Data Processing Agreement
("DPA")

Table of content:

DPA-Exhibits:

DPA-Exhibit I	**Description of the processing**
DPA-Exhibit II	**Technical and organizational measures**
DPA-Exhibit III	**List of authorized sub processors**

Preamble

This Data Processing Agreement ("**DPA**") is included in the contract for the provision of ATOSS products on premises and for an ATOSS CLOUD SERVICE (each and collectively hereinafter referred to as "**ATOSS PRODUCTS**") and other affiliated services or professional services (hereinafter referred to as "**CONTRACT**"). Therefore, this DPA is at the same time an integral part of a contract concluded in writing (also in electronic form) between the contracting ATOSS company (as processor - hereinafter referred to as "**ATOSS**") and the CUSTOMER. Both, ATOSS and the CUSTOMER are hereinafter referred to collectively as the "**PARTIES**", each a "**PARTY**".

The PARTIES agree that the CUSTOMER may also allow its AFFILIATED COMPANIES to use the licensed ATOSS PRODUCTS in accordance with the provisions of the respective CONTRACT. Since in such a case personal data of AFFILIATED COMPANIES of the CUSTOMER are also processed by ATOSS, this DPA shall apply to the following scenarios:

- The CUSTOMER is the sole controller with regard to the personal data made available to ATOSS for the data processing.

- Besides the CUSTOMER, its AFFILIATED COMPANIES also use the licensed ATOSS PRODUCTS; the CUSTOMER and its AFFILIATED COMPANIES are each the sole or joint controller.
- The CUSTOMER is the controller with respect to its own personal data and the processor with respect to the personal data of its AFFILIATED COMPANIES. From the point of view of its AFFILIATED COMPANIES, ATOSS is a sub-processor of the CUSTOMER.
- The CUSTOMER is only a processor of its AFFILIATED COMPANIES and ATOSS is a sub-processor with regard to the personal data.

Notwithstanding the above-listed scenarios, the CUSTOMER shall always be the central and direct operational contact for ATOSS under this DPA.

Insofar as ATOSS processes personal data in this context, the conditions of this DPA shall apply.

For the provision of the ATOSS PRODUCTS in accordance with the CONTRACT the use of sub processors is required. In this respect, the CUSTOMER is aware that ATOSS cannot provide the ATOSS PRODUCTS without sub processors. The use of sub processors shall be governed by § 6 of this DPA.

§ 1 Subject matter of this DPA

1. Purpose and scope: The purpose of this DPA is to ensure compliance with Art. 28 (3) and (4) of the GDPR.

   The PARTIES listed in the CONTRACT have agreed to this DPA in order to ensure compliance with Art. 28 (3) and (4) GDPR. This DPA applies to the processing of personal data as specified in DPA Exhibit I.

   Exhibit I to III are an integral part of this DPA.

   Where in this DPA the terms defined in the GDPR are used, those terms shall have the same meaning as in that Regulation.

   In all other respects, the definition of the CONTRACT shall apply to this DPA.

   This DPA shall be read and interpreted in the light of the provisions of the GDPR. This DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for in the GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

2. Duties of the CUSTOMER: This DPA applies without prejudice to the obligations to which the controller is subject by virtue of the GDPR.

§ 2 Description of the processing

The specific scope of services shall be agreed by the PARTIES in the CONTRACT. The services under consideration regularly include matters in the sense of data processing of personal data. This shall apply accordingly to (remote) testing and (remote) maintenance of automated processes or the use of data processing systems, insofar as access to personal data of the CUSTOMER cannot be excluded in the process.

The details of the relevant processing operations, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the CUSTOMER, are specified in **DPA-Exhibit I - Description of the processing.**

§ 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). ATOSS ensures that it complies with the provisions of Art. 28 (3) lit. c), 32 GDPR. To this end, ATOSS has taken appropriate measures to ensure data security and, while continuing to make any necessary adjustments, ensure a level of protection appropriate to the risk regarding the confidentiality, integrity, availability and resilience of the systems. To determine the appropriate level of protection, particular account shall be taken of the risks associated with data 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 shall at least implement the technical and organizational measures specified in **DPA-Exhibit II - Technical and organizational measures** to ensure the security of the personal data.

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 DPA 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., through e-mail or via an online portal which is accessible via the ATOSS website). By providing this information, ATOSS gives the CUSTOMER the opportunity to object to these changes in writing or text form within six (6) weeks. The CUSTOMER shall only be entitled to object if the changes do not meet the requirements of § 3 clause 1 and § 3 clause 2 of this DPA. If the CUSTOMER does not or not justified object to the changes within the objection period, the approval of the changes shall be deemed to have been given after the deadline. In the event of a justified objection, ATOSS may suspend the part of the service provision which is affected by the CUSTOMER's justified objection.

§ 4 Authority to issue instructions

1. Documented instruction: ATOSS shall process personal data only on the documented instructions from the CUSTOMER, unless ATOSS is required to do so by Union law or by the law of the Member State to which ATOSS is subject. In this case, ATOSS shall inform the CUSTOMER of these legal requirements before processing, unless the law prohibits this on important grounds of public interest. The CONTRACT including this DPA constitutes a documented instruction of the CUSTOMER.

