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: 18. February 2025

Table of contents

- Rights of Data Subjects
- Business services
- Business processes and operations
- Provision of online services and web hosting
- Contact and Inquiry Management
- Video Conferences, Online Meetings, Webinars and Screen-Sharing
- Web Analysis, Monitoring and Optimization
- Profiles in Social Networks (Social Media)
- Plugins and embedded functions and content
- Processing of data in the context of employment relationships
- Job Application Process
- Changes and Updates

Controller

BING Power Origin Kft.
Gyári út 72
H-2310 Szigetszentmiklós
Hungary
E-Mail: info@bp-origin.hu
Managing Director: Patrick Eisenlauer

E-mail address: info@bp-origin.hu

Legal Notice: https://origin.hu/en/imprint/

Overview of processing operations

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

Categories of Processed Data

- Inventory data.
- Employee Data.

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

Special Categories of Data

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

Categories of Data Subjects

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

- Third parties.
- Customers.

Purposes of Processing

- Provision of contractual services and fulfillment of contractual obligations.
- Communication.
- Security measures.
- Web Analytics.
- Targeting.
- Office and organisational procedures.
- Affiliate Tracking.
- Organisational and Administrative Procedures.
- Job Application Process.
- Feedback.
- Marketing.
- Profiles with user-related information.
- Provision of our online services and usability.
- Assessment of creditworthiness.
- Establishment and execution of employment relationships.
- Information technology infrastructure.
- Financial and Payment Management.
- Public relations.
- Sales promotion.
- Business processes and management procedures.

Relevant legal bases

Relevant legal bases according to the GDPR: In the following, you will find an overview of the legal basis of the GDPR on which we base the processing of personal data. Please note that in addition to the provisions of the GDPR, national data protection provisions of your or our country of residence or domicile may

apply. If, in addition, more specific legal bases are applicable in individual cases, we will inform you of these in the data protection declaration.

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

Relevant legal basis according to the Swiss Data Protection Act: If you are located in Switzerland, we process your data based on the Federal Act on Data

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

Reference to the applicability of the GDPR and the Swiss DPA: These privacy policy serves both to provide information pursuant to the Swiss Federal Act on Data Protection (FADP) and the General Data Protection Regulation (GDPR). For this reason, we ask you to note that due to the broader spatial application and comprehensibility, the terms used in the GDPR are applied. In particular, instead of the terms used in the Swiss FADP such as "processing" of "personal data", "predominant interest", and "particularly sensitive personal data", the terms used in the GDPR, namely "processing" of "personal data", as well as "legitimate interest" and "special categories of data" are used. However, the legal meaning of these terms will continue to be determined according to the Swiss FADP within its scope of application.

Security Precautions

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

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

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

advanced and secure version of SSL, ensures that all data transmissions conform to the highest security standards. When a website is secured with an SSL/TLS certificate, this is indicated by the display of HTTPS in the URL. This serves as an indicator to users that their data is being securely and encryptedly transmitted.

Transmission of Personal Data

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

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

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

International data transfers

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

Disclosure of Personal Data Abroad: In accordance with the Swiss Data Protection Act (Swiss DPA), we only disclose personal data abroad when an appropriate level of protection for the affected persons is ensured (Art. 16 Swiss DPA). If the Federal Council does not determine that there is an adequate level of protection (list of states: https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales/anerkennung-staaten.html), we implement alternative security measures. These measures may include international agreements, specific guarantees, data protection clauses in contracts, standard data protection clauses approved by the Federal Data Protection and Information Commissioner (FDPIC), or internal company data protection regulations previously recognised by the FDPIC or a competent data protection authority of another country. Under Art. 16 of the Swiss DSG, exceptions can be made for the disclosure of data abroad if certain conditions are met, including the consent of the affected person, contract execution, public interest, protection of life or physical integrity, publicly made data or data from a legally provided register. Such disclosures always comply with the legal requirements. As part of the so-called "Data Privacy Framework" (DPF), the Switzerland has recognized the data protection level for certain companies from the USA as adequate under the adequacy decision dated June 7, 2024. You can find the list of certified companies and additional information about the DPF on the website of the U.S. Department of Commerce at https://www.dataprivacyframework.gov/ (in English). We inform you in our privacy notice about which service providers we use are certified under the Data Privacy Framework.

