Privacy Policy

Preamble

Rico Brunner AG is committed to protecting your personal data and treats your personal data confidentially.

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").

Last Update: 16. February 2024

Table of contents

- International data transfers
- Erasure of data
- Rights of Data Subjects
- Use of Cookies
- Business services
- Payment Procedure
- Provision of online services and web hosting
- Blogs and publication media
- Contact and Inquiry Management
- Communication via Messenger
- Video Conferences, Online Meetings, Webinars and Screen-Sharing
- Job Application Process
- Cloud Services
- Newsletter and Electronic Communications
- Web Analysis, Monitoring and Optimization
- Online Marketing
- Customer Reviews and Ratings
- Profiles in Social Networks (Social Media)
- Plugins and embedded functions and content
- Management, Organization and Utilities
- Changes and Updates to the Privacy Policy
- Terminology and Definitions

Controller

Rico Brunner AG
Zürcher Straße 170
CH- 9014 St. Gallen
Switzerland

E-mail address: info@rico-brunner.com Phone: 0041 (0)71 220 90 64

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.
- Payment Data.
- Contact data.
- Content data.
- Contract data.
- Usage data.
- Meta, communication and process data.
- Job applicant details.
- Event Data (Facebook).

Special Categories of Data

- Health Data.
- Data related to sexual preferences, sex life, and/or sexual orientation.
- Religious or philosophical beliefs.
- Data revealing racial or ethnic origin.

Categories of Data Subjects

- Customers.
- Employees.
- Prospective customers.
- Communication partner.
- Users.
- Job applicants.
- Business and contractual partners.
- Persons depicted.

Purposes of Processing

- Provision of contractual services and fulfillment of contractual obligations.
- Contact requests and communication.
- Security measures.
- Direct marketing.
- Web Analytics.
- Targeting.
- Office and organisational procedures.
- Conversion tracking.
- Affiliate Tracking.
- A/B Tests.
- Managing and responding to inquiries.
- Job Application Process.
- Content Delivery Network (CDN).
- Firewall.
- Feedback.
- Marketing.
- Profiles with user-related information.
- Provision of our online services and usability.
- Information technology infrastructure.

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)** - Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
- **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.

Relevant legal basis according to the Swiss Data Protection Act: If you are located in Switzerland, we process your data based on the Federal Data Protection Act (abbreviated as "Swiss DPA"). This also applies if our processing of your data otherwise affects you in Switzerland and you are affected by the processing. The Swiss DPA does not generally provide that a legal basis for the processing of personal data must be stated (unlike, for example, the GDPR). We process personal data only when the processing is lawful, is conducted in good faith, and is proportionate (Article 6 (1) and (2) of the Swiss DPA). Furthermore, we only collect personal data for a specific purpose that is recognisable to the person concerned and process it only in a manner that is compatible with these purposes (Article 6 (3) of the Swiss DPA).

Reference to the applicability of the GDPR and the Swiss DPA: These privacy notices serve both to provide information in accordance with the Swiss Federal Act on Data Protection (Swiss DPA) and the General Data Protection Regulation

(GDPR).

Security Precautions

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

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

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

TLS/SSL encryption (https): To protect the data of users transmitted via our online services, we use TLS/SSL encryption. Secure Sockets Layer (SSL) is the standard technology for securing internet connections by encrypting the data transmitted between a website or app and a browser (or between two servers). Transport Layer Security (TLS) is an updated and more secure version of SSL. Hyper Text Transfer Protocol Secure (HTTPS) is displayed in the URL when a website is secured by an SSL/TLS certificate.

Transmission of Personal Data

In the context of our processing of personal data, it may happen that the data is transferred to other places, companies or persons or that it is disclosed to them. Recipients of this data may include, for example, service providers commissioned with IT tasks or providers of services and content that are embedded in a website. In such cases, the legal requirements will be respected and in particular corresponding contracts or agreements, which serve the protection of your data,

will be concluded with the recipients of your data.

International data transfers

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

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

Disclosure of Personal Data Abroad: In accordance with the Swiss Data Protection Act (DSG), we only disclose personal data abroad when an appropriate level of protection for the affected persons is ensured (Art. 16 Swiss DSG). If the Federal Council does not determine that there is an adequate level of protection (list of states: https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales/anerkennung-staaten.html), we implement alternative security measures. These measures may include international agreements, specific guarantees, data protection clauses in contracts, standard data protection clauses approved by the Federal Data Protection and Information Commissioner (FDPIC), or internal company data protection regulations previously recognised by the FDPIC or a competent data protection authority of another country.

Under Art. 16 of the Swiss DSG, exceptions can be made for the disclosure of data

abroad if certain conditions are met, including the consent of the affected person, contract execution, public interest, protection of life or physical integrity, publicly made data or data from a legally provided register. Such disclosures always comply with the legal requirements.

