



Data Processing Agreement ("DPA")

Table of content:

Preamble... 1
§ 1 Subject matter of this DPA... 2
§ 2 Description of the processing... 2
§ 3 Technical and organizational measures... 2
§ 4 Authority to issue instructions ... 3
§ 5 Obligation to maintain confidentiality... 4
§ 6 Commissioning of sub processors ... 4
§ 7 CUSTOMER's obligations and rights; ATOSS's support of the CUSTOMER..... 5
§ 8 Deletion or return following conclusion of processing... 6
§ 9 Liability ... 7
§ 10 Final provisions ... 7

DPA-Exhibits:1

- 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 (as controller - hereinafter referred to as "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 affiliates 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 and the respective affiliated company of the CUSTOMER is then an independent responsible controller within the meaning of the GDPR regarding such personal data, the CUSTOMER hereby concludes this DPA in its own name and at the same time on behalf of such affiliated companies. The CUSTOMER confirms that it has already received a corresponding power of attorney from its affiliated companies for the conclusion of data processing agreements with ATOSS. Under this DPA, the CUSTOMER shall always act as the single point of contact for ATOSS not only on behalf

1 The current Exhibits can be downloaded by our customers in the ATOSS Customer Area.

of the CUSTOMER but also on behalf of all other data controllers using the ATOSS PRODUCTS.

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.

Note on gender neutrality: The selected formulations apply without restriction to the other genders.

§ 1 Subject matter of this DPA

1. Legal basis: The legal basis is formed by the provisions of the EU General Data Protection Regulation (EU) 2016/679 (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 DPA, the terms used such as "personal data", "processing", "controller" or "pseudonymization" shall have the same meaning as in Art. 4 GDPR.

This DPA shall not be interpreted in a way that conflicts with the rights and obligations of the respective CUSTOMER or its affiliated companies as respective controller and the data subjects as provided for in the GDPR.

This DPA serves as a basis for the fulfilment of the legal requirements for data protection regarding the processing of personal data of a CUSTOMER by ATOSS.

2. Responsibility of the CUSTOMER: Under this DPA, 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.

§ 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 commissioned 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). It warrants that it complies with the provisions of Art. 28 (3) lit. 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 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 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 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 of the CUSTOMER only in accordance with documented instructions of the CUSTOMER, unless ATOSS is legally obligated to process such personal data or is contractually entitled to do so in accordance with this DPA. 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 shall review the feasibility of an instruction within a reasonable period of time at the expense of the CUSTOMER and notify the CUSTOMER of the result of the review in text form. 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 contractual obligations under the CONTRACT shall remain unaffected during the period of review.

Instructions confirmed by ATOSS shall be implemented by joint agreement of the PARTIES within a reasonable period of time. If ATOSS incurs additional expenses for the implementation of the instruction, these shall be remunerated by the CUSTOMER. ATOSS shall make reasonable efforts to implement instructions of the CUSTOMER which are to be qualified as a change request of the CONTRACT, insofar as they are required in particular under data protection law and are technically possible or do not require any changes to the ATOSS PRODUCTS. If one of the aforementioned exceptions applies, ATOSS shall inform the CUSTOMER thereof in text form. In the event that no agreement of the change request can be reached, the obligations under the CONTRACT shall remain in force.

4. Notification of illegality: ATOSS shall immediately notify the CUSTOMER if ATOSS 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.
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 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.

§ 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 TTDSG. 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. Definition of sub processor: For the purposes of this regulation, subcontracting relationships are those services that directly relate to the provision of the main service as agreed in the CONTRACT. This does not include generally occurring ancillary services in ATOSS's daily business operation 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 of internal business operation. Nevertheless, to also ensure the privacy and security of the data of the CUSTOMER for such 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 obligated in writing before the commencement of the processing activities to comply with the same data protection obligations, i.e., at least equivalent in terms of their content, as agreed in this DPA, unless expressly agreed otherwise. The subcontracting agreement shall guarantee at least the level of data protection required by this DPA. 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 DPA, the CUSTOMER may agree to this, whereby this DPA 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 party 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 (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: ATOSS' affiliated companies as defined in §§ 15 ff. Stock Corporation Act [AktG] and other sub processors are listed 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 outsourcing to sub processors or the change of existing 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 outsourcing to (other) 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 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.

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 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, 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: 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.
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. 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 DPA 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. 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 **DPA-Exhibit II - Technical and organizational measures**.

§ 8 Deletion or return following conclusion of processing

1. Right to select: Following the expiry of the agreed services, or earlier if requested by the CUSTOMER – nevertheless at the latest upon expiry of the CONTRACT – 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 all 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. [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 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 DPA shall be subject to the limitations of liability agreed in the CONTRACT. The CUSTOMER shall indemnify ATOSS against all claims and damages which go beyond the liability limitations of the CONTRACT, 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 DPA.

§ 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) Notwithstanding the provisions in § 3 clause 3 (Current state of the art and technical adaptations) as well as § 6 clause 4 (Further sub processors), ATOSS shall be entitled to amend or supplement the provisions of this DPA insofar as this does not negatively affect the equivalence relationship agreed upon was concluded with regard to essential elements of the DPA and the amendments are reasonable for the CUSTOMER. The right to amend the DPA in particular shall include changes with regard to (i) technical developments, (ii) changes in the legal framework, (iii) adaptations of the regulations on the handling of personal data, (iv) the elimination of an equivalence disruption that has arisen subsequently or (v) the elimination of regulatory gaps (e.g., in the event of unforeseeable, changed circumstances). ATOSS will inform the CUSTOMER of the planned amendments in advance. The amendments shall be deemed to have been accepted by the CUSTOMER if it does not object to ATOSS in writing or text form within six (6) weeks after notification. In the amendment notice ATOSS shall also draw the CUSTOMER's attention to the intended significance of its conduct.
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 Section 273 German Civil Code [BGB]: Objection based on the right of retention according to Section 273 BGB 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.
