users to log in to our online services using a user account with a provider of Single Sign-On services (e.g. a social network). The prerequisite for Single Sign-On Authentication is that users are registered with the respective Single Sign-On provider and enter the required access data in the online form provided for this purpose, or are already logged in with the Single Sign-On provider and confirm the Single Sign-On login via the button.

Authentication takes place directly with the respective single sign-on provider. Within the scope of such authentication, we receive a user ID with the information that the user is logged in with the respective single sign-on provider under this user ID and an ID that cannot be used for other purposes (so-called "user handle"). Whether we receive further data depends solely on the single sign-on procedure used, the data releases selected as part of authentication and also which data users have released in the privacy or other settings of the user account with the single sign-on provider. Depending on the single sign-on provider and the user's choice, there can be different data, usually the e-mail address and the user name. The password entered by the single sign-on provider as part of the single sign-on procedure is neither visible to us nor is it stored by us.

Users are requested to note that their data stored with us can be automatically compared with their user account with the single sign-on provider, but this is not always possible or actual. If, for example, the e-mail addresses of users change, users must change these manually in their user account with us.

We can use single sign-on authentication, provided that it has been agreed with users in the context of pre-fulfillment or fulfilment of the contract, in the context of consent processing and otherwise use it on the basis of our legitimate interests and the interests of users in an effective and secure authentication system.

Should users decide to no longer want to use the link of their user account with the Single Sign-On provider for the Single Sign-On procedure, they must remove this link within their user account with the Single Sign-On provider. If users wish to delete their data from us, they must cancel their registration with us.

- **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); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Event Data (Facebook) ("Event Data" is data that can be transmitted from us to Facebook, e.g. via Facebook pixels (via apps or other means) and relates to persons or their actions; the data includes, for example, information about visits to websites, interactions with content, functions, installations of apps, purchases of products, etc.; Event data is processed for the purpose of creating target groups for content and advertising information (Custom Audiences). Event Data does not include the actual content (such as written comments), login information, and Contact Information (such as names, email addresses, and phone

numbers). Event Data is deleted by Facebook after a maximum of two years, the Custom Audiences created from them with the deletion of our Facebook account).

- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Security measures; Authentication processes. Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Deletion after termination.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR). Consent (Article 6 (1) (a) GDPR).

Further information on processing methods, procedures and services used:

- **Apple Single-Sign-On:** Authentication services for user logins, provision of single sign-on functionalities, management of identity information and application integrations; **Service provider**: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.apple.com. **Privacy Policy:** https://www.apple.com/legal/privacy/en-ww/.
- **Facebook Single-Sign-On:** Authentication service of the platform Facebook; **Service provider**: Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.facebook.com; **Privacy Policy:** https://www.facebook.com/privacy/policy/; **Data Processing Agreement:** https://www.facebook.com/legal/terms/dataprocessing. **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF), Switzerland – Adequacy decision (Ireland).
- **Google Single-Sign-On:** Authentication services for user logins, provision of single sign-on functionalities, management of identity information and application integrations; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.google.com; **Privacy Policy:** https://policies.google.com/privacy; **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF), Switzerland – Adequacy decision (Ireland). **Opt-Out:** Settings for the Display of Advertisements: https://myadcenter.google.com/personalizationoff.
- **Instagram Single-Sign-On:** Authentication services for user logins, provision of single sign-on functionalities, management of identity information and application integrations. – We are jointly responsible (so-called "joint-controllership") with Meta Platforms Ireland Limited for the collection or receipt as part of a transmission (but not the further processing) of Event Data that Facebook collects or receives as part of a transmission for the following purposes using the Facebook single sign-on registration procedures that are implemented on our online services: a) displaying content advertising information that matches users' presumed interests; b) delivering commercial and transactional messages (e.g. b) delivering commercial and transactional messages (e.g., addressing users via Facebook Messenger); c) improving ad delivery and personalizing features and content (e.g., improving recognition of which content or