Erasure of data

The data processed by us will be erased in accordance with the statutory provisions as soon as their processing is revoked or other permissions no longer apply (e.g. if the purpose of processing this data no longer applies or they are not required for the purpose). If the data is not deleted because they are required for other and legally permissible purposes, their processing is limited to these purposes. This means that the data will be restricted and not processed for other purposes. This applies, for example, to data that must be stored for commercial or tax reasons or for which storage is necessary to assert, exercise or defend legal claims or to protect the rights of another natural or legal person. In the context of our information on data processing, we may provide users with further information on the deletion and retention of data that is specific to the respective processing operation.

Deletion of e-mail addresses: Your e-mail address will be stored for a period of ten years after the termination of the contractual relationship on the basis of our business interests in order to be able to check whether there is a repeated registration.

Deletion of audio files: Audio recordings with analyses by Rico Brunner are deleted after one year from their recording, unless the recordings are still required within the scope of a customer relationship.

Deletion of information within the scope of test offers : Personal and accessibility data provided by interested parties within the scope of the use of test offers will be stored for ten years and then automatically deleted. The storage allows us to ensure that the interested parties can make use of a free test offer once and that they can continue the treatment carried out within the framework of the test offer after the test period and an experience period have expired. This data is only processed in the context of a subsequent treatment request.

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.

Use of Cookies

Cookies are small text files or other data records that store information on end devices and read information from the end devices. For example, to store the login status in a user account, the contents of a shopping cart in an e-shop, the contents accessed or the functions used. Cookies can also be used for various purposes, e.g. for purposes of functionality, security and convenience of online offers as well as the creation of analyses of visitor flows.

Information on consent: We use cookies in accordance with the statutory provisions. Therefore, we obtain prior consent from users, except when it is not required by law. In particular, consent is not required if the storage and reading of information, including cookies, is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. Essential cookies usually include cookies with functions related to the display and operability of the onlineservice, load balancing, security, storage of users' preferences and choices or similar purposes related to the provision of the main and secondary functions of the onlineservice requested by users. The revocable consent will be clearly communicated to the user and will contain the information on the respective cookie use.

Information on legal bases under data protection law: The legal basis under data protection law on which we process users' personal data with the use of cookies depends on whether we ask users for consent. If users consent, the legal basis for processing their data is their declared consent. Otherwise, the data processed with the help of cookies is processed on the basis of our legitimate interests (e.g. in a business operation of our online services and improvement of its usability) or, if this is done in the context of the fulfillment of our contractual obligations, if the use of cookies is necessary to fulfill our contractual obligations. For which purposes the cookies are processed by us, we do clarify in the course of this privacy policy or in the context of our consent and processing procedures.

Retention period: With regard to the retention period, a distinction is drawn

between the following types of cookies:

- **Temporary cookies (also known as "session cookies"):** Temporary cookies are deleted at the latest after a user has left an online service and closed his or her end device (i.e. browser or mobile application).
- **Permanent cookies**: Permanent cookies remain stored even after the terminal device is closed. For example, the login status can be saved, or preferred content can be displayed directly when the user visits a website again. Likewise, user data collected with the help of cookies can be used for reach measurement. Unless we provide users with explicit information about the type and storage duration of cookies (e.g., as part of obtaining consent), users should assume that cookies are permanent and that the storage period can be up to two years.

General notes on revocation and objection (so-called "Opt-Out"): Users can revoke the consents they have given at any time and object to the processing in accordance with legal requirements. Users can restrict the use of cookies in their browser settings, among other options (although this may also limit the functionality of our online offering). A objection to the use of cookies for online marketing purposes can also be made through the websites https://optout.aboutads.info and https://www.youronlinechoices.com/.

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

Further information on processing methods, procedures and services used:

- **Processing Cookie Data on the Basis of Consent:** We use a cookie management solution in which users' consent to the use of cookies, or the procedures and providers mentioned in the cookie management solution, can be obtained, managed and revoked by the users. The declaration of consent is stored so that it does not have to be retrieved again and the consent can be proven in accordance with the legal obligation. Storage can take place server-sided and/or in a cookie (so-called opt-out cookie or with the aid of comparable technologies) in order to be able to assign the consent to a user or and/or his/her device. Subject to individual details of the providers of cookie management services, the following information applies: The duration of the storage of the consent can be up to two years. In this case, a pseudonymous user identifier is formed and stored with the date/time of consent, information on the scope of the consent (e.g. which categories of cookies and/or service providers) as well as the browser, system and used end device; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).

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

Business services

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

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

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

We delete the data after expiry of statutory warranty and comparable obligations, i.e. in principle after expiry of 4 years, unless the data is stored in a customer

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

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

- **Processed data types:** Inventory data (e.g. names, addresses); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. e-mail, telephone numbers); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Special categories of personal data:** Health Data; Data related to sexual preferences, sex life, and/or sexual orientation; Religious or philosophical beliefs. Data revealing racial or ethnic origin.
- **Data subjects:** Customers; Prospective customers. Business and contractual partners.
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations; Security measures; Contact requests and communication; Office and organisational procedures. Managing and responding to inquiries.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Compliance with a legal obligation (Article 6 (1) (c) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- We process the data of our clients in the context of our contractual services which include counselling, treatment, workshops and lectures, sale of books and audiovisual content.
- **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).