2. Certainty and form of instructions: Unless otherwise expressly agreed in this DPA, instructions shall be given in a clear manner (requirement of clarity of instructions). Instructions must be issued in writing or in text form.

3. Feasibility of the instruction: ATOSS will inform the CUSTOMER in text form within a reasonable period of time, insofar as the implementation of the instruction can be con-

figured independently by the CUSTOMER within the scope of the standard functionalities. Instructions of the CUSTOMER which represent a deviation from the services stipulated in the CONTRACT or this DPA shall be treated as a change request of the CONTRACT. The obligations under the CONTRACT and this DPA shall remain unaffected during the period of review. ATOSS will make reasonable efforts to implement instructions from the CUSTOMER that qualify as a request for contract amendment, insofar as they are necessary and technically possible under data protection law and do not require any changes to the ATOSS PRODUCTS. ATOSS will inform the CUSTOMER in advance in text form if it is apparent that ATOSS will incur additional work and/or additional costs for the review and implementation of the instruction. ATOSS will after consultation with the CUSTOMER submit an offer for the commissioning of fee-based services for the further review and implementation of the instruction. In the event that no agreement on an amendment to the CONTRACT is reached, the obligations arising from the CONTRACT shall remain in force.

Instructions confirmed by ATOSS shall be implemented by joint agreement of the PARTIES within a reasonable period of time.

4. Notification of illegality: ATOSS shall immediately inform the CUSTOMER if, in ATOSS opinion instructions given by the CUSTOMER infringe the GDPR or applicable Union or Member State data protection law. 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.

5. 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.

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

§ 5 Obligation to maintain confidentiality

1. Data and telecommunications secrecy: ATOSS and each person subordinate to ATOSS who has access to personal 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 § 3 TDDDG. The obligation to maintain confidentiality continues even after the termination of this DPA.

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 personal data are familiar with the relevant provisions on data and telecommunications secrecy.

§ 6 Commissioning of sub processors

1. [intentionally left blank]

2. Prerequisites for the legitimacy of the commissioning: The commissioning of sub processors is only possible with the CUSTOMER's consent.

a) General requirements: Where ATOSS engages a sub processor for carrying out specific processing activities (on behalf of the CUSTOMER), ATOSS shall do so by way of a contract which imposes on the sub processor, in substance, the same data protection obligations as the ones imposed on ATOSS in accordance with this DPA. ATOSS shall ensure that the sub processor complies with the obligations to which ATOSS is subject pursuant to this DPA and to the GDPR. At the CUSTOMER's request, ATOSS shall provide a copy of such a sub processor agreement and any subsequent amendments to the CUSTOMER. To the extent necessary to protect business secret or other confidential information, including personal data, ATOSS may redact the text of the agreement prior to sharing the copy.

ATOSS shall remain fully responsible to the CUSTOMER for the performance of the sub-processor's obligations in accordance with the CONTRACT with ATOSS. ATOSS shall notify the CUSTOMER of any failure by the Sub-Processor to fulfill its contractual obligations with respect to services to the CUSTOMER.

b) Sub processors in third countries: Any transfer of data to a third country or an international organization by ATOSS shall be done only on the basis of documented instructions from the CUSTOMER (cf. § 4) or in order to fulfil a specific requirement under Union or Member State law to which ATOSS is subject and shall take place in compliance with Chapter V of the GDPR.

The CUSTOMER agrees that where ATOSS engages a sub processor in accordance with this § 6 for carrying out specific processing activities and those processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, ATOSS and the sub processor can ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46 (2) of the GDPR, provided the conditions for the use of those standard contractual clauses are met.

3. Current sub processors: ATOSS has the CUSTOMER's general authorization for the engagement of sub processors in DPA-Exhibit III - List of authorized sub processors to this DPA. With regard to the use of such sub processors the consent of the CUSTOMER shall be deemed to have been granted upon conclusion of this DPA.

4. Further sub processors: Further sub processors or the change of sub processors is permissible under the conditions of § 6 (2) of this DPA even without the explicit consent of the CUSTOMER, providing that ATOSS notifies the CUSTOMER of the use of further sub processors with reasonable advance notice (e.g., through e-mail or via an online portal which is accessible via the ATOSS website) and the following regulations are fulfilled: ATOSS shall inform the CUSTOMER at least 6 weeks in advance of any intended changes to this list by adding or replacing sub-processors and thereby give the CUSTOMER sufficient time to object to these changes before commissioning the sub-processor(s) concerned.

ATOSS shall provide the CUSTOMER with an updated list listing all sub processors processing the CUSTOMER's personal data and the ancillary services provided by them.

By providing this information, ATOSS gives the CUSTOMER the opportunity to object to these changes within six (6) weeks. The CUSTOMER shall only be entitled to object if the changes do not meet the requirements of § 6 clause 2 of this DPA. If the CUSTOMER does not or not justified object to the changes in writing or text form within the objection period, the approval of the changes shall be deemed to have been given after the deadline. In the event of a justified objection, ATOSS may suspend the part of the service provision which is affected by the CUSTOMER's justified objection. In the event that the CUSTOMER objects to the use even after consultation with ATOSS, ATOSS may choose whether it does not commission the sub processor or terminates the CONTRACT in writing with a notice period of two (2) months. This provision supplements the termination provision in the CONTRACT.

