Order pursuant to Art. 28 GDPR

Agreement

Contracting Parties

Controller (Client):

Processor (Contractor):

LexLogik UG

Mahlgasse 4 , 88339 Bad Waldsee

Germany

(represented by Managing Director Jonas Maximilian Regul)

1. Subject Matter and Duration of the Agreement

(1) The subject matter and duration of the agreement are primarily determined by the respective main contractual relationship between the parties regarding the use of the software and cloud services provided by the Processor ("Main Agreement"), unless expressly agreed otherwise therein.

(2) The Processor provides services for the technical processing of documents and related content that the Controller uploads to the platform or otherwise transmits within the contractually agreed scope. The processing is carried out exclusively on behalf of and in accordance with the documented instructions of the Controller within the meaning of Art. 4 No. 2 and Art. 28 GDPR on the basis of this agreement.

(3) The Processor strictly adheres to a zero-retention paradigm. Content data of the Controller is processed exclusively in volatile random-access memory (RAM) for the duration of the technical analysis. Persistent storage on physical data carriers does not occur. Upon completion of the analysis process, all content data in the RAM is irrevocably deleted.

(4) Insofar as technical metadata (e.g., access, error, and performance logs) inevitably arises within the scope of operating the platform, it is processed only to the extent necessary for operation, security, and traceability, and in compliance with statutory requirements as well as Annex 2 (TOMs).

2. Scope, Nature, and Purpose of the Collection, Processing, or Use of Data

(1) The scope, nature, and purpose of the processing of personal data, as well as the categories of personal data and the categories of data subjects, arise from the Main Agreement and Annex 1, if completed by the Controller, unless otherwise specified in the Main Agreement.

(2) The provision of the contractually agreed data processing shall take place exclusively in a Member State of the European Union or in another contracting state of the Agreement on the European Economic Area, unless expressly agreed otherwise.

(3) Any intended transfer of the processing of personal data to a third country requires the prior consent of the Controller and may only occur if the specific requirements of Art. 44 et seq. GDPR are met (including appropriate safeguards and documented risk assessment, if required).

3. Technical and Organizational Measures pursuant to Art. 32 GDPR (Art. 28 Para. 3 Sentence 2 lit. c GDPR)

(1) The Processor must document the implementation of the technical and organizational measures outlined and required prior to the awarding of the contract before the start or continuation of processing, and make them available to the Controller for review upon request (Annex 2). Upon contractual reference to the current Annex 2 or its acceptance by the Controller, these measures become part of the agreement.

(2) The Processor guarantees a level of security appropriate to the risk in accordance with Art. 28 Para. 3 Sentence 2 lit. c, Art. 32 GDPR in conjunction with Art. 5 Para. 1 and 2 GDPR. In particular, the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons must be taken into account.

(3) The technical and organizational measures are subject to technical progress and further development. The Processor is permitted to implement alternative, equivalent, or improved measures, provided the agreed level of security is not reduced. Significant changes to the measures must be documented and communicated to the Controller, insofar as this is relevant to the rights of the Controller.

4. Rectification, Restriction, and Erasure of Data

(1) Upon completion of the respective processing or upon the instruction of the Controller, the Processor must immediately delete or return the content data processed on behalf of the Controller, unless the Processor is subject to a statutory obligation to retain the data.

(2) Insofar as it is covered by the scope of services of the Main Agreement, the Processor shall assist the Controller in fulfilling the rights of data subjects (e.g., access, rectification, erasure, data portability), provided this is technically feasible and involves reasonable effort, and the Controller has issued the necessary instructions.

5. Quality Assurance and Other Obligations of the Processor

(1) The Processor complies with the obligations under Art. 28 to 33 GDPR, insofar as these apply to processors, and in particular ensures:

- Confidentiality in accordance with Art. 28 Para. 3 Sentence 2 lit. b, Art. 29, Art. 32 Para. 4 GDPR;
- Deployment of personnel who are committed to confidentiality and have been familiarized with the relevant data protection regulations;
- Processing of personal data exclusively in accordance with the instructions of the Controller and this agreement, unless the Processor is legally required to process the data;
- Implementation of and compliance with the technical and organizational measures pursuant to Art. 28 Para. 3 Sentence 2 lit. c, Art. 32 GDPR and Annex 2.