- **Online shop, order forms, e-commerce and delivery.:** We process the data of our customers in order to enable them to select, purchase or order the selected products, goods and related services, as well as their payment and delivery, or performance of other services. If necessary for the execution of an order, we use service providers, in particular postal, freight and shipping companies, in order to carry out the delivery or execution to our customers. For the processing of payment transactions we use the services of banks and payment service providers. The required details are identified as such in the course of the ordering or comparable purchasing process and include the details required for delivery, or other way of making the product available and invoicing as well as contact information in order to be able to hold any consultation; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).
- **Coaching:** We process the data of our clients and interested parties and other clients or contractual partners (uniformly referred to as "clients") in order to provide them with our services. The data processed, the type, scope and purpose of their processing and the necessity of their processing are determined by the underlying contractual and client relationship.

  Within the scope of our services, we may also process special categories of data, here in particular information on the health of clients, possibly with reference to their sexual life or sexual orientation and data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs. To this end, we obtain the express consent of clients where necessary and process the special categories of data otherwise for the purposes of health care, if the data is public or wit an other legal persmission.

  Insofar as it is necessary for the fulfilment of our contractual obligations, the protection of vital interests or by law, or with theclients's consent, we disclose or transfer the clients's data to third parties or agents, such as public authorities, accounting offices and in the field of IT, office or comparable services, in compliance with professional regulations; **Legal Basis:**

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

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 (e.g. names, addresses); Payment Data (e.g. bank details, invoices, payment history); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Customers. Prospective customers.
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Further information on processing methods, procedures and services used:

- **Amazon Payments:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider**: Amazon Payments Europe S.C.A. 38 avenue J.F. Kennedy, L-1855 Luxemburg; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://pay.amazon.com; **Privacy Policy:** https://pay.amazon.com/help/201212490. **Basis for third-country transfers:** Switzerland - Adequacy decision (Luxemburg).
- **American Express:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider**: American Express Europe S.A., Theodor-Heuss-Allee 112, 60486 Frankfurt am Main, Germany; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.americanexpress.com/; **Privacy Policy:** https://www.americanexpress.com/de-de/firma/legal/datenschutz-center/online-datenschutzerklarung/. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).
- **Klarna:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider**: Klarna Bank AB (publ), Sveavägen 46, 111 34 Stockholm, Sweden; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.klarna.com; **Privacy Policy:** https://www.klarna.com/de/datenschutz. **Basis for third-country transfers:** Switzerland - Adequacy decision (Sweden).
- **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).
- **Unzer:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider**: heidelpay GmbH, Vangerowstraße 18, 69115 Heidelberg, Germany; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.unzer.com/; **Privacy Policy:** https://www.unzer.com/en/data-protection/. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).

Provision of online services and web hosting

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

terminal device.

- **Processed data types:** Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status); Content data (e.g. text input, photographs, videos); Inventory data (e.g. names, addresses). Contact data (e.g. e-mail, telephone numbers).
- **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; Content Delivery Network (CDN). Firewall.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Collection of Access Data and Log Files:** The access to our online services is logged in the form of so-called "server log files". Server log files may include the address and name of the web pages and files accessed, the date and time of access, data volumes transferred, notification of successful access, browser type and version, the user's operating system, referrer URL (the previously visited page) and, as a general rule, IP addresses and the requesting provider. The server log files can be used for security purposes, e.g. to avoid overloading the servers (especially in the case of abusive attacks, so-called DDoS attacks) and to ensure the stability and optimal load balancing of the servers; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Retention period:** Log file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.
- **E-mail Sending and Hosting:** The web hosting services we use also include sending, receiving and storing e-mails. For these purposes, the addresses of the recipients and senders, as well as other information relating to the sending of e-mails (e.g. the providers involved) and the contents of the respective e-mails are processed. The above data may also be processed for SPAM detection purposes. Please note that e-mails on the Internet are generally not sent in encrypted form. As a rule, e-mails are encrypted during transport, but not on the servers from which they are sent and received (unless a so-called end-to-end encryption method is used). We can therefore accept no responsibility for the transmission path of e-mails between the sender and reception on our server; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

- **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).

- **Cloudflare:** 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**: Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.cloudflare.com; **Privacy Policy:** https://www.cloudflare.com/privacypolicy/; **Data Processing Agreement:** https://www.cloudflare.com/cloudflare-customer-dpa/. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Standard Contractual Clauses (https://www.cloudflare.com/cloudflare-customer-scc/).

- **Wordfence:** firewall and security and error detection functions to detect and prevent unauthorized access attempts as well as technical vulnerabilities that could enable such access. For these purposes, cookies and similar storage procedures required for this purpose may be used and security logs may be created during testing and, in particular, in the event of unauthorized access. In this context, the IP addresses of the users, a user identification number and their activities, including the time of access, are processed and stored and compared with the data provided by the provider of the firewall and security function and transmitted to the latter; **Service provider**: Defiant, Inc., 800 5th Ave Ste 4100, Seattle, WA 98104, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.wordfence.com; **Privacy Policy:** https://www.wordfence.com/privacy-policy/; **Basis for third-country transfers:** EEA - Standard Contractual Clauses (https://www.wordfence.com/standard-contractual-clauses/), Switzerland - Standard Contractual Clauses (https://www.wordfence.com/standard-contractual-clauses/). **Further Information:** https://www.wordfence.com/help/general-data-protection-regulation/.

