ATOSS CSD Software GmbH (as the processor, hereinafter referred to as **"ATOSS"**) and the client (as the controller under data protection law, hereinafter referred to as the "**Customer**") (hereinafter also referred to individually or collectively as the "**Parties**") have concluded a service agreement on the provision of software products by ATOSS and related technical services. The following agreement regarding data processing on the part of ATOSS serves as a basis for fulfilling the statutory provisions on data protection with regard to the existing contractual relationships of the Parties regarding the provision of services by ATOSS in connection with the software solutions (on-premise solution or cloud solution) made available to the Customer by ATOSS.

Insofar as ATOSS processes personal data of the Customer's employees (hereinafter: contract data) in this context, the conditions of the following data processing agreement shall apply.

Data Processing Agreement

Contents:

Annexes:

Preamble

(1) Legal basis

The legal basis is formed by the provisions of the EU General Data Protection Regulation (hereinafter referred to as: GDPR) and the German Federal Data Protection Act (BDSG) in the respectively valid version (hereinafter referred to as: BDSG). Unless expressly defined otherwise within the framework of this Agreement, the terms used such as "personal data", "processing", "controller" or "pseudonymization" shall have the same meaning as in Art. 4 GDPR.

(2) Responsibility of the Controller

Under this Agreement, Customer is also solely responsible for complying with the legal provisions on data protection, in particular for the lawfulness of data transmission to ATOSS, for the lawfulness of the processing of personal data by ATOSS, and for the protection of the rights of data subjects ("Controller" as defined in Art. 4 (7) GDPR).

Section 1 – Object and duration of the processing

(1) Object

ATOSS shall provide services for the Customer with respect to the software products marketed by ATOSS. These services also regularly include aspects of processing on behalf, as ATOSS variously processes personal data of the Customer on behalf of, at the instruction of, and in the interest of the Customer. The Agreement applies accordingly to (remote) testing and maintenance of automated procedures or data processing systems, if access to personal data of the Customer cannot be excluded.

(2) Duration

The term of this Agreement corresponds to the duration of the cooperation between the Parties on the basis of the respective service agreements.

Section 2 – Processed content in detail

(1) Type and purpose of processing

(a) Type

The Customer and ATOSS maintain a business relationship in which ATOSS provides services for the Customer. These can in particular include the following types of processing according to the underlying service agreement:

- Customizing within the meaning of parameterization of the standard software provided by ATOSS as an on-premise solution or as a cloud solution (in particular, assistance in creating employee master records in the database of the standard software provided by ATOSS to the Customer for use, setting up working-time models and time accounts, etc.) and adapting or scripting standard interfaces
- Software maintenance services relating to the standard software provided by ATOSS as an on-premise solution or as a cloud solution (in particular, assistance with software release changes and the elimination of malfunctions reported by the Customer)
- Hotline services relating to the standard software provided by ATOSS as an on-premise solution or as a cloud solution (in particular, assistance in the search for causes of malfunctions reported by the Customer, troubleshooting data transfer to third-party systems via interfaces (e.g., wages and salaries), and data collection with data-acquisition terminals)
- Testing and maintenance of automated procedures or data processing systems to ensure the operational readiness of the standard software provided as part of the cloud solution.
- Administration Services relating to the management of personal data according to the extent of the main contract (in particular, active assistance in the administration of customer's employees personal data in the database of the standard software provided by ATOSS to the Customer for use).

Part of the service provision can be carried out:

- on site at the Customer's premises (at the Customer's option via direct access to its IT systems or by establishing a connection between a client computer of ATOSS and the Customer's IT systems)
- via remote access via a suitable software solution provided by the Customer for remote access (e.g. VPN, desktop sharing), which can be run on current Windows server operating systems (incl. the necessary license).

In all cases, the possibility of read and write access by ATOSS to the contract data contained in the database of the standard software cannot be excluded.

(b) Purpose

The processing is intended to guarantee the functionality and/or the timeliness of the software solution provided to the Customer by ATOSS for use.