advertising information is believed to be of interest to users). We have entered into a special agreement with Facebook ("Controller Addendum", https://www.facebook.com/legal/controller_addendum), which specifically addresses the security measures that Facebook must take (https://www.facebook.com/legal/terms/data_security_terms) and in which Facebook has agreed to comply with the rights of data subjects (i.e., users can, for example, submit information access or deletion requests directly to Facebook). Note: If Facebook provides us with measurements, analyses and reports (which are aggregated, i.e. do not contain information on individual users and are anonymous to us), then this processing is not carried out within the scope of joint responsibility, but on the basis of a DPA ("Data Processing Terms", https://www.facebook.com/legal/terms/dataprocessing), the "Data Security Conditions" (https://www.facebook.com/legal/terms/data_security_terms) and, with regard to processing in the USA, on the basis of Standard Contractual Clauses ("Facebook EU Data Transfer Addendum, https://www.facebook.com/legal/EU_data_transfer_addendum). The rights of users (in particular to access to information, erasure, objection and complaint to the competent supervisory authority) are not restricted by the agreements with Facebook; **Service provider**: Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.instagram.com; **Privacy Policy:** https://privacycenter.instagram.com/policy/. **Basis for third-country transfers:** Switzerland – Adequacy decision (Ireland).

- **X Single-Sign-On:** Authentication services for user logins, provision of single sign-on functionalities, management of identity information and application integrations; **Service provider**: Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2 D02 AX07, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://x.com; **Privacy Policy:** https://x.com/privacy, (Settings: https://x.com/personalization); **Data Processing Agreement:** https://privacy.x.com/en/for-our-partners/global-dpa. **Basis for third-country transfers:** EEA – Standard Contractual Clauses (https://privacy.x.com/en/for-our-partners/global-dpa), Switzerland – Adequacy decision (Ireland).
- **TikTok:** Social network, allows the sharing of photos and videos, commenting on and favouriting posts, messaging, subscribing to accounts; **Service provider**: TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Ireland and TikTok Information Technologies UK Limited, Kaleidoscope, 4 Lindsey Street, London, United Kingdom, EC1A 9HP; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://www.tiktok.com; **Privacy Policy:** https://www.tiktok.com/de/privacy-policy. **Basis for third-country transfers:** EEA – Standard Contractual Clauses (https://ads.tiktok.com/i18n/official/policy/jurisdiction-specific-terms), Switzerland – Standard Contractual Clauses (https://ads.tiktok.com/i18n/official/policy/jurisdiction-specific-terms).

Contact and Inquiry Management

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

the extent necessary to respond to the contact requests and any requested measures.

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

Further information on processing methods, procedures and services used:

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

Push notifications

With the consent of the users, we can send the users so-called “push notifications”. These are messages that are displayed on users’ screens, devices or browsers, even if our online services are not being actively used.

In order to sign up for push messages, users must confirm that their browser or device has requested to receive push messages. This approval process is documented and stored. The storage is necessary to recognize whether users have consented to receive the push messages and to be able to prove their consent. For these purposes, a pseudonymous identifier of the browser (so-called “push token”) or the device ID of a terminal device is stored.

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

- **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:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Communication; Provision of our online services and usability. 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". Deletion after termination.
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Push messages with commercial information:** The push notifications we send may contain commercial information. The commercial push messages are processed on the basis of user consent. If the contents of the push messages are described in detail in the context of the consent to receive the commercial push messages, the descriptions are decisive for the consent of the users. In addition, our newsletters contain information about our services and us; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).

Cloud Services

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

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

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

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

- **Google Workspace:** Cloud storage, cloud infrastructure services and cloud-based application software; **Service provider**: Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://workspace.google.com/; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://cloud.google.com/terms/data-processing-addendum; **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF), Switzerland – Adequacy decision (Ireland). **Further Information:** https://cloud.google.com/privacy.

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).
- **Retention and deletion:** 3 years – Contractual claims (AT) (Data required to consider potential warranty and compensation claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experiences and common industry practices, will be stored for the duration of the regular statutory limitation period of three years (Sections 1478, 1480 of the Austrian Civil Code).). 10 years – Contractual claims (CH) (Data required to consider potential compensation claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experiences and common industry practices, will be stored for the duration of the statutory limitation period of ten years, unless a shorter period of 5 years is applicable, which is relevant in certain cases. This period begins at the end of the calendar year in which the claim arose (Articles 127 and 128 Swiss Code of Obligations (CO))).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR).
- **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).

Sweepstakes and Contests

We process the personal data of participants in We process personal data of participants in competitions, contents, raffles, prize-draws or sweepstakes (hereinafter referred to as “competitions”) only in compliance with the relevant data protection regulations and if the processing is contractually necessary for the provision, execution and handling of the competition, the participants have consented to the processing or the processing serves our legitimate interests (e.g. in the security of the competition or the protection of our interests against misuse by possible recording of IP addresses when submitting entries to the competition.

