Document Version: 2.0

DATA PROCESSING AGREEMENT (“DPA”)

Between

Company
Street #
ZIP, city
Country

- hereinafter referred to as the “Controller” -
and

AskBrian GmbH
Leipziger Straße 51
10117 Berlin Germany

- hereinafter referred to as “Processor” or “AskBrian” -

- The Controller and the Processor hereinafter collectively referred to as the "Parties" and separately as a "Party" -

1 Scope of the Agreement

1.1 The Processor acts as a data processor for the Controller, as the Processor processes personal data for the Controller as set out in Annex 1. The Controller is the solely responsible entity for the processing of personal data under this Agreement.

1.2 The data processing activities concern the purposes, categories of data and categories of data subjects set out in Annex 1.

1.3 "Personal data" means any information relating to an identified or identifiable natural person, see article 4(1) of Regulation (EU) 2016/679 of 27 April 2016 (the General Data Protection Regulation "GDPR"). If other confidential information than personal data is processed for the purpose of fulfilling the Agreement, e.g. information considered confidential according to the Financial Business Act, any reference to "personal data" shall include the other confidential information.

2 Processing of Personal Data

2.1 Instructions: The Processor is instructed to process the personal data only for the purposes of providing the data processing services set out in Annex 1. The Processor may not process or use the Controller's personal data for any other purpose than provided in the instructions. Any additional instructions by the Controller need to be in writing.

Any transfer of personal data to any third country or international organisation may only take place in case the additional requirements under art. 44 ff. GDPR are met.

2.2 If the Processor considers an instruction from the Controller to be in violation of the GDPR, or other Union or member state data protection provisions, the Processor shall immediately inform the Controller in writing about this.

3 The Processor's general obligations

3.1 The Processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2 In accordance with Art. 32 of the GDPR, the Processor shall implement the technical and organisational measures as set out in Annex 3. The Controller deems these technical and organisational measures of the Processor as appropriate in regard to the processing of personal data under this Agreement.

3.3 If applicable, the Processor will also comply with the special data security requirements that apply to the Controller, see Annex 1, and with any other applicable data security requirements that are directly incumbent on the Processor; including the data security requirements in the country of establishment of the Processor, or in the country where the data processing will be performed.

3.4 The Processor shall upon request provide the Controller with sufficient information to enable the Controller to ensure that the Processor complies with its obligations under the Agreement, including ensuring that the appropriate technical and organisational security measures have been implemented.

3.5 If applicable, the Processor processes information the Controllers employees or authorized agents utilizing the Processor’s services (“Users”) provide in form of attached files to emails or within chat applications (“attachments”) in order to fulfil the requested service such as translation, conversion etc.. If Users request the processing of attachments (which might contain personal information), the Processor assumes the Controller’s consent in doing so. After processing the attachments, the Processor deletes the attachments immediately and keeps the meta-data only (file name, file size, time-stamp).

In case of every translation, information and documents are processed according to the following procedure:

a) User writes to Brian incl. attachment (interim saving of files, long-term saving of metadata). Metadata means Email-address, time-stamp, request-text, file name, file-size (no files). The communication is transmitted encrypted using TLS v1.3.

b) The AskBrian Cloud is a secure GCP and the servers are located in Germany. The Subject line and email body are used for intent/entity recognition (not sharing identity, signature, nor attachments). For the next step the information is transmitted encrypted using https via SSL / TLS.

c) In the “Natural Language Processing” structured information of what the user asks for, triggering the right (translation) skill execution. This information is still transmitted encrypted using https via SSL / TLS.

d) Translating raw text of the file on a slide-by-slide / chapter-by-chapter / sheet-by-sheet basis (not sharing whole file, nor identity, file name, or pictures). The text is transmitted with content snippets, no link to the user and no file context. Additionally, it is encrypted using https via SSL / TLS.

e) Sending the result to the User, deleting original and result files. The result is transferred encrypted using TLS v1.3.

3.6 Furthermore, the Controller is entitled at its own cost to appoint an independent auditor who is sworn to professional secrecy and who shall have access to the Processor's data processing facilities and receive the necessary information in order to be able to audit whether the Processor complies with its obligations under the Agreement, including ensuring that the appropriate technical and organisational security measures have been implemented. The auditor shall upon the Processor's request sign a customary non-disclosure agreement, and treat all information obtained or received from the Processor confidentially and may only share the information with the Controller.

3.7 The Processor must give authorities who by union or member state law have a right to enter the Controller's or the Controller's supplier's facilities, or representatives of the authorities, access to the Processor's physical facilities against proper proof of identity.

3.8 The Processor must without undue delay after becoming aware of the facts in writing notify the Controller about:

(i) any request for disclosure of personal data processed under the Agreement by authorities, unless expressly prohibited under Union or member state law,

(ii) any suspicion or finding of (a) breach of security that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the Processor under the Agreement, or (b) other failure to comply with the Processor's obligations under Clause 3.2 and 3.3, or

(iii) any request for access to the personal data received directly from the data subjects or from third parties.