(2) Categories of personal data

Within the scope of this contractual relationship, ATOSS generally processes the following categories of personal data of the Customer. Which categories of personal data are processed in the respective contractual relationship depends on which data the Customer specifically transfers to ATOSS for processing.

Employee master data and time-management information

- Master data, such as:
    - Personnel number
    - Salutation, Name, Forename
    - Date of birth
    - Card number(s) of the badge(s)
    - Employee category (e.g., assignment to settlement model)
    - Other contract-relevant data such as entry, exit, and regrouping data
    - Agreements regarding working hours as well as beginning and end of the time-management consideration
    - Contact details (such as address, email, phone numbers)
    - Employee photo
    - Other organizational aspects
- Information regarding affiliation with specific regions / countries / languages
- Information regarding work locations and travel times
- Information about supervisor, employee, and proxy relationships
- Other personal information stored by end users in freely definable fields
- Information about qualifications and training measures
- Information about time balances / time accounts

- Information on individual contractual, collective and other remuneration, vacation and leisure time entitlements of employees:
    - General agreements
    - Actual values and balances
- Information about planned and actual absences
- Information about bookings / clockings, including time and place of booking / clocking
- Information regarding actual attendance, (on-call) standby and working hours
- Information about affiliation to organizational units, projects, orders, cost centers, workplaces, etc. and the time worked for them
- Cafeteria bookings
- Manual notes on master and transaction data
- System-side warnings and error messages for deviations from specifications or rules

Information from personnel deployment planning

- Information about contractual and planning availability of employees
- Information about planning requests of employees
- Information about staff scheduling and actual hours worked
- Information about plan changes
- Information about shift change procedures of employees
- Information about employee performance profiles

Applications and task management

- Requests for absences, including approval process and approval status
- Applications for work-related or service-planning-related procedures, including approval process and approval status
- Pending and completed tasks
- Information about email and SMS notifications sent by the system

Information on access management

- Information about access rights for specific devices, zones and periods
- Access IDs
- PIN for input at the device
- Identification features for biometric access protection (fingerprint procedure, etc.)
- Information about actual or attempted entry or exit of zones, including time and place of booking

System-related information

- System access information
- Information about rights for specific objects and interactions as users of the system
- Last-used system settings and preferences
- Registered system users
- Login attempts
- Logs of user interactions that change data in the system

(3) Categories of data subjects

The categories of data subjects processed include:

Employees within the meaning of Section 26 (8) BDSG.

(4) Functional and geographical restriction of processing

(a) Functional

ATOSS is prohibited from processing contract data beyond the scope of this Agreement. All processing for other purposes, in particular the unauthorized transfer of contract data to third parties, is not permitted. ATOSS is obligated to process the contract data of different customers separately.

(b) Geographical

The provision of the contractually agreed data processing basically takes place in a member state of the European Union (hereinafter the "EU") or in another contracting state of the Agreement on the European Economic Area (hereinafter the "EEA").

ATOSS will provide the contractually agreed service from the service locations agreed in Annex 2 by using the approved sub-processors (see Section 6). Some of these sub-processors are not domiciled in a member state of the EU or in another contracting state of the EEA (hereinafter: third country).

However, a data transfer to a sub-processor in a third country only takes place if the special requirements of Art. 44 et seq. GDPR have been met beforehand (General principles for transfer of personal data to third countries) (cf. Section 6 Para. 2 (b) of this Agreement).

Section 3 – Technical and organizational measures

(1) Ensuring data security

ATOSS must observe the principles of proper data processing and monitor their compliance (see Art. 5 GDPR). It warrants that it complies with the provisions of Art. 28 (3)c, 32 GDPR. To this end, it has taken appropriate measures to ensure data security and, while continuing to make any necessary adjustments, ensures a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. In order to determine the appropriate level of protection, particular account shall be taken of the risks associated with processing, in particular destruction, loss or alteration, whether accidental or unlawful, or unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. This takes into account the state of the art, implementation costs and the nature, scope and purpose of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons.

