Data Processing Addendum (DPA)

As an Annex to the General Terms and Conditions
– hereinafter referred to as the "Service Agreement" –

between the

Customer

– hereinafter referred to as the "**Controller**" –

and **Empirio UG (haftungsbeschränkt)** (empirio)

– hereinafter referred to as the "Processor" –

– both hereinafter collectively referred to as the "Parties" –

the following Data Processing Agreement is hereby concluded:

Table of Contents

Preamble

Under the Service Agreement concluded between the Parties, the Processor processes personal data on behalf of the Controller. The Controller acts as a controller within the meaning of Art. 4 (7) GDPR, and the Processor acts as a processor within the meaning of Art. 4 (8) GDPR.

This Agreement specifies the rights and obligations of the Parties in connection with the processing of personal data pursuant to Art. 28 GDPR and the relevant provisions of the German Federal Data Protection Act (BDSG).

To the extent applicable, references to the GDPR in this Agreement shall also include the United Kingdom General Data Protection Regulation ("UK GDPR") pursuant to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, as well as the UK Data Protection Act 2018.

To the extent applicable, references to the GDPR in this Agreement shall also include the revised Swiss Data Protection Act (revFADP) and the implementing provisions issued thereunder.

To the extent that the processing involves personal data of data subjects residing in the USA or Canada, the Processor additionally undertakes to comply with the applicable provisions of the California Consumer Privacy Act (CCPA) as amended (including the CPRA) and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), if and to the extent that these laws apply to the specific processing.

To the extent that the processing involves personal data of data subjects residing in Australia, the Processor additionally undertakes to comply with the applicable provisions of the Australian Privacy Act 1988 (including the Australian Privacy Principles), if and to the extent that these laws apply to the specific processing.

§ 1 Scope of Application

This Agreement applies to the collection, processing, and erasure (hereinafter: "processing") of all personal data (hereinafter: "data") that are the subject of the Service Agreement or that arise or become known to the Processor in the course of its performance. Data of the Processor's employees are excluded from the scope of this Agreement, provided that such data exclusively concern the employment relationship with the Processor.

To the extent applicable, this Agreement applies accordingly to the processing of personal data under the United Kingdom General Data Protection Regulation (UK GDPR), the revised Swiss Data Protection Act (revFADP), the Australian Privacy Act, as well as the US (CCPA/CPRA) and Canadian (PIPEDA) data protection regulations.

§ 2 Specification of the Processing Activity

(1) The subject matter and duration of the processing, as well as the scope, nature, and purpose of the intended processing of data, are determined by the Service Agreement. The General Terms and Conditions (https://www.empirio.ai/terms-of-service) constitute the Service Agreement and are explicitly agreed to by the Controller during registration.

(2) The term of this Agreement corresponds to the term of the Service Agreement. Termination of this Agreement shall constitute termination of the Service Agreement.

(3) The nature of the processed data is determined by the Controller through the type of surveys, the use of the services, and the transmission of data.

(4) The categories of data subjects are determined by the Controller through the type of surveys, the use of the services, and the transmission of data.

(5) To the extent the Processor uses AI functionality and/or third-party AI systems (including large language models) to provide the Services, the Processor shall ensure that any personal data transmitted to such third-party providers is processed solely for the purpose of providing the Services on behalf of the Controller and in accordance with the Controller’s documented instructions. The Processor shall ensure, to the extent contractually and technically possible, that such third-party providers do not use personal data transmitted by the Processor for the training or improvement of their general AI models. The Processor shall inform the Controller upon request about the relevant third-party providers and the applicable safeguards.

§ 3 Responsibility and Right of Instruction

(1) Within the framework of the responsibilities assigned to them under data protection regulations, each Party shall be responsible for compliance with data protection laws. The Controller may at any time request the surrender, correction, adjustment, deletion, and restriction of the processing of data.

(2) To ensure the protection of the rights of the data subjects, the Processor shall provide the Controller with appropriate support, in particular by ensuring suitable technical and organizational measures.

