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: 29. January 2026

Table of contents

- Payment Procedure
- Provision of online services and web hosting
- Processing of Data within the Application (App)
- Purchase of applications via Appstores
- Registration, Login and User Account
- Contact and Inquiry Management
- Push notifications
- Artificial Intelligence (AI)
- Cloud Services
- Newsletter and Electronic Communications
- Commercial communication by E-Mail, Postal Mail, Fax or Telephone
- Profiles in Social Networks (Social Media)
- Plugins and embedded functions and content
- Management, Organization and Utilities
- Processing of data in the context of employment relationships
- Changes and Updates
- Terminology and Definitions

Controller

peakleap GmbH
PO Box 600606
81206 Munich
Germany

Authorised Representatives: Anja Kreutzahler

E-mail address: contact@fitiprm.com

Legal Notice: www.fitiprm.com/impressum

Contact information of the Data Protection Officer

Sabine Pohl, contact@fitiprm.com

Overview of processing operations

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

Categories of Processed Data

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

Categories of Data Subjects

- Service recipients and clients.
- Employees.
- Prospective customers.

- Communication partner.
- Users.
- Business and contractual partners.
- Third parties.
- Customers.

Purposes of Processing

- Provision of contractual services and fulfillment of contractual obligations.
- Communication.
- Security measures.
- Direct marketing.
- Web Analytics.
- Office and organisational procedures.
- Conversion tracking.
- Clicktracking.
- Organisational and Administrative Procedures.
- Feedback.
- Marketing.
- Profiles with user-related information.
- Provision of our online services and usability.
- Establishment and execution of employment relationships.
- Information technology infrastructure.
- Financial and Payment Management.
- Public relations.
- Sales promotion.
- Business processes and management procedures.
- Artificial Intelligence (AI).

Relevant legal bases

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

- **Consent (Article 6 (1) (a) GDPR)** - The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- **Performance of a contract and prior requests (Article 6 (1) (b) GDPR)** - Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- **Compliance with a legal obligation (Article 6 (1) (c) GDPR)** - Processing is necessary for compliance with a legal obligation to which the controller is subject.
- **Legitimate Interests (Article 6 (1) (f) GDPR)** - the processing is necessary for the protection of the legitimate interests of the controller or a third party, provided that the interests, fundamental rights, and freedoms of the data subject, which require the protection of personal data, do not prevail.
- **Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR)** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.

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

Relevant legal basis according to the Swiss Data Protection Act: If you are located in Switzerland, we process your data based on the Federal Act on Data Protection (referred to as "Swiss DPA"). Unlike the GDPR, for instance, the Swiss

DPA does not generally require that a legal basis for processing personal data be stated and that the processing of personal data is conducted in good faith, lawfully and proportionately (Art. 6 para. 1 and 2 of the Swiss DPA). Furthermore, we only collect personal data for a specific purpose recognizable to the data subject and process it only in a manner compatible with this purpose (Art. 6 para. 3 of the Swiss DPA).

Reference to the applicability of the GDPR and the Swiss DPA: 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.

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

Securing online connections through TLS/SSL encryption technology (HTTPS): To protect the data of users transmitted via our online services from unauthorized access, we employ TLS/SSL encryption technology. Secure Sockets Layer (SSL) and

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

Transmission of Personal Data

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

Data 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.

Disclosure of Personal Data Abroad: In accordance with the Swiss Data Protection Act (Swiss DPA), we only disclose personal data abroad when an appropriate level of protection for the affected persons is ensured (Art. 16 Swiss DPA). If the Federal Council has not determined an adequate level of protection (list of states: https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales/anerkennung-staaten.html), we implement alternative security measures.

For data transfers to the USA, we primarily rely on the Data Privacy Framework (DPF), which has been recognized as a secure legal framework by Switzerland's adequacy decision of September 15, 2024. Additionally, we have concluded Standard Data Protection Clauses with the respective providers, which have been approved by the Federal Data Protection and Information Commissioner (FDPIC) and establish contractual obligations to protect your data.

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

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

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

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

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

General Information on Data Retention and Deletion

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

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

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

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

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

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

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

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

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

Data Retention and Deletion: The following general retention and archiving periods apply under Swiss law:

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

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

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

Rights of Data Subjects

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

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

format in accordance with the legal requirements, or to request its transmission to another controller.

