Privacy Policy

Preamble

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

The terms used are not gender-specific.

Last Update: 8. July 2026

Created with Datenschutz-Generator.de by Dr. jur. Thomas Schwenke

Table of contents

- Preamble
- Controller
- Overview of processing operations
- Relevant legal bases
- Security Precautions
- Transmission of Personal Data
- International data transfers
- General Information on Data Retention and Deletion
- Rights of Data Subjects
- Performing tasks in accordance with statutes or rules of procedure
- Payment Procedure
- Provision of online services and web hosting
- Use of Cookies
- Processing of data in the context of applications (apps)
- Contact and Inquiry Management
- Artificial Intelligence (AI)
- Video Conferences, Online Meetings, Webinars and Screen-Sharing
- Cloud Services
- Newsletter and Electronic Communications
- Web Analysis, Monitoring and Optimization
- Profiles in Social Networks (Social Media)
- Management, Organization and Utilities

- Processing of data in the context of employment relationships
- Job Application Process
- Changes and Updates
- Terminology and Definitions

Controller

Blue Action Fund
c/o Nature Trust Alliance Stiftungen & Co eGbR
Friedrich-Ebert-Anlage 36
60325 Frankfurt am Main
Germany

Authorised Representatives: Markus Knigge (Executive Director); Judith Weigand-Jahn

E-mail address: info@blueactionfund.org

Legal Notice: https://www.blueactionfund.org/legalnotice/

Overview of processing operations

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

Categories of Processed Data

- Inventory data.
- Employee Data.
- Payment Data.
- Contact data.
- Content data.
- Contract data.
- Usage data.
- Meta, communication and process data.
- Social data.
- Job applicant details.
- Images and/ or video recordings.
- Audio recordings.
- Log data.
- Performance and behavioural data.
- Member data.
- Working hours data.
- Salary data.

Special Categories of Data

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

Categories of Data Subjects

- Service recipients and clients.
- Employees.
- Prospective customers.
- Communication partner.
- Users.
- Job applicants.
- Members.
- Business and contractual partners.
- Participants.
- Persons depicted.
- Donors.
- Third parties.

Purposes of Processing

- Provision of contractual services and fulfilment of contractual obligations.
- Communication.
- Security measures.
- Direct marketing.
- Web Analytics.
- Office and organisational procedures.
- Remarketing.
- Conversion tracking.
- Organisational and Administrative Procedures.
- Job Application Process.
- Feedback.
- Marketing.
- Profiles with user-related information.
- Provision of our online services and usability.
- Establishment and execution of employment relationships.
- Information technology infrastructure.
- Fundraising.
- Public relations and informational purposes.
- Public relations.
- Business processes and management procedures.
- Artificial Intelligence (AI).

Relevant legal bases

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

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

National data protection regulations in Germany: In addition to the data protection regulations of the GDPR, national regulations apply to data protection in Germany.

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

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

Reference to the applicability of the GDPR and the Swiss DPA: This privacy policy is intended to provide information in accordance with both the Swiss Federal Act on Data Protection (FADP) and the General Data Protection Regulation (GDPR). Where references are made to concepts such as the processing of personal data, legitimate interests, or special categories of data, these references are to be understood in accordance with the applicable data protection laws. Within the scope of application of the Swiss FADP, the legal interpretation of these terms is determined exclusively by Swiss law.

Security Precautions

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

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

Securing online connections through TLS/SSL encryption technology (HTTPS): To protect the data of users transmitted via our online services from unauthorized access, we employ TLS/SSL encryption technology. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are the cornerstones of secure data transmission on the internet. These technologies encrypt the information that is transferred between the website or

app and the user's browser (or between two servers), thereby safeguarding the data from unauthorized access. TLS, as the more advanced and secure version of SSL, ensures that all data transmissions conform to the highest security standards. When a website is secured with an SSL/TLS certificate, this is indicated by the display of HTTPS in the URL. This serves as an indicator to users that their data is being securely and encryptedly transmitted.

Transmission of Personal Data

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

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

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

International data transfers

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

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

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

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

For data transfers to other third countries, appropriate safeguards apply, particularly Standard Contractual Clauses, explicit consent, or legally required transfers. Information on third-country transfers and applicable adequacy decisions can be found in the information provided by the EU Commission: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en .

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

General Information on Data Retention and Deletion

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

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

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

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

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

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

- 10 Years - Fiscal Code/Commercial Code - Retention period for books and records, annual financial statements, inventories, management reports,

opening balance sheet as well as the necessary work instructions and other organisational documents (Section 147 Paragraph 1 No. 1 in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 14b Paragraph 1 of the German VAT Act (UStG), Section 257 Paragraph 1 No. 1 in conjunction with Paragraph 4 of the German Commercial Code (HGB)).

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

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.

Performing tasks in accordance with statutes or rules of procedure

We process the data of our members, supporters, prospects, business partners or other persons (collectively, " data subjects ") when we have a membership or other business relationship with them and perform our functions and are recipients of benefits and benefits. Otherwise, we process the data of data subjects on the basis of our legitimate interests, e.g. when it concerns administrative tasks or public relations.

The data processed, the type, scope and purpose and the necessity of their processing, are determined by the underlying membership or contractual relationship, from which the necessity of any data information arises (otherwise we refer to necessary data).