(2) Documentation and submission of measures

ATOSS must document the technical and organizational measures prior to the commencement of processing with a view to the specific execution of the contract and make this documentation available to the Customer for inspection on request.

(3) Current state of the art and technical adaptations

The technical and organizational measures are subject to technical progress and continuous development. As a result, ATOSS is permitted to implement alternative adequate measures. In doing so, the level of security provided by the measures specified in this Agreement must at a minimum be maintained. Material changes to the technical and organizational measures must be documented and communicated to the Customer in an appropriate manner, e.g. via an online portal which is accessible via the ATOSS website. In this case ATOSS will provide the Customer with an updated description of these measures on request, which will enable the Customer to check compliance with the requirements of Section 3 Para. 1 of this Agreement. By providing this information, ATOSS gives the Customer the opportunity to object to these changes within four weeks. The Customer shall only be entitled to object if the changes do not meet the requirements of Section 3 Para. 1 and Section 3 Para. 2 of this Agreement. If the Customer does not object to the changes within the objection period, approval of the changes shall be deemed to have been given. In the event of an objection, ATOSS may suspend the part of the service which is affected by the Customer's objection.

Section 4 – Authority to issue instructions

(1) Documented instructions

The Customer has the right to issue instructions to ATOSS regarding the type, scope and method of data processing. The Customer solely and exclusively decides with respect to the purposes and means of processing of the contract data. ATOSS may process the contract data only on documented instruction from the Customer, unless ATOSS is legally obligated to process said data.

(2) Certainty and form of the instruction

Instructions are to be issued in clear manner (requirement of clarity of instruction). Instructions may also be issued in writing, in text form or, in urgent cases, orally. The Customer must immediately confirm oral instructions in writing or text form.

(3) Notification of illegality

ATOSS shall immediately notify the Customer if it believes that an instruction is unlawful. This notification does not contain a comprehensive legal analysis. ATOSS is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the Customer.

(4) Rights of data subjects

ATOSS may only provide information to data subjects affected by processing on behalf or to third parties following prior instruction by Customer. Insofar as a data subject directly contacts ATOSS in this regard, ATOSS shall immediately forward this request to the Customer.

(5) Non-contract instructions

ATOSS shall decide on the execution of instructions issued by the Customer which extend beyond the services regulated in this Agreement. In this event, ATOSS may claim separate remuneration.

(6) Regress

In the event that the Customer incurs a justified claim for liability as a result of the performance of an unlawful instruction, it shall have the right to indemnity from ATOSS in this respect.

Section 5 – Obligation to maintain confidentiality

(1) Data and telecommunications secrecy

ATOSS and each person subordinate to ATOSS who has access to contract data are obligated to maintain confidentiality, in particular in accordance with the provisions of Art. 5 (1) lit. f), Art. 28 (3) lit. b), Art. 29, Art. 32 (4) GDPR and Section 88 of the German Telecommunications Act (TKG). The obligation to maintain confidentiality continues even after the termination of this Agreement.

(2) Instruction of all persons deployed for processing on behalf

ATOSS shall take appropriate measures such as, in particular, regular training in data protection, to ensure that persons under its authority who are authorized to process contract data are familiar with the relevant provisions on data and telecommunications secrecy.

Section 6 – Commissioning of sub-processors

(1) Definition of sub-processor

For the purposes of this regulation, sub-contracting relationships are those services that directly relate to the provision of the main service. This does not include ancillary services that ATOSS uses, for example telecommunication services, postal/transport services, maintenance and user services or the disposal of documents and data media, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. Nevertheless, to also ensure the privacy and security of the data of the Customer for outsourced services, ATOSS is obligated to effect appropriate and legally compliant contractual agreements and control measures.

(2) Prerequisites for the legitimacy of the commissioning

The commissioning of sub-processors is only possible with the Customer's consent.