(2) The Processor shall immediately inform the Controller if, in its opinion, an instruction from the Controller is unlawful or incompatible with data protection law.

(3) The Processor shall cooperate with the supervisory authority upon the Controller's request, insofar as this is necessary and reasonable within the scope of the agreement.

(4) The Processor shall immediately inform the Controller about control actions and measures by the supervisory authority, insofar as they relate to this agreement. This applies accordingly if authorities investigate the Processor in connection with the data processing, provided notification is legally permissible.

(5) If the Controller is subject to claims by third parties or data subjects due to the data processing, the Processor shall assist the Controller in accordance with statutory requirements and to a reasonable extent, in particular by providing necessary information, provided this is available to the Processor.

(6) The Processor shall regularly review its internal processes as well as the technical and organizational measures to ensure that processing is carried out in accordance with the requirements of applicable data protection law.

6. Subcontractors

(1) Subcontractors within the meaning of this agreement are services that directly relate to the provision of the main service (in particular hosting, operation of data center capacity, infrastructural services, insofar as they serve the processing on behalf of the Controller).

(2) This does not include, in particular, general ancillary and secondary services that the Processor uses without special integration into the data processing (e.g., telecommunications, postal/transport services, general office organization), provided no access to the Controller's personal data occurs or this occurs only within the unavoidable technical framework. For such secondary services, the Processor shall select reliable providers and implement appropriate data protection precautions.

(3) The Processor may only use subcontractors within the framework of statutory requirements. If necessary, the Controller will be informed about intended changes concerning the addition or replacement of other subcontractors or will be granted a right of objection in accordance with the provisions of the Main Agreement.

(4) The Processor ensures that subcontractors comply with the same data protection obligations as agreed in this contract, in particular through contracts pursuant to Art. 28 Para. 4 GDPR.

7. Audit Rights of the Controller

(1) The Controller has the right, following prior notification, to an appropriate extent and at reasonable times, to conduct audits of compliance with the provisions of Art. 28 GDPR and this agreement or to have them conducted by a third party appointed by the Controller, whom the Processor cannot unreasonably reject.

(2) The Processor shall provide the necessary information upon request and demonstrate the implementation of the technical and organizational measures, insofar as the Controller has a need for an audit under Art. 28 GDPR.

(3) Costs: The Processor shall bear the costs of audits that are attributable to demonstrable misconduct by the Processor. Otherwise, the parties may agree on appropriate remuneration for conducting audits, provided the effort is not already covered by the Main Agreement.

8. Notification of Breaches and Support Obligations

(1) The Processor assists the Controller in ensuring compliance with the obligations set out in Articles 32 to 36 GDPR, provided this is possible within the scope of the agreement and with reasonable effort. This includes in particular:

a) technical and organizational measures ensuring a level of security appropriate to the risk and enabling the detection of relevant incidents, if agreed;

b) the immediate notification of a personal data breach to the Controller, provided the notification to the Controller is necessary from the Processor's perspective;

c) the provision of relevant information to the Controller, insofar as the Controller is subject to information obligations towards data subjects or authorities and the information is available to the Processor;

d) assistance with data protection impact assessments and prior consultations, if agreed and reasonable.

(2) For support services that are not included in the scope of services of the Main Agreement and are not attributable to culpable behavior of the Processor, a separate remuneration may be agreed.

9. Authority of the Controller to Issue Instructions

(1) The Controller generally issues instructions regarding the processing of personal data in text form or in the form agreed upon in the Main Agreement (e.g., via platform features).

(2) The Controller shall confirm verbal instructions immediately in text form, should they be given.

(3) The Processor immediately informs the Controller if, in the Processor's opinion, an instruction violates data protection regulations. The Processor may suspend the execution of the relevant instruction until it has been confirmed or modified by the Controller, provided a statutory processing prohibition does not conflict anyway.

10. Deletion and Return of Personal Data

(1) Copies or duplicates of the content data will not be created without the knowledge of the Controller. This does not affect technically necessary temporary storage during processing as well as data that the Processor is legally required to retain.