We delete data that is no longer required for the performance of our statutory and business purposes. This is determined according to the respective tasks and contractual relationships. We retain the data for as long as it may be relevant for the purpose of conducting business and with regard to any warranty or liability obligations on the basis of our legitimate interest in their regulation. The necessity of storing the data is checked regularly; otherwise the statutory storage obligations apply.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Contract data (e.g. contract object, duration, customer category); Member data (e.g. personal data such as name, age, gender, contact details (email address, phone number), membership number, information about membership fees, participation in events, etc.). Payment Data (e.g. bank details, invoices, payment history).

- **Data subjects:** Members; Prospective customers; Communication partner (Recipients of e-mails, letters, etc.); Donors. Third parties.
- **Purposes of processing and legitimate interests:** Communication; Organisational and Administrative Procedures; Public relations and informational purposes. Fundraising.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). Membership Agreement (Statutes) (Article 6 (1) (b) GDPR).

Further information on processing methods, procedures and services used:

- **Events and Organisational Operations:** Planning, execution, and follow-up of events as well as the general operation of activities in accordance with the statutes. Planning includes the collection and processing of participant data, coordination of logistical requirements, and setting the event agenda. Execution encompasses the management of participant registration, updating participant information during the event, and recording attendance and participant activities. Follow-up involves analyzing participant data to evaluate event success, creating reports, and archiving relevant information about the event. General organizational operations include managing member data, communicating with members and prospects, as well as organizing internal meetings and sessions; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR), Membership Agreement (Statutes) (Article 6 (1) (b) GDPR).
- **Public relations:** Public relations processes include the creation and distribution of informational materials, the maintenance of contact data for press and media relations, as well as the organisation and execution of press conferences and public events. The creation of informational materials involves collecting and processing information for press releases, newsletters, reports, and other publications. Distribution is carried out via digital and traditional channels, including email lists, websites, and social media. The maintenance of contact data encompasses the recording and updating of data related to media contacts and other relevant interest groups. The organisation of press conferences and events includes planning and executing these occasions, managing invitations, and coordinating event logistics. Interaction with media and interest groups occurs through direct communication with journalists, bloggers, and other opinion leaders by responding to inquiries and providing information; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR), Membership Agreement (Statutes) (Article 6 (1) (b) GDPR).
- **Fundraising and Donation Collection:** Processes include the planning and execution of campaigns for fundraising, the management of donor data, and communication with donors and potential supporters. Planning campaigns involves developing strategies, setting goals, and selecting channels for fundraising. The execution of campaigns is carried out through the initiation and implementation of specific fundraising actions, collecting donations via online platforms, events, and direct approach. The management of donor data encompasses the collection, updating, and analysis of data to optimise future

campaigns. Communication with donors and potential supporters is conducted through personalised approaches, thank-you letters, and regular updates on project successes and fund usage; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR), Membership Agreement (Statutes) (Article 6 (1) (b) GDPR).

Donation 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"). Payment transactions are carried out exclusively via encrypted connections in accordance with the state of the art, ensuring that the data entered is protected from unauthorized access during transmission.

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

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

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

Further information on donation processing methods, procedures and services used:

- **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/.
- **Apple Pay:** Payment services provider; **Service provider**: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.apple.com/apple-pay/ . **Privacy Policy:** https://www.apple.com/legal/privacy/en-ww/.
- **Google Pay:** Payment services provider; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://pay.google.com/intl/en_uk/about/. **Privacy Policy:** https://business.safety.google/privacy/.
- **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.
- **Stripe:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider**: Stripe, Inc., 510 Townsend Street, San Francisco, CA 94103, USA; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://stripe.com/de ; **Privacy Policy:** https://stripe.com/en-de/privacy . **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Data Privacy Framework (DPF).
- **Visa:** Payment-Service-Provider (technical integration of online-payment-methods); **Service provider**: Visa Europe Services Inc., Zweigniederlassung London, 1 Sheldon Square, London W2 6TT, UK; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.visa.de . **Privacy Policy:** https://www.visa.com/en-us/legal/global-privacy-notice.

Provision of online services and web hosting

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

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Log data (e.g. log files concerning logins or data retrieval or access times.); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Inventory data (For example, the full name, residential address, contact information, customer number, etc.). Contact data (e.g. postal and email addresses or phone numbers).
- **Data subjects:** Users (e.g. website visitors, users of online services); Service recipients and clients; Communication partner (Recipients of e-mails, letters, etc.). Business and contractual partners.
- **Purposes of processing and legitimate interests:** 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; Communication. Organisational and Administrative Procedures.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Provision of online offer on rented hosting space:** For the provision of our online services, we use storage space, computing capacity and software that we rent or otherwise obtain from a corresponding server provider (also referred to as a "web hoster"); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Collection of Access Data and Log Files:** Access to our online service is logged in the form of so-called "server log files". Server log files may include the address and name of the accessed web pages and files, date and time of access, transferred data volumes, notification of successful retrieval, browser type along with version, the user's operating system, referrer URL (the previously visited page), and typically IP addresses and the requesting provider. The server log files can be used for security purposes, e.g., to prevent server overload (especially in the case of abusive attacks, known as DDoS attacks), and to ensure server load management and stability; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Retention period:** Log file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.