(3) If a data subject contacts the Processor directly to exercise a data subject right, the Processor shall immediately forward this request to the Controller.

(4) The Processor may process data exclusively within the framework of the Controller's instructions, unless the Processor is required to perform other processing by Union or Member State law to which the Processor is subject (e.g., investigations by law enforcement or national security authorities). In such a case, the Processor shall notify the Controller of these legal requirements prior to processing, unless the law in question prohibits such notification on important grounds of public interest (Art. 28 (3) sentence 2 lit. a GDPR). An instruction is any written, electronic, or oral order issued by the Controller directing the Processor to handle data in a specific manner. Orders shall be documented. Instructions are initially defined by the Service Agreement and may subsequently be amended, supplemented, or replaced by the Controller in documented form through individual instructions.

(5) The Processor shall immediately inform the Controller if it is of the opinion that an instruction violates data protection regulations. The Processor is entitled to suspend the execution of the relevant instruction until it is confirmed or modified by the Controller. If necessary, considering the severity of the violation, the Processor is entitled to suspend processing or to terminate the Service Agreement for cause (extraordinary termination).

(6) Changes to the subject matter of processing and changes in procedures shall be coordinated and documented jointly. The Processor may provide information to third parties or data subjects only with the prior express written consent of the Controller. The Processor shall not use the data for any other purposes and is specifically not authorized to disclose it to third parties. Copies and duplicates shall not be created without the Controller's knowledge, with the exception of backup copies, provided they are necessary to ensure proper data processing.

(7) The Controller shall maintain the record of processing activities pursuant to Art. 30 (1) GDPR. Upon request, the Processor shall provide the Controller with information for inclusion in said record. The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller in accordance with the requirements of Art. 30 (2) GDPR.

(8) The processing of personal data on behalf of the Controller shall generally take place within the European Union or the European Economic Area. Processing in states outside the European Union or the European Economic Area (third countries) is permitted provided that the requirements of Art. 44 et seq. GDPR are met. This applies in particular if:
a) an adequacy decision by the European Commission exists for the third country concerned, or
b) appropriate safeguards within the meaning of Art. 46 GDPR are provided, in particular through the conclusion of the standard contractual clauses issued by the European Commission.

To the extent that no adequacy decision exists for a transfer and appropriate safeguards pursuant to Art. 46 GDPR are used instead, the standard contractual clauses – provided that the data protection laws of the United Kingdom (UK GDPR) apply – shall additionally be supplemented in the respectively required version under UK law (in particular the UK International Data Transfer Addendum or the International Data Transfer Agreement). To the extent that the Swiss revFADP applies, the standard

contractual clauses shall be supplemented with the necessary adaptations under Swiss law (Swiss Addendum).

The processing of personal data in Switzerland, the United Kingdom, and for commercial organizations in Canada (PIPEDA) is considered processing in a third country with an adequate level of data protection in the sense of an adequacy decision.

The use of sub-processors in third countries is listed in Annex 2 to this Agreement. The Controller hereby grants general authorization for the engagement of the sub-processors named therein. Section 8 of this Agreement remains unaffected.

(9) The Processor shall ensure that natural persons under its authority who have access to data process such data only on the instructions of the Controller. Processing of data outside the Processor's business premises (e.g., telecommuting, working from home, home office, mobile working) requires the prior definition of appropriate technical and organizational measures for the respective processing situation.

(10) Special provisions for international data subjects:
1. The Processor acts as a "Service Provider" within the meaning of the CCPA/CPRA (USA) as well as comparable provisions of PIPEDA (Canada) and the Australian Privacy Act. It will not sell personal data or share it beyond the business purpose.
2. To the extent that the processing concerns data subjects in Canada, Australia, the United Kingdom (UK GDPR), or Switzerland (revFADP), the Processor guarantees compliance with the respective local data protection laws, particularly regarding access, rectification, and deletion.

