Data protection agreement for commissioned processing

in accordance with Art. 28 of the General Data Protection Regulation (GDPR)

between

Johari Gmbh
Margaretenweg 7
86842 Türkeim

- Processor -

and

the in the to this document referring individual offer further specified company

- Principal -

§1 Subject and duration of the agreement, type and purpose of processing, type of personal data, categories of data subject

The subject and duration of the agreement, the nature and purpose of the processing, the type of personal data and the categories of data subjects of the order are set out in Annex 1 (Nos. 1-5).

The processing of the personal data shall take place exclusively on the territory of the Federal Republic of Germany, in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation of data processing, data transmission or other data transfer to a third country requires the prior consent of the principal.

§2 Instruction-bound processing and remonstration obligation

The Processor is responsible for assessing the permissibility of the processing in accordance with Art. 6 (1) GDPR. Data shall be processed exclusively within the scope of the agreement reached and according to the instructions of the Principal. The Processor reserves the right to issue comprehensive instructions on the type, scope and procedure of the processing within the scope of the job description agreed in this agreement, which may be specified by means of individual instructions. Instructions of the Principal shall be documented.

Instructions shall generally be issued by the Principal in text form (e.g. by e-mail). If, in exceptional cases, an instruction is given verbally, it shall be confirmed by the Processor accordingly in text form (e.g. by e-mail).

To the extent that the Processor is otherwise required to process by the law of the Union or the member states to which the Processor is subject, the Processor shall notify the Principals of such legal requirements prior to the processing, unless the relevant law prohibits such notification due to an important public interest.

The Processor shall notify the Principals without undue delay if, in its opinion, compliance with an instruction issued by the Principals violates a provision of data protection law or the provisions of this agreement (obligation to remonstrate).

§3 Confidentiality / secrecy obligation

In order to perform the contract, the Processor shall only employ persons whom it has committed to confidentiality or who are subject to an appropriate legal duty of confidentiality.

§4 Security of processing / Technical and organizational measures according to Art. 32 GDPR

The Processor shall take all necessary technical and organizational measures pursuant to Art. 32 GDPR. These are specified in Annex 2.

If the Processor does not have access to the Principal's data and the Order Processing is carried out in full by another Processor (sub-provider), the security concept within the meaning of Art. 32 GDPR of this other Processor shall be described in Annex 2.

Technical and organizational measures are subject to technical progress and further development. During the term of this order, these shall be continuously adapted by the Processor to the requirements of this order and further developed in accordance with technical progress. The security level of the technical and organizational measures specified here and in Annex 2 may not be undercut. This data security concept shall be submitted regularly in accordance with the requirement under Annex 1 (No. 7).

The Processor undertakes to document any changes to the technical and organizational measures that have a significant impact on the guaranteed level of security in writing as a supplement to Annex 2, which may also be in an electronic format, and to notify the Principal thereof.

§5 Use of the services of other processors

The further processors (sub-processors) used at the time of the conclusion of the contract are listed in Annex 3 to this contract. The Processor is granted consent to the inclusion of the Processors listed in Annex 3.

The Processor shall not use any other processors (sub-processors) without the separate written consent of the Principal, which may also be provided in an electronic format.

If the Processor uses the services of another processor (sub-processor) to carry out certain processing activities on behalf of the Principal, those sub-processors shall be subject to the same data protection obligations as set out in this contract by way of a contract to be drawn up in writing, which may also be in an electronic format, or under another legal instrument under Union law or the law of the Member State concerned. In particular, sufficient guarantees must be provided that the appropriate technical and organizational measures are implemented in such a way that the processing complies with the requirements of the GDPR. In the case of the commissioning of subcontractors based in third countries, the provisions of Art. 44 GDPR must also be complied with. If the subcontractor fails to

comply with its data protection obligations, the first processor shall be liable to the principal for compliance with the obligations of that subcontractor.

§6 Cooperation / support obligations

In view of the nature of the processing, the Processor shall support the Principals with appropriate technical organizational measures in fulfilling its obligation to respond to requests to exercise the rights of the data subject set out in Chapter 3 of the GDPR. These include in particular the consideration of data subject rights with regard to ensuring transparency, the right of access, the right of rectification, the right to erasure and "being forgotten", the right to restriction of processing, the right to notification in the event of rectification and erasure as well as restriction of processing, the right to data portability, the right to object as well as the rights in the event of automated individual case decisions.

§7 Support for the fulfillment of the principal's duties

The Processor shall assist the Principal in complying with the obligations set forth in Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to it. These include, in particular, ensuring the security of the processing, the notification of personal data breaches to the supervisory authorities, the notification of the data subject of a personal data breach, the data protection impact assessment and the prior consultation of one of the competent supervisory authorities.

§8 Deletion and return of personal data

To the extent that there are no statutory or other retention obligations to the contrary, the Processor shall, after termination of the order, release the personal data used to the Principals in a form that can be read and processed by the Principals, unless the Processor instructs it to delete the personal data. If the Processor releases the data, it shall immediately delete any copies in its area of responsibility after the Processor has confirmed the proper receipt of the data.