- **E-mail Sending and Hosting:** The web hosting services we use also include sending, receiving and storing e-mails. For these purposes, the addresses of the recipients and senders, as well as other information relating to the sending of e-mails (e.g. the providers involved) and the contents of the respective e-mails are processed. The above data may also be processed for SPAM detection purposes. Please note that e-mails on the Internet are generally not sent in encrypted form. As a rule, e-mails are encrypted during transport, but not on the servers from which they are sent and received (unless a so-called end-to-end encryption method is used). We can therefore accept no responsibility for the transmission path of e-mails between the sender and reception on our server; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Wordpress.com:** Hosting and software for the creation, provision and operation of websites, blogs and other online services; **Service provider**: Aut O'Mattic A8C Ireland Ltd., Grand Canal Dock, 25 Herbert Pl, Dublin, D02 AY86, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://wordpress.com ; **Privacy Policy:** https://automattic.com/privacy/ ; **Data Processing Agreement:** https://wordpress.com/support/data-processing-agreements/ . **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider).
- **Hornetsecurity:** E-mail security, spam filtering, protection against phishing attacks, e-mail archiving, message encryption, ensuring compliance with legal requirements and providing backup solutions for e-mail data; **Service provider**: Hornetsecurity GmbH, Am Listholze 78, 30177 Hannover, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.hornetsecurity.com/ . **Privacy Policy:** https://www.hornetsecurity.com/en/privacy/.

Use of Cookies

The term "cookies" refers to functions that store information on users' devices and read it from them. Cookies can also be used for different purposes, such as ensuring the functionality, security, and convenience of online services, as well as analyzing visitor traffic. We use cookies in accordance with legal regulations. If necessary, we obtain users' consent in advance. If consent is not required, we rely on our legitimate interests. This applies when storing and reading information is essential to provide explicitly requested content and functions. This includes, for example, saving settings and ensuring the functionality and security of our online services. Consent can be withdrawn at any time. We clearly inform users about the scope of the consent and which cookies are used.

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

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

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

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

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

Further information on processing methods, procedures and services used:

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

Processing of data in the context of applications (apps)

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

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing and legitimate interests:** Provision of contractual services and fulfilment of contractual obligations; Security measures. Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Location history and movement profiles:** The location data is only used selectively and is not processed to create a location history or a movement profile of the devices used or of their users.

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. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing and legitimate interests:** Communication; Organisational and Administrative Procedures; Feedback (e.g. collecting feedback via online form). Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Further information on processing methods, procedures and services used:

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

Artificial Intelligence (AI)

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

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

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

We place particular emphasis on transparency, fairness and maintaining human oversight over AI-supported decision-making processes.

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

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

Further information on processing methods, procedures and services used:

- **DeepL:** Translation of texts into various languages and provision of synonyms as well as context examples. Support with the correction and improvement of texts in different languages; **Service provider**: DeepL SE, Maarweg 165, 50825 Köln, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.deepl.com ; **Privacy Policy:** https://www.deepl.com/en/privacy . **Data Processing Agreement:** Provided by the service provider.
- **Microsoft Copilot:** Microsoft Copilot: Assistance in the creation and editing of texts, spreadsheets, and presentations, data analysis, task automation, and integration into Office applications. Content data (files, conversations, metadata) as well as employee credentials (Org-ID/Entra ID) are processed for the purposes of increasing efficiency and productivity, cost efficiency, flexibility, mobility, and integration with M365. Chat histories are stored for up to 30 days; content is stored until deleted by the user. Additionally, diagnostic data is collected for product stability and improvement; **Service provider**: Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.microsoft.com/en-us/microsoft-copilot/organizations ; **Privacy Policy:** https://www.microsoft.com/en-us/privacy/privacystatement ; **Data Processing Agreement:** https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA . **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA), Switzerland - Data Privacy

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

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

Further information on processing methods, procedures and services used:

- **Microsoft Teams:** Utilisation for conducting online events, conferences, and communication with internal and external participants. Voice transmission, direct messaging, group communication, and collaboration functions are used; name, business contact details, work profile, participation as well as content (audio/video, speech, chat, files, speech transcription) are processed for purposes and interests in efficiency and productivity improvements, cost efficiency, flexibility, mobility, enhanced communication, IT security, use of a central platform as well as business operations by Microsoft. Audio signals are generally not stored unless recording is enabled. Meeting and conference recordings are stored by default for 90 days unless a different duration is specified. Chat and file contents are stored according to the policies determined by the administrator or user; there is no preset automatic deletion. Channels must be renewed every 180 days; otherwise contents are deleted. Additionally processed are system-generated logs, diagnostic and metadata as well as diagnostic data collected for product stability, security and improvement; **Service provider**: Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; Microsoft Corporation, One Microsoft Way, Redmond, WA

98052-6399, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.microsoft.com/en-us/microsoft-teams /; **Privacy Policy:** https://www.microsoft.com/en-us/privacy/privacystatement . **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA).

- **Zoom:** Video conferences, online meetings, webinars, screen sharing, optional recording of sessions, chat function, integration with calendars and other apps; **Service provider**: Zoom Video Communications, Inc., 55 Almaden Blvd., Suite 600, San Jose, CA 95113, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.zoom.com ; **Privacy Policy:** https://www.zoom.com/en/trust/privacy/privacy-statement/ ; **Data Processing Agreement:** https://media.zoom.com/download/assets/zoom-global-dpa.pdf/dd327ebea27e11efb613d6ba63ed4cee . **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://media.zoom.com/download/assets/zoom-global-dpa.pdf/dd327ebea27e11efb613d6ba63ed4cee), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://media.zoom.com/download/assets/zoom-global-dpa.pdf/dd327ebea27e11efb613d6ba63ed4cee).