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

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

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

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

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

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

Surveys and Questionnaires

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Participants.
- **Purposes of processing:** Feedback (e.g. collecting feedback via online form). Polls and Questionnaires (e.g. surveys with input options, multiple choice questions).

- **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:

- **Google Forms:** Creation and evaluation of online forms, surveys, feedback forms, etc; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.google.de/intl/en/forms/about/; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://cloud.google.com/terms/data-processing-addendum. **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF), Switzerland – Adequacy decision (Ireland).
- **SurveyMonkey:** Realization of online surveys; **Service provider**: SurveyMonkey Inc., 1 Curiosity Way, San Mateo, California 94403, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://uk.surveymonkey.com/; **Privacy Policy:** https://de.surveymonkey.com/mp/legal/privacy/. **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF).

Web Analysis, Monitoring and Optimization

Web analysis is used to evaluate the visitor traffic on our website and may include the behaviour, interests or demographic information of users, such as age or gender, as pseudonymous values. With the help of web analysis we can e.g. recognize, at which time our online services or their functions or contents are most frequently used or requested for repeatedly, as well as which areas require optimization.

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

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

Unless otherwise stated below, profiles, that is data summarized for a usage process or user, may be created for these purposes and stored in a browser or terminal device (so-called “cookies”) or similar processes may be used for the same purpose. The information collected includes, in particular, websites visited and elements used there as well as technical information such as the browser used, the computer system used and

information on usage times. If users have consented to the collection of their location data or profiles to us or to the providers of the services we use, these may also be processed, depending on the provider.

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

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

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** 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”. Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users’ devices for a period of two years.).
- **Security measures:** IP Masking (Pseudonymization of the IP address).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Matomo (without cookies):** Matomo is a data protection friendly web analysis software, which is used without cookies and in which the recognition of returning users is carried out with the help of a so-called “digital fingerprint”, which is stored anonymously and changed every 24 hours; in the case of the “digital fingerprint”, user movements within our online services are recorded with the help of pseudonymised IP addresses in combination with user-side browser settings in such a way that conclusions about the identity of individual users are not possible. User data collected through the use of Matomo is processed only by us and is not shared with third parties; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **AppsFlyer:** AppsFlyer provides attribution and marketing analytics services that enable advertisers and developers to (i) measure and analyze the effectiveness of their marketing campaigns by understanding

which marketing campaigns contributed to the download/installation of their mobile applications or such other conversion metric (e.g. relaunch of Application); and measure and analyze certain events and actions within their Application or websites, such as in-app purchases made by End Users; AppsFlyer also helps us to identify and protect against fraudulent behavior related to our marketing campaigns; **Service provider**: AppsFlyer Inc., 100 First Street, Suite 2500, San Francisco, California 94105, USA; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://www.appsflyer.com/; **Privacy Policy:** https://www.appsflyer.com/privacy-policy/; **Data Processing Agreement:** https://www.appsflyer.com/legal/dpa/. **Basis for third-country transfers:** EEA – Standard Contractual Clauses (https://www.appsflyer.com/legal/dpa/), Switzerland – Standard Contractual Clauses (https://www.appsflyer.com/legal/dpa/).

Online Marketing

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

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

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

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

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

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

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

Notes on revocation and objection:

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

a) Europe: https://www.youronlinechoices.eu.

b) Canada: https://www.youradchoices.ca/choices.

c) USA: https://www.aboutads.info/choices.

d) Cross-regional: https://optout.aboutads.info.

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Event Data (Facebook) (“Event Data” is data that can be transmitted from us to Facebook, e.g. via Facebook pixels (via apps or other means) and relates to persons or their actions; the data includes, for example, information about visits to websites, interactions with content, functions, installations of apps, purchases of products, etc.; Event data is processed for the purpose of creating target groups for content and advertising information (Custom Audiences). Event Data does not include the actual content (such as written comments), login information, and Contact Information (such as names, email addresses, and phone numbers). Event Data is deleted by Facebook after a maximum of two years, the Custom Audiences created from them with the deletion of our Facebook account).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Web Analytics (e.g. access statistics, recognition of returning visitors); Targeting (e.g. profiling based on interests and behaviour, use of cookies); Affiliate Tracking; Marketing; Profiles with user-related information (Creating user profiles); Conversion tracking (Measurement of the effectiveness of marketing activities); Provision of our online services and usability. Remarketing.
- **Retention and deletion:** Deletion in accordance with the information provided in the section “General Information on Data Retention and Deletion”. Storage of cookies for up to 2 years (Unless otherwise