(a) General requirements

Each sub-processor shall be obliged to undertake in writing before the commencement of the processing activities to comply with the same data protection obligations as agreed in this Agreement, unless expressly agreed otherwise. The subcontracting agreement shall guarantee at least the level of data protection required by this Agreement. In particular, each sub-processor must undertake to comply with the agreed technical and organizational security measures pursuant to Art. 32 GDPR and to provide ATOSS with a list of the implemented technical and organizational measures which will be made available to the Customer upon request. The measures taken by the sub-processor may differ from those agreed between the Customer and ATOSS, but may not fall below the level of data protection guaranteed by the measures taken by ATOSS. If a sub-processor refuses to submit to the same data protection obligations as those laid down in this Agreement, the Customer may agree to this, whereby this agreement may not be unreasonably withheld.

(b) Sub-processors in third countries

In the event that a sub-processor is not domiciled in a third country which offers an adequate level of data protection pursuant to Art. 45 GDPR, ATOSS will take sufficient account of this fact. ATOSS will enter into a contract with this sub-processor for data processing on behalf of the sub-processor which, in addition to the provisions listed in (a), is based on the EU standard contract clauses for sub-processors (EU COM decision 2021/914 - Module Three - Transfer of Processors to Processors) or other standard data protection clauses for sub-processors, insofar as these are permitted under Art. 46 para. 2 lit. c GDPR. ATOSS is also entitled to conclude standard contractual clauses or other standard data protection clauses in the name of and in favor of the Customer. The Customer hereby authorizes ATOSS to conclude such an agreement on its behalf.

(3) Current sub-processors

With regard to the companies associated with ATOSS as defined in §§ 15 ff. Stock Corporation Act (AktG) and other sub-processors, all of which are listed in Annex 2 to this Agreement, the consent of the Customer shall be deemed to have been granted upon conclusion of this Agreement.

(4) Further sub-processors

Further outsourcing to sub-processors or the change of existing sub-processors is permissible under the conditions of Section 6 para. 2 of this Agreement even without the separate consent of the Customer, providing that ATOSS notifies the Customer of the outsourcing to (other) sub-processors with reasonable advance notice in text form and the following regulations are fulfilled. Alternatively, ATOSS may provide a website or other type of notification listing all sub-processors accessing the personal data of the Customer and the limited or supplementary services provided by them. At least two weeks before a new sub-processor is authorized to access personal data, ATOSS will notify the Customer and, if applicable, update the website. By notifying the Customer, ATOSS grants the Customer the right to object to the change within two weeks for legitimate reasons. If the Customer does not object within this objection period, consent shall be deemed to have been given. At the Customer's request ATOSS shall provide all necessary information to prove that the sub-processor fulfils all data protection requirements of this agreement. In the event that the Customer objects to the outsourcing, ATOSS may choose whether it does not commission the sub-processor or terminates the service agreement in writing with a notice period of two months.

(5) Validity of the provisions of this agreement also for sub-processors

At the request of the Customer, ATOSS shall provide the Customer with information on relevant data protection obligations undertaken by the sub-processor, including, but not limited to, granting the necessary access to the relevant contractual documents. ATOSS shall regularly inspect its sub-processors and shall, at the Customer's request, confirm compliance with data protection law and the sub-processor's obligations under the contract concluded with it. The Customer shall only be entitled to issue instructions to ATOSS to carry out further tests, which ATOSS will carry out within the scope of what is permissible, if there are justified reasons for doing so.

Section 7 – Customer's obligations and rights; ATOSS's support of the Customer

In order to protect the rights of the data subject (Art. 12 et seq. GDPR and Sections 32 et seq. BDSG), the Customer is obligated to undertake technical and organizational measures, report and communicate data breaches, cooperate with the regulatory authority (Art. 32 to 36 GDPR), and implement quality assurance (Art. 28 (1) GDPR). ATOSS shall support the Customer in observing these obligations. In this context, it shall provide the Customer with all information, insofar as the latter does not possess said information. ATOSS is not obligated to obtain information, which it does not possess for the purpose of providing support. ATOSS shall support the Customer as follows:

(1) Protection of the rights of data subjects

The Customer is obligated to protect the rights of data subjects. If necessary, ATOSS shall assist the Customer in the event that data subjects assert their rights.