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

Rights of the data subjects under the Swiss DPA:

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

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

Business services

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

We process this data in order to fulfill our contractual obligations. These include, in particular, the obligations to provide the agreed services, any update obligations and remedies in the event of warranty and other service disruptions. In addition, we process the data to protect our rights and for the purpose of administrative tasks associated with these obligations and company organization. Furthermore, we

process the data on the basis of our legitimate interests in proper and economical business management as well as security measures to protect our contractual partners and our business operations from misuse, endangerment of their data, secrets, information and rights (e.g. for the involvement of telecommunications, transport and other auxiliary services as well as subcontractors, banks, tax and legal advisors, payment service providers or tax authorities). Within the framework of applicable law, we only disclose the data of contractual partners to third parties to the extent that this is necessary for the aforementioned purposes or to fulfill legal obligations. Contractual partners will be informed about further forms of processing, e.g. for marketing purposes, within the scope of this privacy policy.

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

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Contract data (e.g. contract object, duration, customer category); 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). Log data (e.g. log files concerning logins or data retrieval or access times.).
- **Data subjects:** Service recipients and clients; Prospective customers; Business and contractual partners; Communication partner (Recipients of e-mails, letters, etc.). Customers.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Communication; Office and organisational

procedures; Organisational and Administrative Procedures. Business processes and management procedures.

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

Further information on processing methods, procedures and services used:

- **Software and Platform Services:** We process the data of our users, registered and any test users (hereinafter uniformly referred to as "users") in order to provide them with our contractual services and on the basis of legitimate interests to ensure the security of our offer and to develop it further. The required details are identified as such within the context of the conclusion of the agreement, order or comparable contract and include the details required for the provision of services and invoicing as well as contact information in order to be able to hold any further consultations; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).
- **Customer Management and Customer Relationship Management (CRM):** Processes required in the context of customer management and Customer Relationship Management (CRM) include customer acquisition in compliance with data protection regulations, measures to promote customer retention and loyalty, effective customer communication, complaint management and customer service with consideration of data protection, data management and analysis to support the customer relationship, management of CRM systems, secure account management, customer segmentation and targeting; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Project and Development Services:** We process the data of our customers and clients (hereinafter uniformly referred to as "customers") in order to enable them to select, acquire or commission the selected services or works as well as associated activities and to pay for and make available such services or works or to perform such services or works.

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

Business processes and operations

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

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

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties). Log data (e.g. log files concerning logins or data retrieval or access times.).
- **Data subjects:** Service recipients and clients; Prospective customers; Communication partner (Recipients of e-mails, letters, etc.); Business and contractual partners; Customers; Third parties. Employees (e.g. employees, job applicants, temporary workers, and other personnel.).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Business processes and management procedures; Security measures; Provision of our online services and usability; Communication; Information technology

infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)). Financial and Payment Management.

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

Further information on processing methods, procedures and services used:

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

(Article 6 (1) (f) GDPR).

- **General Payment Transactions:** Procedures required for carrying out payment transactions, monitoring bank accounts, and controlling payment flows (e.g., creation and verification of transfers, processing of direct debit transactions, checking of account statements, monitoring of incoming and outgoing payments, management of chargebacks, account reconciliation, cash management); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Use of online platforms for listing and sales purposes

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

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

Further information on processing methods, procedures and services used:

- **Apple App Store:** App and software distribution platform; **Service provider**: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Legitimate

Interests (Article 6 (1) (f) GDPR); **Website:** https://www.apple.com/app-store/. **Privacy Policy:** https://www.apple.com/privacy/privacy-policy/.

- **Google Play:** App and software distribution platform; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://play.google.com/store/apps?hl=en. **Privacy Policy:** https://policies.google.com/privacy.

Providers and services used in the course of business

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Service recipients and clients; Prospective customers; Business and contractual partners; Employees (e.g. employees, job applicants, temporary workers, and other personnel.); Users (e.g. website visitors, users of online services); Third parties. Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Business processes and management procedures; Organisational and Administrative Procedures; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)); Direct marketing (e.g. by e-mail or postal); Web Analytics (e.g. access statistics, recognition of returning visitors); Conversion tracking (Measurement of the effectiveness of marketing activities); Clicktracking; Marketing; Profiles with user-related information (Creating user profiles);

Provision of our online services and usability. 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). Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Further information on processing methods, procedures and services used:

- **DATEV:** Software for accounting, communication with tax advisors as well as authorities and including document storage; **Service provider**: DATEV eG, Paumgartnerstr. 6 - 14, 90429 Nürnberg, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.datev.de/web/de/mydatev/online-anwendungen/; **Privacy Policy:** https://www.datev.de/web/de/m/ueber-datev/datenschutz/. **Data Processing Agreement:** Provided by the service provider.
- **sevDesk:** Online software for invoicing, accounting, banking and tax filing with document storage; **Service provider**: sevDesk GmbH, Hauptstraße 115, 77652 Offenburg, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://sevdesk.com/; **Privacy Policy:** https://sevdesk.com/privacy-policy. **Data Processing Agreement:** https://sevdesk.com/security-data-protection.
- **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).
- **Apple Pay:** Payment services provider; **Service provider**: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://www.apple.com/apple-pay/. **Privacy Policy:** https://www.apple.com/legal/privacy/en-ww/.
- **Google Pay:** Payment services provider; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://pay.google.com/intl/en_uk/about/. **Privacy Policy:** https://policies.google.com/privacy.
- **Supabase:** Cloud-based platform that provides developers with a set of tools for building and scaling applications, including authentication (secure way to add authentication to the application, with support for multiple authentication providers, passwordless sign-in, social login, and multi-factor authentication),

