This is a template for a data processing agreement (DPA) of Vimmera AI Solutions GmbH. We provide this template solely for reasons of transparency toward our prospective customers and customers. The appendices and attachments referenced in the contractual template are intentionally omitted. Our customers will, of course, receive the appendices and an individually drafted and signed DPA if and where required. We ask for your understanding that we cannot disclose all information at this point. This contractual template does not replace a valid DPA.

Data Processing Agreement (DPA) pursuant to Art. 28 GDPR

between

Vimmera AI Solutions GmbH

Löwestrasse 66

14612 Falkensee

– hereinafter the “Processor” –

and

[Customer, address]

– hereinafter the “Controller” –

Preamble

This Data Processing Agreement specifies the rights and obligations of the parties in connection with the processing of personal data by the Processor on behalf of the Controller. The Agreement serves to fulfill the requirements of Art. 28 GDPR and, where applicable, other relevant data protection provisions. The Processor processes personal data exclusively on documented instructions of the Controller and never for its own purposes. This Agreement is an inseparable part of the main agreement. In the event of contradictions between the main agreement or other arrangements and this DPA, this DPA shall prevail insofar as the data-protection-law processing of personal data is concerned.

Part 1 – General Provisions

§ 1 Subject matter, service context, term and termination

(1) The subject matter of this Agreement is the processing of personal data by the Processor in connection with the performance of the services agreed in the main agreement. This includes, in particular, the development, implementation, provision, operation, administration, maintenance, further development, customization and support of software solutions, platforms and systems including frontend and backend components, user and role management, data management, retrieval-augmented-generation components (RAG), analysis and processing modules as well as—if agreed—functions for AI use, training or fine-tuning processes.

(2) The nature, scope and purpose of the processing result from the main agreement, the service description, the Processor's general terms and conditions and the annexes to this DPA, in particular the annex "Technical and Organizational Measures" (TOM). Insofar as different documents contain differing statements, the following order of precedence shall apply: first this DPA including annexes, then the respective specifically data-protection-related service descriptions, then the main agreement, then the general terms and conditions.

(3) The term of this Data Processing Agreement corresponds to the term of the main agreement. The DPA ends automatically upon termination of the main agreement, without requiring a separate notice of termination.

(4) Obligations under this Agreement which by their nature are intended to have effect beyond its term, such as in particular confidentiality obligations, obligations to support the Controller, documentation obligations as well as deletion and return obligations, shall continue to apply beyond termination of the Agreement.

§ 2 Nature, scope and purpose of the processing

(1) The Processor processes personal data exclusively within the scope of fulfilling the contractually agreed services and exclusively on the basis of the Controller's instructions.

(2) Any processing beyond the assignment for the Processor's own purposes is expressly excluded. In particular, it is excluded that the Processor uses personal data of the Controller or of the data subjects—including content data, chat histories, documents, metadata, files or other data—for its own development, training, analysis, optimization, product development or marketing purposes. Such use is only permitted if the Controller expressly, unambiguously and in documented form approves this in an agreement intended for that purpose and this is clearly regulated within the scope of the DPA.

(3) Insofar as training or fine-tuning processes, configuration optimizations, establishment of knowledge bases, RAG indices or similar processes are carried out, these shall be performed exclusively upon express, documented instruction of the Controller, exclusively purpose-bound for the benefit of the Controller's systems, without the Processor's own interests.

(4) The processing may in particular include the following operations: collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, making available, alignment, combination, restriction, erasure and destruction of personal data.

(5) Operation, hosting, provision, maintenance, support, analysis, processing, storage, retrieval and deletion of personal data shall be performed on behalf of the Controller within the scope of the use of the contractually agreed software and AI systems.

§ 3 Categories of personal data and data subjects

(1) Depending on the scope of services, the Processor processes in particular the following categories of personal data:

Master data and contact data (e.g., name, email address, username, organizational affiliation),

Authentication and authorization data (e.g., roles, rights, tokens, password hashes),

System, log and usage data (e.g., timestamps, access logs, security logs, error logs),

Content and communication data (e.g., text inputs, files, documents, chat content),

Result and processing data insofar as these contain personal elements.

(2) Special categories of personal data pursuant to Art. 9 GDPR are generally not the subject of this contractual relationship. Such data shall be processed only if expressly commissioned by the Controller, legally permissible, documented accordingly and clearly regulated by contract, and if additional protective measures have been agreed.

(3) Data subjects may in particular be employees and users of the Controller, customers, contact persons, contractual partners as well as other natural persons whose personal data are processed by the Controller and used within the scope of the systems.