5. Validity of the provisions of this DPA 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.

§ 7 CUSTOMER's obligations and rights; ATOSS's support of the CUSTOMER

To protect the rights of the data subject (Art. 12 et seq. GDPR), 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, ATOSS 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: ATOSS shall inform the CUSTOMER with undue delay of any request received from a data subject of the CUSTOMER. ATOSS shall not respond to the request itself. 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 ATOSS PRODUCTS 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 personal 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 DPA, 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 personal 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. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall as it becomes available subsequently be provided without undue delay.

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) 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 CONTRACT. This also applies if a competent authority investigates as part of administrative or criminal proceedings with regard to personal 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 personal data processing by ATOSS, ATOSS is obligated to support the CUSTOMER to the best of its ability.

b) 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. Documentation and compliance:

a) Audits: The Parties shall be able to demonstrate compliance with this DPA. ATOSS shall deal promptly and adequately with inquiries from the CUSTOMER about the processing of data in accordance with this DPA. ATOSS shall make available to the CUSTOMER all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from GDPR. At the CUSTOMER's request, ATOSS shall also permit and contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on an audit, CUSTOMER may take into account relevant information and certifications held by ATOSS.

The CUSTOMER may choose to conduct the audit by itself or mandate an independent auditor. ATOSS may object to the inspection by an independent auditor if the auditor selected by the CUSTOMER is in a competitive relationship with ATOSS or has not been obliged to observe confidentiality.

The costs of audits pursuant to § 7 (5) lit. a) shall be borne by the CUSTOMER.

b) Documentation: In particular, proof of documentation of technical and organizational measures can 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 **DPA-Exhibit II - Technical and organizational measures.**

§ 8 Deletion or return following conclusion of processing

1. Deletion or return: The deletion and return of personal data is governed by the provisions in **DPA-Exhibit I - Description of processing** and the contractual provisions.
2. [intentionally left blank]
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 this DPA. To relieve itself of this obligation, ATOSS may turn said documentation over to the CUSTOMER at the end of this DPA.
4. Costs: Additional costs incurred as a result of CUSTOMER instructions which deviate from, or which exceed the scope of this § 8 (1) shall be borne by the CUSTOMER.

§ 9 Right to compensation and liability

1. The PARTIES are liable under this DPA in accordance with the statutory provisions of the GDPR.
2. [intentionally left blank]
3. [intentionally left blank]

§ 10 Final provisions

1. Replacement clause; changes and additions:

a) This DPA shall enter into force upon conclusion of the CONTRACT 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) Unless explicitly agreed otherwise, all changes and additions to this DPA, as well as all ancillary agreements, must be in written or text form to be effective.

c) [intentionally left blank]

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 DPA.
3. Exclusion of the right of retention: Objection based on the right of retention is excluded regarding the processed personal data and the associated data media.
4. [intentionally left blank]
5. Obligation to provide information in the event of endangerment of processed personal 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 undue delay.
6. Place of jurisdiction: The provisions of § 10 clause 7 of this DPA shall apply.

7. Choice of law and place of jurisdiction: The applicable data protection provisions shall apply to legal remedies of a data subject against ATOSS as a processor. For legal remedies of the PARTIES arising from or in connection with this DPA, the provisions of the CONTRACT shall apply with regard to the choice of law and the place of jurisdiction.

8. Severability: Should individual parts of this DPA 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.

DPA – Exhibit I

- Description of the processing -

1. **Categories of data subjects whose personal data is transferred**

Depending on the respective CUSTOMER, the following data subjects may be concerned by the processing:

- Employees as defined in § 26 (8) BDSG [German Federal Data Protection Act]
- Civil servants and aspiring civil servants of the countries
- Employees who are subject to collective agreements, as well as trainees

2. **Categories of personal data transferred**

The categories of personal data that are processed in the respective individual CONTRACT depend on the configuration and parametrization selected by the CUSTOMER in each case and the agreed module selection.

Additional information can be found in the respective contractual documents and/or other information provided (e.g., in the context of using our website, digital customer lounge).

Relevant categories of personal data can be in particular:

a) Employee master data and time management information

- Master data such as:
  - Personnel number
  - Title, surname, first name
  - Date of birth
  - Identity card(s) no.
  - Employee category (for example, payroll model assignment)
  - Other contract-relevant data such as entry, exit and regrouping data
  - Agreements on working time and the start and end of time management considerations
  - Contact details (such as address, email, telephone numbers)
  - Staff photo
  - Other organisational features
- Information about affiliation to certain regions / countries / languages
- Information about work locations and travel times
- Information on supervisor, employee and deputy relationships
- Other personal data stored by end users in freely definable fields
- Information on qualifications and training
- Information about time balances / time accounts
- Information on individual contractual, collectively agreed and other remuneration, holiday and time off entitlements of employees:
  - general arrangements
  - Values and balances
- Information on planned and actual absences
- Information about bookings / stamping incl. time and place of booking / stamping
- Information on actual attendance, (call) on-call and working hours