real-time database, APIs (interfaces with built-in support for access control, filtering, sorting, and pagination as well as serverless functions), storage (file storage services in the cloud with support for object and relational storage, image resizing, and server-side rendering), and analytics (analysis services for measuring user behavior and application usage, with support for custom event tracking, cohort analysis, and user segmentation, as well as integration with other analytics platforms); **Service provider**: Supabase, Inc., 970 Toa Payoh North #07-04, Singapore 318992; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://supabase.com/; **Privacy Policy:** https://supabase.com/privacy; **Data Processing Agreement:** https://supabase.com/legal/dpa. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (https://supabase.com/legal/dpa), Switzerland - Standard Contractual Clauses (https://supabase.com/legal/dpa).

- **Resend:** Sending, receiving, and managing emails; tools for analyzing and optimizing email campaigns; **Service provider**: Plus Five Five, Inc., 2261 Market Street #5039, San Francisco, CA 94114, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://resend.com/. **Privacy Policy:** https://resend.com/legal/privacy-policy.

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

- **GitHub:** Platform for version control of software projects. Developers are enabled to upload their code to repositories and track changes, as well as use tools for project management in software development; **Service provider**: GitHub B.V., Netherlands, https://support.github.com/contact/privacy; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://github.com. **Privacy Policy:** https://docs.github.com/en/site-policy/privacy-policies/github-general-privacy-statement.

- **Microsoft Azure OpenAI Service:** Interface access (so-called "API") to AI-based services designed to understand and generate natural language and related inputs, analyze information, and make predictions ("AI", i.e., "Artificial Intelligence", is to be understood in the legal sense of the term as applicable). The provision of AI services includes the processing (including collection, storage, organization, and structuring) of personal data as part of a machine learning process based on natural language; conducting activities to verify or maintain the quality of the services; identifying and correcting errors that

impair the existing intended functionality, as well as supporting efforts to ensure the security and integrity of the AI services; **Service provider**: Microsoft Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://azure.microsoft.com/de-de/products/ai-foundry/models/openai/; **Privacy Policy:** https://www.microsoft.com/en-us/privacy/privacystatement; **Data Processing Agreement:** https://azure.microsoft.com/en-us/support/legal/. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://azure.microsoft.com/de-de/support/legal/), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://azure.microsoft.com/de-de/support/legal/).

- **RevenueCat :** Provision of technical and organizational infrastructure for the creation as well as administration and transaction handling of in-app purchases and subscriptions; **Service provider**: Revenuecat, Inc., 1032 E Brandon Blvd #3003 Brandon, Fl 33511USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.revenuecat.com/. **Privacy Policy:** https://www.revenuecat.com/privacy/.
- **Apple App Store:** App and software distribution platform; **Service provider**: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.apple.com/app-store/. **Privacy Policy:** https://www.apple.com/privacy/privacy-policy/.
- **Google Play:** App and software distribution platform; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://play.google.com/store/apps?hl=en. **Privacy Policy:** https://policies.google.com/privacy.
- **Upstash:** Cloud-based database service used for storing, caching, and processing application data, including performance optimization, session handling, and technical operations of the app.
  Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); **Service provider**: Upstash, Inc., 548 Market Street, PMB 97212, San Francisco, CA 94104, USA; **Website:** https://upstash.com/. **Privacy Policy:** https://upstash.com/trust/privacy.pdf.
- **Replit:** Development and hosting platform used for building, running, and maintaining software applications. Processing of technical usage data and project-related data for development, testing, and operation of the app.
  Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); **Service provider**: Replit, Inc., 767 Bryant Street, Suite 100, San Francisco, CA 94107, USA; **Website:** https://replit.com/. **Privacy Policy:** https://replit.com/privacy-policy.

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

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

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **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://policies.google.com/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.de/datenschutz.

Provision of online services and web hosting

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

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Log data (e.g. log files concerning logins or data retrieval or access times.). Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.).
- **Data subjects:** Users (e.g. website visitors, users of online services). Business and contractual partners.
- **Purposes of processing:** Provision of our online services and usability; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)). Security measures.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

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

file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.