(2) Technical and organizational measures

ATOSS shall assist the Customer in ensuring an adequate level of protection by way of technical and organizational measures which take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a possible infringement of rights resulting from security vulnerabilities, as well as enable prompt detection of relevant infringement events.

In this context, the Customer shall ensure that the software solutions provided by ATOSS and the associated technical interfaces are protected against unauthorized access, in particular in a suitable and protective manner (e.g., by granting only temporarily valid access IDs and/or regular password changes and/or by restricting the authorized IP address range, or other comparable measures).

(3) Duty to Report und Duty to Communicate

In the event of ATOSS's breach of the protection of contract data, ATOSS is obligated to support the Customer with regard to the latter's

- reporting obligation vis-a-vis the competent regulatory authority

- duty to notify the data subjects

In the event of a serious operational interruption, suspected breaches of data protection, or violations of this Agreement, whether caused by the Customer, a third party or ATOSS, ATOSS shall immediately and fully inform the Customer of the time, nature and extent of the contract data concerned. The Customer shall immediately be provided with all relevant information required to fulfill the obligation to report vis-a-vis the regulatory authority.

(4) Cooperation with regulatory authorities

The Parties shall cooperate with the competent regulatory authority in the performance of their duties as necessary and in accordance with the following principles.

(a) Logging of processing operations

Both Parties undertake to exclusively access the contract data contained in the database of the software solutions provided by ATOSS using separate user IDs. Consequently, the Customer must assign corresponding separate user IDs to ATOSS for use as part of processing on behalf and/or assist in their preparation to the degree required. ATOSS will make access IDs available only to the relevant persons and, where applicable, to an employee responsible for the management of the access IDs, as well as implement suitable and appropriate measures to secure them against unauthorized viewing and/or use.

(b) Monitoring procedures carried out on the premises of ATOSS or the Customer

(aa) ATOSS shall inform the Customer without delay of monitoring procedures and measures taken by the supervisory authority insofar as they relate to the service agreement. This also applies if a competent authority investigates as part of administrative or criminal proceedings with regard to contract data processing by ATOSS.

(bb) Insofar as the Customer is subject to monitoring by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or third party or any other claim in connection with contract data processing by ATOSS, ATOSS is obliged to support the Customer to the best of its ability.

(c) Data protection impact assessment

Insofar as the Customer itself has a legal obligation to compile a data protection impact assessment, ATOSS shall assist it in carrying out the data protection impact assessment and with any necessary prior consultation with the regulatory authority. This includes in particular the transmission of any required information or the disclosure of any required documents upon the associated request by the Customer.

(5) Quality assurance

(a) Performance of checks

The Customer shall have the right to use spot checks to assure itself of compliance with statutory obligations and with ATOSS's obligations assumed under this Agreement in its business operations during business hours. These spot checks must be notified to ATOSS with a reasonable lead time. The Customer may perform these checks itself or have them performed at its own expense by a third party to be designated by it and obligated to maintain confidentiality in accordance with Section 5 of this Agreement. Third parties in this sense may not be representatives of competitors of ATOSS.

ATOSS may object to be reviewed by an external auditor in the event that the auditor selected by the Customer maintains a competitive relationship with ATOSS.

(b) Documentation

ATOSS shall ensure that the Customer is able to assure itself of compliance with ATOSS's obligations in accordance with Art. 28 GDPR with respect to processing on behalf. ATOSS undertakes to provide the Customer with the necessary information upon request and, in particular, to provide documentation pertaining to technical and organizational measures.

In particular, proof of documentation of technical and organizational measures can also be provided by way of compliance with approved codes of conduct pursuant to Art. 40 GDPR or suitable certification by means of an IT security or data protection audit.

(c) Data protection officer

The contact details of the data protection officer of ATOSS are listed in Annex 1 (Technical and Organizational Measures).

(6) Other support services

ATOSS may charge a separate fee for further support services that are not included in the Service Agreements or which are not the result of wrongdoing by ATOSS.