Further, the Processor shall take all reasonable steps to preclude continued unauthorized access to the Principal's data.

Documents evidencing compliance with this Agreement shall be retained by the processor at the end of the agreement for a reasonable period of time beyond the end of the agreement and shall be released as required.

$9 Proof of obligations and support for reviews

The Processor shall provide the Principal with all information necessary to demonstrate compliance with the obligations set forth in Art. 28 GDPR. The Processor shall enable and contribute to audits - including inspections - carried out by the Principal or another auditor appointed by the Principal.

§10 Other duties

The Processor warrants that it has appointed a data protection officer to the extent required by law.

In the event of suspected data protection violations or other disruptions in the processing of the Principal's personal data, as well as in the event of inspections and measures by the competent supervisory authority at the Processor, the Processor shall be informed without undue delay. To the extent that a data subject directly contacts the Processor for the purpose of responding to requests to exercise the rights of the data subject set forth in Chapter 3 of the GDPR, the Processor shall pass on such request to the Principal and await the Principal's instruction in this regard.

In particular, the Processor shall exercise due diligence to ensure that its employees comply with the statutory provisions on data protection and do not disclose to third parties or otherwise exploit the information obtained from the Principal. Upon request of the Principal, the Processor shall provide evidence of the data protection training and obligation.

§11 Other regulations

Should the fulfillment of the subject matter of the order in accordance with § 1 of this agreement be endangered at the Processor by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall inform the Principals without undue delay. The Processor shall immediately inform all parties involved in this context that the powers of disposal over the data are vested exclusively in the Principals.

In the event of any contradictions between this contract and a principal contract, the provisions of this contract shall take precedence over the provisions of the principal contract.

Should individual parts of this contract be invalid, this shall not affect the validity of the rest of the contract.

Any change to this agreement, including its termination and this clause, must be in writing, which may also be in an electronic format.

The liability provisions from Art. 82 et seq. GDPR.

§12 Enactment

The agreement enters into force upon approval by the Processor and Principal of the original offer that refers to this document.

Annex 1 General information on the contract

Annex 2 Technical and organizational measures according to Art. 32 GDPR

Annex 3 Further processors (subcontractors)

Annex 1

General information on the contract

1. Subject of the agreement

The subject of the contract is the provision, maintenance and support of Johari Software

2. Duration of the agreement

The agreement is valid upon signature by the parties and is concluded for the duration of the business relationship.

3. Nature and purpose of the data processing

The activities of the Processor serves to support and maintain the Platform and/or the Service operated thereon.

4. Type of personal data (types of data)

The following types of data are the subject of this order:

General data/ Personal contact information

- Names
- (Personal) profiles

Contract data

- Contract data
- Billing and payment data
- Bank details/ credit card data
- Contract/usage histories

Services and IT (usage) data

- Access data
- Identification data/IDs
- Telecommunication data/ message content
- Image/video data

Professional data

- Master data
- Qualifications/ development potential/ professional profiles

5. Categories of persons covered

In the course of the performance of the contract, the processor uses personal data. The following categories of data subjects are the subject of the order:

- Employees
- Trainees/ Interns

6. Regular provision of the data security concept

An up-to-date version of the technical and organizational measures listed in Annex 2 and, if applicable, the data security concept shall be submitted to the Principal at regular intervals.

Annex 2

Technical and organizational measures to be taken in accordance with Art. 32 GDPR, which must be ensured for the fulfillment of the order by the processor

Appendix 2 specifies the technical and organizational measures taken by the Processor. The subsequent assessment of the appropriate level of protection is the responsibility of the principal.

Taking into account the

- State of the technology
- the implementation costs and
- the nature, scope, circumstances and
- the purposes of the processing, and
- the varying likelihood and severity of the risk to the rights and freedoms of natural persons

The processor takes appropriate technical and organizational measures to ensure a level of protection appropriate to the risk.

When assessing the appropriate level of protection, particular account shall be taken of the risks associated with the processing, in particular through - whether accidental or unlawful - destruction, loss, alteration or unauthorized disclosure of or access to personal data which have been transmitted, stored or otherwise processed.

If the Processor does not have access to the Principal's data and the order processing is fully carried out by one or more processors (sub-providers), the security concepts within the meaning of Art 32 GDPR of these sub-providers shall be described in Annex 2.

The Processor shall take the following measures:

1. **Pseudonymization**

Personal data of the Principal may be processed in such a way that it can no longer be attributed to a specific data subject without the inclusion of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures that prevent unauthorized identification of the data subjects.

Nevertheless, data pseudonymized in this way remains personal data within the meaning of the GDPR. Pseudonymization is a technical and organizational measure, and can be implemented by the Processor as follows.