(2) Upon completion of the contractually agreed work or upon request by the Controller – at the latest upon termination of the Main Agreement – the Processor must hand over to the Controller all content data and, if agreed, processing results, or delete them in compliance with data protection regulations according to documented instructions, provided no statutory retention obligation conflicts. The same applies to test and scrap material, if any.

(3) Documentation serving as proof of orderly and proper data processing shall be retained by the Processor according to statutory or documented retention periods and may be used by the Processor as proof towards authorities. Upon request of the Controller, a handover for the purpose of retention by the Controller may be agreed.

11. Miscellaneous Provisions

11.1 Remuneration

(1) No separate remuneration is required for this Data Processing Agreement, unless expressly agreed otherwise (e.g., in the Main Agreement).

(2) Insofar as the Controller requests support services according to Section 4 or 8 to an extent exceeding the services agreed upon in the Main Agreement, appropriate remuneration may be agreed.

(3) Insofar as the Controller exercises audit rights according to Section 7 to an extent exceeding the usual measure, appropriate remuneration may be provided subject to prior agreement (e.g., based on time and effort).

11.2 Term of the Agreement

(1) This agreement is contingent upon the existence of the Main Agreement pursuant to Section 1. The cancellation or other termination of the Main Agreement simultaneously terminates this agreement, unless statutory provisions dictate otherwise.

(2) The right to extraordinary termination for good cause as well as statutory rights of withdrawal remain unaffected.

11.3 Governing Law

The law of the Federal Republic of Germany shall apply, excluding its conflicts of law rules, where permissible.

11.4 Jurisdiction

If the Controller is a merchant within the meaning of the German Commercial Code (HGB), a legal entity under public law, or a special fund under public law, the exclusive place of jurisdiction for all disputes arising from or in connection with this agreement – as far as legally permissible – is the registered office of the Processor (88339 Bad Waldsee).

11.5 International Applicability

Insofar as the data protection law of Switzerland or the United Kingdom (UK) is applicable to the processing, all references to the GDPR in this agreement shall be deemed references to the corresponding, materially comparable provisions of the Swiss FADP (DSG) or the UK GDPR, respectively.

Signatures

Controller (Client)

Processor (Contractor)

LexLogik UG, represented by Managing Director

Jonas Maximilian Regul

Annexes

Annex 1 to the Order pursuant to Art. 28 GDPR

List of personal data and purpose of their processing

Type of data

The agreement covers the following data types and categories:

- Personal master data (e.g., names, salutations)
- Communication data (e.g., email addresses, telephone numbers, if entered or contained in documents)
- Contract and business master data (e.g., file numbers, references in documents)
- Content data from documents (e.g., texts, images, metadata in files, as far as technically present)
- Technical usage and log data to a reasonable extent (e.g., to ensure the operation and integrity of the services)

Categories of Data Subjects

The group of individuals affected by this supplementary agreement includes:

- Clients and prospects of the Controller

Annex 2 to the Order pursuant to Art. 28 GDPR

Technical and organizational measures (TOMs) according to Art. 32 GDPR and Annex

I. Confidentiality

The Processor does not use its own servers but servers rented from a German hosting provider. In doing so, the Processor ensures that the hosting provider implements the necessary security measures.

- Physical access controls
- System access controls
- Data access controls
- Data carrier controls
- Separation control

II. Integrity (Art. 32 Para. 1 lit. b GDPR)

Transfer control

- All employees are instructed and committed in the sense of Art. 32 Para. 4 GDPR to ensure the data protection-compliant handling of personal data.
- Data protection-compliant deletion of data after termination of the order.
- Options for encrypted data transmission are provided within the scope of the service description of the main contract.

Input control

for administration systems of the Processor:

- The data is entered or recorded by the Controller itself.
- Changes to the data are logged.

for the service of the Processor:

- The data is transmitted by the Controller itself.

III. Availability and Resilience (Art. 32 Para. 1 lit. b GDPR)

Availability control

The Processor ensures that its service has high availability. Since it does not process or store any Controller data beyond the individual cloud processing operations, these are not subject to any special availability requirements.