- **Content-Delivery-Network:** We use a so-called "Content Delivery Network" (CDN). A CDN is a service with whose help contents of our online services, in particular large media files, such as graphics or scripts, can be delivered faster and more securely with the help of regionally distributed servers connected via the Internet; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **GitHub:** Platform for version control of software projects. Developers are enabled to upload their code to repositories and track changes, as well as use tools for project management in software development; **Service provider**: GitHub B.V., Netherlands, https://support.github.com/contact/privacy; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://github.com. **Privacy Policy:** https://docs.github.com/en/site-policy/privacy-policies/github-general-privacy-statement.
- **Vercel:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities) as well as development environment; **Service provider**: Vercel Inc., 340 S Lemon Ave #4133, Walnut, CA 91789, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://vercel.com; **Privacy Policy:** https://vercel.com/legal/privacy-policy; **Data Processing Agreement:** https://vercel.com/legal/dpa. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (https://vercel.com/legal/dpa), Switzerland - Standard Contractual Clauses (https://vercel.com/legal/dpa).
- **JSDelivr:** Content Delivery Network (CDN) that helps deliver media and files quickly and efficiently, especially under heavy load; **Service provider**: ProspectOne, Królewska 65A/1, 30-081, Kraków, Poland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.jsdelivr.com. **Privacy Policy:** https://www.jsdelivr.com/terms/privacy-policy-jsdelivr-net.

Processing of Data within the Application (App)

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

information in this privacy policy with regard to the processing of user data.

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

Information on the functions of the application:

- The app enables users to upload and manage user-generated content within a personal asset area.

- The camera function is used to capture images and store them directly as files in the asset folder. Access is granted only with explicit user consent and solely for this purpose.

- The microphone function is used for voice input features, including dictating notes, interacting with AI features, and entering contact information. There is no continuous or automatic audio recording.

- Location data is used exclusively for entering and processing address information. There is no continuous location tracking and no creation of movement profiles.

- Access to contacts stored on the device is used for managing contact data, maintaining relationships, and providing reminder features for contact follow-ups. Access is granted only with user 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); Payment Data (e.g. bank details, invoices, payment history); Contract data (e.g. contract object, duration, customer category); Images and/ or video recordings (e.g. photographs or video recordings of a person); Audio recordings. Location data (Information on the geographical position of a device or person).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Security measures. Provision of our online services

and usability.

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

Further information on processing methods, procedures and services used:

- **Commercial use:** We process the data of the users of our application, registered and any test users (hereinafter uniformly referred to as "users") in order to provide them with our contractual services and on the basis of legitimate interests to ensure the security of our application and to develop it further. The required details are identified as such within the scope of the conclusion of a contract for the use of the application, the conclusion of an order, an order or a comparable contract and may include the details required for the provision of services and any invoicing as well as contact information in order to be able to hold any consultations; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).
- **Storage of the universally unique identifier (UUID):** The application stores a so-called Universally Unique Identifier (UUID) for the purpose of analysing the use and functionality of the application and storing the user's settings. This identifier is generated when the application is installed (but is not connected to the device, so no device ID in this sense), remains stored between the start of the application and its updates and is deleted when users remove the application from their device.
- **Device authorizations for access to functions and data:** The use of certain functions of our application may require access to the camera and the stored recordings of the users. By default, these authorizations must be granted by the user and can be revoked at any time in the settings of the respective devices. The exact procedure for controlling app permissions may depend on the user's device and software. Users can contact us if they require further explanation. We would like to point out that the refusal or revocation of the respective authorizations can affect the functionality of our application.
- **Accessing the camera and stored recordings:** In the course of using our application, image and/or video recordings (whereby audio recordings are also included) of the users (and of other persons captured by the recordings) are processed by accessing the camera functions or stored recordings. Access to the camera functions or stored recordings requires an authorization by the user that can be withdrawn at any time. The processing of the image and/or video recordings serves only to provide the respective functionality of our application, according to its description to the users or the typical and expectable functionality of the application.

- **Use of the microphone functions:** The use of certain functions of our application may require access to the camera and the stored recordings of the users. By default, these authorizations must be granted by the user and can be revoked at any time in the settings of the respective devices. The exact procedure for controlling app permissions may depend on the user's device and software. Users can contact us if they require further explanation. We would like to point out that the refusal or revocation of the respective authorizations can affect the functionality of our application.
- **Processing of stored contacts:** When using our application, the contact information of persons (e.g. name, e-mail address and telephone number) stored in the contact directory of the device is processed. The use of the contact information requires user authorization, which can be withdrawn at any time. The use of the contact information serves only to provide the respective functionality of our application, according to its description to the users, or its typical and expectable functionality. Users are advised that permission to process the contact information must be granted and, especially in the case of natural persons, their consent or a legal permission is required.
- **Use of contact data for contact matching purposes:** The data of contacts stored in the contact directory of the device can be used to check whether these contacts also use our application. For this purpose, the contact data of the respective contacts (which includes the telephone number and e-mail address) are uploaded to our server and used only for the purpose of matching.
- **Processing of location data:** Within the course of using our application, the location data collected by the device used or otherwise entered by the user are processed. The use of the location data requires an authorization of the users, which can be revoked at any time. The use of the location data serves only to provide the respective functionality of our application, according to its description to the users or its typical and expectable functionality.