- Information about affiliation to organisational units, projects, orders, cost centres, workplaces etc. and the times worked for them
- Canteen bookings
- Manual annotations to master and transaction data
- System warnings and error messages in case of deviations from specifications or rules
- Communication data (e.g., data in chats)

b) Information from workforce planning

- Information on contractual and planning availability of employees
- Information about planning requests from employees
- Information on employee scheduling and actual hours worked
- Information about plan changes
- Information about shift swaps of employees
- Information about employee performance profiles

c) Application and task management

- Requests for absences incl. approval history and status
- Requests for operations relevant to working time or duty scheduling, including approval progress and status
- Pending and completed tasks
- Information about e-mail and SMS notifications sent by the system

d) Information of the access management

- Information about access authorisations for specific devices, zones and time periods
- Access IDs
- PIN for input on the device
- Identification features for biometric access control (fingerprint method, etc.)
- Information about actual or attempted entry or exit of zones incl. time and place of booking

e) System related information

- System access information
- Information about authorisations for certain objects and interactions as a user of the system
- Internet Protocol (IP), Paket information, including URLs, time stamps, telemetric data, ports related to the use of ATOSS Cloud Services
- Browser information (browser user agents, log data) related to use of ATOSS Cloud Services
- Last used system settings and preferences
- Logged in system users
- Login attempts
- Logs of user interactions that modify data in the system.

f) Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the processor shall apply specific restrictions and/or additional safeguards.

3. Nature of the processing

a) Processing activities

ATOSS's services may include the following processing activities without limitation, - as described in more detail in the respective individual CONTRACT with the CUSTOMER:

- Customizing in the sense of parameterising ATOSS PRODUCTS (particularly support in creating employee master data in the database of the standard software provided to the CUSTOMER by ATOSS for use, in setting up working time models and time accounts, etc.) and adapting or scripting standard interfaces.
- Software maintenance for the ATOSS PRODUCTS (particularly support with software release changes, the import of continuous modifications, and eliminating reported malfunctions);
- Hotline services for ATOSS PRODUCTS (particularly receiving information or supporting the analysis for reported malfunctions; troubleshooting for data transfer via interface to third-party systems (e.g., payroll and salary) as well as for data entry with data entry terminals);
- Testing and maintenance work of automated processes or of data processing systems to ensure the operational readiness of ATOSS PRODUCTS.
- Administration services relating to the management of personal data according to the extent of the CONTRACT (in particular, active assistance in the administration of customer's employee's personal data in the database of the ATOSS PRODUCTS provided by ATOSS to the Customer for use).

To that end, the processing activities – whether in whole or in part – may be carried out:

- locally, on the CUSTOMER's premises (at the CUSTOMER's option by direct access to its IT systems or by establishing a connection between a client computer of ATOSS and the IT systems of the CUSTOMER);
- by remote access, via a secure VPN connection and a suitable software solution for remote access provided by the CUSTOMER (e.g., VPN, desktop sharing) which is executable on current Windows server operating systems (incl. the necessary licence) or, in the case of ATOSS PRODUCTS, by remote access via a secure VPN connection to the IT systems of the operator of the cloud infrastructures on which the CUSTOMER's personal data are processed.

In all cases, the possibility of read and write access by ATOSS to the database integrated in the ATOSS PRODUCTS and, if applicable, to the further information-processing systems connected thereto at the respective CUSTOMER's premises which contain personal data cannot be excluded.

b) Substantive limitation of the processing

ATOSS is not permitted to process the CUSTOMER's personal data beyond the scope of this DPA. Processing for other purposes, in particular the unauthorized transfer of order data to THIRD PARTIES, is not permitted. ATOSS is obliged to process the personal data of different customers separately.

c) Local restriction

The provision of the data processing agreed under a CONTRACT shall generally take place in a member state of the European Union (EU) or in another contracting state of the Agreement on the European Economic Area (EEA) or in Switzerland (CH).

If the data processing takes place in a third country (i.e., outside the EU, the EEA or Switzerland), ATOSS shall ensure that the special requirements of Art. 44 et seqq. GDPR and the provisions of this DPA are fulfilled.

d) Access logs

The PARTIES undertake to access the database integrated in the ATOSS PRODUCTS and the personal data processed therein exclusively by using separate user IDs. This requires that the CUSTOMER allocates corresponding separate user IDs for ATOSS and cooperates in setting them up to the extent required. ATOSS shall make these user IDs accessible exclusively to the personnel required for the performance of the services and shall secure them against unauthorised inspection and use by taking suitable and appropriate measures.

4. Purpose(s) of the processing

ATOSS shall process the personal data of the respective CUSTOMER only for the specific purposes stated in the CONTRACT, unless further instructions are given by the CUSTOMER to ATOSS. The basic purpose of the processing is to ensure the functionality and up-to-dateness of the ATOSS PRODUCTS made available to the CUSTOMER by ATOSS for use.