Cloud Services

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

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

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as

details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Images and/ or video recordings (e.g. photographs or video recordings of a person).

- **Data subjects:** Prospective customers; Communication partner (Recipients of e-mails, letters, etc.). Business and contractual partners.
- **Purposes of processing and legitimate interests:** Office and organisational procedures; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)). Provision of contractual services and fulfillment of contractual obligations.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Adobe Creative Cloud:** Cloud storage, cloud infrastructure services, and cloud-based application software, among others for photo editing, video editing, graphic design, web development; **Service provider**: Adobe Systems Software Ireland, 4-6, Riverwalk Drive, Citywest Business Campus, Brownsbarn, Dublin 24, D24 DCW0, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.adobe.com/creativecloud.html ; **Privacy Policy:** https://www.adobe.com/privacy.html ; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider).
- **Microsoft 365 and Microsoft Cloud Services:** Provision of applications, protection of data and IT systems, as well as the use of system-generated log, diagnostic, and metadata for contract execution by Microsoft. The data processed includes contact details (name, email address), content data (files, comments, profiles), software setup and inventory data, device connectivity and configuration data, work interactions (badge swipe), as well as log and metadata. The processing is carried out for purposes of improving efficiency and productivity, cost efficiency, flexibility, mobility, enhanced communication, integration of Microsoft services, IT security and business operations of Microsoft. Data retention is determined by the respective document and company policies: up to 12 months for Defender (protection of data and IT systems) and 10 days for print management. Additionally, diagnostic data is collected for product stability and improvement; **Service provider**: Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://microsoft.com ; **Privacy Policy:** https://privacy.microsoft.com/de-de/privacystatement , Security information: https://www.microsoft.com/de-de/trustcenter ; **Data Processing Agreement:** https://www.microsoft.com/licensing/docs/view/Microsoft-

Products-and-Services-Data-Protection-Addendum-DPA . **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA).

Newsletter and Electronic Communications

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

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

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

Contents:

Information about us, our services, promotions and offers.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing and legitimate interests:** Direct marketing (e.g. by e-mail or postal).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

- **Opt-Out:** You can cancel the receipt of our newsletter at any time, i.e. revoke your consent or object to further receipt. You will find a link to cancel the newsletter either at the end of each newsletter or you can otherwise use one of the contact options listed above, preferably e-mail.

Further information on processing methods, procedures and services used:

- **Mailjet:** Email distribution and email marketing platform; **Service provider**: Mailjet SAS,13-13 bis, rue de l'Aubrac, 75012 Paris, France; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.mailjet.com . **Privacy Policy:** https://www.mailjet.com/privacy-policy/ .
- **Salesforce:** E-mail dispatch and automation services; **Service provider**: salesforce.com Deutschland GmbH, Erika-Mann-Str. 31, 80636 München, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.salesforce.com ; **Privacy Policy:** https://www.salesforce.com/company/privacy/ ; **Data Processing Agreement:** https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf ; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/scc-amendment.pdf), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/scc-amendment.pdf); **Further Information:** Data Protection Impact Assessments & Salesforce Services: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Privacy/dpia-and-salesforce-services.pdf .

Web Analysis, Monitoring and Optimization

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

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

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

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

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

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing and legitimate interests:** Web Analytics (e.g. access statistics, recognition of returning visitors); Profiles with user-related information (Creating user profiles); Provision of our online services and usability; Remarketing; Conversion tracking (Measurement of the effectiveness of marketing activities). Marketing.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.).
- **Security measures:** IP Masking (Pseudonymization of the IP address).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Google Analytics:** We use Google Analytics to perform measurement and analysis of the use of our online services by users based on a pseudonymous user identification number. This identification number does not contain any unique data, such as names or email addresses. It is used to assign analysis information to an end device in order to recognize which content users have accessed within one or various usage processes, which search terms they have used, have accessed again or have interacted with our online services. Likewise, the time of use and its duration are stored, as well as the sources of users referring to our online services and technical aspects of their end devices and browsers.
  In the process, pseudonymous profiles of users are created with information from the use of various devices, and cookies may be used. Google Analytics does not log or store individual IP addresses. Analytics does provide coarse geo-location data by deriving the following metadata from IP addresses: City (and

the derived latitude, and longitude of the city), Continent, Country, Region, Subcontinent (and ID-based counterparts). For EU-based traffic, IP-address data is used solely for geo-location data derivation before being immediately discarded. It is not logged, accessible, or used for any additional use cases. When Analytics collects measurement data, all IP lookups are performed on EU-based servers before forwarding traffic to Analytics servers for processing; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://marketingplatform.google.com/intl/en/about/analytics/ ; **Security measures:** IP Masking (Pseudonymization of the IP address); **Privacy Policy:** https://business.safety.google/privacy/ ; **Data Processing Agreement:** https://business.safety.google/adsprocessorterms/ ; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://business.safety.google/adsprocessorterms), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://business.safety.google/adsprocessorterms); **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en , Settings for the Display of Advertisements: https://myadcenter.google.com/personalizationoff . **Further Information:** https://business.safety.google/adsservices/ (Types of processing and data processed).

