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

- Changes and Updates

Controller

HXS GmbH
Kundmanngasse 21
1030 Vienna
Austria / Europe

E-mail address: office@hxs.at

Phone: +43 (1) 344 1 344

Legal Notice: https://www.hxs.at/impressum/

Contact information of the Data Protection Officer

Peter Oskar Miller
hxs@datenschutzbeauftragter.at

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.
- Images and/ or video recordings.
- Audio recordings.
- Log data.
- Creditworthiness Data.

Categories of Data Subjects

- Service recipients and clients.

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

Purposes of Processing

- Provision of contractual services and fulfillment of contractual obligations.
- Communication.
- Security measures.
- Direct marketing.
- Web Analytics.
- Targeting.
- Office and organisational procedures.
- Conversion tracking.
- Clicktracking.
- A/B Tests.
- Organisational and Administrative Procedures.
- Feedback.
- Heatmaps.
- Marketing.
- Profiles with user-related information.
- Provision of our online services and usability.
- Assessment of creditworthiness.
- Information technology infrastructure.
- Public relations.
- Business processes and management procedures.

Automated Individual Decision-Making

- Credit report.

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.

National data protection regulations in Austria: In addition to the data protection regulations of the GDPR, national regulations apply to data protection in Austria. This includes in particular the Federal Act on the Protection of Individuals with regard to the Processing of Personal Data (Data Protection Act - DSG). In particular, the Data Protection Act contains special provisions on the right of access, rectification or cancellation, processing of special categories of personal data, processing for other purposes and transmission and automated decision making in individual cases.

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.

International data transfers

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

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

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

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

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

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

General Information on Data Retention and Deletion

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

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

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

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

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

Data Retention and Deletion: The following general deadlines apply to retention and archiving according to Austrian law:

- 10 Years - Retention period for books and records, annual financial statements, inventories, annual reports, opening balance sheets, booking receipts and invoices, as well as any necessary work instructions and other organisational documents (Austrian Federal Tax Code (BAO §132), Austrian Commercial Code (UGB §§190-212)).
- 6 Years - Remaining business documents: Received business or trading letters, copies of sent business or trading letters, and other documents, if they are relevant for taxation. These could be hourly wage sheets, operational accounting sheets, calculation documents, price tags, and payroll documents, as long as they aren't already booking receipts and cash register strips (Austrian Federal Tax Code (BAO §132), Austrian Commercial Code (UGB §§190-212)).
- 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 (Sections 1478, 1480 of the Austrian Civil Code).

Rights of Data Subjects

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

- **Right to Object: You have the right, on grounds arising from your particular situation, to object at any time to the processing of your personal data which is based on letter (e) or (f) of Article 6(1) GDPR, including profiling based on those provisions. Where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of the personal data concerning you for the purpose of such marketing, which includes profiling to the extent that it is related to such direct marketing.**
- **Right of withdrawal for consents:** You have the right to revoke consents at any time.
- **Right of access:** You have the right to request confirmation as to whether the data in question will be processed and to be informed of this data and to receive further information and a copy of the data in accordance with the provisions of the law.

- **Right to rectification:** You have the right, in accordance with the law, to request the completion of the data concerning you or the rectification of the incorrect data concerning you.
- **Right to Erasure and Right to Restriction of Processing:** In accordance with the statutory provisions, you have the right to demand that the relevant data be erased immediately or, alternatively, to demand that the processing of the data be restricted in accordance with the statutory provisions.
- **Right to data portability:** You have the right to receive data concerning you which you have provided to us in a structured, common and machine-readable format in accordance with the legal requirements, or to request its transmission to another controller.
- **Complaint to the supervisory authority:** In accordance with the law and without prejudice to any other administrative or judicial remedy, you also have the right to lodge a complaint with a data protection supervisory authority, in particular a supervisory authority in the Member State where you habitually reside, the supervisory authority of your place of work or the place of the alleged infringement, if you consider that the processing of personal data concerning you infringes the GDPR.

