

Attachment to META-LEVEL Software AG's "aas-suite" GTCs

Data processing agreement in accordance with Article 28 (3) of the General Data Protection Regulation (GDPR)

concluded by and between

Users of the aas-suite web application

– hereinafter referred to as **“the Client”** –

and

*Meta-Level Software AG
Lyonerring 1
66121 Saarbrücken*

– hereinafter referred to as **“the Contractor”** –

1. General information

(1) The Contractor shall process personal data on the Client's behalf under Article 4 (8) and Article 28 of Regulation (EU) 2016/679 – the General Data Protection Regulation (GDPR). This contract regulates the Parties' rights and obligations in connection with personal data processing.

(2) Insofar as the term “data processing” or “processing” (of data) is used in this contract, the definition of “processing” under Article 4 (2) of the GDPR is used a basis.

2. Subject matter of the order

The subject matter of the processing, the nature and purpose of the processing, the type of personal data, and the categories of data subjects are set out in **Annex 1** to this agreement.

3. The Client's rights and obligations

(1) The Client is the controller under Article 4 (7) of the GDPR for commissioned data processing by the Contractor. In accordance with Section 4 (5), the Contractor shall

have the right to notify the Client if, in its opinion, data processing that is legally inadmissible forms the subject matter of the order and/or an instruction.

(2) As the controller, the Client is responsible for safeguarding the rights of data subjects. The Contractor shall inform the Client without delay if data subjects assert their rights as data subjects against the Contractor in connection with its commissioned data processing activities.

(3) The Client shall inform the Contractor without delay if it discovers mistakes or irregularities in connection with personal data processing by the Contractor.

(4) In the event that there exists an obligation to provide information to third parties in accordance with Articles 33 and 34 of the GDPR or any other legal reporting obligation applicable to the Client, the Client shall be responsible for compliance with such obligation.

(5) In the event of termination, the Client undertakes to erase the personal data that it has stored in the services prior to termination of the contract.

(6) At the Contractor's request, the Client shall appoint a contact person for data protection matters.

4. The Contractor's general obligations

(1) The Contractor shall process personal data exclusively in the context of the agreements made. These are initially set out in the main contract and may subsequently be amended by the Client in writing or in an electronic format (in text form) by means of individual instructions ("individual instruction"). Verbal instructions must be confirmed without delay in writing or in text form. Exceptions to this rule are legal regulations that may obligate the Contractor to process the data in another way. In a case such as this, the Contractor shall notify the Client of these legal requirements prior to processing, unless the law in question prohibits such notification on important grounds of public interest. The purpose, nature and scope of data processing shall otherwise be governed exclusively by this contract and/or the Client's instructions. The Contractor is prohibited from processing data in any other way unless the Client has consented to this in writing.

(2) The Contractor undertakes to carry out data processing on the Client's behalf only in member states of the European Union (EU) or the European Economic Area (EEA). Personal data processing in a third country requires the Client's prior consent, which must at least be given in text form (e.g. by email). The Client's consent shall only be taken into consideration if it is ensured that the legal provisions to be complied with in accordance with Articles 44 – 49 of the GDPR are observed to ensure an adequate level of protection for the protection of personal data.

(3) The Contractor shall ensure that all of the agreed measures are carried out in accordance with the contract with respect to personal data processing in accordance with the order.

(4) The Contractor is obligated to structure its company and its operations in such a way that the data it processes on the Client's behalf is secured to the extent necessary and is protected against unauthorized access by third parties. The Contractor shall coordinate changes to the organization of commissioned data processing that are significant for the security of the data with the Client in advance.

(5) The Contractor shall inform the Client without delay if, in its opinion, an instruction issued by the Client violates legal regulations. The Contractor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client. If the Contractor can demonstrate that processing in accordance with the Client's instruction may lead to liability on the Contractor's part under Article 82 of the GDPR, the Contractor shall be entitled to suspend further processing in this respect until the liability between the Parties has been clarified.