Purchase of applications via Appstores

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Contract data (e.g. contract object,

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

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

Further information on processing methods, procedures and services used:

- **Apple App Store:** App and software distribution platform; **Service provider**: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.apple.com/app-store/. **Privacy Policy:** https://www.apple.com/privacy/privacy-policy/.
- **Google Play:** App and software distribution platform; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://play.google.com/store/apps?hl=en. **Privacy Policy:** https://policies.google.com/privacy.

Registration, Login and User Account

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

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

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

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

Further information on processing methods, procedures and services used:

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

Contact and Inquiry Management

When contacting us (e.g. via mail, contact form, e-mail, telephone or via social

media) as well as in the context of existing user and business relationships, the information of the inquiring persons is processed to the extent necessary to respond to the contact requests and any requested measures.

- **Processed data types:** 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). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.); Users (e.g. website visitors, users of online services). Business and contractual partners.
- **Purposes of processing:** Communication; Organisational and Administrative Procedures; Feedback (e.g. collecting feedback via online form). Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Further information on processing methods, procedures and services used:

- **Contact form:** Upon contacting us via our contact form, email, or other means of communication, we process the personal data transmitted to us for the purpose of responding to and handling the respective matter. This typically includes details such as name, contact information, and possibly additional information provided to us that is necessary for appropriate processing. We use this data exclusively for the stated purpose of contact and communication; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Outlook:** Sending and receiving messages, storing contacts, and using filtering and protection functions (spam, viruses). Contact data (name, email address), content data (messages, attachments), and metadata are processed for the purposes of efficiency and productivity improvements, cost-efficiency, flexibility, mobility, and integration of the email software. Retention is according to the specified guidelines, typically without automatic deletion; mailboxes are generally removed 30 days after departure. 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-365/outlook/email-and-calendar-software-microsoft-outlook. **Privacy Policy:** https://www.microsoft.com/en-us/privacy/privacystatement.

Push notifications

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

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

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

Contents:

Reminders related to contact management, networking activities, tasks, and functional notifications regarding app usage.

Our settings and options to unsubscribe:

Push notifications can be disabled at any time in the device settings or within the app settings.

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Communication. Provision of our online services and usability.

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

Artificial Intelligence (AI)

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

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

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

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

- **Processed data types:** Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).

- **Data subjects:** Users (e.g. website visitors, users of online services). Third parties.
- **Purposes of processing:** Artificial Intelligence (AI).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Microsoft Azure OpenAI Service:** Interface access (so-called "API") to AI-based services designed to understand and generate natural language and related inputs, analyze information, and make predictions ("AI", i.e., "Artificial Intelligence", is to be understood in the legal sense of the term as applicable). The provision of AI services includes the processing (including collection, storage, organization, and structuring) of personal data as part of a machine learning process based on natural language; conducting activities to verify or maintain the quality of the services; identifying and correcting errors that impair the existing intended functionality, as well as supporting efforts to ensure the security and integrity of the AI services; **Service provider**: Microsoft Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://azure.microsoft.com/de-de/products/ai-foundry/models/openai/; **Privacy Policy:** https://www.microsoft.com/en-us/privacy/privacystatement; **Data Processing Agreement:** https://azure.microsoft.com/en-us/support/legal/. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://azure.microsoft.com/de-de/support/legal/), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://azure.microsoft.com/de-de/support/legal/).

Cloud Services

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

Within this framework, personal data may be processed and stored on the provider's servers insofar as this data is part of communication processes with us or is otherwise processed by us in accordance with this privacy policy. This data may include in particular master data and contact data of data subjects, data on

processes, contracts, other proceedings and their contents. Cloud service providers also process usage data and metadata that they use for security and service optimization purposes.

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features).
- **Data subjects:** Prospective customers; Communication partner (Recipients of e-mails, letters, etc.). Business and contractual partners.
- **Purposes of processing:** Office and organisational procedures. Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **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 our app, services, features, product updates, and guidance on how to use and benefit from the application.

- **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). Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.); Service recipients and clients; Employees (e.g. employees, job applicants, temporary workers, and other personnel.). Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Direct marketing (e.g. by e-mail or postal); Provision of contractual services and fulfillment of contractual obligations. Office and organisational procedures.
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).
- **Opt-Out:** You can cancel the receipt of our newsletter at any time, i.e. revoke your consent or object to further receipt. You will find a link to cancel the newsletter either at the end of each newsletter or you can otherwise use one of the contact options listed above, preferably e-mail.