- **Information on recipients of consent and cookie-less analytics:** Information on recipients of consent: The consent given by users in the context of a consent dialogue (also known as "Cookie Opt-In/Consent", "Cookie Banner", etc.) serves multiple purposes. Firstly, it helps us to fulfil our obligation to obtain consent for the storage and reading of information on and from the end-user's device (in accordance with ePrivacy Directives). Secondly, it covers the processing of users' personal data in accordance with data protection requirements. Additionally, this consent is also applicable to Google, as the company is required by the Digital Markets Act to obtain consent for personalised services. Therefore, we share the status of consents given by users with Google. Our consent management software informs Google about whether consents have been given or not. The aim is to ensure that user consents—or their absence—are taken into account when using Google Analytics and integrating features and external services. Thus, user consents and their revocation can be dynamically adjusted within our online offerings through Google Analytics and other Google services, depending on user selection.
  Cookieless Analysis: We utilise the advanced implementation of consent mode of Google Analytics. This means that if users do not give consent for the storage and reading of information on their end devices – particularly regarding cookies – no cookies or similar information will be stored on the user's devices. Likewise, no user profiles will be created.In this case, Google's code generates a random identification number on the user's end device and transmits it to Google (known as a "ping"). There is no storage of the identification in the browser, in apps, or other devices used by the user. This identification number is unique for each website visit, so that users' behaviour or interests cannot be tracked across devices or websites. Only a minimum amount of information about user activity is sent. This includes details about consent status and

information for conversion measurement, i.e., whether a user was directed to our online service via a Google advertisement.Additionally, where available, the following information may be transmitted: a) Function-related information such as headers (technical details transmitted by the browser), b) Timestamps (date and time of access), c) User-Agent (information about the browser and device used, web only), d) Referrer URL (the URL of the page from which the user arrived), e) Aggregated/pseudonymous information: This includes an indication of whether the current or a previous page in the user's navigation history contains information about ad clicks in its URL (e.g., GCLID/DCLID, specific tracking codes from Google), a random number generated with each page view, and details about the platform used by the website owner for consent management (e.g., developer ID); **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://support.google.com/analytics/answer/9976101?hl=de . **Privacy Policy:** https://business.safety.google/privacy/ .

Profiles in Social Networks (Social Media)

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

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

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

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

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

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

Further information on processing methods, procedures and services used:

- **Bluesky:** Decentralised social media network - allows for the creation, sharing and commenting on content, as well as following user profiles; **Service provider**: Bluesky, PBLLC., Seattle, USA, support@bsky.app; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://bsky.social/. **Privacy Policy:** https://bsky.social/about/support/privacy-policy.
- **Instagram:** Social network, allows the sharing of photos and videos, commenting on and favouriting posts, messaging, subscribing to profiles and pages; **Service provider**: Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.instagram.com; **Privacy Policy:** https://privacycenter.instagram.com/policy /. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Data Privacy Framework (DPF).
- **LinkedIn:** Social network - We are jointly responsible with LinkedIn Ireland Unlimited Company for the collection (but not the further processing) of visitor data, which is used to create "Page Insights" (statistics) for our LinkedIn profiles. This data includes information about the types of content users view or interact with, as well as the actions they take. It also includes details about the devices used, such as IP addresses, operating systems, browser types, language settings, and cookie data, as well as profile details of users, such as job function, country, industry, seniority, company size, and employment status. Privacy information regarding the processing of user data by LinkedIn can be found in LinkedIn's privacy policy: https://www.linkedin.com/legal/privacy-policy .
  We have entered into a special agreement with LinkedIn Ireland ("Page Insights Joint Controller Addendum," https://legal.linkedin.com/pages-joint-controller-addendum), which specifically regulates the security measures LinkedIn must comply with and in which LinkedIn has agreed to fulfill the rights of data subjects (i.e., users can, for example, direct requests for information or deletion directly to LinkedIn). The rights of users (particularly the right to

information, deletion, objection, and to lodge a complaint with the competent supervisory authority) are not restricted by our agreements with LinkedIn. The joint responsibility is limited to the collection of data and its transmission to LinkedIn Ireland Unlimited Company, a company based in the EU. Further processing of the data is the sole responsibility of LinkedIn Ireland Unlimited Company, particularly concerning the transfer of data to the parent company LinkedIn Corporation in the USA; **Service provider**: LinkedIn Ireland Unlimited Company, Wilton Plaza, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.linkedin.com ; **Privacy Policy:** https://www.linkedin.com/legal/privacy-policy ; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.linkedin.com/legal/privacy-policy), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.linkedin.com/legal/privacy-policy). **Opt-Out:** https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out .

Management, Organization and Utilities

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

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

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

- **Processed data types:** Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties). Contract data (e.g. contract object, duration, customer category).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.); Users (e.g. website visitors, users of online services). Business and contractual partners.
- **Purposes of processing and legitimate interests:** Provision of contractual services and fulfilment of contractual obligations; Office and organisational

procedures; Provision of our online services and usability. Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)).