Rights of Data Subjects

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

- **Right to Object: You have the right, on grounds arising from your particular situation, to object at any time to the processing of your personal data which is based on letter (e) or (f) of Article 6(1) GDPR, including profiling based on those provisions. Where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of the personal data concerning you for the purpose of such marketing, which includes profiling to the extent that it is related to such direct marketing.**
- **Right of withdrawal for consents:** You have the right to revoke consents at any time.
- **Right of access:** You have the right to request confirmation as to whether the data in question will be processed and to be informed of this data and to receive further information and a copy of the data in accordance with the provisions of the law.
- **Right to rectification:** You have the right, in accordance with the law, to request the completion of the data concerning you or the rectification of the incorrect data concerning you.
- **Right to Erasure and Right to Restriction of Processing:** In accordance with the statutory provisions, you have the right to demand that the relevant data be erased immediately or, alternatively, to demand that the processing of the data be restricted in accordance with the statutory provisions.
- **Right to data portability:** You have the right to receive data concerning you which you have provided to us in a structured, common and machine-readable format in accordance with the legal requirements, or to request its transmission to another controller.
- **Complaint to the supervisory authority:** In accordance with the law and without prejudice to any other administrative or judicial remedy, you also have the right to lodge a complaint with a data protection supervisory authority, in particular a supervisory authority in the Member State where you habitually reside, the supervisory authority of your place of work or the place of the alleged infringement, if you consider that the processing of personal data concerning you infringes the GDPR.

Rights of the data subjects under the Swiss DPA:

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

- **Right to information:** You have the right to request confirmation as to whether personal data concerning you are being processed, and to receive the information necessary for you to assert your rights under the Swiss DPA and to ensure transparent data processing.

- **Right to data release or transfer:** You have the right to request the release of your personal data, which you have provided to us, in a common electronic format, as well as its transfer to another data controller, provided this does not require disproportionate effort.
- **Right to rectification:** You have the right to request the rectification of inaccurate personal data concerning you.
- **Right to object, deletion, and destruction:** You have the right to object to the processing of your data, as well as to request that personal data concerning you be deleted or destroyed.

Business services

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

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

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

We delete the data after expiry of statutory warranty and comparable obligations, i.e. in principle after expiry of 4 years, unless the data is stored in a customer account or must be kept for legal reasons of archiving. The statutory retention period for documents relevant under tax law as well as for commercial books,

inventories, opening balance sheets, annual financial statements, the instructions required to understand these documents and other organizational documents and accounting records is ten years and for received commercial and business letters and reproductions of sent commercial and business letters six years. The period begins at the end of the calendar year in which the last entry was made in the book, the inventory, the opening balance sheet, the annual financial statements or the management report was prepared, the commercial or business letter was received or sent, or the accounting document was created, furthermore the record was made or the other documents were created.

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

- **Automotive Industry and Vehicle Technology:** We process the data of our customers and clients to enable them to develop, produce, and provide vehicles and vehicle technologies and related services. The required information includes that needed for project implementation and billing, as well as contact information for necessary coordination. To the extent that we have access to information from end customers, employees, or other persons, we process this in accordance with legal and contractual requirements; **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).

Business processes and operations

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

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

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

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Log data (e.g. log files concerning logins or data retrieval or access times.); Creditworthiness Data (e.g. received credit score, estimated default probability, risk classification based on this, historical payment behaviour). Employee Data (Information about employees and other individuals in an employment relationship).
- **Data subjects:** Service recipients and clients; Prospective customers; Communication partner (Recipients of e-mails, letters, etc.); Business and contractual partners; Third parties; Users (e.g. website visitors, users of online services); Employees (e.g. employees, job applicants, temporary workers, and other personnel.). Customers.

- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Business processes and management procedures; Communication; Marketing; Sales promotion; Public relations; Assessment of creditworthiness; Financial and Payment Management. 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:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR). Compliance with a legal obligation (Article 6 (1) (c) GDPR).

Further information on processing methods, procedures and services used:

- **Customer Management and Customer Relationship Management (CRM):** Processes required in the context of customer management and Customer Relationship Management (CRM) include customer acquisition in compliance with data protection regulations, measures to promote customer retention and loyalty, effective customer communication, complaint management and customer service with consideration of data protection, data management and analysis to support the customer relationship, management of CRM systems, secure account management, customer segmentation and targeting; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Contact management and contact maintenance:** Processes required in the context of organizing, maintaining, and securing contact information (e.g., setting up and maintaining a central contact database, regular updates of contact information, monitoring data integrity, implementing data protection measures, ensuring access controls, conducting backups and restorations of contact data, training employees in effective use of contact management software, regular review of communication history and adjustment of contact strategies); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **General Payment Transactions:** Procedures required for carrying out payment transactions, monitoring bank accounts, and controlling payment flows (e.g., creation and verification of transfers, processing of direct debit transactions, checking of account statements, monitoring of incoming and outgoing payments, management of chargebacks, account reconciliation, cash management); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Accounting, accounts payable, accounts receivable:** Procedures required for the collection, processing, and control of business transactions in the area

of accounts payable and receivable accounting (e.g., creation and verification of incoming and outgoing invoices, monitoring and management of outstanding items, execution of payment transactions, handling of dunning processes, account reconciliation within the scope of receivables and payables, accounts payable accounting, and accounts receivable accounting); **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).

- **Financial Accounting and Taxes:** Procedures required for the collection, management, and control of finance-related business transactions as well as for the calculation, reporting, and payment of taxes (e.g., accounting and posting of business transactions, preparation of quarterly and annual financial statements, execution of payment transactions, handling of dunning processes, account reconciliation, tax consulting, preparation and submission of tax returns, management of tax affairs); **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).
- **Purchasing:** Processes required in the procurement of goods, raw materials, or services (e.g., selection and evaluation of suppliers, price negotiations, placement and monitoring of orders, inspection and control of deliveries, invoice verification, management of orders, inventory management, creation and maintenance of purchasing policies); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Sales:** Procedures required for the planning, implementation, and control of measures for marketing and selling products or services (e.g., customer acquisition, preparation and tracking of offers, order processing, customer consultation and support, sales promotion, product training, sales controlling and analysis, management of distribution channels); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Marketing, advertising, and sales promotion:** Processes required in the context of marketing, advertising, and sales promotion (e.g., market analysis and audience targeting, development of marketing strategies, planning and execution of advertising campaigns, design and production of advertising materials, online marketing including SEO and social media campaigns, event marketing and trade show participation, customer loyalty programs, sales promotion measures, performance measurement and optimisation of marketing activities, budget management and cost control); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Economic Analyses and Market Research:** To fulfill business management purposes and to identify market trends, desires of contractual partners, and

users, the present data regarding business transactions, contracts, inquiries, etc., are analyzed. The group of affected individuals may include contractual partners, interested parties, customers, visitors, and users of the online service managed by the responsible entity. The execution of these analyses serves the purposes of business economic evaluations, marketing, and market research (e.g., to determine customer groups with different characteristics). Where available, profiles of registered users along with their information on services utilized are considered. The analyses are exclusively for the use of the responsible entity and are not disclosed externally unless they pertain to anonymous analyses with aggregated, thus anonymized values. Moreover, user privacy is accounted for; data is processed for analysis purposes in as pseudonymized a manner as possible and anonymized when feasible (e.g., as aggregated data); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

- **Public Relations:** Processes required in the context of public relations and public relations activities (e.g., development and implementation of communication strategies, planning and execution of PR campaigns, creation and distribution of press releases, maintenance of media contacts, monitoring and analysis of media response, organisation of press conferences and public events, crisis communication, creation of content for social media and corporate websites, management of corporate branding); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

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).
- **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).
- **Plesk:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider**: Plesk International GmbH, Vordergasse 59, 8200 Schaffhausen, Switzerland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.parallels.com/; **Privacy Policy:** https://www.plesk.com/legal/#privacy-policy; **Data Processing Agreement:** Provided by the service provider. **Basis for third-country transfers:** EEA -

Adequacy decision (Switzerland).