§ 4 Compliance with Mandatory Legal Obligations by the Processor

(1) The Processor shall ensure that persons authorized to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(2) The Parties shall support each other in demonstrating and documenting the accountability incumbent upon them with regard to the principles of proper data processing, including the implementation of the necessary technical and organizational measures (Art. 5 (2), Art. 24 (1) GDPR).

(3) The Processor shall appoint a Data Protection Officer who shall perform their duties in accordance with statutory requirements. The contact details of the Data Protection Officer are: Empirio UG (haftungsbeschränkt), Data Protection Officer, 31785 Hameln, Germany, info@empirio.ai.

§ 5 Technical and Organizational Measures and their Monitoring

(1) The Parties agree on the specific technical and organizational security measures set forth in Annex 1 "Technical and Organizational Measures" to this Agreement. The Annex is an integral part of this Agreement.

(2) Technical and organizational measures are subject to technical progress. In this respect, the Processor is permitted to implement alternative adequate measures. In doing so, the security level of the measures specified in the Annex "Technical and Organizational Measures" must not be compromised.

(3) The Processor shall provide the Controller with all necessary information required to demonstrate compliance with the requirements set forth in this Agreement as well as with statutory requirements.

(4) The Processor shall provide the Controller with all necessary information required for the assessment of the impact of the planned processing operations on the protection of data (Data Protection Impact Assessment) and shall assist the Controller with any prior consultation of the supervisory authority pursuant to Art. 36 GDPR using the means available to the Processor. Information shall be provided only to the extent that the Controller cannot obtain it itself.

(5) In consultation with the Controller, the Processor shall take all necessary measures to secure the data and the security of processing, particularly taking into account the state of the art, as well as to mitigate possible adverse consequences for data subjects.

§ 6 Notification of Breaches by the Processor

The Processor shall immediately inform the Controller in the event of serious disruptions to its operations, suspected violations of this Agreement or statutory data protection provisions, violations of such provisions, or other irregularities in the processing of the Controller's data. This applies in particular with regard to the notification obligation pursuant to Art. 33 (2) GDPR as well as corresponding obligations of the Controller pursuant to Art. 33 and Art. 34 GDPR. The Processor undertakes to provide the Controller with appropriate support in its obligations under Art. 33 and 34 GDPR where necessary. The Processor may only carry out notifications pursuant to Art. 33 or 34 GDPR on behalf of the Controller following prior instructions in accordance with Section 3 of this Agreement.

§ 7 Deletion and Return of Data

(1) Data carriers and data sets provided shall remain the property of the Controller.

(2) Upon deletion of the account or earlier upon request by the Controller, but at the latest upon termination of the Service Agreement, the Processor shall, at the Controller's discretion, either hand over to the Controller or – subject to the Controller's prior consent – destroy in a data-protection-compliant manner all documents, results of processing and use, and data sets (including any copies or reproductions thereof) that have come into its possession in connection with the contractual relationship. The same applies to test and scrap material. The erasure shall be confirmed to the Controller upon request.

(3) The Processor may retain documentation that serves as proof of the orderly and compliant processing of data in accordance with the respective retention periods, even beyond the end of the

contract. Alternatively, the Processor may hand such documentation over to the Controller at the end of the contract for its own discharge. For data retained pursuant to sentence 1, the obligations under paragraph 2 shall apply after the end of the retention period. The Processor also retains personal data in aggregated form for statistical purposes, provided that such data are subject to appropriate safeguards, in particular in accordance with Art. 5 (1) (b), Art. 14 (5) (b), Art. 17 (3) (d), Art. 21 (6), and Art. 89 GDPR.

§ 8 Sub-processing

(1) The Processor is entitled to engage further processors (sub-processors) to fulfill the contractually owed services. The Controller hereby grants its general authorization for the engagement of sub-processors within the meaning of Art. 28 (2) GDPR. The sub-processors engaged at the time of the conclusion of this Agreement are listed in Annex 2 to this Agreement. The Processor shall inform the Controller in a timely manner of any intended changes concerning the addition or replacement of sub-processors.