- **JSDelivr:** Content Delivery Network (CDN) that helps deliver media and files quickly and efficiently, especially under heavy load; **Service provider**: ProspectOne, Królewska 65A/1, 30-081, Kraków, Poland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:**

https://www.jsdelivr.com; **Privacy Policy:** https://www.jsdelivr.com/terms/privacy-policy-jsdelivr-net. **Basis for third-country transfers:** Switzerland - Adequacy decision (Poland).

- **MODX:** Cloud storage, cloud infrastructure services and cloud-based application software; **Service provider**: MODX Systems, LLC, 25 Highland Park Village Suite 100-413, Dallas, TX 75205-2789, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://modx.com/; **Privacy Policy:** https://modx.com/policy/privacy; **Data Processing Agreement:** https://modx.com/policy/terms-of-service/data-processing. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (https://modx.com/policy/terms-of-service/data-processing), Switzerland - Standard Contractual Clauses (https://modx.com/policy/terms-of-service/data-processing).
- **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).
- **ProCloud:** Cloud storage, cloud infrastructure services, and cloud-based application software as well as IT security and maintenance services; **Service provider**: ProCloud AG, Stephan Mahler, Sägestrasse 50, 5600 Lenzburg, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.procloud.ch/en/; **Privacy Policy:** https://www.procloud.ch/en/privacypolicy/. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).
- **Nebula Cloud Solutions:** Development and maintenance of software, cloud, and digital infrastructure solutions; **Service provider**: Nebula Inzhenering DOO, Jane Sandanski 111/8 1200, Tetovo, Nordmazedonien; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://nebulaci.com/; **Privacy Policy:** https://nebulaci.com/; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (Provided by the service provider), Switzerland - Standard Contractual Clauses (Provided by the service provider).

Blogs and publication media

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

- **Processed data types:** Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations; Feedback (e.g. collecting feedback via online form); Provision of our online services and usability. Security measures.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Akismet Anti-Spam Checking:** Akismet Anti-Spam Checking - We use the "Akismet" service on the basis of our legitimate interests. With the help of Akismet, comments from real people are distinguished from spam comments. All comments are sent to a server in the USA, where they are analyzed and stored for four days for comparison purposes. If a comment has been classified as spam, the data will be stored beyond that time. This information includes the name entered, the e-mail address, the IP address, the comment content, the referrer, information about the browser used, the computer system and the time of the entry.

  Users are welcome to use pseudonyms, or to refrain from entering their name or email address. You can completely prevent the transmission of data by not using our comment system. That is a pity, but unfortunately we do not see any alternatives that work just as effectively; **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://automattic.com; **Privacy Policy:** https://automattic.com/privacy. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

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:** Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status); Inventory data (e.g. names, addresses). Contract data (e.g. contract object, duration, customer category).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.); Customers; Prospective customers. Business and contractual partners.
- **Purposes of Processing:** Contact requests and communication; Managing and responding to inquiries; Feedback (e.g. collecting feedback via online form); Provision of our online services and usability; Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures. Marketing.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **HelpSpot:** Management of contact requests and communication; **Service provider**: Userscape, Inc., 2600 South Rd Ste 44-175, Poughkeepsie, NY 12601, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.helpspot.com; **Privacy Policy:** https://userscape.com/privacy; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Standard Contractual Clauses (Provided by the service provider).

Communication via Messenger

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

You can also contact us by alternative means, e.g. telephone or e-mail. Please use

the contact options provided to you or use the contact options provided within our online services.

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

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

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

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

Reservation of reference to other means of communication: Finally, we would like to point out that we reserve the right, for reasons of your safety, not to answer inquiries about messenger services. This is the case if, for example, internal contractual matters require special secrecy or if an answer via the messenger services does not meet the formal requirements. In such cases we refer you to more appropriate communication channels.

- **Processed data types:** Contact data (e.g. e-mail, telephone numbers); Usage

data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status). Content data (e.g. text input, photographs, videos).

- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of Processing:** Contact requests and communication. Direct marketing (e.g. by e-mail or postal).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Slack:** Instant messaging service; **Service provider**: Slack Technologies, Inc., 500 Howard Street, San Francisco, CA 94105, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://slack.com/; **Privacy Policy:** https://slack.com/legal; **Data Processing Agreement:** https://slack.com/intl/de-de/terms-of-service/data-processing; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Standard Contractual Clauses (https://slack.com/intl/de-de/terms-of-service/data-processing). **Further Information:** Security measures: https://slack.com/intl/en-gb/security-practices.