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); 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.
- **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; Conversion tracking (Measurement of the effectiveness of marketing activities); Marketing. Provision of our online services and usability.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** 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:

- **Consulting:** We process the data of our clients as well as prospects and other commissioning parties or contractual partners (collectively referred to as

"clients") in order to be able to provide our services to them. The processes that are part of and for the purposes of consulting include: contacting and communicating with clients, conducting needs and requirements analyses, planning and implementing consulting projects, documenting project progress and results, capturing and managing client-specific information and data, scheduling and organising appointments, providing consulting resources and materials, invoicing and payment management, post-processing and follow-up of consulting projects, quality assurance and feedback processes. The processed data, the nature, scope, purpose, and necessity of their processing are determined by the underlying contractual relationship with the client.
If it is necessary for our contract performance, for the protection of vital interests or legally required, or if there is consent from the clients, we disclose or transmit client data in compliance with professional legal requirements to third parties or agents such as authorities, subcontractors or in the field of IT, office or similar services; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

- **IT Services:** We process the data of our clients as well as contractors to enable them to plan, implement, and support IT solutions and associated services. The required information is marked as such during the contract, project, or similar agreement phase and includes details necessary for service provision and billing, as well as contact information to facilitate any necessary consultations. Insofar as we gain access to information from end customers, employees, or other individuals, we process this in accordance with legal and contractual requirements.

  Processing processes include project management and documentation, which cover all phases from initial requirement analysis to project completion. This involves creating and managing project timelines, budgets, and resource allocations. Data processing also supports change management, where changes in the project flow are documented and tracked to ensure compliance and transparency.

  Another process is customer relationship management (CRM), which involves recording and analyzing customer interactions and feedback to improve service quality and efficiently address individual customer needs. Additionally, the processing process encompasses technical support and trouble-shooting, which includes capturing and handling support requests, error resolutions, and regular maintenance.

  Furthermore, reporting and performance analysis are conducted by capturing and evaluating performance metrics to assess the effectiveness of provided IT solutions continuously optimizing them. All these processes are aimed at ensuring high customer satisfaction and compliance with all relevant 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).

- **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).
- **Amazon:** Online marketplace for e-commerce; **Service provider**: Amazon EU S.à r.l. (Société à responsabilité limitée), 38 avenue John F. Kennedy, L-1855 Luxembourg; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.amazon.de/; **Privacy Policy:** https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010. **Basis for third-country transfers:** Data Privacy Framework (DPF).

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).
- **Data subjects:** Service recipients and clients; Prospective customers; Communication partner (Recipients of e-mails, letters, etc.). Business and contractual partners.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures. Business processes and management procedures.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Providers and services used in the course of business

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Contract data (e.g. contract object, duration, customer category). 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:** Service recipients and clients; Prospective customers; Business and contractual partners. 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. 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:

- **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:** Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA).
- **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 Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.microsoft.com/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 transfers:** Data Privacy Framework (DPF). **Further Information:** https://www.microsoft.com/en-gb/trust-center.
- **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:** Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA).

Credit Assessment

Insofar as we make advance payments or enter into comparable economic risks (e.g. when ordering on account), we reserve the right to obtain identity and credit information from specialised service providers (credit agencies) for the purpose of assessing the credit risk on the basis of mathematical-statistical procedures in order to safeguard legitimate interests.

We process the information received from credit agencies on the statistical probability of non-payment as part of an appropriate discretionary decision on the establishment, execution and termination of the contractual relationship. In the event of a negative result of the credit assessment, we reserve the right to refuse payment on account or any other advance payment.

In accordance with the law, the decision as to whether we will provide goods or services prior to payment is made solely on the basis of an automated decision in the individual case, which our software makes on the basis of the information provided by the credit agency.

If we obtain the express consent of contractual partners, the legal basis for the credit information and the transmission of the customer's data to the credit agencies is consent. If no consent is obtained, the credit rating will be based on our legitimate interests in the security of our payment claims.

- **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). Creditworthiness Data (e.g. received credit score, estimated default probability, risk classification based on this, historical payment behaviour).
- **Data subjects:** Service recipients and clients; Prospective customers. Business and contractual partners.
- **Purposes of processing:** Assessment of creditworthiness.
- **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).
- **Automated individual decision-making:** Credit report (Decision based on a credit report).

Further information on processing methods, procedures and services used:

- **KSV1870 - Kreditschutzverband von 1870:** Credit agency; **Service provider**: KSV1870 Holding AG, Wagenseilgasse 7, A-1120 Wien, Austria; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.ksv.at/. **Privacy Policy:** https://www.ksv.at/datenschutzerklaerung.