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

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

Further information on processing methods, procedures and services used:

- **Facebook Ads:** Placement of ads within the Facebook platform and analysis of ad results; **Service provider**: Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://www.facebook.com; **Privacy Policy:** https://www.facebook.com/privacy/policy/; **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF), Switzerland – Adequacy decision (Ireland); **Opt-Out:** We refer to the privacy and advertising settings in the users' profiles on the Facebook platforms, as well as to Facebook's consent procedures and contact options for exercising access and other data subject rights, as described in Facebook's privacy policy. **Further Information:** User event data, i.e. behavioral and interest data, is processed for the purposes of targeted advertising and audience building on the basis of the joint controllership agreement ("Controller Addendum", https://www.facebook.com/legal/controller_addendum). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).
- **Instagram Ads:** Placement of ads within the Instagram platform and analysis of ad results; **Service provider**: Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://www.instagram.com; **Privacy Policy:** https://privacycenter.instagram.com/policy/; **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF), Switzerland – Adequacy decision (Ireland); **Opt-Out:** We refer to the data protection and advertising settings in the user's profile on the Instagram platform as well as Instagram's consent procedure and Instagram's contact options for exercising information and other data subject rights in Instagram's privacy policy. **Further Information:** User event data, i.e. behavioral and interest data, is processed for the purposes of targeted advertising and audience building on the basis of the joint controllership agreement ("Controller Addendum", https://www.facebook.com/legal/controller_addendum). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).
- **Tiktok Ads:** Placement of ads within the Tiktok platform and analysis of ad results – We and TikTok are jointly responsible for the collection and transmission of event data as well as for the measurement and creation of insights reports (statistics) for profile holders. This event data includes information about the

types of content users view or interact with, actions they take, and information about the devices used by users (e.g., IP addresses, operating system, browser type, language settings, cookie data) and details from user profiles such as country or location. Data protection information regarding the processing of user data by TikTok can be found in TikTok's privacy notices: https://www.tiktok.com/legal/page/eea/privacy-policy/en. We have entered into a special agreement on joint responsibility with TikTok, which specifically regulates the security measures that TikTok must observe and in which TikTok has agreed to fulfill data subject rights (i.e., users can, for example, direct inquiries or deletion requests directly to TikTok). The rights of users (in particular the right to access, deletion, objection, and complaint to a competent supervisory authority) are not restricted by the agreements with TikTok. The agreement on joint responsibility can be found in TikTok's "Jurisdiction Specific Terms": https://ads.tiktok.com/i18n/official/policy/jurisdiction-specific-terms.
Furthermore, TikTok acts as our processor in contact matching, developer tool functionality, use of the Custom Audiences product—i.e., creating target audiences and collecting data from interested parties within advertising campaigns ("Lead Generation"). Otherwise, TikTok acts independently as a third party. The contract on commissioned processing can be found in TikTok's "Jurisdiction Specific Terms": https://ads.tiktok.com/i18n/official/policy/jurisdiction-specific-terms; **Service provider**: TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Ireland and TikTok Information Technologies UK Limited, Kaleidoscope, 4 Lindsey Street, London, United Kingdom, EC1A 9HP; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://ads.tiktok.com/; **Privacy Policy:** https://www.tiktok.com/legal/page/eea/privacy-policy/en; **Data Processing Agreement:** https://ads.tiktok.com/i18n/official/policy/jurisdiction-specific-terms. **Basis for third-country transfers:** EEA – Standard Contractual Clauses (https://ads.tiktok.com/i18n/official/policy/jurisdiction-specific-terms), Switzerland – Standard Contractual Clauses (https://ads.tiktok.com/i18n/official/policy/jurisdiction-specific-terms).

Profiles in Social Networks (Social Media)

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

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

In addition, user data is usually processed within social networks for market research and advertising purposes. For example, user profiles can be created on the basis of user behaviour and the associated interests of users. The user profiles can then be used, for example, to place advertisements within and outside the networks which are presumed to correspond to the interests of the users. For these purposes, cookies are usually stored on the user's computer, in which the user's usage behaviour and interests are stored.

Furthermore, data can be stored in the user profiles independently of the devices used by the users (especially if the users are members of the respective networks or will become members later on).