Section 8 – Deletion or return following conclusion of processing

(1) Right to select

Following the conclusion of the contractually agreed work, or earlier if requested by the Customer – nevertheless at the latest upon termination of the Service Agreements – ATOSS shall, at its own expense, either delete or destroy in a data-protection-compliant manner all documents, data media, processing and utilization results and databases which have come into its possession in connection with the processing on behalf, or return them to the Customer, at the latter's choice. The same applies to test and discarded material. The deletion log must be submitted upon request.

(2) Copies of the contract data

Copies or duplicates of the contract data shall not be created without the Customer's knowledge. This does not include backup copies insofar as these are required to ensure proper data processing, the production and temporary storage of screenshots of contract data as part of parameterized standard software on the IT systems of ATOSS for the purpose of error analysis relating to malfunctions reported by the Customer, as well as data that is required to comply with statutory retention requirements.

(3) Retention periods

Documentation which serves as evidence of orderly and proper data processing must be retained by ATOSS in accordance with the applicable statutory retention periods beyond the end of the contract. To relieve itself of this obligation, ATOSS may turn said documentation over to the Customer at the end of the contract.

(4) Costs

Additional costs incurred as a result of Customer instructions which deviate from or which exceed the scope of this Section 8 (1) shall be borne by the Customer.

Section 9 - Liability

(1) External liability

The Customer and ATOSS shall each be liable for damages to persons affected in accordance with Art. 82 GDPR (external liability).

(2) Internal liability

Each Party shall be entitled to recover from the other party that part of the compensation which corresponds to the other party's share of responsibility for the damage (internal liability).

(3) Liability agreement

With regard to internal liability and without prejudice to external liability towards the data subjects, the Parties agree that, notwithstanding the provisions contained herein, ATOSS's liability for breach of this Agreement shall be subject to the limitations of liability agreed in the service agreement. The Customer shall indemnify ATOSS against all claims and damages which go beyond the liability limitations of the framework agreement, insofar as ATOSS has suffered these in connection with claims of the data subjects due to an alleged violation of provisions of the GDPR or this processing agreement.

Section 10 – Final provisions

(1) Replacement clause; changes and additions

(a) This Agreement shall enter into force upon signature of the service agreement on which the contract data processing is based and, once entered into force in its area of application, shall supersede any potentially existing agreements between the Parties for processing (data) on behalf.

(b) All changes and additions to this Agreement, as well as all ancillary agreements, must be in written or text form to be effective.

(2) Non-applicability of the Customer’s Terms and Conditions/General Conditions of Purchase

It is agreed by the parties that the Customer’s "Terms and Conditions" and/or "General Conditions of Purchase" of the Customer do not apply to this Agreement.

(3) Exclusion of Section 273 BGB

Objection based on the right of retention according to Section 273 German Civil Code (BGB) is excluded with regard to the processed data and the associated data media.

(4) Obligation to maintain confidentiality

The Parties undertake to treat confidentially all business and trade secrets obtained in the course of processing on behalf as well as the data protection measures of the respective other party. Business and trade secrets means all facts, circumstances and processes relating to the business of one of the Parties which are not public but which are accessible to only a limited group of persons and in whose non-disclosure the relevant party has a legitimate interest. Data protection measures means all technical and organizational measures taken by a party within the meaning of Annex 1 to this Agreement. This obligation to maintain confidentiality continues following the termination of this contract.

(5) Obligation to provide information in the event of endangerment of processed data

In the event of the endangerment of the processed data at ATOSS due to attachment or confiscation, insolvency or settlement proceedings, or other events or third-party actions, ATOSS is obligated to inform the Customer without delay.

(6) Legal venue

Subject to any exclusive legal venue, the sole legal venue for all disputes arising from and in connection with this Agreement is Munich.

(7) Governing law

This Agreement is governed by German law.

(8) Severability

Should individual parts of this Agreement be or become wholly or partially invalid or unenforceable, this shall not affect the validity of the remaining provisions. The Parties agree to replace the invalid or unenforceable provision with an effective and enforceable provision that comes as close as possible to the originally intended purpose of the ineffective or unenforceable provision. This applies accordingly in the event of a regulatory gap or omission.