(6) The Contractor shall process the data that it is processing on the Client's behalf separately from other data. Physical separation is not absolutely necessary.

5. The Contractor's Data Protection Officer

(1) The Contractor confirms that it has appointed a Data Protection Officer in accordance with Article 37 of the GDPR and that the Data Protection Officer performs their duties in accordance with Articles 38 and 39 of the GDPR.

Contact details are published on the Contractor's website.

(2) The obligation to appoint a Data Protection Officer in accordance with (1) may be waived at the Client's discretion if the Contractor can demonstrate that it is not required by law to appoint a Data Protection Officer and that there are company regulations that ensure personal data processing in compliance with legal provisions, the provisions set out in this contract and any further instructions issued by the Client.

6. The Contractor's reporting obligations

(1) The Contractor is obligated to notify the Client without delay of any breach of data protection regulations or of the contractual agreements made and/or the Client's instructions issued in the course of data processing by the Contractor or other persons involved in the processing. The same shall apply to any breach of the protection of personal data that the Contractor processes on the Client's behalf.

(2) Furthermore, the Contractor shall inform the Client without delay if a supervisory authority takes action against the Contractor in accordance with Article 58 of the GDPR and this may also concern monitoring of the processing that the Contractor performs on the Client's behalf.

7. The Contractor's duties to cooperate

(1) The Contractor shall assist the Client in its obligation to respond to data subjects' requests to exercise their rights in accordance with Articles 12 to 23 of the GDPR. The provisions set out in Section 11 of this contract shall apply.

(2) The Contractor shall assist the Client in drawing up the records of processing activities. It shall inform the Client of the information required in this respect in an appropriate manner. The Contractor is entitled to demand reasonable compensation from the Client for these services, unless the assistance was necessary due to a violation of law or breach of contract by the Contractor. The Contractor shall provide the Client with cost information in advance.

(3) The Contractor shall assist the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to it. The Contractor is entitled to demand reasonable compensation from the Client for these services, unless the assistance was necessary due to a violation of law or breach of contract by the Contractor. The Contractor shall provide the Client with cost information in advance.

8. Supervisory powers

(1) The Client shall have the right to monitor the Contractor's compliance with the legal provisions on data protection and/or compliance with the contractual provisions agreed between the Parties and/or compliance with the Client's instructions at any time to the extent necessary.

(2) The Contractor is obligated to provide the Client with information insofar as doing so is necessary for the performance of the monitoring under (1).

(3) The Client may request to inspect the data that the Contractor processes for the Client, as well as the data processing systems and programs used.

(4) The Client may carry out monitoring under (1) on the Contractor's premises during normal business hours following prior notification with a reasonable notice period. The Client shall ensure that the monitoring is only carried out to the extent necessary, so as not to disproportionately disrupt the Contractor's operations.

(5) Where the supervisory authority takes action against the Client under Article 58 of the GDPR, in particular with regard to information and monitoring obligations, the Contractor is obligated to provide the Client with the necessary information and to enable the competent supervisory authority to carry out an on-site inspection. The Client must be informed by the Contractor of any such planned action.

(6) The Contractor may demand reasonable compensation for information and assistance activities, unless the inspection was necessary due to a violation of law or breach of contract by the Contractor. The Contractor shall provide the Client with cost information in advance.

9. Subcontracting relationships

(1) The Client grants the Contractor general permission to use other processors under Article 28 of the GDPR to fulfill the contract. The Contractor shall specify all subcontracting relationships that already exist at the time the contract was concluded in **Annex 2** to this contract. The Client agrees to the use of such subcontractors.

(2) The Contractor shall carefully select subcontractors and check before engaging their services that they can comply with the agreements made between the Client and the Contractor. In particular, the Contractor must check in advance and regularly during the term of the contract that subcontractors have taken the technical and organizational measures required under Article 32 of the GDPR to protect personal data. The result of the check must be documented by the Contractor and sent to the Client on request.