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

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

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

Further information on processing methods, procedures and services used:

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

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

- **LinkedIn:** Social network – We are jointly responsible with LinkedIn Ireland Unlimited Company for the collection (but not the further processing) of data from visitors for the purposes of creating „Page-Insights” (statistics) for our LinkedIn profiles. This data includes information about the types of content that users view or interact with, or the actions they take, as well as information about the devices used by the users (e.g., IP addresses, operating system, browser type, language settings, cookie data) and details from the users’ profiles, such as job function, country, industry, seniority, company size, and employment status. Privacy information regarding the processing of user data by LinkedIn can be found in LinkedIn’s privacy notices: https://www.linkedin.com/legal/privacy-policy
  We have concluded a special agreement with LinkedIn Irland, the ‘Page Insights Joint Controller Addendum (the ‘Addendum’)’ (https://legal.linkedin.com/pages-joint-controller-addendum), which specifically regulates the security measures that LinkedIn must observe and wherein LinkedIn has agreed to fulfill the rights of the affected parties (i.e., users can, for example, direct requests for information or deletion directly to LinkedIn). The rights of the users (in particular to access to information, erasure, objection, and complaint to the competent supervisory authority) are not restricted by the agreements with LinkedIn. The joint responsibility is limited to the collection of data by and transmission to Ireland Unlimited Company, a company based in the EU. The further processing of the data is the sole responsibility of Ireland Unlimited Company, particularly regarding the transmission of data to the parent company LinkedIn Corporation in the USA; **Service provider**: LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.linkedin.com; **Privacy Policy:** https://www.linkedin.com/legal/privacy-policy; **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF), Switzerland – Adequacy decision (Ireland). **Opt-Out:** https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out.

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

Processing of data in the context of employment relationships

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

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

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

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

- **Processed data types:** Employee Data (Information about employees and other individuals in an employment relationship); Payment Data (e.g. bank details, invoices, payment history); Contract data (e.g. contract object, duration, customer category); Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Social data (Data subject to a special social confidentiality obligation and processed, for example, by social insurance institutions, social welfare institutions or pension authorities.); Log data (e.g. log files concerning logins or data retrieval or access times.); Performance and behavioural data (For example, performance and behavioural data aspects such as performance evaluations, feedback from supervisors, training attendance, compliance with company policies, self-assessments, and behavioural assessments.); Working hours data (e.g. start of work time, end of work time, actual working hours, target working hours, break times, overtime, vacation days, special leave days, sick days, absences, home office days, business trips); Salary data (e.g. basic salary, bonus payments, premiums, tax class information, surcharges for night work/overtime, tax deductions, social security contributions, net payout amount); Images and/ or video recordings (e.g. photographs or video recordings of a person); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Special categories of personal data:** Health Data; Religious or philosophical beliefs. Trade union membership.
- **Data subjects:** Employees (e.g. employees, job applicants, temporary workers, and other personnel.).
- **Purposes of processing:** Establishment and execution of employment relationships (Processing of employee data in the context of the establishment and execution of employment relationships); Business processes and management procedures; Provision of contractual services and fulfillment of contractual obligations; Public relations; Security measures. Office and organisational procedures.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Compliance with a legal obligation (Article 6 (1) (c) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR); Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR). Consent (Article 6 (1) (a) GDPR).

Further information on processing methods, procedures and services used:

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

the human resources department; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Authorization Management:** Procedures required for the definition, management, and control of access rights and user roles within a system or an organisation (e.g., creation of authorisation profiles, role- and access-based control, review and approval of access requests, regular review of access rights, tracking and auditing of user activities, creation of security policies and procedures); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Special categories of personal data:** Special categories of personal data are processed in the context of employment relationships or to fulfil legal obligations. The processed special categories of personal data include information concerning the health, trade union membership, or religious affiliation of employees. This data may be transferred to health insurance companies or processed for assessing the employees' work capacity, for corporate health management, or for declarations to the tax authorities; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Sources of Processed Data:** Personal data received during the application process and/or employment relationship will be processed. Furthermore, where required by law, personal data will be collected from other sources. These may include financial authorities for tax-related information, the respective health insurance company for information on work incapacity, third parties such as employment agencies, or publicly accessible sources like professional social networks in the context of application procedures; **Legal Basis:** Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Purposes of Data Processing:** The personal data of employees are primarily processed for the establishment, execution, and termination of the employment relationship. Furthermore, the processing of this data is necessary to fulfil legal obligations in the field of tax and social security law. In addition to these primary purposes, the data of employees are also used to meet regulatory and supervisory requirements, to optimise processes of electronic data processing, and to compile company-internal or cross-company data, possibly including statistical data. Moreover, the data of employees may be processed for the assertion of legal claims and defense in legal disputes; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Transmission of Employee Data to Third Countries:** The transfer of employee data to third countries, meaning countries outside the European Union (EU) and the European Economic Area (EEA), occurs only if it is necessary for the fulfilment of the employment relationship, legally required, or if employees have given their consent. Employees will be informed about the details separately, as far as legally required; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Transmission of Employee Data:** The data of employees is processed internally only by those departments that require it to fulfil operational, contractual, and legal obligations. The transfer of data to

