Data Processing Agreement

(hereafter referred to as “Agreement”)

between

Brighter AI Technologies GmbH, Litfaß-Platz 2, 10178 Berlin, Germany (hereafter referred to as “brighter AI”)

and

“Client” (legal entity as stated in the order document)

Preamble

This agreement specifies the data protection obligations of the contracting parties in the commissioned contractual relationship pursuant to Art. 28 GDPR. The Processor processes personal data for the Controller within the meaning of Article 4 No. 2 and Art. 28 GDPR on the basis of this DPA. It shall apply to all activities of the Processor in connection with the agreement in which employees or agents of the Processor process personal data by order of the Controller.

§ 1 Subject and Automatic Termination

The subject matter of the assignment results for brighter AI’s ‘Identity Protection Suite (IPS)’ services.

§ 2 Content specification: Types of data, nature and purpose of the processing

1. Types and categories of personal data (Art. 4 No. 1, 13, 14 and 15 GDPR)
The following types (categories) of personal data are being processed:
Biometric data, e.g. faces of pedestrians, and vehicle owners (car license plates) in image data.

2. Type and purpose of processing (Art. 4 No. 2 GDPR)
Anonymization of faces and license plates with brighter AI’s Identity Protection Suite.

3. Processing within EU/EEA or third country with adequate level of protection
Any transfer of personal data to a third country requires the prior consent of the controller and may only take place if the special requirements of Art. 44 ff. GDPR are fulfilled.

§ 3 Technical and organizational measures

1. The Processor must document the implementation of the necessary technical and organizational measures before the start of processing, in particular with regard to the concrete execution of the order and must inform the customer in advance. It is the responsibility of the Controller to ensure that the measures for the risks of the data to be processed provide an adequate level of protection. For the agreed technical and organizational measures, see Attachment 1.

2. The Processor shall provide the security pursuant to Art. 28 para. 3 c), 32 GDPR in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are measures of data security 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 different probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR are thereby to be taken into account (also see Attachment 1).

3. The technical and organizational measures are subject to general technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. The safety level of the defined measures must not be undercut. Personal data must be transmitted and stored in encrypted form as far as possible. Significant changes must be documented.

4. The Processor undertakes to prove the technical and organizational measures taken (see Attachment 1) to the Controller within the framework of the Controller's powers of control in accordance with § 7 of this contract.

§ 4 Rights of data subjects; Correction; Restriction and Deletion of data

1. The Processor may not rectify, delete or restrict the processing of the data processed in the order on his own authority, but only after the documented instructions of the Controller. If a person concerned contacts the Processor directly in this regard, the latter shall immediately forward the request to the Controller.

2. To the extent that the scope of services includes disclosure, deletion or erasure ("right to be forgotten"), correction and data portability, those are to be safeguarded directly by the Processor in accordance with the documented instructions of the Controller. The Controller shall bear the additional costs incurred by the Processor as a result.

§ 5 Other obligations of the Processor, in particular quality assurance

The Processor undertakes to comply with the legal obligations pursuant to Articles 28 to 33 GDPR.

1. A data protection officer is appointed in writing who carries out his duties in accordance with Art. 38 and 39 GDPR.

Dr. Daniel Taraz
JENTZSCH IT Rechtsanwaltsgesellschaft mbH
Alsterarkaden 13
20354 Hamburg
Phone 040-22 8683860
Mail: daniel.taraz@jentzsch-it.de

2. In particular, the Processor undertakes to maintain confidentiality in accordance with Art. 28 para. 3 sentence 2 b), 29, 32 para. 4 GDPR: The Processor confirms that he is aware of the relevant data protection regulations for commissioned data processing; in carrying out the work, he only employs employees who are bound to confidentiality and who have been familiarized beforehand with the data protection regulations relevant to them. The Processor and any person subordinated to the Processor who has access to personal data may process such data exclusively in accordance with the instructions of the Controller, including the powers granted in this contract, unless they are legally obliged to process such data (e.g. by a request for surrender from investigative authorities).

3. On request, both the Controller and the Processor shall cooperate with the supervisory authority in the performance of its tasks.

4. The Controller shall be informed without delay of any control actions and measures taken by the supervisory authority in so far as they relate to this mandate. This also applies if a competent authority investigates in the context of administrative or criminal proceedings with regard to the processing of personal data during commissioned processing at the Processor.