(3) The Contractor is obligated to obtain confirmation from the subcontractor that they have appointed a Data Protection Officer in accordance with Article 37 of the GDPR. In the event that a Data Protection Officer has not been appointed at the subcontractor's company, the Contractor must inform the Client to this effect and provide information indicating that the subcontractor is not legally obligated to appoint a Data Protection Officer.

(4) The Contractor shall ensure that the provisions agreed in this contract and any supplementary instructions issued by the Client also apply to the subcontractor.

(5) The Contractor must conclude a commissioned data processing contract that meets the requirements set out in Article 28 of the GDPR with the subcontractor. In addition, the Contractor must impose the same obligations that are defined between the Client and the Contractor on the subcontractor with respect to the protection of personal data. A copy of the commissioned data processing contract must be sent to the Client on request.

(6) Subcontracting relationships under (1) to (6) do not include third-party services that the Contractor uses as purely ancillary services to carry out its business activities. This includes the likes of cleaning services, pure telecommunication services without any specific reference to services that the Contractor provides for the Client, postal and courier services, transportation services and security services. Nevertheless, the Contractor is obligated to ensure that appropriate precautions and technical and organizational measures have been taken to ensure the protection of personal data, even in the case of ancillary services provided by third parties. The maintenance and servicing of IT systems or applications constitutes a subcontracting relationship that is subject to approval and commissioned data processing under Article 28 of the GDPR if such maintenance and servicing relate to IT systems that are also used in connection with the provision of services for the Client and personal data processed on the Client's behalf can be accessed during maintenance.

10. Confidentiality obligation

(1) When processing data for the Client, the Contractor is obligated to maintain the confidentiality of data that it receives or becomes aware of in connection with the order. The Contractor undertakes to observe the same confidentiality rules that are also incumbent on the Client. The Client is obligated to inform the Contractor of any particular confidentiality rules.

(2) The Contractor warrants that it is aware of the applicable data protection regulations and is familiar with their application. The Contractor further warrants that it has familiarized its employees with the data protection provisions applicable to them and has obligated them to maintain confidentiality. The Contractor further warrants that it has in particular obligated the employees involved in carrying out the work to maintain confidentiality and has informed them of the Client's instructions.

(3) The obligation incumbent on the employees in accordance with (2) shall be demonstrated to the Client on request.

(4) The confidentiality / secrecy obligation shall continue to apply even after completion of the order.

11. Safeguarding the rights of data subjects

(1) The Client is solely responsible for safeguarding the rights of data subjects. The Contractor is obligated to assist the Client in its obligation to process requests from data subjects in accordance with Articles 12 to 23 of the GDPR. In particular, the Contractor must ensure that the information required in this respect is provided to the Client without delay, so that the Client can fulfill its obligations under Article 12 (3) of the GDPR.

(2) Insofar as the Contractor's cooperation is necessary to help the Client safeguard the rights of data subjects (in particular the right of access, right to rectification, right of blocking or right to erasure), the Contractor shall take the necessary action in each case in accordance with the Client's instructions. Where possible, the Contractor shall assist the Client in complying with its obligation to respond to data subjects' requests to exercise their rights by taking suitable technical and organizational measures.

(3) This shall be without prejudice to provisions on any compensation for additional expenses that the Contractor incurs as a result of cooperation services in connection with the data subjects asserting their rights vis-à-vis the Client.

(4) In the event that a data subject asserts their rights under Articles 12 to 23 of the GDPR vis-à-vis the Contractor, although this obviously concerns personal data processing that the Client is responsible for, the Contractor is entitled to inform the data subject that the Client is the controller for data processing. In this regard, the Contractor may provide the data subject with the controller's contact details.

12. Liability and compensation for damages

(1) In the event that a data subject asserts a claim for damages in accordance with Article 82 of the GDPR, the Parties undertake to assist one another and to help clarify the underlying facts.