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

Use of Cookies

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

requested content and functions. This includes, for example, saving settings and ensuring the functionality and security of our online services. Consent can be withdrawn at any time. We clearly inform users about the scope of the consent and which cookies are used.

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

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

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

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

- **Processed data types:** Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Conversion tracking (Measurement of the effectiveness of marketing activities); Clicktracking; A/B Tests; Heatmaps ("Heatmaps" are mouse movements of the users, which are combined to an overall picture.); Profiles with user-related information (Creating user profiles). Provision of our online services and usability.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). Consent (Article 6 (1) (a) GDPR).

Further information on processing methods, procedures and services used:

- **Processing Cookie Data on the Basis of Consent:** We implement a consent management solution that obtains users' consent for the use of cookies or for the processes and providers mentioned within the consent management

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

- **Klaro!:** Cookie Consent Management: Procedures for obtaining, recording, managing, and revoking consents, particularly for the use of cookies and similar technologies for storing, accessing, and processing information on users' devices as well as their processing; **Service provider**: KIProtect GmbH, Bismarckstr. 10-12, 10625 Berlin, Germany; **Website:** https://klaro.org/. **Privacy Policy:** https://kiprotect.com/resources/privacy.
- **Clarity:** Software for the analysis and optimisation of online services on the basis of feedback functions as well as pseudonymously conducted measurements and analyses of user behaviour, which may include in particular A/B tests (measurement of the preference and user-friendliness of different contents and functions), measurement of click paths and other interactions with contents and functions of the online services; **Service provider**: Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://clarity.microsoft.com/; **Privacy Policy:** https://privacy.microsoft.com/en-GB/privacystatement, Security information: https://www.microsoft.com/en-GB/trust-center. **Basis for third-country transfers:** Data Privacy Framework (DPF).

Contact and Inquiry Management

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

- **Processed data types:** Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** 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).
- **LiveAgent:** Management of contact requests and communication; **Service provider**: Quality Unit, s. r. o. Vajnorska 100/A, 83104Bratislava, Slovakia; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.liveagent.com. **Privacy Policy:** https://www.liveagent.com/security-privacy-policy/.

Communication via Messenger

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

You can also contact us by alternative means, e.g. telephone or e-mail. Please use the contact options provided to you or use the contact options provided within our online services.

In the case of encryption of content (i.e. the content of your message and attachments), we point out that the communication content (i.e. the content of the message and

attachments) is encrypted end-to-end. This means that the content of the messages is not visible, not even by the messenger service providers themselves. You should always use a current version of the messenger service with activated encryption, so that the encryption of the message contents is guaranteed.

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

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

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

Reservation of reference to other means of communication: For your security, we kindly ask for your understanding that we may not respond to enquiries via messenger for specific reasons. This applies in situations where contract details require heightened confidentiality or a response via messenger does not meet formal requirements. In such cases, we recommend using more appropriate communication channels.

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

interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of processing:** Communication. Direct marketing (e.g. by e-mail or postal).
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR); Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Apple iMessage:** Send and receive text messages, voice messages, and video calls. Conduct group conversations. Share files, photos, videos, and locations. Secure communication through end-to-end encryption. Synchronise messages across multiple devices; **Service provider**: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.apple.com/. **Privacy Policy:** https://www.apple.com/privacy/privacy-policy/.
- **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/de-de/microsoft-365; **Privacy Policy:** https://privacy.microsoft.com/en-GB/privacystatement, Security information: https://www.microsoft.com/en-GB/trust-center. **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses

(https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA).

- **Signal:** Signal Messenger with end-to-end encryption; **Service provider**: Privacy Signal Messenger, LLC 650 Castro Street, Suite 120-223 Mountain View, CA 94041, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://signal.org/. **Privacy Policy:** https://signal.org/legal/.
- **WhatsApp:** A communication service that enables the sending and receiving of text messages, voice messages, images, videos, documents, as well as voice and video calls over the internet. Communication is conducted through end-to-end encryption, ensuring that content is accessible only to the involved communication partners. To provide the service, the platform processes metadata (e.g., phone numbers, timestamps, device information) and may use this data for functionality enhancement, security, and service optimisation; **Service provider**: WhatsApp Ireland Limited, Merrion Road 4, D04 X2K5 Dublin, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.whatsapp.com/; **Privacy Policy:** https://www.whatsapp.com/legal/privacy-policy-eea. **Basis for third-country transfers:** Data Privacy Framework (DPF).