external recipients only occurs if it is legally required, or if the affected employees have given their consent. Possible scenarios for this can include requests for information from authorities or in the case of asset formation benefits. Furthermore, the controller may transfer personal data to further recipients as far as this is necessary for fulfilling his contractual and legal obligations as an employer. These recipients can include: a) banks b) health insurance companies, pension insurance institutions, providers of old-age provisions and other social insurance carriers c) authorities, courts (e.g., tax authorities, labour courts, further supervisory authorities within the framework of fulfilling reporting and information obligations) d) tax and legal advisors e) third-party debtors in the case of wage and salary garnishments f) other entities to which legally obligatory declarations must be made.
In addition, data can be transferred to third parties if this is necessary for communication with business partners, suppliers or other service providers. Examples include details in the sender area of emails or letterheads as well as creating profiles on external platforms; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

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

  - General personnel records – General personnel records (such as employment contracts, references, supplementary agreements) are retained for up to three years after the termination of the employment relationship (§ 195 German Civil Code (BGB)).
    Tax-relevant documents – Tax-relevant documents in the personnel file are kept for six years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
    Information on wages and working hours – Information on wages and working hours for (accident) insured with wage proof are kept for five years (§ 165 I 1, IV 2 Social Code Book VII (SGB VII)).

- Payrolls including lists for special payments – Payrolls including lists for special payments, if a booking receipt is available, are kept for ten years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
- Wage lists for interim, final, and special payments – Wage lists for interim, final, and special payments are kept for six years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
- Documents on employee insurance – Documents on employee insurance, if booking receipts are available, are kept for ten years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
- Contribution statements to social security institutions – Contribution statements to social security institutions are kept for ten years (§ 165 Social Code Book VII (SGB VII)).
  Wage accounts – Wage accounts are kept for six years (§ 41 I 9 Income Tax Act (EStG)).
- Applicant data – Kept for a maximum of six months from the receipt of rejection.
- Working time records (for more than 8 hours on workdays) – Kept for two years (§ 16 II Working Time Act (ArbZG)).
- Application documents (following online job advertisement) – Kept for three to a maximum of six months from the receipt of rejection (§ 26 Federal Data Protection Act (BDSG) n.F., § 15 IV General Act on Equal Treatment (AGG)).
- Certificates of incapacity for work (AU) – Kept for up to five years (§ 6 I Act on the Compensation of Expenses (AAG)).
- Documents on company pension schemes – Kept for 30 years (§ 18a Act to Improve Occupational Pensions (BetrAVG)).
- Sickness data of employees – Kept for twelve months from the start of the illness, if the absence in a year does not exceed six weeks.
- Documents on maternity protection – Kept for two years (§ 27 para. 5 Maternity Protection Act (MuSchG)).

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 file management:** Procedures required for the organisation, updating, and management of employee data and records (e.g., recording of basic personnel data, retention of employment contracts, certificates and attestations, updating data upon changes, compilation of documents for employee discussions, archiving of personnel files, compliance with data protection regulations); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).
- **Personnel development, performance evaluation, and staff appraisals:** Procedures required in the area of employee promotion and development, as well as in assessing their performance and during employee discussions (e.g., needs analysis for further training, planning and implementation of training measures,

creation of performance evaluations, conducting goal-setting and feedback discussions, career planning and talent management, succession planning); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).

- **Obligation to Provide Data:** The person in charge informs the employees that the provision of their data is required. This is generally the case when the data are necessary for the establishment and execution of the employment relationship, or when their collection is mandated by law. The provision of data may also be required when employees assert claims or are entitled to claims. The implementation of these measures or fulfilment of services depends on the provision of such data (for example, providing data for the receipt of wages); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Publication and Disclosure of Employee Data:** The data of employees will only be published or disclosed to third parties if it is necessary for the performance of work tasks according to the employment contract. This applies, for example, when employees are named as contact persons in correspondences, on the website, or in public registers following an agreement or specified job description, or if their field of work includes representative functions. Similarly, this may occur if representation or communication with the public takes place as part of performing these tasks, such as image recordings during public relations activities. Otherwise, employee data is published only with their consent or based on the legitimate interests of the employer, for example, in the case of stage or group photographs taken during a public event; **Legal Basis:** Consent (Article 6 (1) (a) GDPR), Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Job Application Process