Further information on processing methods, procedures and services used:

- **Measurement of opening rates and click rates:** The newsletters contain a so-called "web beacons", which is a pixel-sized file that is retrieved from our server, or the server of the dispatch service provider if one is used, when the newsletter is opened. In the course of this retrieval, technical information such as details about the browser and your system, as well as your IP address and the time of access are collected. This information is used to technically improve our newsletter based on technical data or target audiences and their reading behavior, which can be determined by their access locations (identifiable by IP address) or access times. This analysis also includes determining whether and when newsletters are opened and which links are clicked. The information is assigned to individual newsletter recipients and stored in their profiles until deletion. The evaluations serve to recognize the reading habits of our users and adjust our content to them or send different content according to the interests of our users. The measurement of opening and click rates, as well as the storage of the measurement results in user profiles and their further processing, are based on user consent. Unfortunately, it is not possible to revoke success measurement separately; in this case, the entire newsletter subscription must be cancelled or objected to.

In that case, stored profile information will be deleted; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).

- **Order process reminder emails:** When users cancel an order process, we can send them a notice of the cancellation and remind them to continue. This function can be useful, for example, if the purchase process could not be continued due to a browser crash, oversight or forgetting. The dispatch is based on consent, which users can object to at any time; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).
- **monday.com:** Project management - organization and administration of teams, groups, workflows, projects and processes; **Service provider**: monday.com ltd, 6 Yitzhak Sadeh Street, Tel Aviv 6777506, Israel; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://monday.com; **Privacy Policy:** https://monday.com/l/privacy/privacy-policy/; **Data Processing Agreement:** https://monday.com/l/privacy/dpa/. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (https://monday.com/l/privacy/https-monday-com-l-scc-controller-to-processor/ (Controller to Processors), https://monday.com/l/privacy/https-monday-com-l-scc-processor-to-processor/ (Processor to Processor)), Switzerland - Standard Contractual Clauses (https://monday.com/l/privacy/https-monday-com-l-scc-controller-to-processor/ (Controller to Processors), https://monday.com/l/privacy/https-monday-com-l-scc-processor-to-processor/ (Processor to Processor)).

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

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

The recipients have the right to withdraw their consent at any time or to object to the advertising communication at any time free of charge using the contact options mentioned above.

After revocation or objection, we store the data required to prove the past authorization to contact or send up to three years from the end of the year of revocation or objection on the basis of our legitimate interests. The processing of this data is limited to the purpose of a possible defense against claims. Based on the legitimate interest to permanently observe the revocation, respectively objection of the users, we further store the data necessary to avoid a renewed contact (e.g.

depending on the communication channel, the e-mail address, telephone number, name).

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). 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.); Service recipients and clients; Employees (e.g. employees, job applicants, temporary workers, and other personnel.). Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Direct marketing (e.g. by e-mail or postal); Marketing; Sales promotion; Provision of contractual services and fulfillment of contractual obligations. Office and organisational procedures.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **monday.com:** Project management - organization and administration of teams, groups, workflows, projects and processes; **Service provider**: monday.com ltd, 6 Yitzhak Sadeh Street, Tel Aviv 6777506, Israel; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://monday.com; **Privacy Policy:** https://monday.com/l/privacy/privacy-policy/; **Data Processing Agreement:** https://monday.com/l/privacy/dpa/. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (https://monday.com/l/privacy/https-monday-com-l-scc-controller-to-processor/ (Controller to Processors), https://monday.com/l/privacy/https-monday-com-l-scc-processor-to-processor/ (Processor to Processor)), Switzerland - Standard Contractual Clauses (https://monday.com/l/privacy/https-monday-com-l-scc-controller-to-processor/ (Controller to Processors), https://monday.com/l/privacy/https-monday-com-l-scc-processor-to-processor/ (Processor to Processor)).

Profiles in Social Networks (Social Media)

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

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

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

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

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

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

Further information on processing methods, procedures and services used:

- **Instagram:** Social network, allows the sharing of photos and videos, commenting on and favouriting posts, messaging, subscribing to profiles and pages; **Service provider**: Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.instagram.com; **Privacy Policy:** https://privacycenter.instagram.com/policy/. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Data Privacy Framework (DPF).
- **LinkedIn:** Social network - We are jointly responsible with LinkedIn Ireland Unlimited Company for the collection (but not the further processing) of visitor data, which is used to create "Page Insights" (statistics) for our LinkedIn profiles. This data includes information about the types of content users view or interact with, as well as the actions they take. It also includes details about the devices used, such as IP addresses, operating systems, browser types, language settings, and cookie data, as well as profile details of users, such as job function, country, industry, seniority, company size, and employment status. Privacy information regarding the processing of user data by LinkedIn can be found in LinkedIn's privacy policy: https://www.linkedin.com/legal/privacy-policy.
  We have entered into a special agreement with LinkedIn Ireland ("Page Insights Joint Controller Addendum," https://legal.linkedin.com/pages-joint-controller-addendum), which specifically regulates the security measures LinkedIn must comply with and in which LinkedIn has agreed to fulfill the rights of data subjects (i.e., users can, for example, direct requests for information or deletion directly to LinkedIn). The rights of users (particularly the right to information, deletion, objection, and to lodge a complaint with the competent supervisory authority) are not restricted by our agreements with LinkedIn. The joint responsibility is limited to the collection of data and its transmission to LinkedIn Ireland Unlimited Company, a company based in the EU. Further processing of the data is the sole responsibility of LinkedIn Ireland Unlimited Company, particularly concerning the transfer of data to the parent company LinkedIn Corporation in the USA; **Service provider**: LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.linkedin.com; **Privacy Policy:** https://www.linkedin.com/legal/privacy-policy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://legal.linkedin.com/dpa), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://legal.linkedin.com/dpa). **Opt-Out:** https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out.
- **YouTube:** Social network and video platform; **Service provider**: Google

Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Privacy Policy:** https://policies.google.com/privacy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Data Privacy Framework (DPF). **Opt-Out:** https://myadcenter.google.com/personalizationoff.

Plugins and embedded functions and content

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

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

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

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

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); 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:** Communication partner (Recipients of e-mails, letters, etc.); Users (e.g. website visitors, users of online services); Service recipients and clients; Employees (e.g. employees, job applicants, temporary workers, and other personnel.); Business and contractual partners. Third parties.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Organisational and Administrative Procedures; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)). Business processes and management procedures.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Jira:** Web application for error management, troubleshooting and operational project management; **Service provider**: Atlassian Pty Ltd, 350 Bush Street, Floor 13, San Francisco, CA 94104, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.atlassian.com/de/software/jira;

Privacy Policy: https://www.atlassian.com/legal/privacy-policy; **Data Processing Agreement:** https://www.atlassian.com/legal/data-processing-addendum. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.atlassian.com/legal/data-processing-addendum#europe-uk-switzerland), Switzerland - Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.atlassian.com/legal/data-processing-addendum#europe-uk-switzerland).

- **monday.com:** Project management - organization and administration of teams, groups, workflows, projects and processes; **Service provider**: monday.com ltd, 6 Yitzhak Sadeh Street, Tel Aviv 6777506, Israel; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://monday.com; **Privacy Policy:** https://monday.com/l/privacy/privacy-policy/; **Data Processing Agreement:** https://monday.com/l/privacy/dpa/. **Basis for third-country transfers:** EEA - Standard Contractual Clauses (https://monday.com/l/privacy/https-monday-com-l-scc-controller-to-processor/ (Controller to Processors), https://monday.com/l/privacy/https-monday-com-l-scc-processor-to-processor/ (Processor to Processor)), Switzerland - Standard Contractual Clauses (https://monday.com/l/privacy/https-monday-com-l-scc-controller-to-processor/ (Controller to Processors), https://monday.com/l/privacy/https-monday-com-l-scc-processor-to-processor/ (Processor to Processor)).

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

- **Microsoft 365 Outlook:** The use of email and calendar functions for communication and organisation of meetings involves processing contact data (name, email address), content data (messages, attachments, meeting content) and metadata for purposes and interests in efficiency and productivity improvements, cost efficiency, flexibility, mobility, enhanced communication, and integration with M365. The retention of emails and calendar entries is determined by policies set by the administrator or user; by default, there is no automatic deletion. Mailboxes and calendars are generally removed 30 days after departure. 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).

- **Microsoft Sharepoint:** Support for collaboration through storage and access management for documents, spreadsheets, presentations, among others. Content data (files) and contact data (name, email address) are processed for purposes and out of interest in efficiency and productivity improvements, cost efficiency, flexibility, mobility, integration with M365, and enhanced collaboration. Retention is determined by the business function of the content; SharePoint pages must be renewed every 180 days; otherwise, content will be deleted. 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).

- **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).

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).

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

Further information on processing methods, procedures and services used:

- **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).