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

Further information on processing methods, procedures and services used:

- **Adobe Document Cloud:** Cloud storage, cloud infrastructure services, and cloud-based application software for creating, editing, signing, and sharing PDF documents; **Service provider**: Adobe Systems Software Ireland, 4-6, Riverwalk Drive, Citywest Business Campus, Brownsbarn, Dublin 24, D24 DCW0, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.adobe.com/creativecloud.html ; **Privacy Policy:** https://www.adobe.com/privacy.html ; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider).
- **DocuSign:** Electronic signature of documents, sending documents for signature, tracking the status of documents, storage of signed documents ; **Service provider**: DocuSign, Inc., 221 Main Street Suite 1000 San Francisco, CA 94105, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.docusign.com/ ; **Privacy Policy:** https://www.docusign.com/privacy ; **Data Processing Agreement:** https://www.docusign.com/legal/terms-and-conditions/data-protection-attachment ; **Basis for third-country transfers:** EEA - Standard Contractual Clauses (https://www.docusign.com/legal/terms-and-conditions/data-protection-attachment), Switzerland - Standard Contractual Clauses (https://www.docusign.com/legal/terms-and-conditions/data-protection-attachment). **Further Information:** The processing as processor and controller is also carried out on the basis of approved Binding Corporate Rules, which ensure a level of data protection in accordance with the requirements of the GDPR (Article 47 GDPR): https://www.docusign.com/trust/privacy/binding-corporate-rules .

Processing of data in the context of employment relationships

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

The data processing covers various aspects ranging from contract initiation to termination. Included are the organization and management of daily working hours,

management of access rights and permissions, as well as handling personnel development measures and staff appraisals. The processing also serves payroll accounting and management of wage and salary payments, which represent critical aspects of contract execution.

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

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

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

establishment and execution of employment relationships); Business processes and management procedures; Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Public relations. Security measures.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Compliance with a legal obligation (Article 6 (1) (c) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR). Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).

Further information on processing methods, procedures and services used:

- **Time Recording:** Processes for recording employees' working hours include both manual and automated methods, such as the use of punch clocks, time tracking software, or mobile apps. Activities involved include entering clock-in and clock-out times, break times, overtime, and absences. To verify and validate the recorded working hours, they are compared with deployment or shift schedules, checked for absences, and approved for overtime by supervisors. Reports and analyses are generated based on the recorded working hours to provide work time records, overtime reports, and absence statistics for management and the human resources department; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Authorization Management:** Procedures required for the definition, management, and control of access rights and user roles within a system or an organisation (e.g., creation of authorisation profiles, role- and access-based control, review and approval of access requests, regular review of access rights, tracking and auditing of user activities, creation of security policies and procedures); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Special categories of personal data:** Special categories of personal data are processed in the context of employment relationships or to fulfil legal obligations. The processed special categories of personal data include information concerning the health, trade union membership, or religious affiliation of employees. This data may be transferred to health insurance companies or processed for assessing the employees' work capacity, for corporate health management, or for declarations to the tax authorities; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Sources of Processed Data:** Personal data received during the application process and/or employment relationship will be processed. Furthermore, where required by law, personal data will be collected from other sources. These may include financial authorities for tax-related information, the respective health insurance company for information on work incapacity, third parties such as employment agencies, or publicly accessible sources like professional social networks in the context of application procedures; **Legal**

Basis: Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Purposes of Data Processing:** The personal data of employees are primarily processed for the establishment, execution, and termination of the employment relationship. Furthermore, the processing of this data is necessary to fulfil legal obligations in the field of tax and social security law. In addition to these primary purposes, the data of employees are also used to meet regulatory and supervisory requirements, to optimise processes of electronic data processing, and to compile company-internal or cross-company data, possibly including statistical data. Moreover, the data of employees may be processed for the assertion of legal claims and defense in legal disputes; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Transmission of Employee Data:** The data of employees is processed internally only by those departments that require it to fulfil operational, contractual, and legal obligations. The transfer of data to external recipients only occurs if it is legally required, or if the affected employees have given their consent. Possible scenarios for this can include requests for information from authorities or in the case of asset formation benefits. Furthermore, the controller may transfer personal data to further recipients as far as this is necessary for fulfilling his contractual and legal obligations as an employer. These recipients can include: a) banks b) health insurance companies, pension insurance institutions, providers of old-age provisions and other social insurance carriers c) authorities, courts (e.g., tax authorities, labour courts, further supervisory authorities within the framework of fulfilling reporting and information obligations) d) tax and legal advisors e) third-party debtors in the case of wage and salary garnishments f) other entities to which legally obligatory declarations must be made.
  In addition, data can be transferred to third parties if this is necessary for communication with business partners, suppliers or other service providers. Examples include details in the sender area of emails or letterheads as well as creating profiles on external platforms; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Transmission of Employee Data to Third Countries:** The transfer of employee data to third countries, meaning countries outside the European Union (EU) and the European Economic Area (EEA), occurs only if it is necessary for the fulfilment of the employment relationship, legally required, or if employees have given their consent. Employees will be informed about the details separately, as far as legally required; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Business Travel and Travel Expense Settlement:** Procedures required for planning, executing, and accounting for business trips (e.g., booking of travel, organizing accommodations and transportation, managing travel expense advances, submitting and reviewing travel expense reports, controlling and recording incurred costs, compliance with travel policies, handling of the travel