3.9 Taking into account the nature of the processing the Processor will promptly assist the Controller with the handling of any requests from data subjects under Chapter III of the GDPR, including requests for access, rectification, blocking, or deletion. The Processor must also assist the controller by implementing appropriate technical and organisational measures, for the fulfilment of the Controller's obligation to respond to such requests.

3.10 The Processor will assist the Controller with meeting the other obligations that may be incumbent on the Controller according to Union or member state law where the assistance of the Processor is implied, and where the assistance of the Processor is necessary for the Controller to comply with its obligations. This includes, but is not limited to, at request to provide the Controller with all necessary information about an incident under Clause 3.8 (ii), and all necessary information for an impact assessment in accordance with article 35 and 36 of the GDPR.

3.11 In Annex 1, the Processor has stated the physical location of the servers, service centers etc. used to provide the data processing services. The Processor undertakes to keep the information about the physical location updated by providing a prior written notice of two months to the Controller. This does not require a formal amendment of Annex 1, prior written notice by mail or email suffices.

4 Further sub-processing of the Processor

4.1 If the Processor engages further sub-processor for the processing of personal data under this Agreement he will provide written information to the Controller. The Controller may reject any such authorisation to the use of a sub-processor without cause. The Processor must inform the Controller in writing of the discontinued use of a sub-processor.

4.2 Any listed sub-processors under link provided in Annex 2 of this Agreement shall be deemed authorized by the Controller with the execution of this Agreement.

4.1 Prior to the engagement of a sub-processor, the Processor shall conclude a written agreement with the sub-processor, in which at least the same data protection obligations as set out in the Agreement shall be imposed on the sub-processor, including an obligation to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR.

4.2 The Controller has the right to receive a copy of the Processor's agreement with the sub-processor as regards the provisions related to data protection obligations. The Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations. The fact that the Controller has given consent to the Processor's use of a sub-processor is without prejudice for the Processor's duty to comply with the Agreement.

5 Confidentiality

5.1 The Processor shall keep personal data confidential for the run-time of the underlying contract and beyond.

5.2 The Processor shall not disclose the personal data to third parties or take copies of personal data unless strictly necessary for the performance of the Processor's obligations towards the Controller according to the Agreement, and on condition that whoever personal data is disclosed to is familiar with the confidential nature of the data and has accepted to keep the personal data confidential in accordance with this Agreement.

5.3 If the Processor is a legal entity all terms of the Agreement apply to any of the Processor's employees and the Processor will ensure that its employees comply with the Agreement.

5.4 The Processor must limit the access to personal data to employees for whom access to said data is necessary to fulfil the Processor's obligations towards the Controller.

5.5 The obligations of the Processor under Clause 5 persist without time limitation and regardless of whether the cooperation of the Parties has been terminated.

5.6 The Controller shall treat confidential information received from the Processor confidentially and may not unlawfully use or disclose the confidential information.

6 Amendments and Assignments

6.1 The Parties may at any time agree to amend this Agreement. Amendments must be in writing.

6.2 The Processor may not assign or transfer any of its rights or obligations arising from this Agreement without the Controller's prior, written consent.

7 Term and termination of the Agreement

7.1 The Agreement enters into force when signed by both Parties and remains in force until terminated by one of the Parties.

7.2 Each party may terminate the Agreement upon 3 months written notice.

7.3 Regardless of the term of the Agreement, the Agreement shall be in force as long as the Processor processes the personal data, for which the Controller is data controller.

7.4 On the Controller's request the Processor shall immediately transfer or delete personal data, which the Processor is processing for the Controller, unless Union or member state law requires storage of the personal data.

7.5 The Processor is under no circumstances entitled to condition the full and unlimited compliance with the Controller's instructions on the Controller's payment of outstanding invoices etc., and the Processor has no right of retention in the personal data.

8 Priority

8.1 If any of the provisions of the Agreement conflict with the provisions of any other written or oral agreement concluded between the Parties, then the provisions of the Agreement shall prevail. However, the requirements in Clause 3 do not apply to the extent that the Parties in another agreement have set out stricter obligations for the Processor. Furthermore, the Agreement shall not apply if and to the extend the EU Commission's Standard Contractual Clauses for the transfer of personal data to third countries are concluded and such clauses set out stricter obligations for the Processor and/or for sup-suppliers.

8.2 This Agreement does not determine the Controller's remuneration of the Processor for the Processor's services according to the Agreement.

For and on behalf of AskBrian	For and on behalf of the Controller
Date, Place:	Date, Place:
_____	_____
Name: Pavol Sikula	Name:

ANNEX 1

This Annex constitutes the Controller's instruction to the Sub-Processor in connection with the Processor's data processing for the Controller and is an integrated part of the Agreement.