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

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

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

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

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

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

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

Further information on processing methods, procedures and services used:

- **LinkedIn:** Social network – We are jointly responsible with LinkedIn Ireland Unlimited Company for the collection (but not the further processing) of data from visitors for the purposes of creating „Page-Insights" (statistics) for our LinkedIn profiles. This data includes information about the types of content that users view or interact with, or the actions they take, as well as information about the devices used by the users (e.g., IP addresses, operating system, browser type, language settings, cookie data) and details from the users' profiles, such as job function, country, industry, seniority, company size, and employment status. Privacy information regarding the processing of user data by LinkedIn can be found in LinkedIn's privacy notices: https://www.linkedin.com/legal/privacy-policy
  We have concluded a special agreement with LinkedIn Irland, the 'Page Insights Joint Controller Addendum (the 'Addendum')' (https://legal.linkedin.com/pages-joint-controller-addendum), which specifically regulates the security measures that LinkedIn must observe and wherein LinkedIn has agreed to fulfill the rights of the affected parties (i.e., users can, for example, direct requests for information or deletion directly to LinkedIn). The rights of the users (in particular to access to information, erasure, objection, and complaint to the competent supervisory authority) are not restricted by the agreements with LinkedIn. The joint responsibility is limited to the collection of data by and transmission to Ireland Unlimited Company, a company based in the EU. The further processing of the data is the sole responsibility of Ireland Unlimited Company, particularly regarding the transmission of data to the parent company LinkedIn Corporation in the USA; **Service provider**: LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.linkedin.com; **Privacy Policy:** https://www.linkedin.com/legal/privacy-policy; **Basis for third-country transfers:** EEA – Data Privacy Framework (DPF), Switzerland – Adequacy decision (Ireland). **Opt-Out:** https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out.

Changes and Updates

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

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

Terminology and Definitions

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

- **Affiliate Tracking:** Custom Audiences refers to the process of determining target groups for advertising purposes, e.g. the display of advertisements. For example, a user's interest in certain products or topics on the Internet may be used to conclude that the user is interested in advertisements for similar products or the online store in which the user viewed the products. "Lookalike Audiences" is the term used to describe content that is viewed as suitable by users whose profiles or interests presumably correspond to the users for whom the profiles were created. For the purposes of creating custom audiences and lookalike audiences, cookies and web beacons are typically used.
- **Contact data:** Contact details are essential information that enables communication with individuals or organizations. They include, among others, phone numbers, postal addresses, and email addresses, as well as means of communication like social media handles and instant messaging identifiers.
- **Content data:** Content data comprise information generated in the process of creating, editing, and publishing content of all types. This category of data may include texts, images, videos, audio files, and other multimedia content published across various platforms and media. Content data are not limited to the content itself but also include metadata providing information about the content, such as tags, descriptions, authorship details, and publication dates.
- **Contract data:** Contract data are specific details pertaining to the formalisation of an agreement between two or more parties. They document the terms under which services or products are provided, exchanged, or sold. This category of data is essential for managing and fulfilling contractual obligations and includes both the identification of the contracting parties and the specific terms and conditions of the agreement. Contract data may encompass the start and end dates of the contract, the nature of the agreed-upon services or products, pricing arrangements, payment terms, termination rights, extension options, and special conditions or clauses. They serve as the legal foundation for the relationship between the parties and are crucial for clarifying rights and duties, enforcing claims, and resolving disputes.
- **Controller:** "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Conversion tracking:** Conversion tracking is a method used to evaluate the effectiveness of marketing measures. For this purpose, a cookie is usually stored on the devices of the users within the websites on which the marketing measures take place and then called up again on the target website (e.g. we can thus trace whether the advertisements placed by us on other websites were successful).
- **Employees:** As employees, individuals are those who are engaged in an employment relationship, whether as staff, employees, or in similar positions. Employment refers to a legal relationship between an employer and an employee, established through an employment contract or agreement. It entails the obligation of the employer to pay the employee remuneration while the employee performs their work. The employment relationship encompasses various stages, including establishment, where the employment contract is concluded, execution, where the employee carries out their work activities, and termination, when the employment relationship ends, whether through termination, mutual agreement, or otherwise. Employee data encompasses all information pertaining to these individuals within the context of their employment.