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

- **Payroll and wage accounting:** Procedures required for calculating, disbursing, and documenting wages, salaries, and other remuneration for employees (e.g., recording of working hours, calculation of deductions and surcharges, remittance of taxes and social security contributions, preparation of payroll statements, management of wage accounts, reporting to the tax authorities and social security institutions); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR).
- **Deletion of Employee Data:** Employment data will be deleted under German law when it is no longer required for the purpose for which it was collected, unless there is a legal obligation to retain or archive it, or it needs to be kept for the interests of the employer. The following retention and archiving obligations are observed:
    - General personnel records - General personnel records (such as employment contracts, references, supplementary agreements) are retained for up to three years after the termination of the employment relationship (§ 195 German Civil Code (BGB)).
      Tax-relevant documents - Tax-relevant documents in the personnel file are kept for six years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
      Information on wages and working hours - Information on wages and working hours for (accident) insured with wage proof are kept for five years (§ 165 I 1, IV 2 Social Code Book VII (SGB VII)).
    - Payrolls including lists for special payments - Payrolls including lists for special payments, if a booking receipt is available, are kept for ten years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
    - Wage lists for interim, final, and special payments - Wage lists for interim, final, and special payments are kept for six years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
    - Documents on employee insurance - Documents on employee insurance, if booking receipts are available, are kept for ten years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
    - Contribution statements to social security institutions - Contribution statements to social security institutions are kept for ten years (§ 165 Social Code Book VII (SGB VII)).
      Wage accounts - Wage accounts are kept for six years (§ 41 I 9 Income Tax Act (EStG)).
    - Applicant data - Kept for a maximum of six months from the receipt of rejection.
    - Working time records (for more than 8 hours on workdays) - Kept for two years (§ 16 II Working Time Act (ArbZG)).
    - Application documents (following online job advertisement) - Kept for three to a maximum of six months from the receipt of rejection (§ 26

Federal Data Protection Act (BDSG) n.F., § 15 IV General Act on Equal Treatment (AGG)).
    - Certificates of incapacity for work (AU) - Kept for up to five years (§ 6 I Act on the Compensation of Expenses (AAG)).
    - Documents on company pension schemes - Kept for 30 years (§ 18a Act to Improve Occupational Pensions (BetrAVG)).
    - Sickness data of employees - Kept for twelve months from the start of the illness, if the absence in a year does not exceed six weeks.
    - Documents on maternity protection - Kept for two years (§ 27 para. 5 Maternity Protection Act (MuSchG)).

Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).

- **Personnel file management:** Procedures required for the organisation, updating, and management of employee data and records (e.g., recording of basic personnel data, retention of employment contracts, certificates and attestations, updating data upon changes, compilation of documents for employee discussions, archiving of personnel files, compliance with data protection regulations); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).
- **Personnel development, performance evaluation, and staff appraisals:** Procedures required in the area of employee promotion and development, as well as in assessing their performance and during employee discussions (e.g., needs analysis for further training, planning and implementation of training measures, creation of performance evaluations, conducting goal-setting and feedback discussions, career planning and talent management, succession planning); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).
- **Obligation to Provide Data:** The person in charge informs the employees that the provision of their data is required. This is generally the case when the data are necessary for the establishment and execution of the employment relationship, or when their collection is mandated by law. The provision of data may also be required when employees assert claims or are entitled to claims. The implementation of these measures or fulfilment of services depends on the provision of such data (for example, providing data for the receipt of wages); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Publication and Disclosure of Employee Data:** The data of employees will only be published or disclosed to third parties if it is necessary for the performance

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

Job Application Process

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

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

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

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

Ereasure of data: In the event of a successful application, the data provided by the applicants may be further processed by us for the purposes of the employment relationship. Otherwise, if the application for a job offer is not successful, the applicant's data will be deleted. Applicants' data will also be deleted if an application is withdrawn, to which applicants are entitled at any time. Subject to a justified

revocation by the applicant, the deletion will take place at the latest after the expiry of a period of six months, so that we can answer any follow-up questions regarding the application and comply with our duty of proof under the regulations on equal treatment of applicants. Invoices for any reimbursement of travel expenses are archived in accordance with tax regulations.

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

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

Changes and Updates

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

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

Supervisory authority competent for us:

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
Postfach 3163
65021 Wiesbaden
Germany

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.

- **Artificial Intelligence (AI):** The purpose of processing data through Artificial Intelligence (AI) includes the automated analysis and processing of user data to identify patterns, make predictions, and improve the efficiency and quality of our services. This involves the collection, cleansing, and structuring of data, training and applying AI models, as well as the continuous review and optimisation of results, and is carried out exclusively with users' consent or based on legal authorisation grounds.
- **Contact data:** Contact details are essential information that enables communication with individuals or organizations. They include, among others, phone numbers, postal addresses, and email addresses, as well as means of communication like social media handles and instant messaging identifiers.
- **Content data:** Content data comprise information generated in the process of creating, editing, and publishing content of all types. This category of data may include texts, images, videos, audio files, and other multimedia content published across various platforms and media. Content data are not limited to the content itself but also include metadata providing information about the content, such as tags, descriptions, authorship details, and publication dates.
- **Contract data:** Contract data are specific details pertaining to the formalisation of an agreement between two or more parties. They document the terms under which services or products are provided, exchanged, or sold. This category of data is essential for managing and fulfilling contractual obligations and includes both the identification of the contracting parties and the specific terms and conditions of the agreement. Contract data may encompass the start and end dates of the contract, the nature of the agreed-upon services or products, pricing arrangements, payment terms, termination rights, extension options, and special conditions or clauses. They serve as the legal foundation for the relationship between the parties and are crucial for clarifying rights and duties, enforcing claims, and resolving disputes.
- **Controller:** "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Conversion tracking:** Conversion tracking is a method used to evaluate the effectiveness of marketing measures. For this purpose, a cookie is usually stored on the devices of the users within the websites on which the marketing measures take place and then called up again on the target website (e.g. we can thus trace whether the advertisements placed by us on other websites were successful).
- **Employees:** As employees, individuals are those who are engaged in an employment relationship, whether as staff, employees, or in similar positions. Employment refers to a legal relationship between an employer and an employee, established through an employment contract or agreement. It