5. Period for which the personal data will be retained

The personal data of the CUSTOMER shall be processed by ATOSS only for the duration specified in the CONTRACT between the PARTIES. This usually corresponds to the contractual term of the CONTRACT including any post-contractual obligations. If the term of the CONTRACT is not specified, the duration of the commissioned processing shall begin with the commencement of the services owed and shall end with the end of the provision of the services. The obligation to delete data does not exist if there is an obligation to store the data under Union law or applicable national law, which includes, in particular, obligations to retain data under tax law or commercial balance sheet retention obligations.

***

DPA – Exhibit II

- Technical and organisational measures -

All offices and all group companies of ATOSS Software SE use the entire IT infrastructure of the company headquarters in Munich. All activities - including remote activities - are carried out exclusively with IT resources and equipment provided and centrally controlled by ATOSS Software SE. The internal data center is located in Munich.

The technical and organizational measures taken by ATOSS with regard to the internal IT systems and internal business processes of the offices and group companies of ATOSS Software SE are listed below. Depending on the respective ATOSS location, (minor) deviations are possible.

I. CONFIDENTIALITY

1. Physical access control

Measures suitable for preventing unauthorized persons from access to office buildings, workplaces, and internal data processing systems.

I.1.1	**Office building and workplaces**	
	Technical measures	**Organizational measures**
	☒ Burglar alarm system (BAS) ☒ Electronic locking system ☒ Access technologies (e.g. RFID, PIN, or mechanical keys) with person-specific allocation ☒ Mechanical locking system for the building / offices ☒ Smart cards ☒ Bell system with camera ☒ Video surveillance of the entrance areas ☒ Motion detector, attack reporter ☒ Guard duty	☒ Site office managers ☒ Issuance of keys is protocolled by means of issuance and return protocols ☒ Security zones ☒ Reception/visitor areas ☒ Restriction of access for persons not belonging to the company (e.g. visitors) ☒ Visitor management process, incl. registration, deregistration, visitor passes, and accompaniment by staff ☒ Due care in the selection of the guard service
I.1.2	**Internal data center**	
	Technical measures	**Organizational measures**
	☒ Operation of the internal data center by the ATOSS IT department ☒ Intrusion alarm system (IAS) ☒ Electronic locking system ☒ Access technology (e.g. RFID and mechanical keys) with person-specific allocation ☒ Video surveillance	☒ Limitation of key issuance and restriction of access rights to the data center to privileged personnel of the ATOSS IT department ☒ Issuance of keys is protocolled by means of issuance and return protocols ☒ Visitor management process, incl. registration, deregistration, visitor passes, and accompaniment by staff

2. Digital access control

Measures suitable to prevent internal data processing systems and information from being used by unauthorized persons.

I.2	**Internal systems, applications, notebooks, smartphones**	
	Technical measures	**Organizational measures**
	☒ Connection of the offices and group companies via an encrypted server network (domain controller) ☒ Exclusive use of IT equipment, applications, and systems that have been approved internally by ATOSS ☒ Ban on BYOD ☒ BIOS-supported hard disk authentication of mobile end devices (e.g. notebooks, tablets) ☒ Housing lock ☒ Login with personalized user accounts + password ☒ Login with privileged accounts + password + 2nd factor ☒ Logging of logins and logouts, login attempts ☒ Automatic password-protected desktop / screen lock ☒ Prohibition with exception for use of hardware-encrypted removable media (e.g. USB sticks with 256-bit AES) ☒ Use of VPN connection for remote access ☒ Mobile device management ☒ Hard disk encryption (256-bit AES) ☒ Virus, spyware, malware protection ☒ SIEM ☒ Firewalls ☒ Spam filter ☒ Web Proxies (incl. virus protection) ☒ Intrusion detection/prevention system (IDS/IPS) ☒ Password server ☒ Encryption of data transfer (e.g. BIOS passwords, VPN connections, Cryptshare, Ironkeys incl. virus scanner) ☒ Applications are checked for the technical possibility to prevent or close interfaces	☒ User and authorization management ☒ Password management ☒ Limitation of login attempts and automatic access blocking ☒ Policy for handling passwords and access protection ☒ Specifications for manual locking ☒ Password history ☒ Policy on handling company assets, incl. erasure / destruction ☒ Policy on data protection and information security in the organization ☒ Smart phone policy ☒ Social media policy ☒ Control and storage of the logs ☒ Security updates ☒ Vulnerability scans (monthly) ☒ Penetration tests (annually) ☒ Incident management ☒ Change management ☒ IT emergency management

3. Access control

Measures to ensure that those authorized to use internal data processing systems can only access the information subject to their access authorization and that information cannot be read, copied, modified, or removed by unauthorized persons during processing, use and after storage.