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

- **Inventory data:** Inventory data encompass essential information required for the identification and management of contractual partners, user accounts, profiles, and similar assignments. These data may include, among others, personal and demographic details such as names, contact information (addresses, phone numbers, email addresses), birth dates, and specific identifiers (user IDs). Inventory data form the foundation for any formal interaction between individuals and services, facilities, or systems, by enabling unique assignment and communication.
- **Location data:** Location data is created when a mobile device (or another device with the technical requirements for a location determination) connects to a radio cell, a WLAN or similar technical means and functions of location determination. Location data serve to indicate the geographically determinable position of the earth at which the respective device is located. Location data can be used, for example, to display map functions or other information dependent on a location.
- **Log data:** Protocol data, or log data, refer to information regarding events or activities that have been logged within a system or network. These data typically include details such as timestamps, IP addresses, user actions, error messages, and other specifics about the usage or operation of a system. Protocol data is often used for analyzing system issues, monitoring security, or generating performance reports.
- **Meta, communication and process data:** Meta-, communication, and procedural data are categories that contain information about how data is processed, transmitted, and managed. Meta-data, also known as data about data, include information that describes the context, origin, and structure of other data. They can include details about file size, creation date, the author of a document, and modification histories. Communication data capture the exchange of information between users across various channels, such as email traffic, call logs, messages in social networks, and chat histories, including the involved parties, timestamps, and transmission paths. Procedural data describe the processes and operations within systems or organisations, including workflow documentations, logs of transactions and activities, and audit logs used for tracking and verifying procedures.
- **Payment Data:** Payment data comprise all information necessary for processing payment transactions between buyers and sellers. This data is crucial for e-commerce, online banking, and any other form of financial transaction. It includes details such as credit card numbers, bank account information, payment amounts, transaction dates, verification numbers, and billing information. Payment data may also contain information on payment status, chargebacks, authorizations, and fees.
- **Performance and behavioural data:**
  Performance and behavioral data refer to information related to how individuals perform tasks or behave within a certain context, such as in an educational, work, or social setting. This data may include metrics such as productivity, efficiency, quality of work, attendance, and adherence to policies or procedures. Behavioral data could encompass interactions with colleagues, communication styles, decision-making processes, and responses to various situations. These types of data are often used for performance evaluations, training and development purposes, and decision-making within organizations.

- **Personal Data:** “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processing:** The term “processing” covers a wide range and practically every handling of data, be it collection, evaluation, storage, transmission or erasure.
- **Profiles with user-related information:** The processing of “profiles with user-related information”, or “profiles” for short, includes any kind of automated processing of personal data that consists of using these personal data to analyse, evaluate or predict certain personal aspects relating to a natural person (depending on the type of profiling, this may include different information concerning demographics, behaviour and interests, such as interaction with websites and their content, etc.) (e.g. interests in certain content or products, click behaviour on a website or location). Cookies and web beacons are often used for profiling purposes.
- **Remarketing:** Remarketing” or “retargeting” is the term used, for example, to indicate for advertising purposes which products a user is interested in on a website in order to remind the user of these products on other websites, e.g. in advertisements.
- **Targeting:** “Tracking” is the term used when the behaviour of users can be traced across several websites. As a rule, behavior and interest information with regard to the websites used is stored in cookies or on the servers of the tracking technology providers (so-called profiling). This information can then be used, for example, to display advertisements to users presumably corresponding to their interests.
- **Usage data:** Usage data refer to information that captures how users interact with digital products, services, or platforms. These data encompass a wide range of information that demonstrates how users utilise applications, which features they prefer, how long they spend on specific pages, and through what paths they navigate an application. Usage data can also include the frequency of use, timestamps of activities, IP addresses, device information, and location data. They are particularly valuable for analysing user behaviour, optimising user experiences, personalising content, and improving products or services. Furthermore, usage data play a crucial role in identifying trends, preferences, and potential problem areas within digital offerings
- **Web Analytics:** Web Analytics serves the evaluation of visitor traffic of online services and can determine their behavior or interests in certain information, such as content of websites. With the help of web analytics, website owners, for example, can recognize at what time visitors visit their website and what content they are interested in. This enables them, for example, to better adapt the content of their websites to the needs of their visitors. For the purposes of web analytics , pseudonymous cookies and web beacons are often used to recognize returning visitors and thus obtain more precise analyses of the use of an online service.