Changes and Updates

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

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

Terminology and Definitions

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

- **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.
- **Clicktracking:** Clicktracking allows users to keep track of their movements within an entire website. Since the results of these tests are more accurate if the interaction of the users can be followed over a certain period of time (e.g. if a user likes to return), cookies are usually stored on the computers of the users for these test purposes.
- **Contact data:** Contact details are essential information that enables communication with individuals or organizations. They include, among others, phone numbers, postal addresses, and email addresses, as well as means of communication like social media handles and instant messaging identifiers.
- **Content data:** Content data comprise information generated in the process of creating, editing, and publishing content of all types. This category of data may include texts, images, videos, audio files, and other multimedia content published across various platforms and media. Content data are not limited to the content itself but also include metadata providing information about the content, such as tags, descriptions, authorship details, and publication dates.
- **Contract data:** Contract data are specific details pertaining to the formalisation of an agreement between two or more parties. They document the terms under which services or products are provided, exchanged, or sold. This category of data is essential for managing and fulfilling contractual obligations and includes both the identification of the contracting parties and the specific terms and conditions of the agreement. Contract data may encompass the start and end dates of the contract, the nature of the agreed-upon services or products, pricing arrangements, payment terms, termination rights, extension options, and special conditions or clauses. They serve as the legal foundation for the relationship between the parties and are crucial for clarifying rights and duties, enforcing claims, and resolving disputes.
- **Controller:** "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the

purposes and means of the processing of personal data.

- **Conversion tracking:** Conversion tracking is a method used to evaluate the effectiveness of marketing measures. For this purpose, a cookie is usually stored on the devices of the users within the websites on which the marketing measures take place and then called up again on the target website (e.g. we can thus trace whether the advertisements placed by us on other websites were successful).
- **Employees:** As employees, individuals are those who are engaged in an employment relationship, whether as staff, employees, or in similar positions. Employment refers to a legal relationship between an employer and an employee, established through an employment contract or agreement. It entails the obligation of the employer to pay the employee remuneration while the employee performs their work. The employment relationship encompasses various stages, including establishment, where the employment contract is concluded, execution, where the employee carries out their work activities, and termination, when the employment relationship ends, whether through termination, mutual agreement, or otherwise. Employee data encompasses all information pertaining to these individuals within the context of their employment. This includes aspects such as personal identification details, identification numbers, salary and banking information, working hours, holiday entitlements, health data, and performance assessments.
- **Inventory data:** Inventory data encompass essential information required for the identification and management of contractual partners, user accounts, profiles, and similar assignments. These data may include, among others, personal and demographic details such as names, contact information (addresses, phone numbers, email addresses), birth dates, and specific identifiers (user IDs). Inventory data form the foundation for any formal interaction between individuals and services, facilities, or systems, by enabling unique assignment and communication.
- **Location data:** Location data is created when a mobile device (or another device with the technical requirements for a location determination) connects to a radio cell, a WLAN or similar technical means and functions of location determination. Location data serve to indicate the geographically determinable position of the earth at which the respective device is located. Location data can be used, for example, to display map functions or other information dependent on a location.
- **Log data:** Protocol data, or log data, refer to information regarding events or activities that have been logged within a system or network. These data typically include details such as timestamps, IP addresses, user actions, error messages, and other specifics about the usage or operation of a system. Protocol data is often used for analyzing system issues, monitoring security, or generating performance reports.

- **Meta, communication and process data:** Meta-, communication, and procedural data are categories that contain information about how data is processed, transmitted, and managed. Meta-data, also known as data about data, include information that describes the context, origin, and structure of other data. They can include details about file size, creation date, the author of a document, and modification histories. Communication data capture the exchange of information between users across various channels, such as email traffic, call logs, messages in social networks, and chat histories, including the involved parties, timestamps, and transmission paths. Procedural data describe the processes and operations within systems or organisations, including workflow documentations, logs of transactions and activities, and audit logs used for tracking and verifying procedures.
- **Payment Data:** Payment data comprise all information necessary for processing payment transactions between buyers and sellers. This data is crucial for e-commerce, online banking, and any other form of financial transaction. It includes details such as credit card numbers, bank account information, payment amounts, transaction dates, verification numbers, and billing information. Payment data may also contain information on payment status, chargebacks, authorizations, and fees.
- **Performance and behavioural data:** Performance and behavioral data refer to information related to how individuals perform tasks or behave within a certain context, such as in an educational, work, or social setting. This data may include metrics such as productivity, efficiency, quality of work, attendance, and adherence to policies or procedures. Behavioral data could encompass interactions with colleagues, communication styles, decision-making processes, and responses to various situations. These types of data are often used for performance evaluations, training and development purposes, and decision-making within organizations.
- **Personal Data:** "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processing:** The term "processing" covers a wide range and practically every handling of data, be it collection, evaluation, storage, transmission or erasure.
- **Profiles with user-related information:** The processing of "profiles with user-related information", or "profiles" for short, includes any kind of automated processing of personal data that consists of using these personal data to analyse, evaluate or predict certain personal aspects relating to a natural person (depending on the type of profiling, this may include different information concerning demographics, behaviour and interests, such as

interaction with websites and their content, etc.) (e.g. interests in certain content or products, click behaviour on a website or location). Cookies and web beacons are often used for profiling purposes.

- **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.