The processing of personal data

a) Purpose and nature of the processing operations
The supplier is providing translation, conversion, transcription, sanitization, and further digital services for the controller.

b) Categories of data subjects
I. Potential customers
II. Controller
III. User
IV. Other data subjects (mentioned in request texts and documents submitted for processing by the User)

c) Categories of personal data
Re b) I: Name, email address

Re b) II: Name, address, email address, telephone number

Re b) III: Name, address, email address, telephone number

Re b) IV: Any personal data the user shares in his/her request texts and in the documents submitted for processing

d) Special categories of data
The processor is not processing or storing special categories of data unless provided by the user in his/her service request (request texts or submitted documents for processing).

Submitted documents for processing by the user are (independent from the content) automatically deleted applying the Processor's general deleting routines after processing.

In the unlikely scenario in which the user shares special categories of data in his/her request text, the data is stored together with other request metadata.

'Special categories of data' include race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, and personal data about criminal convictions and offences.

e) Location(s), including name of country/countries of processing
The processing will be performed by AskBrian GmbH. Leipziger Straße 51, DE-10117, Berlin, Germany on the secure servers of GCP in Germany.

f) Special requirements to security measures that apply to the Controller: N/A

ANNEX 2

Subcontractors

The Processor is continuously adding new skills what might cause additional subcontractors or replacing the existing ones. The Processor does not consider solely the quality of the subcontractor, but always checks for highest data privacy and security possible. The current list of subcontractors can be found at https://askbrian.ai/subprocessors/. It should be noted that for more transparency, the Processor also includes the period of data processing.

ANNEX 3

Technical and organisational measures in accordance with Art. 32 of the GDPR

M.1 Confidentiality measures
M.1.1 Description of access control:

- Reception - visitor control at reception
- Manual locking system - Manual locking system with locking cylinder
- Locking system - Use of a locking system
- Key management - key regulation with documentation of the keys (e.g. key book)

M.1.2 Description of access control:

- Authentication with user + password
- User authorizations - Manage user authorizations (e.g. when entering, changing, leaving)
- Careful selection of personnel - Careful selection of cleaning and security personnel

M.1.3 Description of access control:

- Authorization concept - Creation and deployment of an authorization concept
- Data deletion - Secure deletion of data media before reuse (e.g. by multiple overwriting)
- Use of document shredders - Use of document shredders (min. security level 3 and protection class 2)
- Secure storage - Secure storage of data media

M.1.4 Description of the transfer control:

- Email Encryption - Email encryption using S/MIME or PGP (or other state-of-the-art method)
- SSL / TLS Encryption - Use of SSL / TLS encryption for data transmission on the Internet

M.1.5 Description of the separation requirement:

- Logical client separation - Logical client separation (software-side)
- Production and test system - Separation of production and test system

M.1.6 Description of pseudonymisation:

- Separation of contact data - separation of contact data and other data
- Separation of master data - separation of customer master data and order data

M.1.7 Description of encryption:

- Transmission - Encrypted data transmission (e.g. e-mail encryption according to PGP or S/Mime, VPN, encrypted Internet connections using TLS/SSL, use of FTAPI - data transfer tool)

M.2 Integrity measures

M.2.1 Description of the input controls

- Personalised user names - traceability of entry, modification and deletion of data through individual user names (not user groups)
- Logging - logging of data entry, modification and deletion
- Access rights - Personalized access rights for traceability of access.

M.3 Availability and resilience measures

M.3.1 Description of availability control:

- Off-site data protection - Keeping data protection in a secure, off-site location
- Backup & Recovery concept - Creation of a backup & recovery concept
- Fire alarm systems - Fire and smoke detection systems
- Redundant data storage - Redundant data storage (e.g. mirrored hard drives, RAID 1 or higher, mirrored server room)
- Protective socket strips - Protective socket strips in server rooms

M.3.2 Description of rapid recoverability:

- Data recovery - Regular and documented data recovery

M.4 Further measures for data protection

M.4.1 Description of job control:

- Selection - selection of the contractor with regard to due diligence (especially with regard to data security)
- AV contract - Conclusion of an agreement on contract processing in accordance with Art. 28 DS-GVO.
- DPO - Appointment of a data protection officer

- Ongoing review - Ongoing review of the contractor and its activities
- Training - Training of all employees with access rights. Regular follow-up training n.
- Obligation - Obligation of confidentiality according to Article 28 (3) sentence 2 lit. b, 29, 32 (4) DS-GVO

M.4.2 Description of the management system for data protection:

- Software presettings - Use of software with data-protection-friendly presettings in accordance with (Art. 25 para. 2 DS-GVO)
- Software-supported tools - Use of software-supported tools for compliance with data protection requirements (e.g. audatis MANAGER)