5. Insofar as the Controller for his part is subject to an inspection by the supervisory authority, an administrative offence or criminal procedure, the liability claim of a person concerned or a third party or any other claim in connection with the processing of the order with the Processor, the Processor must provide him with the best possible support.

6. The Processor shall regularly monitor internal processes as well as technical and organizational measures to ensure that processing within his area of responsibility is carried out in accordance with the requirements of the applicable data protection legislation and that the rights of the data subjects are protected.

7. The Processor must ensure that the technical and organizational measures taken can be proven to the customer.

§ 6 Subcontracts with subcontractors

1. The Processor may only commission subcontractors as further processors with the prior written consent of the Controller. It is agreed in this regard: The assignment of subcontractors is generally permissible. On request, the Controller will be provided with a list of the subcontractors used and their role.

2. A forwarding of the Controller's personal data is only permitted if the conditions specified in § 6 No. 1 are met.

3. If the services of the Subcontractor are provided outside the EU or the European Economic Area, the Processor is responsible for compliance with data protection measures.

4. Further outsourcing by the Subcontractor is permitted with the consent of the Processor (written or text form in simple electronic format).

5. All obligations of this agreement shall also be imposed on the other Subcontractor in the contract chain.

§ 7 Control rights of the Controller

1. The Processor agrees that within the framework of his control obligations pursuant to Art. 28 para. 3 h) GDPR, the Controller may monitor compliance with the provisions on data protection and in particular the contractual agreements to an appropriate and necessary extent, in particular by obtaining relevant information and inspecting the stored data and the data processing programs used.

2. The Processor shall in principle support the Controller in carrying out inspections and shall in particular also provide him with the information and evidence required for the implementation of the technical and organizational measures.

Proof of these measures can be provided by:
- compliance with approved rules of conduct in accordance with Art. 40 GDPR
- certification according to an approved certification procedure according to Art. 42 GDPR
- current certificates, reports or report extracts from independent bodies (e.g. auditors, data protection officers, IT security department, data protection auditors, quality auditors);
- suitable certification through IT security or data protection audits (e.g. according to BSI Grundschutz, ISO 27001).

§ 8 Notification of data protection violations

The Processor shall assist the Controller in complying with the obligations set out in Articles 32 to 36 GDPR concerning the security of personal data, reporting obligations in the event of data leaks, data protection impact assessments and prior consultations with the supervisory authority. Among other things, these include:

Ensuring an adequate level of protection through technical and organizational measures which take into account the circumstances and purposes of the processing as well as the predicted probability and severity of a possible infringement of rights due to security gaps and enable an immediate determination of relevant infringement events;
Violations of personal data must be reported immediately and exclusively to the Controller;
The obligation to inform the Controller within the scope of his duty to provide information;
To support those concerned and in this connection to make all relevant information available to them without delay;
Supporting the Controller in his prior consultations with the supervisory authority.

Support services which are not included in the service description or which are attributable to misconduct on the part of the Controller must be reimbursed by the Controller to the Processor.

§ 9 Instructions of the Controller

1. Instructions or information from the Controller to the Processor shall be provided in text or written form. Oral instructions must be confirmed immediately in writing or in text form.

2. The Processor shall inform the Controller immediately if an instruction may violate data protection regulations or the provisions of this contract. In this case, the Processor shall be entitled to suspend the execution of the relevant instructions until they are confirmed or amended by the Controller.

§ 10 Erasure and return of personal data

1. Copies or duplicates of the data will not be made without the Controller's knowledge. Backup copies, insofar as they are necessary to guarantee proper data processing, and statutory retention periods remain unaffected by this.

2. After completion of the contractually agreed service provision or before upon request by the customer – at the latest, however, upon termination of the agreement – the Processor must hand over to the Controller all documents, processing and usage results created and data stocks in connection with the contractual relationship or destroy them in accordance with data protection regulations after prior consent. The same applies to test and scrap material. A deletion report must be created and submitted to the Controller upon request.

3. Documentation that serves as proof of orderly and proper data processing must be kept by the Processor after the end of the contract in accordance with the respective retention periods. He may hand them over to the Controller at the end of the contract.

§ 11 Liability and contractual penalty

The Controller and the Processor shall be liable to the persons concerned in accordance with the provisions of Art. 82 GDPR. In accordance with Art. 82 para. 2 sentence 2 GDPR, the Processor is only liable for the damage caused by the processing if he has not complied with his obligations specifically imposed as a Processor, or has acted in breach of the legally issued instructions of the data Controller or against these instructions.