I.3	**Information (irrespective, whether in electronic or physical form)**	
	Technical measures	**Organizational measures**
	☒ Access authorizations are defined, coordinated, and controlled by a central Microsoft Active Directory or a company's own domain. ☒ Logging of access to applications (entry, modification, and erasure of access authorizations) ☒ Data protection safe ☒ Staff lockers ☒ Destruction of electronic data carriers by an external disposal service provider (standard DIN 66399-3) ☒ Disposal of classified documents in sealed data bins ☒ Document destruction and emptying by an external disposal service provider	☒ Role-based authorization concept ☒ User and authorization management (incl. specifications for entry, change of function, departure) ☒ Limited number of administrators / privileged user accounts ☒ Policy on handling company assets, incl. erasure / destruction ☒ Clean desk policy ☒ Issuance of staff locker keys is protocolled by means of issuance and return protocols ☒ Control and storage of the logs ☒ Due care in the selection of the disposal service provider ☒ Separate access points for external IT systems

4. Separation control

Measures to ensure that data collected for different purposes are processed separately either logically or physically.

I.4	**System control / storage control**	
	Technical measures	**Organizational measures**
	☒ Separation of personal data of the CUSTOMER in terms of commissioned data processing and other internal business information ☒ Separation of productive and test environments ☒ Multi-tenant capability of relevant applications ☒ Testing of software / hardware takes place in isolated virtual environments (sandboxing)	☒ Prohibition of transmitting personal data of the CUSTOMER in the sense of commissioned data processing outside defined transmission and communication channels to ATOSS ☒ Definition of internal database rights ☒ Internal domain management ☒ Internal network topology plans ☒ Change management

II. INTEGRITY

1. Input control

Measures to ensure it is possible to check and retrospectively determine whether information has been entered into internal data processing systems, modified while in those systems, or removed from them, and by whom.

II.1	Logging (e.g., operating systems, networks, firewalls, databases, applications)	
	Technical measures	**Organizational measures**
	☒ Technical logging of user logins and logouts on ATOSS internal data processing systems ☒ Central storage of log data in relation to ATOSS internal data processing systems ☒ Clock synchronization / timeserver	☒ Role-based input, modification and erasure restrictions are managed and controlled via user and authorization management ☒ Retention of logs in accordance with legal requirements ☒ Manual or automated control of logs

2. Transfer control

Measures to ensure that personal data cannot be read, copied, altered, or removed by unauthorized persons during electronic transmission or during their transport or storage on data media, and that it is possible to verify and establish the bodies to which personal data are intended to be transmitted by data transmission equipment.

II.2	Electronic and physical data transfers	
	Technical measures	**Organizational measures**
	☒ E-mail encryption (S/MIME, TLS, certificates) ☒ Content filter for e-mail and web ☒ Telephony encryption (SAML, TLS, certificates) ☒ Use of VPN on mobile devices ☒ Ban on using hardware-encrypted removable media (e.g., USB sticks with 256-bit AES) without special permission ☒ Locked letterboxes ☒ Use of predefined communication and transmission channels	☒ Policy for dealing with external files ☒ Collection of letter post exclusively by the company's in-house reception staff ☒ Personal distribution for external letter post ☒ Personal distribution for internal, (very) confidentially marked letter mail / documents ☒ Deliveries of goods only within delivery zones with personal acceptance ☒ Defined specifications for remote access (see supplementary information below*) ☒ Prevention / erasure of transmissions of non-anonymized personal data of the CUSTOMER outside of agreed and specified transmission paths (see supplementary information*).

***Supplementary information:**

The transmission of non-anonymized personal data of the CUSTOMER may only be carried out by the CUSTOMER itself, either via the established transmission paths in the ATOSS Cloud Services or on the CUSTOMER's own IT systems. The sending of non-anonymized personal data of the CUSTOMER via e-mail traffic to recipients at ATOSS is to be refrained from.

For the provision of parameterization, software maintenance and hotline services with access to the licensed customer installation, the CUSTOMER must ensure access and transfer control through appropriate configurations in user management:

- The registration or deregistration of users (including ATOSS hotline and customer service consultants) can only be carried out by the CUSTOMER and monitored in accordance with test cycles specified by the CUSTOMER.
- Parameterization, software maintenance and hotline services with access to the licensed customer installation on the CUSTOMER's IT systems on site or by remote access require prior user authorization or activation by the CUSTOMER.
- Parameterization, software maintenance and hotline services via remote access shall be provided exclusively via secure connections and in compliance with the technical and organizational measures for the protection of personal data described in this Exhibit.
- To the extent necessary, ATOSS hotline and customer service consultants shall cooperate in the configuration of technical control devices on the instructions of the CUSTOMER. If remote access is to be made to the CUSTOMER's own IT systems, the CUSTOMER shall provide a suitable software solution for remote access (e.g. VPN, desktop sharing) that is executable on current Windows server operating systems (including the necessary license). Remote access is controlled and managed by the ATOSS Remote Access Services (RAS) department.
- The CUSTOMER is authorized to monitor remote accesses and to stop them at any time.
- Personal data of the CUSTOMER may be stored on removable data storage devices of ATOSS only on the explicit instruction of the CUSTOMER. Corresponding copies are deleted by ATOSS after completion of the specific access.

III. AVAILABILITY

Measures to ensure that personal data are protected against accidental destruction or loss.