- **Microsoft Azure:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider**: Microsoft Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://azure.microsoft.com; **Privacy Policy:** https://www.microsoft.com/en-us/privacy/privacystatement; **Data Processing Agreement:** https://azure.microsoft.com/en-us/support/legal/. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

Contact and Inquiry Management

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

- **Processed data types:** 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). 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).

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:** Audio and video conferencing, chat, file sharing, integration with Office 365 applications, real-time collaboration on documents, calendar functions, task management, screen sharing, optional recording; **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/microsoft-teams/; **Privacy Policy:** https://privacy.microsoft.com/de-de/privacystatement, Security information:

https://www.microsoft.com/de-de/trustcenter. **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland).

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.
- **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:** EEA - Data Privacy Framework (DPF), Switzerland - Adequacy decision (Ireland); **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en, Settings for the Display of

Advertisements: https://myadcenter.google.com/personalizationoff. **Further Information:** https://business.safety.google/adsservices/ (Types of processing and data processed).

- **Google as a recipient of consent:** The consent given by users in the context of a consent dialogue (also known as "Cookie Opt-In/Consent", "Cookie Banner", etc.) serves multiple purposes. Firstly, it helps us to fulfil our obligation to obtain consent for the storage and reading of information on and from the end-user's device (in accordance with ePrivacy Directives). Secondly, it covers the processing of users' personal data in accordance with data protection requirements. Additionally, this consent is also applicable to Google, as the company is required by the Digital Markets Act to obtain consent for personalised services. Therefore, we share the status of consents given by users with Google. Our consent management software informs Google about whether consents have been given or not. The aim is to ensure that user consents—or their absence—are taken into account when using Google Analytics and integrating features and external services. Thus, user consents and their revocation can be dynamically adjusted within our online offerings through Google Analytics and other Google services, depending on user selection; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://support.google.com/analytics/answer/9976101?hl=en; **Privacy Policy:** https://policies.google.com/privacy. **Basis for third-country transfers:** Switzerland - Adequacy decision (Ireland).

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:

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

Plugins and embedded functions and content

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

The integration always presupposes that the third-party providers of this content process the IP address of the user, since they could not send the content to their browser without the IP address. The IP address is therefore required for the

presentation of these contents or functions. We strive to use only those contents, whose respective offerers use the IP address only for the distribution of the contents. Third parties may also use so-called pixel tags (invisible graphics, also known as "web beacons") for statistical or marketing purposes. The "pixel tags" can be used to evaluate information such as visitor traffic on the pages of this website. The pseudonymous information may also be stored in cookies on the user's device and may include technical information about the browser and operating system, referring websites, visit times and other information about the use of our website, as well as may be linked to such information from other sources.

- **Processed data types:** Usage data (e.g. 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; Web Analytics (e.g. access statistics, recognition of returning visitors); Targeting (e.g. profiling based on interests and behaviour, use of cookies); Affiliate Tracking. Marketing.
- **Retention and deletion:** Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion". Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **YouTube videos:** Video contents; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, , parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://www.youtube.com; **Privacy Policy:** https://policies.google.com/privacy; **Basis for third-country transfers:** EEA - Data Privacy Framework (DPF), Switzerland - Data Privacy Framework (DPF). **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en, Settings for the Display of Advertisements: https://myadcenter.google.com/personalizationoff.

Processing of data in the context of employment relationships

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

The data processing covers various aspects ranging from contract initiation to termination. Included are the organization and management of daily working hours, management of access rights and permissions, as well as handling personnel development measures and staff appraisals. The processing also serves payroll accounting and management of wage and salary payments, which represent critical aspects of contract execution.