- Separate storage of additional information for identification purposes
- Encryption of additional information for identification
- Management and documentation of differentiated authorizations for additional identification information
- Authorization process or approval routines for permissions to process additional identification information

2. **Measures for encryption**

- Encryption of mobile devices such as laptops, tablets, smartphones
- Encryption of mobile storage media (CD/DVD- ROM, USB sticks, external hard drives)
- Encryption of files
- Encryption of systems/equipment

- Encryption of passwords
- Encryption of e-mail or e-mail attachments
- Secured data transfer (e.g. SSL, FTPS, TLS)
- Secured WLAN

3. **Measures to ensure confidentiality**

a) **Measures to prevent unauthorized persons from entering**

- Access control system
- Door security (electronic door opener, combination lock, etc.)
- Key management/ documentation of key allocation
- Alarm system
- Video surveillance
- Special protective measures for the server room
- Special protective measures for the storage of back-ups and/or other data media
- Non-reversible destruction of data media
- Employee and authorization badges
- Restricted areas
- Visitor regulations (e.g., pick-up at reception, documentation of visit times, visitor badge, escort after visit to exit)

b) Measures to prevent unauthorized persons from using the processing systems

- Personal and individual user log-in when logging on to the system or corporate network
- Authorization process for access rights
- Limitation of authorized users
- Single sign-on
- Two-factor authentication
- BIOS passwords
- Password procedure (specification of password parameters in terms of complexity and update interval)
- Electronic documentation of passwords and protection of this documentation against unauthorized access
- Personalized tokens, Pin-/TAN, etc.
- Logging of access
- Additional system log-in for certain applications
- Automatic locking of clients after a certain period of time without user activity (also password-protected screen saver or automatic pause)
- Firewall

c) Measures to ensure that only authorized persons have access to the processing systems and cannot read, copy, modify or remove personal data without authorization

- Management and documentation of differentiated authorizations
- Evaluation/logging of data processing
- Authorization process for permissions

- Authorization routines
- Profiles/roles
- Encryption of CD/DVD ROM, external hard disks and/or laptops
- Measures to prevent unauthorized transfer of data to external usable data media
- Mobile Device Management System
- Segregation of duties
- Expert destruction of files and data media in accordance with DIN 66399
- Non-reversible deletion of data media
- Privacy films for mobile data processing systems

d) Measures to ensure that data collected for different purposes can be processed separately

- Storage of data records in physically separate databases
- Separate systems
- Access authorizations according to functional responsibility
- Separate data processing through differentiated access regulations
- Multi-client capability of IT systems
- Use of test data
- Separation of development and production environment

4. Measures to ensure integrity

- Access rights
- System logging
- Document Management System (DMS) with change history
- Security/logging software
- Functional responsibilities, organizationally defined responsibilities
- Tunneled remote data connections (VPN)
- Data Loss Prevention (DLP) system
- Electronic signature
- Logging of data transmission or data transport
- Logging of read accesses
- Logging of copying, modification or removal of data

5. Measures to ensure and restore availability

- Security concept for software and IT applications
- Backup procedure
- Retention process for backups
- Ensuring data storage in the secured network
- Importing security updates as needed
- Mirroring of hard disks
- Establishment of an uninterruptible power supply
- Suitable archiving space for paper documents
- Fire protection of the server room
- Fire protection of the archiving rooms
- Air-conditioned server room

- Virus protection
- Firewall
- Emergency plan
- Successful emergency drills
- Redundant, locally separated data storage (offsite storage)

6. Measures to ensure resilience

- Contingency plan for machine failure
- Redundant power supply
- Sufficient capacity of IT systems and equipment
- Redundant systems installations
- Resilience and fault management

7. Procedures for regular review, assessment and evaluation of the effectiveness of technical and organizational measures

- Procedure for regular checks/audits
- Concept for regular review, assessment and evaluation
- Reporting system
- Penetration testing
- Emergency tests

8. Instruction control/ order control

- Contract for commissioned data processing pursuant to Art. 28. para. 3 GDPR with regulations on the rights and obligations of the processor and principal
- Process for issuing and/or following instructions
- Designation of contact persons and/or principals employees
- Control/verification of order execution according to instructions
- Training/instruction of all employees at the processor who are authorized to access the data
- Obligation of employees to maintain confidentiality
- Appointment of a data protection officer pursuant to Art. 37 et seq. GDPR
- Data protection manager/coordinator
- Maintaining a register of processing activities pursuant to Art. 30 para. 2 GDPR
- Documentation and escalation process for personal data breaches
- Guidelines/provisions for ensuring technical/organizational measures for the security of processing
- Process for forwarding data subject inquiries

Annex 3

Other processors (subcontractors)

Name of the subcontractors	Subject of the subcontract	Date of the subcontracting agreement
Amazon Web Services, Inc. (AWS)	Server hosting, mail, backups	17.02.2021
Netcup GmbH	Server hosting, mail, backups	31.10.2018
Elasticsearch B.V.	Search	19.11.2021
Google LLC.	Use of various services, such as Tag Manager, Fonts, Analytics, Translate and Calendar	24.03.2019
Stonly SAS	Interactive user guides	15.01.2021
Microsoft Azure	Cognitive Service for Language	21.02.2022