I.1.1	**Office building and workplaces, hardware, IT resources**	
	Technical measures	**Organizational measures**
	☒ Fire protection precautions (e.g., fire and smoke detection systems) ☒ Fire doors and escape routes ☒ Emergency power supply ☒ Certified and approved electrical installations (including surge protection and area-oriented power distribution) ☒ Synchronized UPS system ☒ Telecommunication and provider connections via at least two fiber optic connections and separate transmission technology ☒ Redundant connection of all important components ☒ Electrical revision (VDS) ☒ Structured wiring	☒ Electrical checks of all electronic devices according to the test cycle from the manufacturer ☒ Regular functional tests ☒ Performance of maintenance and due care by service providers ☒ Due care in the selection of service providers ☒ Documentation of the switch ports ☒ Security updates ☒ Incident management ☒ Change management ☒ IT emergency management

	☒ Separate "network cabinet" for connection and network ☒ Computer-controlled monitoring system of the connections	
I.1.2	**Internal data center**	
	Technical measures	**Organizational measures**
	☒ Fire protection precautions (e.g., through a proprietary fire protection section, connection to fire alarm center, smoke detectors) ☒ Humidity sensors ☒ Smoke aspiration system (RAS) ☒ Redundant air conditioning ☒ Emergency power system (GRS, diesel generator) ☒ Redundant uninterruptible power supply ☒ Separate circuits ☒ Telecommunication and provider connections via at least two fiber optic connections and separate transmission technology. ☒ Redundant connection of all important components ☒ Electrical revision (VDS) ☒ Structured LAN cabling ☒ Separate "network cabinet" for connection and network ☒ Computer-controlled monitoring system of the connections ☒ Redundant internal storage systems ☒ Backup tapes, retention of backups in redundant storage system in the data center ☒ Security service at another location	☒ Backup and disaster recovery plan ☒ Geographical separation of the backup storage locations from the location of the primary server ☒ Data backups are carried out several times a day (for relevant internal IT systems) ☒ Backups are encrypted ☒ Regular data recovery tests and logging of results ☒ Backups are created via real-time mirroring ☒ Transport of the security tapes by security service ☒ Due care in the selection of the security service ☒ Security updates ☒ Incident management ☒ Change management ☒ IT emergency management

IV. ENCRYPTION AND PSEUDONYMIZATION

☒ The electronic transmission of e-mail traffic is encrypted.
☒ The electronic transmission of personal data may only take place via encrypted and defined transmission and communication channels. The transmission of non-anonymized, personal CUSTOMER DATA (e.g., test data, employee master data, etc.) via transmission and communication channels that have not been jointly defined in advance is not permitted.
☒ Personal data shall be stored on IT systems of the CUSTOMER or in the ATOSS Cloud Services.
☒ The storage of personal data in the ATOSS internal business operations shall be encrypted.
☒ All data on mobile computers and storage media are encrypted.
☒ All encryption technologies used productively are state of the art*.
☒ The management of the key material is defined and documented for the relevant IT systems.
☒ Transport encryption is implemented exclusively end-to-end.
☒ A set of rules with requirements for encryption strength, algorithm, and key management is implemented.
☒ Pseudonymization of personal data using one-way functions.
☒ Pseudonymization by assignment tables, these are separated from the rest of the data processing.

**Definition* - state of the art comprises the technical knowledge gained up to the respective point in time, which has found its way into operational practice and is generally recognized.

V. PROCEDURES FOR REGULAR REVIEW, ASSESSMENT, AND EVALUATION

1. Data protection management

IV.1	**Compliance with and verification of the measures**	
	Technical measures	**Organizational measures**
	☒ A review of the effectiveness of the technical and organizational protection measures is carried out at least once a year (external GDPR audit). ☒ Tool-supported control of regular staff training and attendance	☒ Internal data protection officer (contact details are posted on the ATOSS website) ☒ Staff training concept ☒ Regular sensitization of employees (at least annually) ☒ Compliance with the information obligations pursuant to Art. 13 and Art. 14 GDPR ☒ Formalized process for handling data protection requests and notifications (also with regard to the obligation to notify supervisory authorities) ☒ Data protection impact assessments (DPIAs) are carried out as required. ☒ Involvement of data protection officers in internal and external data protection matters

2. Processor control

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the CUSTOMER's instructions.

IV.3	**Authorized sub processors**	
	Technical measures	**Organizational measures**
	☒ Certified, documented security measures of (hosting) service providers	☒ Due care in the selection of ATOSS sub processors ☒ Submission and verification of evidence of control measures and GDPR compliance of (hosting) service providers (e.g. audit reports, certificates) ☒ Conclusion of a data processing agreement ☒ Documentation of instructions ☒ Obligation of ATOSS sub processors to confidentiality and data secrecy ☒ Conclusion of EU standard contractual clauses or other guarantees under Art. 46 GDPR (if required) ☒ Regular audits of sub processors with regard to data protection and information security ☒ Obligation of sub processors that a transfer impact assessment has been carried out regarding the further sub processors in the event of third country transfers and that the result of this assessment is positive / GDPR-compliant.

***

DPA – Exhibit III

- List of authorized sub processors -

ATOSS has the CUSTOMER's general authorization for the engagement of sub processors as listed in this DPA-Exhibit III.

ATOSS may select and switch between the sub processors listed in this DPA-Exhibit III and thus are already authorized by the CUSTOMER at any time during the period of processing of personal data at its own discretion. ATOSS reserves the right not to use each of the sub processors listed below for the processing of personal data.