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

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

- **Processed data types:** Employee Data (Information about employees and other individuals in an employment relationship); Payment Data (e.g. bank details, invoices, payment history); Contract data (e.g. contract object, duration, customer category); Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Social data (Data subject to a special social confidentiality obligation and processed, for example, by social insurance institutions, social welfare institutions or pension authorities.); Log data (e.g. log files concerning logins or data retrieval or access times.); Performance and behavioural data (For example, performance and behavioural data aspects such as performance evaluations, feedback from supervisors, training attendance, compliance with company policies, self-assessments, and behavioural assessments.); Working hours data (e.g. start of work time, end of work time, actual working hours, target working hours, break times, overtime, vacation days, special leave

days, sick days, absences, home office days, business trips); Salary data (e.g. basic salary, bonus payments, premiums, tax class information, surcharges for night work/overtime, tax deductions, social security contributions, net payout amount); Images and/ or video recordings (e.g. photographs or video recordings of a person); 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).

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

Further information on processing methods, procedures and services used:

- **Time Recording:** Processes for recording employees' working hours include both manual and automated methods, such as the use of punch clocks, time tracking software, or mobile apps. Activities involved include entering clock-in and clock-out times, break times, overtime, and absences. To verify and validate the recorded working hours, they are compared with deployment or shift schedules, checked for absences, and approved for overtime by supervisors. Reports and analyses are generated based on the recorded working hours to provide work time records, overtime reports, and absence statistics for management and the human resources department; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Authorization Management:** Procedures required for the definition, management, and control of access rights and user roles within a system or an organisation (e.g., creation of authorisation profiles, role- and access-based control, review and approval of access requests, regular review of access rights, tracking and auditing of user activities, creation of security

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

- **Special categories of personal data:** Special categories of personal data are processed in the context of employment relationships or to fulfil legal obligations. The processed special categories of personal data include information concerning the health, trade union membership, or religious affiliation of employees. This data may be transferred to health insurance companies or processed for assessing the employees' work capacity, for corporate health management, or for declarations to the tax authorities; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Sources of Processed Data:** Personal data received during the application process and/or employment relationship will be processed. Furthermore, where required by law, personal data will be collected from other sources. These may include financial authorities for tax-related information, the respective health insurance company for information on work incapacity, third parties such as employment agencies, or publicly accessible sources like professional social networks in the context of application procedures; **Legal Basis:** Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Purposes of Data Processing:** The personal data of employees are primarily processed for the establishment, execution, and termination of the employment relationship. Furthermore, the processing of this data is necessary to fulfil legal obligations in the field of tax and social security law. In addition to these primary purposes, the data of employees are also used to meet regulatory and supervisory requirements, to optimise processes of electronic data processing, and to compile company-internal or cross-company data, possibly including statistical data. Moreover, the data of employees may be processed for the assertion of legal claims and defense in legal disputes; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Transmission of Employee Data:** The data of employees is processed internally only by those departments that require it to fulfil operational, contractual, and legal obligations. The transfer of data to external recipients only occurs if it is legally required, or if the affected employees have given their consent. Possible scenarios for this can include requests for information from authorities or in the case of asset formation benefits. Furthermore, the controller may transfer personal data to further recipients as far as this is necessary for fulfilling his contractual and legal obligations as an employer. These recipients can include: a) banks b) health insurance companies,

pension insurance institutions, providers of old-age provisions and other social insurance carriers c) authorities, courts (e.g., tax authorities, labour courts, further supervisory authorities within the framework of fulfilling reporting and information obligations) d) tax and legal advisors e) third-party debtors in the case of wage and salary garnishments f) other entities to which legally obligatory declarations must be made.
In addition, data can be transferred to third parties if this is necessary for communication with business partners, suppliers or other service providers. Examples include details in the sender area of emails or letterheads as well as creating profiles on external platforms; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