(2) The Controller is entitled to object to the engagement of a new or replacement sub-processor for important reasons related to data protection law. The objection must be declared in text form within 14 days after receipt of the notification. If the Controller objects in a timely manner and if it is not reasonable for the Processor to refrain from engaging the sub-processor, both Parties are entitled to terminate the Service Agreement for cause (extraordinary termination).

(3) If sub-processors are engaged by the Processor, the Processor shall ensure that its contractual agreements with the sub-processor are designed in such a way that the level of data protection corresponds at least to the agreement between the Controller and the Processor and that all contractual and statutory requirements are complied with; this applies in particular with regard to the use of suitable technical and organizational measures to ensure a level of security for the processing that is appropriate to the risk.

(4) If the sub-processor fails to fulfill its data protection obligations, the Processor shall remain liable to the Controller for the fulfillment of the sub-processor's obligations.

§ 9 Data Protection Audits

The Processor undertakes to provide, upon request by the Controller and on an annual basis, the necessary information to demonstrate compliance with the obligations set forth in Art. 28 GDPR, in particular the implementation of and compliance with the technical and organizational measures pursuant to Section 5 of this Agreement, in document-based form, provided that the Controller cannot obtain this information itself and it is available to the Processor. The Controller may obtain documentation, certifications, and audit reports for this purpose. The expenses caused by such audits shall be charged at an hourly rate of €90 and shall be borne by the Controller. The Controller shall document the audit result and communicate it to the Processor. In the event of errors or irregularities discovered by the Controller, particularly during the inspection of processing results, the Controller shall inform the Processor without delay. Should a supervisory authority audit the

Processor due to culpable conduct on the part of the Controller, the resulting personnel and material expenses shall be borne by the Controller.

§ 10 Final Provisions

(1) The Processor may amend or replace this Annex and all its components with a notice period of two weeks. The Controller shall be notified of amendments or replacements to the Agreement by email or within their account. The Controller shall have an extraordinary right of termination, which may be exercised within 30 days of the notification.

(2) Should individual provisions of this Agreement be or become invalid or unenforceable, the validity of the remaining provisions shall not be affected thereby. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision whose effects come closest to the objective pursued by the Parties with the invalid or unenforceable provision. The foregoing provisions shall apply accordingly in the event that the Agreement proves to be incomplete.

(3) German law shall apply.

(4) This Agreement is available in German and English. In the event of discrepancies or questions of interpretation, the German version shall prevail. The English version is for informational purposes only.

Annex 1 – Technical and Organizational Measures

Section 5 of the Data Processing Agreement refers to this Annex for the specification of technical and organizational measures.

Section 1 – Technical and Organizational Security Measures The Parties are obliged to implement appropriate technical and organizational measures in such a way that the processing of data is carried out in accordance with statutory requirements and the protection of the rights of the data subjects is ensured in an appropriate manner.

Section 2 – Internal Organization of the Processor The Processor shall organize its internal operations in such a way that they meet the specific requirements of data protection. In doing so, measures shall be taken that are suitable depending on the nature of the data or categories of data to be protected.

Section 3 – Specification of Individual Measures (1) Specifically, the following measures are determined, which serve to implement the requirements of Art. 32 GDPR:

Measure	**Implementation of the Measure**
Physical Access Control Unauthorized persons must be denied access to data processing facilities used to process personal data.	Physical access control system for office premises; storage of confidential documents under lock and key in lockable cabinets.
System Access Control The use of data processing systems by unauthorized persons must be prevented.	Use of state-of-the-art technology; regular password changes; password protection for all systems; two-factor authentication (2FA) for access to personal data; encryption procedures.
Data Access Control It must be ensured that persons authorized to use a data processing system can only access the data subject to their access authorization, and that personal data cannot be read, copied, modified, or removed without authorization during processing.	Authorization concept with defined roles and permissions; automated monitoring of data access.

Transmission Control It must be ensured that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or during transport or storage on data carriers, and that it is possible to verify and establish to which entities the transfer of personal data by means of data transmission facilities is intended.	SSL/TLS encryption, firewall, antivirus software, Data Processing Agreements (DPA), password protection for individual documents, VPN tunnels.