(2) The liability provision agreed between the Parties in the main service provision contract shall also apply to claims arising from this agreement on commissioned data processing and in the internal relationship between the Parties for third-party claims in accordance with Article 82 of the GDPR, unless expressly agreed otherwise.

13. Confidentiality obligations

(1) Both Parties undertake to treat all of the information that they receive in connection with the execution of this contract as confidential for an unlimited period of time and to use it only for the execution of the contract. Neither Party is entitled to use this information in whole or in part for purposes other than those just mentioned or to make this information accessible to third parties.

(2) The above obligation shall not apply to information that one of the Parties has demonstrably received from third parties without any obligation to maintain confidentiality or to information that is general public knowledge.

14. Compensation

Any provisions concerning compensation for services shall be agreed separately between the Parties.

15. Technical and organizational measures for data security

(1) The Contractor undertakes vis-à-vis the Client to comply with the technical and organizational measures required to comply with the applicable data protection regulations. This includes in particular the requirements set out in Article 32 of the GDPR.

(2) The status of the technical and organizational measures in place at the time the contract is concluded is enclosed as **Annex 3** to this contract. The Parties agree that changes to the technical and organizational measures may be necessary to adapt to technical and legal circumstances. The Contractor shall adapt the measures taken over time to developments in the state of technology and the risk situation. The Contractor reserves the right to change the technical and organizational measures taken, provided that the level of protection does not fall below that indicated in Article 32 of the GDPR. The Client may request an up-to-date version of the technical and organizational measures taken by the Contractor at any time.

(3) The Contractor shall check the effectiveness of the technical and organizational measures it has taken on both a regular and an ad-hoc basis. The Contractor shall inform the Client in the event that there is a need for optimization and/or changes.

16. Duration of the order

(1) The agreement shall commence on conclusion by the Client. It shall end following completion of the last contract under the respective customer number. If commissioned data processing continues following termination of this contract, the provisions set out in these agreements shall apply until processing actually ends.

(2) The Contractor may amend the agreement at its reasonable discretion by giving appropriate notice. In particular, it expressly reserves the right to amend this agreement unilaterally if significant legal changes arise in relation to this agreement. The Contractor shall inform the Client separately of the significance of the planned change and shall also grant the Client a reasonable period of time to object. The Contractor shall point out to the Client in the notice of change that the change shall take effect if it does not object within the set period. If the Client does object, the Contractor shall be entitled to an extraordinary right of termination.

(3) The Client recognizes this agreement as part of the GTCs for the product(s) it has booked. If there are any contradictions, the provisions set out in this agreement on commissioned data processing shall take precedence over the provisions set out in the main contract. Should individual parts of this agreement be invalid, this shall not affect the validity of the remaining agreements.

17. Termination

(1) On completion of provision of the processing services, the Contractor shall, at the Client's discretion, return to the Client all documents, data and processing or usage results that have come into its possession in connection with the contractual relationship, or anonymize them or erase them. Any legal retention requirements or other obligations to store the data shall remain unaffected. If the Client does not make use of this option, anonymization shall be deemed to have been agreed. If the Client chooses to have the Contractor return the documents, data and processing or usage results, the Contractor may demand reasonable compensation. The Contractor shall provide the Client with cost information in advance.

(2) The Contractor may store personal data that has been processed in connection with the order beyond the termination of the contract if and to the extent that the Contractor has a legal obligation to retain it. In such cases, the data may only be processed for the purposes of implementing the respective legal retention requirements. Once the retention requirement has elapsed, the data must be erased without delay.

18. Right of retention

The Parties agree that the defense of the right of retention by the Contractor under Section 273 of the German Civil Code is excluded with regard to the processed data and the associated data carriers.

19. Final provisions

(1) Should the Client's ownership on the Contractor's premises be jeopardized by third-party action (such as seizure or confiscation), insolvency proceedings or other events, the Contractor must inform the Client without delay. The Contractor shall without delay inform the creditors of the fact that data is being processed on the Client's behalf.

