

# 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.

## Preamble

With the following privacy policy we would like to inform you about the types of personal data (hereinafter also referred to as "data") we process, for which purposes and to what extent in the context of providing our application.

The terms used are not gender-specific.

Last Update: 31. January 2024

## Table of contents

- Preamble
- Preamble
- Controller
- Overview of processing operations
- Relevant legal bases
- Security Precautions
- Transmission of Personal Data
- International data transfers

- Erasure of data
- Use of Cookies
- Business services
- Providers and services used in the course of business
- Provision of online services and web hosting
- Single Sign-on Authentication
- Contact and Inquiry Management
- Video Conferences, Online Meetings, Webinars and Screen-Sharing
- Cloud Services
- Management, Organization and Utilities
- Changes and Updates to the Privacy Policy

## **Controller**

Marina Breytman  
Erfurter Str. 1  
36093 Künzell  
Deutschland

E-mail address: [breytman@rakudoitsu.com](mailto:breytman@rakudoitsu.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.
- Payment Data.
- Contact data.
- Content data.
- Contract data.
- Usage data.

- Meta, communication and process data.

## **Categories of Data Subjects**

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

## **Purposes of Processing**

- Provision of contractual services and fulfillment of contractual obligations.
- Contact requests and communication.
- Security measures.
- Office and organisational procedures.
- Managing and responding to inquiries.
- Authentication processes.
- Provision of our online services and usability.
- Information technology infrastructure.

## **Relevant legal bases**

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

- **Performance of a contract and prior requests (Article 6 (1) (b) GDPR) -** Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- **Compliance with a legal obligation (Article 6 (1) (c) GDPR)** - Processing is necessary for compliance with a legal obligation to which the controller is subject.
- **Legitimate Interests (Article 6 (1) (f) GDPR)** - Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

**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.

## 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.

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

## Transmission of Personal Data

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

## International data transfers

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

[https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection\\_en](https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en).

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

## Erasure of data

The data processed by us will be erased in accordance with the statutory provisions

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

## Use of Cookies

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

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

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

**Retention period:** With regard to the retention period, a distinction is drawn between the following types of cookies:

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

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

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

## Business services

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

We process this data in order to fulfill our contractual obligations. These include, in particular, the obligations to provide the agreed services, any update obligations and remedies in the event of warranty and other service disruptions. In addition, we process the data to protect our rights and for the purpose of administrative tasks associated with these obligations and company organization. Furthermore, we process the data on the basis of our legitimate interests in proper and economical business management as well as security measures to protect our contractual partners and our business operations from misuse, endangerment of their data, secrets, information and rights (e.g. for the involvement of telecommunications,

transport and other auxiliary services as well as subcontractors, banks, tax and legal advisors, payment service providers or tax authorities). Within the framework of applicable law, we only disclose the data of contractual partners to third parties to the extent that this is necessary for the aforementioned purposes or to fulfill legal obligations. Contractual partners will be informed about further forms of processing, e.g. for marketing purposes, within the scope of this privacy policy.

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

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

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

- **Processed data types:** Inventory data (e.g. names, addresses); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. e-mail, telephone numbers). Contract data (e.g. contract object, duration, customer category).
- **Data subjects:** Prospective customers. Business and contractual partners.
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations; Contact requests and communication; Office and organisational procedures. Managing and responding to inquiries.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Compliance with a legal obligation (Article 6 (1) (c) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

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



- **Agency Services:** We process the data of our customers within the scope of our contractual services, which may include e.g. conceptual and strategic consulting, campaign planning, software and design development / consulting or maintenance, implementation of campaigns and processes, handling, server administration, data analysis / consulting services and training services; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).
- **Consulting:** We process the data of our clients, clients as well as interested parties and other clients or contractual partners (uniformly referred to as "clients") in order to provide them with our consulting services. The data processed, the type, scope and purpose of the processing and the necessity of its processing are determined by the underlying contractual and client relationship.

Insofar as it is necessary for the fulfilment of our contract, for the protection of vital interests or by law, or with the consent of the client, we disclose or transfer the client's data to third parties or agents, such as authorities, courts, subcontractors or in the field of IT, office or comparable services, taking into account the professional requirements; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

- **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).

## 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 (e.g. names, addresses); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Contract data (e.g. contract object, duration, customer category); Usage data

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

- **Data subjects:** Customers; Prospective customers; Users (e.g. website visitors, users of online services). Business and contractual partners.
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations. Office and organisational procedures.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

#### **Further information on processing methods, procedures and services used:**

- **Papierkram:** Software for invoicing, accounting, banking and tax filing with document storage; **Service provider:** odacer Finanzsoftware GmbH, Konrad-Adenauer-Ring 13, 65187 Wiesbaden, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.papierkram.de/>; **Privacy Policy:** <https://www.papierkram.de/datenschutz>. **Data Processing Agreement:** Provided by the service provider.