entails the obligation of the employer to pay the employee remuneration while the employee performs their work. The employment relationship encompasses various stages, including establishment, where the employment contract is concluded, execution, where the employee carries out their work activities, and termination, when the employment relationship ends, whether through termination, mutual agreement, or otherwise. Employee data encompasses all information pertaining to these individuals within the context of their employment. This includes aspects such as personal identification details, identification numbers, salary and banking information, working hours, holiday entitlements, health data, and performance assessments.

- **Inventory data:** Inventory data encompass essential information required for the identification and management of contractual partners, user accounts, profiles, and similar assignments. These data may include, among others, personal and demographic details such as names, contact information (addresses, phone numbers, email addresses), birth dates, and specific identifiers (user IDs). Inventory data form the foundation for any formal interaction between individuals and services, facilities, or systems, by enabling unique assignment and communication.
- **Log data:** Protocol data, or log data, refer to information regarding events or activities that have been logged within a system or network. These data typically include details such as timestamps, IP addresses, user actions, error messages, and other specifics about the usage or operation of a system. Protocol data is often used for analyzing system issues, monitoring security, or generating performance reports.
- **Member data:** Membership data includes information related to the individuals who are part of an organization, association, online service, or other group. These data serve to manage memberships, facilitate communication, and provide services or benefits associated with membership. Membership data can include personal identification information, contact information, information on membership status and duration, payment of dues, participation in events and activities, as well as preferences and interests. They may also include data on the use of the organization's offerings. The collection and processing of this data occur in compliance with data protection regulations and serve both the administrative handling and the promotion of members' engagement and satisfaction.
- **Meta, communication and process data:** Meta-, communication, and procedural data are categories that contain information about how data is processed, transmitted, and managed. Meta-data, also known as data about data, include information that describes the context, origin, and structure of other data. They can include details about file size, creation date, the author of a document, and modification histories. Communication data capture the exchange of information between users across various channels, such as email traffic, call logs, messages in social networks, and chat histories, including the involved parties, timestamps, and transmission paths. Procedural data describe the processes and operations within systems or organisations, including workflow documentations, logs of transactions and activities, and audit logs used for tracking and verifying procedures.

- **Payment Data:** Payment data comprise all information necessary for processing payment transactions between buyers and sellers. This data is crucial for e-commerce, online banking, and any other form of financial transaction. It includes details such as credit card numbers, bank account information, payment amounts, transaction dates, verification numbers, and billing information. Payment data may also contain information on payment status, chargebacks, authorizations, and fees.
- **Performance and behavioural data:** Performance and behavioral data refer to information related to how individuals perform tasks or behave within a certain context, such as in an educational, work, or social setting. This data may include metrics such as productivity, efficiency, quality of work, attendance, and adherence to policies or procedures. Behavioral data could encompass interactions with colleagues, communication styles, decision-making processes, and responses to various situations. These types of data are often used for performance evaluations, training and development purposes, and decision-making within organizations.
- **Personal Data:** "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processing:** The term "processing" covers a wide range and practically every handling of data, be it collection, evaluation, storage, transmission or erasure.
- **Profiles with user-related information:** The processing of "profiles with user-related information", or "profiles" for short, includes any kind of automated processing of personal data that consists of using these personal data to analyse, evaluate or predict certain personal aspects relating to a natural person (depending on the type of profiling, this may include different information concerning demographics, behaviour and interests, such as interaction with websites and their content, etc.) (e.g. interests in certain content or products, click behaviour on a website or location). Cookies and web beacons are often used for profiling purposes.
- **Remarketing:** Remarketing" or "retargeting" is the term used, for example, to indicate for advertising purposes which products a user is interested in on a website in order to remind the user of these products on other websites, e.g. in advertisements.
- **Usage data:** Usage data refer to information that captures how users interact with digital products, services, or platforms. These data encompass a wide range of information that demonstrates how users utilise applications, which features they prefer, how long they spend on specific pages, and through what paths they navigate an application. Usage data can also include the frequency of use, timestamps of activities, IP addresses, device information, and location data. They are particularly valuable for analysing user behaviour, optimising user experiences, personalising content, and improving products or services. Furthermore, usage data play a crucial role in identifying trends, preferences, and potential problem areas within digital offerings

- **Web Analytics:** Web Analytics serves the evaluation of visitor traffic of online services and can determine their behavior or interests in certain information, such as content of websites. With the help of web analytics, website owners, for example, can recognize at what time visitors visit their website and what content they are interested in. This enables them, for example, to better adapt the content of their websites to the needs of their visitors. For the purposes of web analytics, pseudonymous cookies and web beacons are often used to recognize returning visitors and thus obtain more precise analyses of the use of an online service.