A liability clause agreed between the parties in the service contract (main contract for the provision of services) shall also apply to the data processing, unless expressly agreed otherwise in this agreement.

§ 12 Final clauses

1. Amendments and changes to this agreement and the service contract require the written form or text form in simple electronic format within the meaning of Article 28 para. 9 GDPR. This also applies to any waiver of this formal requirement

2. Should any provision of this DPA be invalid or unenforceable, this shall not affect the validity of the other provisions. In such a case, the parties undertake to replace the invalid provision with another legally effective provision that fulfils the purpose of the deleted provision.

3. Should the property of the controller be endangered at the Processor by measures of third parties, such as seizure, insolvency proceedings or other events, the Processor must inform the Controller immediately and before these measures occur.

4. The right of retention in the sense of § 273 BGB (German Civil Code) shall be Excluded.

Attachment 1: Technical and organizational measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

1.1. Physical Access Control

No unauthorized access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems

- Definition of authorized persons
- Documentation of the issuing and return of cards/keys
- Manual locking system and security locks
- Electronic access control
- Construction measures (burglar-proof windows)
- Protection of IT and network equipment against unauthorized access
- Security services employed outside working times
- Video surveillance of entrances
- Security concept for data centers/server rooms

1.2. Electronic Access Control

No unauthorized use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media

- Server and SAN/NAS are hosted in server rooms or data center areas which fulfil the ISO 27001 requirements
- Individual username and password
- Password regulation for users including regular prompts to change password
- Close accounts of employees who have left the company including documentation
- Automatically block workstations after 15 minutes / Clear screen policy
- 2 factor authentication
- WLAN secured against unauthorized access
- Regular check of existing access authorizations

1.3. Internal Access Control (permissions for user rights of access to and amendment of data)

No unauthorized Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorization concept, need-based rights of access, logging of system access events

- BIOS password and boot sequence definition
- Access restrictions to network limits
- Configure authorization concept and assign by roles
- Implementation of the need-to-know principle
- Logging of access (log protocols)
- Analyze log files for irregularities (for example SIEM)
- Logging of file access
- Logging of database access
- Logging of data access or transfer
- Reporting of all automatically detected attempts at misuse (for example SIEM)
- Definition and documentation of authorized persons
- Written documentation of authorization rights
- Regular check of existing authorizations
- Restriction of the person subgroup assigned with transfer authorization rights
- Regular check of log data

1.4. Isolation Control

The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;

- Network segmentation depending on level of protection required
- Separation of functions by multi-client enabled systems
- Physical separation of data
- Separation of development, testing, and live systems
- Sandboxing
- Data records with function attributes

1.5. Pseudonymization (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)

The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures.

- Pseudonymization of personal identifiable data

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

2.1. Data Transfer Control

No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

- Encryption of laptops
- Safe transmission of sent data (e.g. SFTP, VPN, TLS, SSL, PGP, S/MIME)
- Central management of keys for encrypted systems
- Deletion and destruction of data storage media according to DIN 32757
- Secure transport of removable media (for example backup, tapes)

2.2. Data Entry Control

Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

- Logging input of personal data
- Regularly check log data
- Integrity and authentication check

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

3.1. Availability Control

Prevention of accidental or willful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning; Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);

- Operation and regular inspection of UPS, emergency power, overvoltage protection
- Use of virus scanners and firewalls
- Monitoring of operating parameters in data centers/server rooms
- Fire/smoke alarm installation
- Use of penetration tests
- Data security concept with regular backups
- Regularly check the status and labeling of storage medias and data backups
- Offsite archive of removable backup media
- Ability to restore in a timely manner

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

4.1. Data Protection Management: data privacy management

4.2. Incident Response Management: Operate and testing of incident response plans

4.3. Data Protection by Design and Default (Article 25 Paragraph 2 GDPR): data privacy friendly pre-settings

4.4. Order or Contract Control

No third-party data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalized Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

- Contractual regulations in compliance with Article 28 Paragraph 3 GDPR (Processing by a processor)
- Contractual regulations in compliance with EU standard contractual clauses
- Strict controls on the Selection of contractors, especially in terms of their carefulness and reliability (particularly regarding data security) and in compliance with regulations
- Data confidentiality obligation of employees at the contractors
- Documented formalized contract management
- Ensure that personal data is destroyed after contract completion