Video Conferences, Online Meetings, Webinars and Screen-Sharing

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

Data processed by Conference Platforms: In the course of participation in a Conference, the Data of the participants listed below are processed. The scope of the processing depends, on the one hand, on which data is requested in the context of a specific Conference (e.g., provision of access data or clear names) and which optional information is provided by the participants. In addition to processing for the purpose of conducting the conference, participants' Data may also be processed by the Conference Platforms for security purposes or service optimization. The processed Date includes personal information (first name, last name), contact information (e-mail address, telephone number), access data (access codes or passwords), profile pictures, information on professional position/function, the IP

address of the internet access, information on the participants' end devices, their operating system, the browser and its technical and linguistic settings, information on the content-related communication processes, i.e. entries in chats and audio and video data, as well as the use of other available functions (e.g. surveys). The content of communications is encrypted to the extent technically provided by the conference providers. If participants are registered as users with the Conference Platforms, then further data may be processed in accordance with the agreement with the respective Conference Provider.

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

Data protection measures of the participants: Please refer to the data privacy information of the Conference Platforms for details on the processing of your data and select the optimum security and data privacy settings for you within the framework of the settings of the conference platforms. Furthermore, please ensure data and privacy protection in the background of your recording for the duration of a Conference (e.g., by notifying roommates, locking doors, and using the background masking function, if technically possible). Links to the conference rooms as well as access data, should not be passed on to unauthorized third parties.

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

- **Processed data types:** Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.); Users (e.g. website visitors, users of online services). Persons depicted.
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations; Contact requests and communication. Office and organisational procedures.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Microsoft Teams:** Conference and communication software; **Service provider**: Microsoft Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.microsoft.com/de-de/microsoft-365; **Privacy Policy:** https://privacy.microsoft.com/de-de/privacystatement, Security information: https://www.microsoft.com/de-de/trustcenter. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

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.

If made available, applicants can submit their applications via an online form. The data will be transmitted to us encrypted according to the state of the art. Applicants can also send us their applications by e-mail. Please note, however, that e-mails on the Internet are generally not sent in encrypted form. As a rule, e-mails are encrypted during transport, but not on the servers from which they are sent and received. We can therefore accept no responsibility for the transmission path of the application between the sender and the reception on our server. For the purposes of searching for applicants, submitting applications and selecting applicants, we may make use of the applicant management and recruitment software, platforms and services of third-party providers in compliance with legal requirements. Applicants are welcome to contact us about how to submit their application or send it to us by regular mail.

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 (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos). 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).
- **Legal Basis:** Job application process as a pre-contractual or contractual relationship (Article 6 (1) (b) 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 (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Customers; Employees (e.g. Employees, job applicants); Prospective customers. Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of Processing:** Office and organisational procedures. Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.).).
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Dropbox:** Cloud storage service; **Service provider**: Dropbox, Inc., 333 Brannan Street, San Francisco, California 94107, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.dropbox.com; **Privacy Policy:** https://www.dropbox.com/privacy; **Data Processing Agreement:** https://assets.dropbox.com/documents/en/legal/dfb-data-processing-agreement.pdf. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Standard Contractual Clauses (https://assets.dropbox.com/documents/en/legal/dfb-data-processing-agreement.pdf).
- **Microsoft Cloud Services:** Cloud storage, cloud infrastructure services and cloud-based application software; **Service provider**: Microsoft Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://microsoft.com; **Privacy Policy:** https://privacy.microsoft.com/de-de/privacystatement, Security information: https://www.microsoft.com/de-de/trustcenter; **Data Processing Agreement:** https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA. **Basis for third-country transfers:** EEA

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

Newsletter and Electronic Communications

We send newsletters, e-mails and other electronic communications (hereinafter referred to as "newsletters") only with the consent of the recipient or a legal permission. Insofar as the contents of the newsletter are specifically described within the framework of registration, they are decisive for the consent of the user. Otherwise, our newsletters contain information about our services and us.

In order to subscribe to our newsletters, it is generally sufficient to enter your e-mail address. We may, however, ask you to provide a name for the purpose of contacting you personally in the newsletter or to provide further information if this is required for the purposes of the newsletter.

Double opt-in procedure: The registration to our newsletter takes place in general in a so-called Double-Opt-In procedure. This means that you will receive an e-mail after registration asking you to confirm your registration. This confirmation is necessary so that no one can register with external e-mail addresses.

The registrations for the newsletter are logged in order to be able to prove the registration process according to the legal requirements. This includes storing the login and confirmation times as well as the IP address. Likewise the changes of your data stored with the dispatch service provider are logged.

Deletion and restriction of processing: We may store the unsubscribed email addresses for up to three years based on our legitimate interests before deleting them to provide evidence of prior consent. The processing of these data is limited to the purpose of a possible defense against claims. An individual deletion request is possible at any time, provided that the former existence of a consent is confirmed at the same time. In the case of an obligation to permanently observe an objection, we reserve the right to store the e-mail address solely for this purpose in a blocklist.

The logging of the registration process takes place on the basis of our legitimate interests for the purpose of proving its proper course. If we commission a service provider to send e-mails, this is done on the basis of our legitimate interests in an efficient and secure sending system.

Contents:

Information about us, our services and news from the consulting practice.

- **Processed data types:** Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status). Usage

data (e.g. websites visited, interest in content, access times).

- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of Processing:** Direct marketing (e.g. by e-mail or postal). Web Analytics (e.g. access statistics, recognition of returning visitors).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).
- **Opt-Out:** You can cancel the receipt of our newsletter at any time, i.e. revoke your consent or object to further receipt. You will find a link to cancel the newsletter either at the end of each newsletter or you can otherwise use one of the contact options listed above, preferably e-mail.

