Order processing according to Art. 28 DS-GVO

Agreement

between the company

- Responsible person - hereinafter referred to as the client -

and the

Johari GmbH

- Processors - hereinafter referred to as the Contractor

1. Subject and duration of the contract

(1) Subject

The subject of the order is determined by the offer and the general terms and conditions referred to here (hereinafter referred to as the Service Agreement).

(2) Duration

The duration of this contract (duration) corresponds to the duration of the service agreement.

2. Specification of the order

1) the nature and purpose of the envisaged processing of data

A more detailed description of the subject of the contract with regard to the nature and purpose of the tasks of the contractor:

Contractor enables its customers to use a collaboration management system as Software as a Service or Cloud Offer to create and manage enterprise content, whereby this enterprise content is hosted on a server for the customer (hereinafter collectively "Service").

The Service provided allows Users to independently design, adapt and further develop the Content. The subject matter of the order is otherwise based on the main contractual relationship concluded between the parties. This is based on the Johari GTCs, which have been effectively incorporated into the contractual relationship between the parties. This contract for order processing applies in addition to the Johari GTCs (https://johari-solution.de/de/agb).

The order from the Principal to the Contractor includes the following work and/or services:

The technical operation, adaptation and provision of the Service and first-level support

(2) Types of personal data

The following types of data are regularly subject to processing:

▪ Personal master data (such as name)

▪ Communication data (e.g. email address)

▪ Contract master data (e.g. product description, prices)

▪ Contract billing and payment data

▪ Customer history

(3) Categories of data subjects

The group of persons concerned by the data processing:

▪ Employee of the client

▪ External parties such as suppliers, customers and freelancers of the client (if set up in the system)

The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another state that is a party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the customer and may only take place if the special conditions of Art. 44 et seq. DS-GVO are fulfilled. The appropriate level of protection in the United States is established by a Commission Decision on Adequacy (Art. 45 (3) DS-GVO). Other third countries where data can be processed within the order processing agreement are Chile, Taiwan, Singapore, Ireland, the Netherlands, Denmark, Finland and Belgium. The special requirements of Art. 44 ff. DS-GVO are fulfilled.

(4) Nature of the data

The type of personal data used is described in detail in the service agreement under: 2. (2)

(5) Categories of data subjects

The categories of data subjects concerned by the processing are specifically described in the service level agreement at 2.(3)

3. Technical-organizational measures

(1) The Contractor shall document the implementation of the technical and organisational measures described and required prior to the award of the contract prior to the commencement of processing, in particular with regard to the concrete execution of the contract, and shall hand them over to the Client for inspection. If accepted by the customer, the documented measures shall become the basis of the order. If the examination/audit of the client reveals a need for adjustment, this must be implemented by mutual agreement.

(2) The contractor must provide the security in accordance with Art. 28 Para. 3 lit. c, 32 DS-GVO, in particular in connection with Art. 5 Para. 1, Para. 2 DS-GVO. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the type, scope and purposes of processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the DS-GVO must be taken into account [details in Annex 1].

(3) The technical and organisational measures are subject to technical progress and further development. In this respect the contractor is permitted to implement alternative adequate measures. In doing so, the safety level of the specified measures may not be undercut. Significant changes shall be documented.

4. Correction, restriction and deletion of data

(1) The Contractor may not correct, delete or restrict the processing of the data processed under the contract on his own authority, but only after documented instructions from the Client. Insofar as a data subject contacts the contractor directly in this respect, the contractor shall forward this request to the principal without delay.

(2) Insofar as included in the scope of services, the deletion concept, the right to be forgotten, correction, data portability and information shall be ensured directly by the contractor in accordance with the documented instructions of the customer.

5. Quality assurance and other obligations of the contractor

In addition to complying with the provisions of this contract, the contractor has statutory obligations in accordance with Art. 28 to 33 DS-GVO; in this respect, the contractor guarantees in particular compliance with the following requirements:

a) The maintenance of confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 DS-GVO. In performing the work, the Contractor shall only employ employees who are bound to confidentiality and who have previously been made familiar with the provisions on data protection relevant to them. The Contractor and any person subordinate to the Contractor who has access to personal data may process such data exclusively in accordance with the instructions of the Client, including the powers granted in this Agreement, unless they are legally obliged to process such data.

b) The implementation of and compliance with all technical and organisational measures required for this contract in accordance with Art. 28 para. 3 sentence 2 lit. c, 32 DS-GVO [details in Annex 1].

c) The principal and the contractor shall, upon request, cooperate with the supervisory authority in the performance of its duties.

d) Immediate information of the principal about control actions and measures of the supervisory authority, insofar as they relate to this contract. This shall also apply where a competent authority, in the course of administrative or criminal proceedings, investigates the processing of personal data relating to the processing of the contract at the contractor³s premises.

e) In so far as the contracting authority is itself subject to control by the supervisory authority, to administrative or criminal proceedings, to liability of a data subject or third party or to any other claim relating to the processing of personal data in connection with the processing at the contractor³s premises, the contractor shall use his best endeavours to assist him.

f) Contractor shall regularly monitor internal processes and technical and organisational measures to ensure that processing within its sphere of responsibility is carried out in accordance with the requirements of applicable data protection law and that the rights of the data subject are protected.

g) Verifiability of the technical and organizational measures taken vis-à-vis the principal within the scope of his powers of control under Section 7 of this contract.