Video Conferences, Online Meetings, Webinars and Screen-Sharing

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

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

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

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

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

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Images and/ or video recordings (e.g. photographs or video recordings of a person); Audio recordings. Log data (e.g. log files concerning logins or data retrieval or access times.).
- **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; Communication. 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:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Microsoft Teams:** Utilisation for conducting online events, conferences, and communication with internal and external participants. Voice transmission, direct messaging, group communication, and collaboration functions are used; name, business contact details, work profile, participation as well as content (audio/video, speech, chat, files, speech transcription) are processed for purposes and interests in efficiency and productivity improvements, cost efficiency, flexibility, mobility, enhanced communication, IT security, use of a central platform as well as business operations by Microsoft. Audio signals are generally not stored unless recording is enabled. Meeting and conference recordings are stored by default for 90 days unless a different duration is specified. Chat and file contents are stored according to the policies determined by the administrator or user; there is no preset automatic deletion. Channels must be renewed every 180 days; otherwise contents are deleted. Additionally processed are system-generated logs, diagnostic and metadata as well as diagnostic data collected for product stability, security and improvement; **Service provider**: Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.microsoft.com/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:** 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 (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:** Data

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

- **Microsoft EU Data Boundary:** Our use of Microsoft Cloud services takes place within the framework of the so-called "EU Data Boundary", which ensures that data is stored and processed within the European Union (EU) and the European Free Trade Association (EFTA).

  The EU Data Boundary is a designated region where Microsoft commits to storing and processing customer data and personal data for certain online services (Microsoft 365, Azure, Dynamics 365, and the Power Platform). Companies using these services can ensure that their data remains within the EU/EFTA region. This includes both general customer data and support data generated as part of technical services. In many cases, pseudonymised data is also processed within this region.

  The EU Data Boundary includes all EU countries as well as EFTA states (Liechtenstein, Iceland, Norway, and Switzerland). Microsoft operates data centres in several of these countries, including Germany, France, Ireland, the Netherlands, Sweden, Spain, and Switzerland. Additional locations may be added.

  As part of operations, Microsoft automatically generates logs to ensure the security and functionality of its services. These logs mainly contain technical information but may include personal data in certain cases, such as when user actions are documented.

  To protect this data, Microsoft employs techniques like encryption, masking, and tokenisation (replacing sensitive data with non-traceable strings). This ensures that Microsoft employees only see pseudonymised data without being able to directly infer individual users. Additionally, there are strict access rules and deletion deadlines for this data.

  Are any transfers made outside of the EU? Microsoft has assured that transfers outside of the EU occur only in a few precisely defined cases. This may be necessary to implement global cybersecurity measures or ensure cloud service functionality. These transfers always take place under high-security standards such as encryption and pseudonymisation.

  Further information on the EU Data Boundary and Microsoft's privacy measures can be found at the Microsoft EU Data Boundary Trust Center: https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb.

Web Analysis, Monitoring and Optimization

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

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

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

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

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

- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of processing:** Web Analytics (e.g. access statistics, recognition of returning visitors); Profiles with user-related information (Creating user profiles); Provision of our online services and usability. Targeting (e.g. profiling based on interests and behaviour, use of cookies).

- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.).
- **Security measures:** IP Masking (Pseudonymization of the IP address).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Google Analytics:** We use Google Analytics to perform measurement and analysis of the use of our online services by users based on a pseudonymous user identification number. This identification number does not contain any unique data, such as names or email addresses. It is used to assign analysis information to an end device in order to recognize which content users have accessed within one or various usage processes, which search terms they have used, have accessed again or have interacted with our online services. Likewise, the time of use and its duration are stored, as well as the sources of users referring to our online services and technical aspects of their end devices and browsers.
  In the process, pseudonymous profiles of users are created with information from the use of various devices, and cookies may be used. Google Analytics does not log or store individual IP addresses. Analytics does provide coarse geo-location data by deriving the following metadata from IP addresses: City (and the derived latitude, and longitude of the city), Continent, Country, Region, Subcontinent (and ID-based counterparts). For EU-based traffic, IP-address data is used solely for geo-location data derivation before being immediately discarded. It is not logged, accessible, or used for any additional use cases. When Analytics collects measurement data, all IP lookups are performed on EU-based servers before forwarding traffic to Analytics servers for processing; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://marketingplatform.google.com/intl/en/about/analytics/; **Security measures:** IP Masking (Pseudonymization of the IP address); **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://business.safety.google/adsprocessorterms/; **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (https://business.safety.google/adsprocessorterms); **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en, Settings for the Display of Advertisements: https://myadcenter.google.com/personalizationoff. **Further Information:** https://business.safety.google/adsservices/ (Types of processing and data processed).