Further information on processing methods, procedures and services used:

- **Measurement of opening rates and click rates:** The newsletters contain a so-called "web-beacon", i.e. a pixel-sized file, which is retrieved from our server when the newsletter is opened or, if we use a mailing service provider, from its server. Within the scope of this retrieval, technical information such as information about the browser and your system, as well as your IP address and time of retrieval are first collected.

  This information is used for the technical improvement of our newsletter on the basis of technical data or target groups and their reading behaviour on the basis of their retrieval points (which can be determined with the help of the IP address) or access times. This analysis also includes determining whether newsletters are opened, when they are opened and which links are clicked. This information is assigned to the individual newsletter recipients and stored in their profiles until the profiles are deleted. The evaluations serve us much more to recognize the reading habits of our users and to adapt our content to them or to send different content according to the interests of our users.

  The measurement of opening rates and click rates as well as the storage of the measurement results in the profiles of the users and their further processing are based on the consent of the users.

  A separate objection to the performance measurement is unfortunately not possible, in this case the entire newsletter subscription must be cancelled or objected to. In this case, the stored profile information will be deleted; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).

- **Brevo:** E-mail dispatch and automation services; **Service provider**: Sendinblue GmbH, Köpenicker Str. 126, 10179 Berlin, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.brevo.com/; **Privacy Policy:**

https://www.brevo.com/de/legal/privacypolicy/; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** Switzerland - Adequacy decision (Germany).

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

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.

- **Processed data types:** Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Web Analytics (e.g. access statistics, recognition of returning visitors). Profiles with user-related information (Creating user profiles).
- **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:

- **Jetpack (WordPress Stats):** Jetpack (WordPress Stats) is a set of analysis functions for Wordpress software; **Service provider**: Aut O'Mattic A8C Ireland Ltd., Grand Canal Dock, 25 Herbert Pl, Dublin, D02 AY86, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://automattic.com; **Privacy Policy:** https://automattic.com/privacy. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).
- **Google Optimize:** Software for the analysis and optimization of online services based on feedback functions as well as pseudonymously performed measurements and analyses of user behavior, which may include in particular A/B tests (measurement of the popularity and user-friendliness of different content and functions), measurement of click paths and interaction with content and functions of the online service; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://optimize.google.com; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://business.safety.google/adsprocessorterms; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** https://business.safety.google/adsservices/ (Types of processing and data processed).

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.

- **Processed data types:** Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status); 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). Customers.
- **Purposes of Processing:** Web Analytics (e.g. access statistics, recognition of returning visitors); Targeting (e.g. profiling based on interests and behaviour, use of cookies); Conversion tracking (Measurement of the effectiveness of marketing activities); Affiliate Tracking; Marketing; Profiles with user-related information (Creating user profiles); Provision of our online services and usability. A/B Tests.
- **Security measures:** IP Masking (Pseudonymization of the IP address).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).
- **Opt-Out:** 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.

Further information on processing methods, procedures and services used:

- **Meta Pixel and Custom Audiences (Custom Audiences):** With the help of the Meta-Pixel (or equivalent functions, to transfer Event-Data or Contact Information via interfaces or other software in apps), Meta is on the one hand able to determine the visitors of our online services as a target group for the

presentation of ads (so-called "Meta ads"). Accordingly, we use Meta-Pixels to display Meta ads placed by us only to Meta users and within the services of partners cooperating with Meta (so-called "audience network" https://www.facebook.com/audiencenetwork/) who have shown an interest in our online services or who have certain characteristics (e.g. interests in certain topics or products that are determined on the basis of the websites visited) that we transmit to Meta (so-called "custom audiences"). With the help of Meta-Pixels, we also want to ensure that our Meta ads correspond to the potential interest of users and do not appear annoying. The Meta-Pixel also enables us to track the effectiveness of Meta ads for statistical and market research purposes by showing whether users were referred to our website after clicking on a Meta ad (known as "conversion tracking"); **Service provider**: Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://www.facebook.com; **Privacy Policy:** https://www.facebook.com/about/privacy; **Data Processing Agreement:** https://www.facebook.com/legal/terms/dataprocessing; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** User event data, i.e. behavioral and interest data, is processed for the purposes of targeted advertising and audience building on the basis of the joint controllership agreement ("Controller Addendum", https://www.facebook.com/legal/controller_addendum). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).

- **Google Ad Manager:** We use the service "Google Ad Manager" to place ads in the Google advertising network (e.g. in search results, videos, websites, etc.). The Google Ad Manager stands out because ads are displayed in real time based on users' presumed interests. This allows us to display ads for our online offering to users who may have a potential interest in our offering or who have previously shown interest, and measure the success of the ads; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://marketingplatform.google.com; **Privacy Policy:** https://policies.google.com/privacy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further Information:** Types of processing and data processed: https://business.safety.google/adsservices/; Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: https://business.safety.google/adscontrollerterms. where Google acts as processor, Data Processing Conditions for Google Advertising

Products and standard contractual clauses for data transfers to third countries: https://business.safety.google/adsprocessorterms apply.