§ 4 Responsibilities

(1) The Controller remains responsible for the lawfulness of the processing of personal data within the meaning of the GDPR. In particular, it ensures that an appropriate legal basis exists and that data subject rights are complied with.

(2) The Processor processes personal data exclusively on documented instructions, implements appropriate technical and organizational measures and supports the Controller in accordance with this Agreement.

(3) The Controller ensures that the data transmitted to the Processor may be processed lawfully.

Part 2 – Obligations of the Processor

§ 5 Instructions and objection

(1) The Processor processes personal data exclusively on instructions of the Controller, unless a legal obligation provides otherwise.

(2) Instructions shall generally be issued in text form. Oral instructions must be confirmed subsequently in writing or in text form without undue delay.

(3) If the Processor considers an instruction to be unlawful, it shall inform the Controller without undue delay and suspend the instruction until clarification.

(4) The Processor shall also delete personal data during the term of the Agreement upon documented instruction of the Controller, insofar as no statutory retention obligations prevent this.

§ 6 Confidentiality

All employees and other persons who process personal data at the Processor are bound to confidentiality and are sensitized accordingly. Access is granted exclusively on a need-to-know basis.

§ 7 Security of processing and technical measures

(1) The Processor undertakes to implement appropriate technical and organizational measures in accordance with Art. 32 GDPR that ensure a level of security appropriate to the risk.

(2) These measures are described in the annex "Technical and Organizational Measures (TOM)" and form part of this Agreement.

(3) The Processor further develops measures in accordance with the state of the art without falling below the agreed security level. Material changes are documented and communicated to the Controller.

§ 8 Assistance with data subject rights

The Processor supports the Controller in fulfilling data subject rights pursuant to Chapter III GDPR. Requests from data subjects received directly by the Processor are forwarded to the Controller without undue delay.

§ 9 Assistance with statutory obligations

The Processor supports the Controller with obligations under Art. 32 to 36 GDPR, in particular security obligations, reporting of personal data breaches, notification of data subjects, data protection impact assessments and, where applicable, coordination with authorities.

§ 10 Personal data breaches

(1) The Processor shall report personal data breaches without undue delay after becoming aware of them, preferably within 24 hours, to the Controller.

(2) The notification contains the information required under Art. 33 GDPR.

(3) The Processor supports the Controller in notification and assessment.

§ 11 Sub-processors

(1) The Processor is entitled to engage sub-processors. The sub-processors existing at the time this Agreement is concluded are listed in Annex 2.

(2) The Processor informs the Controller about changes; the Controller may object within 14 days.

(3) Sub-processors are contractually obligated at least to the same extent.

(4) The Processor remains responsible.

(5) The Processor regularly reviews compliance with the data protection obligations of the sub-processors and documents this.

§ 12 Transfers to third countries

A transfer to third countries takes place only if it is necessary, expressly agreed and permissible under Art. 44 et seq. GDPR. Appropriate safeguards are used and additional protective measures are taken. The Processor informs about authority access insofar as permissible.

§ 13 Return and deletion

After the end of the Agreement, the Processor deletes or returns personal data. Backups are deleted in accordance with the backup cycles. Deletions are documented. Statutory retention obligations remain unaffected.

§ 14 Evidence and audits

The Processor provides the information required to demonstrate compliance. Audits are possible after reasonable notice. Alternatively, suitable certificates or audit reports may be used.

Audits are conducted during usual business hours, while safeguarding business and trade secrets, and not more frequently than once per year, unless there is a specific reason.

§ 15 Measures by third parties

The Processor informs the Controller in the event of seizure, attachment, insolvency or comparable events, insofar as legally permissible.

§ 16 Liability

Liability is governed by the statutory provisions, in particular Art. 82 GDPR.

Contractual liability provisions apply additionally insofar as they do not violate data protection law.

Part 3 – Final provisions

§ 17 Form

Amendments or supplements to this DPA require at least text form, unless a stricter form is prescribed by law.

§ 18 Severability clause

Should a provision of this Data Processing Agreement be or become wholly or partly invalid, void or unenforceable, the validity of the remaining provisions shall remain unaffected. In place of the invalid, void or unenforceable provision, such valid, legally permissible and enforceable provision shall be deemed agreed that comes as close as possible to the economic purpose and the allocation of risk of the invalid provision. The same applies in the event of regulatory gaps. The parties expressly undertake to replace an invalid provision without undue delay with a valid provision that best corresponds to the legal and economic purpose of the original provision. This does not involve a reversal of the burden of proof.

§ 19 Order of precedence

In the event of contradictions, the following order applies:

this DPA including annexes,

expressly overriding data protection service descriptions,

main agreement,

general terms and conditions.

Place, date

Signatures of both parties