Company	**Registered address**	**Description of activity**	**Remark**
ATOSS companies			
ATOSS Software SE (Germany)	Rosenheimer Str. 141h 81671 Munich **Germany**	Parameterization, software maintenance services, hotline services	ATOSS affiliate (unless contracting party)
ATOSS CSD Software GmbH	Rodinger Str. 19 93413 Cham **Germany**	Parameterization, software maintenance services, hotline services	ATOSS affiliate (unless contracting party)
ATOSS Software Ges.m.b.H.	Ungargasse 64-66 Stiege 3 Top 503 1030 Vienna **Austria**	Parameterization, software maintenance services, hotline services	ATOSS affiliate (unless contracting party)
ATOSS Software AG (Schweiz)	Schärenmoosstr. 77 8052 Zürich **Switzerland**	Parameterization, software maintenance services, hotline services	ATOSS affiliate (unless contracting party)
SC ATOSS Software SRL	Calea Torontalului 69 Timisoara 300668 **Romania**	Parameterization, software maintenance services, hotline services	ATOSS affiliate (unless contracting party)

Company	Registered address	Description of activity	Remark
Sub processors for professional services			
Accenture N.V/SA	Rue Picard/ Picardstraat 11 Boîte/Bus 100 1000 Brussel **The Netherlands**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
AIKAVA GmbH	Amselstr. 15 93413 Cham **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
b.it³ Business Software+IT GmbH	Birkenstr. 2 5300 Salzburg / Hallwang **Austria**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
Business4HR GmbH & Co. KG	Bismarckstraße 60 50672 Köln **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
Bosch Sicherheitssysteme GmbH	Robert-Bosch-Ring 5 85630 Grasbrunn **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
Capgemini Deutschland GmbH	Potsdamer Platz 5 10785 Berlin **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
Delaware Consulting CV	Kapel ter Bede 86, 8500 Kortrijk **Belgium**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
DELOITTE Consulting GmbH	Dammtorstraße 12 20149 Hamburg **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
Effective People A/S	Øster Allé 56, 1. th. 2100 Copenhagen **Denmark**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)

Company	Registered address	Description of activity	Remark
EMPAL GmbH	Bügelestorstr. 7/2 74354 Besigheim **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
Fourtexx GmbH	Grünewalder Str. 28 42657 Solingen **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
GZ Gute Zeiten e. K.	Geistenbecker Str. 50 41199 Mönchengladbach **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
Ringer Zeiterfassung GmbH & Co. KG	Vollmerstraße 17 88400 Biberach a.d. Riss **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
SOFT-CONSULT Häge GmbH	Riedheimer Straße 5 89129 Langenau **Germany**	Parameterization, software maintenance services, hotline services	Sub processor (as far as necessary for the provision of such services)
Sub processors for interfaces			
SHAPEiN GmbH	Ruländerweg 10 60168 Wiesloch **Germany**	Interface service provider including software maintenance services	Sub processor (as far as necessary for the provision of such services)
Pentos AG	Landsberger Str. 110 80339 Munich **Germany**	Interface service provider including software maintenance services	Sub processor (as far as necessary for the provision of such services)
HR Force EDV-Beratung GmbH	Wambachergasse 10 1130 Vienna **Austria**	Interface service provider including software maintenance services	Sub processor (as far as necessary for the provision of such services)
All for One HR GmbH (formerly known as EMPLEOX GmbH)	Ferdinand-Braun-Str. 24 74074 Heilbronn **Germany**	Interface service provider including software maintenance services	Sub processor (as far as necessary for the provision of such services)

Company	Registered address	Description of activity	Remark
Sub processors for hardware components			
All for One OSC BX GmbH (formerly known as OSC Business Xpert GmbH)	Werftstr. 15 30163 Hannover **Germany**	Service provider for connection of hardware components incl. support/maintenance services and parameterization	Sub processor (as far as necessary for the provision of such services)
Sub processors for the operation of the ATOSS CLOUD SERVICE			
Microsoft Ireland Operations Limited	South County Business Park Leopardstown Dublin 18 **Ireland**	Hosting provider including managed IT services (hosting and operation of the cloud infrastructure)	Sub processor (as far as necessary for the provision of such services)
Telekom Deutschland GmbH	Landgrabenweg 151 53227 Bonn **Germany**	Hosting provider including managed IT services (hosting and operation of the cloud infrastructure)	Sub processor (as far as necessary for the provision of such services)
UMB AG	Müllerenstr. 3 8604 Volketswil **Switzerland**	Hosting provider including managed IT services (hosting and operation of the cloud infrastructure)	Sub processor (as far as necessary for the provision of such services)
Google Ireland Limited	Gordon House Barrow Street Dublin 4 **Ireland**	<u>For ATOSS Mobile Workforce Management (to provide a push notification service:</u> Transmission of push messages from the ATOSS Mobile Workforce Management and Mobile Employee Self Service User und Mobile Manager Self Service User module to users with mobile devices.	Sub processor (as far as necessary for the provision of such services)

***