- **Google Ads and Conversion Tracking:** Online marketing process for purposes of placing content and advertisements within the provider's advertising network (e.g., in search results, in videos, on web pages, etc.) so that they are displayed to users who have a presumed interest in the ads. Furthermore, we measure the conversion of the ads, i.e. whether the users took them as a reason to interact with the ads and make use of the advertised offers (so-called conversion). However, we only receive anonymous information and no personal information about individual users; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://marketingplatform.google.com; **Privacy Policy:** https://policies.google.com/privacy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further Information:** Types of processing and data processed: https://business.safety.google/adsservices/. Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: https://business.safety.google/adscontrollerterms.
- **Google Analytics:** Web AnalyticsWe use Google Analytics to perform measurement and analysis of the use of our online services by users based on a pseudonymous user identification number. This identification number does not contain any unique data, such as names or email addresses. It is used to assign analysis information to an end device in order to recognize which content users have accessed within one or various usage processes, which search terms they have used, have accessed again or have interacted with our online services. Likewise, the time of use and its duration are stored, as well as the sources of users referring to our online services and technical aspects of their end devices and browsers. In the process, pseudonymous profiles of users are created with information from the use of various devices, and cookies may be used. Google Analytics does not log or store individual IP addresses. Analytics does provide coarse geo-location data by deriving the following metadata from IP addresses: City (and the derived latitude, and longitude of the city), Continent, Country, Region, Subcontinent (and ID-based counterparts). For EU-based traffic, IP-address data is used solely for geo-location data derivation before being immediately discarded. It is not logged, accessible, or used for any additional use cases. When Analytics collects measurement data, all IP lookups are performed on EU-based servers before forwarding traffic to Analytics servers for processing; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://marketingplatform.google.com/intl/en/about/analytics/; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://business.safety.google/adsprocessorterms/; **Basis for third-country**

transfers: EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en, Settings for the Display of Advertisements: https://myadcenter.google.com/personalizationoff. **Further Information:** https://business.safety.google/adsservices/ (Types of processing and data processed).

- **Google Tag Manager:** Google Tag Manager is a solution with which we can manage so-called website tags via an interface and thus integrate other services into our online services (please refer to further details in this privacy policy). With the Tag Manager itself (which implements the tags), for example, no user profiles are created or cookies are stored. Google only receives the IP address of the user, which is necessary to run the Google Tag Manager; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://marketingplatform.google.com; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://business.safety.google/adsprocessorterms/; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** https://business.safety.google/adsservices/ (Types of processing and data processed).

Customer Reviews and Ratings

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

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

- **Processed data types:** Contract data (e.g. contract object, duration, customer category); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Customers. Users (e.g. website visitors, users of online services).

- **Purposes of Processing:** Feedback (e.g. collecting feedback via online form). Marketing.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **upreview:** Review and rating platform; **Service provider**: endorsal.io, Dean Walton, Worcester, WR5 3NP UK; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://upreview.io/; **Privacy Policy:** https://endorsal.io/privacy/. **Basis for third-country transfers:** EEA - Adequacy decision (UK), Switzerland - Adequacy decision (UK).

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. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites

visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).

- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Contact requests and communication; Feedback (e.g. collecting feedback via online form). Marketing.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Facebook Pages:** Profiles within the social network 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/about/privacy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Further Information:** 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/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/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.

- **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); **Privacy Policy:** https://twitter.com/privacy, (Settings: https://twitter.com/personalization). **Basis for third-country transfers:** Switzerland - Adequacy decision (Ireland).
- **YouTube:** Social network and video platform; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Privacy Policy:** https://policies.google.com/privacy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Opt-Out:** https://myadcenter.google.com/personalizationoff.

Plugins and embedded functions and content

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

The integration always presupposes that the third-party providers of this content process the IP address of the user, since they could not send the content to their browser without the IP address. The IP address is therefore required for the presentation of these contents or functions. We strive to use only those contents, whose respective offerers use the IP address only for the distribution of the contents. Third parties may also use so-called pixel tags (invisible graphics, also known as "web beacons") for statistical or marketing purposes. The "pixel tags" can be used to evaluate information such as visitor traffic on the pages of this website. The pseudonymous information may also be stored in cookies on the user's device and may include technical information about the browser and operating system, referring websites, visit times and other information about the use of our website, as well as may be linked to such information from other sources.