(2) Should individual parts of this agreement be invalid, this shall not affect the validity of the remaining provisions of the contract.

Annex 1 – Subject matter of the order

1. Subject matter and purpose of processing

The Client's order to the Contractor includes the following work and/or services:

The subject matter of the agreement is the Parties' rights and obligations in the context of the provision of services in accordance with the service description and GTCs (hereinafter referred to as the "main contract"), insofar as personal data is processed by Meta-Level Software AG (the Contractor) as the processor for the customer as the controller (the Client) in accordance with Article 28 of the GDPR. This includes all activities that the Contractor performs to fulfill the order and that constitute commissioned data processing. This shall also apply if the order does not expressly refer to this agreement on commissioned data processing.

2. Types of personal data

The following types of data are regularly processed:

- Last name, first name, email address, password (as hash)
- Company name and company address (of the Client)
- Communication data (e.g. information about the device used, IP address)

3. Categories of data subjects

Group of data subjects affected by data processing:

- Internal and external employees employed by the Client

Annex 2 – Subcontractors

For data processing on the *Client's* behalf, the *Contractor* engages the services of third parties who process data on its behalf (“subcontractors”).

Subcontracting is provided by the following companies:

<i>Subcontractor</i>	<i>Address</i>	<i>Brief description of the service</i>
lonos SE	Elgendorfer Strasse 7, 56410 Montabaur	Provision and operation of dedicated and virtual servers. (Hosting provider)

Annex 3

Technical and organizational measures taken by the Contractor

The Contractor shall take the following technical and organizational measures for data security under Article 32 of the GDPR.

1. Confidentiality

Admittance control

Unauthorized individuals must be denied access to data processing systems.

- Chip card / transponder locking system (building access / floor access)
- Chip cards are assigned to employees
- Chip cards that are reported lost are deactivated immediately
- Security zones with mechanical locking system
- Processing in ISO 27001-certified data centers (see the subcontractor(s) listed in **Annex 2**)

Access control

The use of data processing systems by unauthorized individuals must be prevented.

- Assignment of user privileges and profiles to IT systems
- Authentication with username / password or username / token
- Systems / applications block access in case of inactivity
- Secure (encrypted) transmission of authentication secrets
- Servers' and clients' access to the internet secured by firewalls
- Information security policies are binding for all employees

Entry control

The use of the data processing systems and the stored data must be ensured in accordance with the permissions.

- Creation of a role-based permission concept
- Implementation of access restrictions
- Management of privileges by system administrator(s)

Separation

It must be ensured that data collected for different purposes can be processed separately.

- Data economy when handling personal data
- Secure client access centrally controlled by the Entity Framework
- Customer data stored and processed separately in relation to the intended use.

Encryption

Unauthorized individuals must be denied access to data.

- Encryption of data carriers
- Encryption of communication (SSL / TLS connections or VPN tunnels) between client and server and to the backend

2. Integrity

Input control

Tracking of intentional and unintentional data manipulation must be ensured.

- Traceability of data input, modification and erasure by individual usernames (not user groups)
- Allocation of data input, modification and erasure privileges based on a permission concept

Transfer control

Data may only be transferred to authorized recipients.

- Personal data is only disclosed to the extent necessary to provide the contractual services for the customer
- Data is transferred to recipients in encrypted form
- Employees are obligated to handle personal data confidentially

3. Availability and resilience

Data must be secured against accidental destruction or loss.

- Creation of a contingency plan
- Creation and implementation of a backup and recovery concept
- Processing in ISO 27001-certified data centers (see the subcontractor(s) listed in **Annex 2**)

4. Procedures for regular review, assessment and evaluation

Internal measures for data protection.

- Involvement of the company DPO in the planning and execution of activities and measures that (could) lead to personal data processing.
- Obligation to maintain confidentiality among all employees who come into contact with personal data as a supplement to their employment contract
- Central documentation of all data protection procedures and regulations
- Information security management according to TISAX