brighter AI

Data Processing Agreement

for the Licensing Agreement between

Company
Address

(herein referred to as the "Controller")

and

Brighter AI Technologies GmbH
Litfaß-Platz 2
10178 Berlin
Germany

(herein referred to as the "Processor" or "brighter AI")

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 Licensing Agreement in which employees or agents of the Processor process personal data of the Controller.

§ 1 Subject and Automatic Termination

The subject matter of the assignment results from the above-mentioned Licensing Agreement for brighter AI's software solution.

§ 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:
Image data that might contain persons (biometric data, i.e. faces) and vehicle owners (car license plates).

2. Type and purpose of processing (Art. 4 No. 2 GDPR)
Anonymization[1] of faces, full bodies, and car license plates with brighter AI's software solution brighter Redact.

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 organisational 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 organisational 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 organisational 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.

[1] Anonymization is defined here as blurring/blackening of the face or natural anonymization of technical identifiers. Effective anonymization depends also on customer behavior and dataset and domain in question, and is to be assessed on a case by case basis by the controller. For example the deletion/security of original data is regularly a precondition to effective anonymization, as well as the size of the dataset and the amount of and general knowledge of data subjects.

§ 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. Volker Wodianka, LL.M. (IT&T)
Wodianka privacy legal GmbH
Dockenhudener Str. 12a
22587 Hamburg, Germany
Mail: volker.wodianka@privacy-legal.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 organisational 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 organisational measures taken can be proven to the customer.

§ 6 Subcontracts with subcontractors

1. Processor may commission Subcontractors as further processors with prior general written authorization of the Controller.

As a condition precedent to the Controller forwarding any personal data to the Processor, by signing this agreement it is agreed that the Controller grants general authorization for current subcontractors as processors in accordance with Art. 28 para. 2 GDPR and grants Processor general written authorization to appoint new Subcontractors. On request, the Controller will be provided a current list of subcontractors and their roles.

2. Controller will only forward personal data to the Processor if the conditions specified in § 6 No. 1 are met.

3. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Subcontractors acting as processors with sufficient time and information to provide the Controller the opportunity to object to such changes as required under Art. 28 para. 2 GDPR.

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. 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.

§ 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 organisational 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 organisational 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. 30 days after completion of the contractually agreed service provision, or before upon request by the customer, the Processor must hand over to the Controller all documents 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.

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.

5. The priority ratio is as follows:
In the event of contradictions in content between this agreement and the service contract, the provisions of this agreement shall take precedence.

6. This agreement is governed by the laws and regulations of the Federal Republic of Germany. The courts of Berlin, Germany shall have exclusive jurisdiction for any disputes arising out of or in connection to this agreement.

7. The Attachments are part of this DPA:

- Attachment 1: Technical and organizational measures
https://brighter.ai/wp-content/uploads/2024/10/TOMs_brighterAI.pdf
- Attachment 2: Professional secrecy amendment,
https://brighter.ai/wp-content/uploads/2024/09/Professional_Secrecy_Amendment_brighterAI.pdf

Controller:	Processor:
Place, Date	Place, Date
Name, Position	Name, Position
Signature	Signature