- **Processed data types:** Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status); Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers). Content data (e.g. text input, photographs, videos).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Provision of our online services and usability. Profiles with user-related information (Creating user profiles).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6

(1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Google Fonts (from Google Server):** Obtaining fonts (and symbols) for the purpose of a technically secure, maintenance-free and efficient use of fonts and symbols with regard to timeliness and loading times, their uniform presentation and consideration of possible restrictions under licensing law. The provider of the fonts is informed of the user's IP address so that the fonts can be made available in the user's browser. In addition, technical data (language settings, screen resolution, operating system, hardware used) are transmitted which are necessary for the provision of the fonts depending on the devices used and the technical environment. This data may be processed on a server of the provider of the fonts in the USA - When visiting our online services, users' browsers send their browser HTTP requests to the Google Fonts Web API. The Google Fonts Web API provides users with Google Fonts' cascading style sheets (CSS) and then with the fonts specified in the CCS. These HTTP requests include (1) the IP address used by each user to access the Internet, (2) the requested URL on the Google server, and (3) the HTTP headers, including the user agent describing the browser and operating system versions of the website visitors, as well as the referral URL (i.e., the web page where the Google font is to be displayed). IP addresses are not logged or stored on Google servers and they are not analyzed. The Google Fonts Web API logs details of HTTP requests (requested URL, user agent, and referring URL). Access to this data is restricted and strictly controlled. The requested URL identifies the font families for which the user wants to load fonts. This data is logged so that Google can determine how often a particular font family is requested. With the Google Fonts Web API, the user agent must match the font that is generated for the particular browser type. The user agent is logged primarily for debugging purposes and is used to generate aggregate usage statistics that measure the popularity of font families. These aggregate usage statistics are published on Google Fonts' Analytics page. Finally, the referral URL is logged so that the data can be used for production maintenance and to generate an aggregate report on top integrations based on the number of font requests. Google says it does not use any of the information collected by Google Fonts to profile end users or serve targeted ads; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://fonts.google.com/; **Privacy Policy:** https://policies.google.com/privacy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland). **Further Information:** https://developers.google.com/fonts/faq/privacy?hl=en.
- **YouTube videos:** Video contents; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, , parent company: Google

LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://www.youtube.com; **Privacy Policy:** https://policies.google.com/privacy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF). **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en, Settings for the Display of Advertisements: https://myadcenter.google.com/personalizationoff.

- **Vimeo-Videoplayer:** Integration of a video player; **Service provider**: Vimeo Inc., Attention: Legal Department, 555 West 18th Street New York, New York 10011, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://vimeo.com; **Privacy Policy:** https://vimeo.com/privacy; **Data Processing Agreement:** https://vimeo.com/enterpriseterms/dpa. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (https://vimeo.com/enterpriseterms/dpa), Switzerland - Standard Contractual Clauses (https://vimeo.com/enterpriseterms/dpa).
- **Font Awesome (from the server of the provider):** Obtaining fonts (and symbols) for the purpose of a technically secure, maintenance-free and efficient use of fonts and symbols with regard to timeliness and loading times, their uniform presentation and consideration of possible restrictions under licensing law. The provider of the fonts is informed of the user's IP address so that the fonts can be made available in the user's browser. In addition, technical data (language settings, screen resolution, operating system, hardware used) are transmitted which are necessary for the provision of the fonts depending on the devices used and the technical environment; **Service provider**: Fonticons, Inc. ,6 Porter Road Apartment 3R, Cambridge, MA 02140, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://fontawesome.com/. **Privacy Policy:** https://fontawesome.com/privacy.

Management, Organization and Utilities

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

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

If users are referred to the third-party providers or their software or platforms in the context of communication, business or other relationships with us, the third-party provider processing may process usage data and metadata that can be

processed by them for security purposes, service optimisation or marketing purposes. We therefore ask you to read the data protection notices of the respective third party providers.

- **Processed data types:** Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.). Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations. Office and organisational procedures.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Confluence:** Software for the creation and administration of Wiki & knowledge platforms; **Service provider**: Atlassian Inc. (San Francisco, Harrison Street Location), 1098 Harrison Street, San Francisco, California 94103, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.atlassian.com/software/confluence; **Privacy Policy:** https://www.atlassian.com/legal/privacy-policy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Standard Contractual Clauses (Part of the Data Processing Agreement). **Further Information:** Data Transfer Impact Assessment: https://www.atlassian.com/legal/data-transfer-impact-assessment.
- **Jira:** Web application for error management, troubleshooting and operational project management; **Service provider**: Atlassian Inc. (San Francisco, Harrison Street Location), 1098 Harrison Street, San Francisco, California 94103, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.atlassian.com/de/software/jira; **Privacy Policy:** https://www.atlassian.com/legal/privacy-policy; **Data Processing Agreement:** https://www.atlassian.com/legal/data-processing-addendum; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Standard Contractual Clauses (Part of the Data Processing Agreement). **Further Information:** Data Transfer Impact Assessment: https://www.atlassian.com/legal/data-transfer-impact-assessment.

Changes and Updates to the Privacy Policy

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.

- **A/B Tests:** A/B tests are designed to improve the usability and performance of online services. For example, users are presented with different versions of a website or its elements, such as input forms, on which the placement of the contents or labels of the navigation elements can differ. The behaviour of users, e.g. prolonged visits to the site or more frequent interaction with the elements, can then be used to determine which of these sites or elements are more responsive to users' needs.
- **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.
- **Content Delivery Network (CDN):** A "Content Delivery Network" (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.
- **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).

- **Firewall:** A firewall is a security system that protects a computer network or a single computer from unwanted network access.
- **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.
- **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.
- **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.

Many thanks to Dr. Thomas Schwenke for the pleasant cooperation, support and assistance during the preparation and implementation phase.

Last examination was carried out on the 16. February 2024