## **Provision of online services and web hosting**

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

- **Processed data types:** Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status). Content data (e.g. text input, photographs, videos).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Provision of our online services and usability; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.). Security measures.
- **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:** The access to our online services is logged in the form of so-called "server log files". Server log files may include the address and name of the web pages and files accessed, the date and time of access, data volumes transferred, notification of successful access, browser type and version, the user's operating system, referrer URL (the previously visited page) and, as a general rule, IP addresses and the requesting provider. The server log files can be used for security purposes, e.g. to avoid overloading the servers (especially in the case of abusive attacks, so-called DDoS attacks) and to ensure the stability and optimal load balancing of the servers; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).  
**Retention period:** Log file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.
- **E-mail Sending and Hosting:** The web hosting services we use also include sending, receiving and storing e-mails. For these purposes, the addresses of the recipients and senders, as well as other information relating to the sending of e-mails (e.g. the providers involved) and the contents of the respective e-mails are processed. The above data may also be processed for SPAM detection purposes. Please note that e-mails on the Internet are generally not sent in encrypted form. As a rule, e-mails are encrypted during transport, but not on the servers from which they are sent and received (unless a so-called end-to-end encryption method is used). We can therefore accept no responsibility for the transmission path of e-mails between the sender and reception on our server; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **ALL-INKL:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider:** ALL-INKL.COM - Neue Medien Münnich, Inhaber: René Münnich, Hauptstraße 68, 02742 Friedersdorf, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://all-inkl.com/>; **Privacy Policy:** <https://all-inkl.com/datenschutzzinformationen/>. **Data Processing Agreement:** Provided by the service provider.

## Single Sign-on Authentication

"Single Sign-On" or "Single Sign-On Authentication or Logon" are procedures that allow users to log in to our online services using a user account with a provider of Single Sign-On services (e.g. a social network). The prerequisite for Single Sign-On

Authentication is that users are registered with the respective Single Sign-On provider and enter the required access data in the online form provided for this purpose, or are already logged in with the Single Sign-On provider and confirm the Single Sign-On login via the button.

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

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

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

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

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

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

- **Microsoft Single-Sign-On:** Authentication services for user logins, provision

of single sign-on functionalities, management of identity information and application integrations; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.microsoft.com/en-gb/security/business/identity-access/azure-active-directory-single-sign-on>; **Privacy Policy:** <https://privacy.microsoft.com/en-gb/privacystatement>; **Basis for third country transfer:** EU-US Data Privacy Framework (DPF). **Further Information:** <https://www.microsoft.com/en-gb/trust-center>.

## 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.

## Video Conferences, Online Meetings, Webinars and Screen-Sharing

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

**Data processed by Conference Platforms:** In the course of participation in a Conference, the Data of the participants listed below are processed. The scope of the processing depends, on the one hand, on which data is requested in the context of a specific Conference (e.g., provision of access data or clear names) and which optional information is provided by the participants. In addition to processing for the purpose of conducting the conference, participants' Data may also be processed by the Conference Platforms for security purposes or service optimization. The processed Data includes personal information (first name, last name), contact information (e-mail address, telephone number), access data (access codes or passwords), profile pictures, information on professional position/function, the IP address of the internet access, information on the participants' end devices, their operating system, the browser and its technical and linguistic settings, information on the content-related communication processes, i.e. entries in chats and audio and video data, as well as the use of other available functions (e.g. surveys). The content of communications is encrypted to the extent technically provided by the

conference providers. If participants are registered as users with the Conference Platforms, then further data may be processed in accordance with the agreement with the respective Conference Provider.

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

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

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

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

#### **Further information on processing methods, procedures and services used:**

- **Microsoft Teams:** Conference and communication software; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal**

**Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.microsoft.com/de-de/microsoft-365>; **Privacy Policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security information: <https://www.microsoft.com/de-de/trustcenter>. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>).

## Cloud Services

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

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

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

- **Processed data types:** Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Customers; Employees (e.g. Employees, job applicants); Prospective customers; Communication partner (Recipients of e-mails, letters, etc.); Users (e.g. website visitors, users of online services). Business and contractual partners.
- **Purposes of Processing:** Office and organisational procedures; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.). Provision of our online services and usability.

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

#### **Further information on processing methods, procedures and services used:**

- **Microsoft Cloud Services:** Cloud storage, cloud infrastructure services and cloud-based application software; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://microsoft.com>; **Privacy Policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security information: <https://www.microsoft.com/de-de/trustcenter>; **Data Processing Agreement:** <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>).
- **Microsoft Azure:** Cloud storage, cloud infrastructure services and cloud-based application software; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://azure.microsoft.com>; **Privacy Policy:** <https://privacy.microsoft.com/en-us/privacystatement>; **Data Processing Agreement:** <https://azure.microsoft.com/en-us/support/legal/>. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (<https://azure.microsoft.com/en-us/support/legal/>).

## **Management, Organization and Utilities**

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

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

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



purposes. We therefore ask you to read the data protection notices of the respective third party providers.

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

#### **Further information on processing methods, procedures and services used:**

- **Microsoft Teams:** Conference and communication software; **Service provider:** Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://www.microsoft.com/de-de/microsoft-365>; **Privacy Policy:** <https://privacy.microsoft.com/de-de/privacystatement>, Security information: <https://www.microsoft.com/de-de/trustcenter>. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>).

## **Changes and Updates to the Privacy Policy**

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

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