6. Subcontracting

(1) For the purposes of this regulation, subcontracting relationships are understood to be those services which are directly related to the provision of the main service. This does not include ancillary services which the Contractor uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The Contractor is, however, obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Customer's data even in the case of outsourced ancillary services.

(2) The Customer agrees to the commissioning of the following subcontractors under the condition of a contractual agreement in accordance with Art. 28 Para. 2-4 DS-GVO:

Company Subcontractor	**Service**
Amazon Web Services, Inc. (AWS)	Serverhosting
Netcup GmbH	Serverhosting
Google LLC.	Use of various Google services such as Google Tag Manager, Google Fonts, Google Analytics and Google Cloud Natural Language API on own websites and within our service

(3) The passing on of personal data of the Client to the subcontractor and the Client's first action are only permitted when all requirements for subcontracting have been met.

(4) If the subcontractor performs the agreed service outside the EU/EEA, the Contractor shall ensure the permissibility under data protection law by taking appropriate measures. The same applies if service providers within the meaning of Paragraph 1 Sentence 2 are to be used.

(5) Any further outsourcing by the subcontractor requires the express consent of the main contractor (at least text form).
All contractual regulations in the contractual chain must also be imposed on the further subcontractor.

7. Control rights of the client

(1) The Contractor shall assist the Client in complying with the obligations regarding the security of personal data as set out in Articles 32 to 36 of the DS-GVO, notification obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes among other things

a) ensuring an adequate level of protection by technical and organisational measures that take into account the circumstances and purposes of the processing and the predicted probability and severity of a possible breach of law by security breaches and enable relevant breach events to be identified immediately

(b) the obligation to notify the contracting entity without delay of any breach of personal data

(c) the obligation to assist the contracting entity in the performance of its duty to inform the data subject and to make available to him without delay all relevant information in this connection

(d) assisting the contracting authority in its data protection impact assessment

(e) assisting the contracting entity in prior consultations with the supervisory authority

(2) The Contractor may claim remuneration for support services which are not included in the performance specification or which are not due to misconduct on the part of the Contractor.

9. Authority of the client

(1) Verbal instructions shall be confirmed by the client without delay (at least in text form).

(2) The contractor must inform the client immediately if he believes that an instruction violates data protection regulations. The contractor is entitled to suspend the execution of the corresponding instruction until it is confirmed or amended by the client.

10. Deletion and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of the client. Excluded from this are back-up copies, insofar as they are necessary to ensure proper data processing, as well as data which is required in order to comply with statutory storage obligations.

(2) Upon completion of the contractually agreed work or earlier upon request by the Customer - at the latest upon termination of the service agreement - the Contractor shall hand over to the Customer all documents, processing and usage results produced and data stocks that have come into its possession in connection with the contractual relationship or, with prior consent, destroy them in accordance with data protection regulations. The same applies to test and reject material. The protocol of the deletion must be presented on request.

(3) Documentation which serves as proof of the orderly and proper data processing shall be kept by the Contractor in accordance with the respective retention periods beyond the end of the contract. He can hand them over to the customer for his discharge at the end of the contract.

Annex - Technical-organizational measures

1. confidentiality (Article 32(1)(b) DS-GVO)

Access control

No unauthorised access to data processing equipment, e.g: magnetic or chip cards, keys, electric door openers, plant security or gatekeepers, alarm systems, video systems;

No unauthorized system use, e.g: (secure) passwords, automatic locking mechanisms, encryption of data carriers;

No unauthorized reading, copying, modification or removal within the system, e.g: Authorization concepts and demand-oriented access rights, logging of accesses;

Disconnection control

Separate processing of data collected for different purposes, e.g. multi-client capability

2. Integrity (Art. 32 (1) lit. b DS-GVO)

Passing on control

No unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g: Encryption, Virtual Private Networks (VPN)

Input control

Determining whether and by whom personal data have been entered, modified or removed from data processing systems, e.g: logging, document management

3. Availability and resilience (Art. 32(1)(b) DS-GVO)

Availability control
Protection against accidental or deliberate destruction or loss, e.g: Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans
Rapid recoverability (Art. 32 (1) lit. c DS-GVO);

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d DS-GVO; Art. 25 para. 1 DS-GVO)

Data protection management;

incident response management;

Data protection-friendly default settings (Art. 25 (2) DS-GVO);

Order control

No commissioned data processing within the meaning of Art. 28 DS-GVO without corresponding instructions from the client, e.g: Clear contract design, formalised contract management, strict selection of the service provider, obligation to convince in advance, follow-up checks.