- **Transmission of Employee Data to Third Countries:** The transfer of employee data to third countries, meaning countries outside the European Union (EU) and the European Economic Area (EEA), occurs only if it is necessary for the fulfilment of the employment relationship, legally required, or if employees have given their consent. Employees will be informed about the details separately, as far as legally required; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Business Travel and Travel Expense Settlement:** Procedures required for planning, executing, and accounting for business trips (e.g., booking of travel, organizing accommodations and transportation, managing travel expense advances, submitting and reviewing travel expense reports, controlling and recording incurred costs, compliance with travel policies, handling of the travel expense management); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).
- **Payroll and wage accounting:** Procedures required for calculating, disbursing, and documenting wages, salaries, and other remuneration for employees (e.g., recording of working hours, calculation of deductions and surcharges, remittance of taxes and social security contributions, preparation of payroll statements, management of wage accounts, reporting to the tax authorities and social security institutions); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR).
- **Deletion of Employee Data:** Employment data will be deleted under German law when it is no longer required for the purpose for which it was collected, unless there is a legal obligation to retain or archive it, or it needs to be kept for the interests of the employer. The following retention and archiving obligations are observed:
    - General personnel records - General personnel records (such as employment contracts, references, supplementary agreements) are retained for up to three years after the termination of the employment

relationship (§ 195 German Civil Code (BGB)).
Tax-relevant documents - Tax-relevant documents in the personnel file are kept for six years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
Information on wages and working hours - Information on wages and working hours for (accident) insured with wage proof are kept for five years (§ 165 I 1, IV 2 Social Code Book VII (SGB VII)).

- Payrolls including lists for special payments - Payrolls including lists for special payments, if a booking receipt is available, are kept for ten years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
- Wage lists for interim, final, and special payments - Wage lists for interim, final, and special payments are kept for six years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
- Documents on employee insurance - Documents on employee insurance, if booking receipts are available, are kept for ten years (§ 147 Tax Code (AO), § 257 Commercial Code (HGB)).
- Contribution statements to social security institutions - Contribution statements to social security institutions are kept for ten years (§ 165 Social Code Book VII (SGB VII)).
  Wage accounts - Wage accounts are kept for six years (§ 41 I 9 Income Tax Act (EStG)).
- Applicant data - Kept for a maximum of six months from the receipt of rejection.
- Working time records (for more than 8 hours on workdays) - Kept for two years (§ 16 II Working Time Act (ArbZG)).
- Application documents (following online job advertisement) - Kept for three to a maximum of six months from the receipt of rejection (§ 26 Federal Data Protection Act (BDSG) n.F., § 15 IV General Act on Equal Treatment (AGG)).
- Certificates of incapacity for work (AU) - Kept for up to five years (§ 6 I Act on the Compensation of Expenses (AAG)).
- Documents on company pension schemes - Kept for 30 years (§ 18a Act to Improve Occupational Pensions (BetrAVG)).
- Sickness data of employees - Kept for twelve months from the start of the illness, if the absence in a year does not exceed six weeks.
- Documents on maternity protection - Kept for two years (§ 27 para. 5 Maternity Protection Act (MuSchG)).

Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR),

Legitimate Interests (Article 6 (1) (f) GDPR), Healthcare, occupational and social security processing of special categories of personal data (Article 9 (2)(h) GDPR).

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

employee data is published only with their consent or based on the legitimate interests of the employer, for example, in the case of stage or group photographs taken during a public event; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Job Application Process

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

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

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

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

Ereasure of data: In the event of a successful application, the data provided by the applicants may be further processed by us for the purposes of the employment relationship. Otherwise, if the application for a job offer is not successful, the applicant's data will be deleted. Applicants' data will also be deleted if an application is withdrawn, to which applicants are entitled at any time. Subject to a justified revocation by the applicant, the deletion will take place at the latest after the expiry of a period of six months, so that we can answer any follow-up questions regarding the application and comply with our duty of proof under the regulations

on equal treatment of applicants. Invoices for any reimbursement of travel expenses are archived in accordance with tax regulations.

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

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

Changes and Updates

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

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