- **Google Tag Manager:** We use Google Tag Manager, a software provided by Google, which enables us to manage so-called website tags centrally via a user interface. Tags are small code elements on our website that serve to record and analyse visitor activities. This technology assists us in improving our website and the content offered on it. Google Tag Manager itself does not create user profiles, store cookies with user profiles, or perform any independent analyses. Its function is limited to simplifying and making the integration and management of tools and services we use on our website more efficient. Nevertheless, when using Google Tag Manager, users' IP addresses are transmitted to Google, which is technically necessary to implement the services we use. Cookies may also be set in this process. However, this data processing only occurs if services are integrated via the Tag Manager. For more detailed information about these services and their data processing, please refer to the further sections of this privacy policy; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://marketingplatform.google.com; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://business.safety.google/adsprocessorterms. **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (https://business.safety.google/adsprocessorterms).
- **Google Analytics:** We use Google Analytics to perform measurement and analysis of the use of our online services by users based on a pseudonymous user identification number. This identification number does not contain any unique data, such as names or email addresses. It is used to assign analysis information to an end device in order to recognize which content users have accessed within one or various usage processes, which search terms they have used, have accessed again or have interacted with our online services. Likewise, the time of use and its duration are stored, as well as the sources of users referring to our online services and technical aspects of their end devices and browsers. In the process, pseudonymous profiles of users are created with information from the use of various devices, and cookies may be used. Google Analytics does not log or store individual IP addresses. Analytics does provide coarse geo-location data by deriving the following metadata from IP addresses: City (and the derived latitude, and longitude of the city), Continent, Country, Region, Subcontinent (and ID-based counterparts). For EU-based traffic, IP-address data is used solely for geo-location data derivation before being immediately discarded. It is not logged, accessible, or used for any additional use cases. When Analytics collects measurement data, all IP lookups are performed on EU-based servers before forwarding traffic to Analytics servers for processing; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://marketingplatform.google.com/intl/en/about/analytics/; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:**

https://business.safety.google/adsprocessorterms/; **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (https://business.safety.google/adsprocessorterms); **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en, Settings for the Display of Advertisements: https://myadcenter.google.com/personalizationoff. **Further Information:** https://business.safety.google/adsservices/ (Types of processing and data processed).

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:

- **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:** Data Privacy Framework (DPF), Standard Contractual Clauses (https://legal.linkedin.com/dpa). **Opt-Out:** https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out.

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. Provision of contractual services and fulfillment of contractual obligations.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". 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 (Provision on own server):** Provision of font files for the purpose of a user-friendly presentation of our online services; **Service provider**: The Google Fonts are hosted on our server, no data is transmitted to Google; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Google Maps APIs and SDKs:** Interfaces to the map and location services provided by Google, which, for example, allow the addition of address entries, location determinations, distance calculations or the provision of supplementary information on locations and other places; **Service provider**: Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://mapsplatform.google.com/; **Privacy**

Policy: https://policies.google.com/privacy. **Basis for third-country transfers:** Data Privacy Framework (DPF).

- **reCAPTCHA:** We integrate the "reCAPTCHA" function to be able to recognise whether entries (e.g. in online forms) are made by humans and not by automatically operating machines (so-called "bots"). The data processed may include IP addresses, information on operating systems, devices or browsers used, language settings, location, mouse movements, keystrokes, time spent on websites, previously visited websites, interactions with ReCaptcha on other websites, possibly cookies and results of manual recognition processes (e.g. answering questions asked or selecting objects in images). The data processing is based on our legitimate interest to protect our online services from abusive automated crawling and spam; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, , parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.google.com/recaptcha/; **Privacy Policy:** https://policies.google.com/privacy. **Basis for third-country transfers:** Data Privacy Framework (DPF).

Changes and Updates

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

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

Supervisory authority competent for us:

Austrian Data Protection Authority
Barichgasse 40-42,
1030 Vienna
Austria / Europe

Phone: +43 (1) 521 52-25 69
Email: dsb@dsb.gv.at