Input Control It must be ensured that it is possible to retrospectively verify and establish whether and by whom personal data have been entered into, modified in, or removed from data processing systems.	Internal history tracking and logging of modifications.
Contract Control It must be ensured that personal data processed on behalf of a Controller can only be processed in accordance with the Controller's instructions.	Definition of competencies between Controller and Processor through clear contractual drafting, including the delineation of responsibilities; appointment of a Data Protection Officer.
Availability Control It must be ensured that personal data are protected against accidental destruction or loss.	Daily backup procedures, firewall & antivirus software, disaster recovery plan, Service Level Agreements (SLA) with sub-processors.
Separation Control It must be ensured that data collected for different purposes can be processed separately.	Functional separation between production and testing environments; only test data is used during development.

The technical and organizational measures are reviewed regularly and adapted to the state of the art as necessary, provided that this does not result in a security level lower than the one agreed upon.

Annex 2 – Sub-processing and Third Country Processing

Sections 3 and 8 of the Data Processing Agreement refer to this Annex for the specification of sub-processors. The sub-processors listed below are engaged to provide the contractually owed services. To the extent that the processing of personal data takes place in a third country, this is carried out in compliance with the requirements of Art. 44 et seq. GDPR, in particular on the basis of appropriate safeguards within the meaning of Art. 46 GDPR.

- **Lebenslauf.de GmbH**; Deisterstraße 20, 31785 Hameln, Germany
  - **Service:** Hosting, operation of the software
  - **Data Processing:** European Union
- **Synatix GmbH**; Deisterstraße 20, 31785 Hameln, Germany
  - **Service:** Hosting, operation of the software
  - **Data Processing:** European Union
- **Sendinblue GmbH** (Brevo); Köpenicker Straße 126, 10179 Berlin, Germany
  - **Service:** Dispatch of marketing emails
  - **Data Processing:** European Union
- **METAVISION GmbH**; Untere Bachgasse 15, 93047 Regensburg, Germany
  - **Service:** Hosting and operational tasks
  - **Data Processing:** European Union
- **Supabase, Inc., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513**
  - **Service:** Hosting and operational tasks
  - **Transfer Basis:** Appropriate safeguards pursuant to Art. 46 GDPR (in particular EU Standard Contractual Clauses) and, where applicable, the EU-U.S. Data Privacy Framework
  - **Data Processing:** European Union (Database) / Singapore (Administration & Metadata)
- **Amazon Web Services EMEA SARL**; 38 Avenue John F. Kennedy, L-1855 Luxembourg
  - **Service:** Hosting and operational tasks
  - **Transfer Basis:** Appropriate safeguards pursuant to Art. 46 GDPR (in particular EU Standard Contractual Clauses) and, where applicable, the EU-U.S. Data Privacy Framework
  - **Data Processing:** European Union
- **Vercel Inc.**; 440 N Barranca Ave #4133, Covina, CA 91723, USA
  - **Service:** Hosting and operational tasks
  - **Transfer Basis:** Appropriate safeguards pursuant to Art. 46 GDPR (in particular EU Standard Contractual Clauses) and, where applicable, the EU-U.S. Data Privacy Framework
  - **Data Processing:** USA / European Union (Edge Network)
- **Groq, Inc.**; 2700 Zanker Road, Suite 150, San Jose, CA 95134, USA
  - **Service:** Provision of AI tools
  - **Transfer Basis:** Appropriate safeguards pursuant to Art. 46 GDPR (in particular EU Standard Contractual Clauses) and, where applicable, the EU-U.S. Data Privacy Framework
  - **Data Processing:** USA
- **OpenAI OpCo, LLC.**; 1455 3rd Street, San Francisco, CA 94158, USA
  - **Service:** Provision of AI tools

- **Transfer Basis:** Appropriate safeguards pursuant to Art. 46 GDPR (in particular EU Standard Contractual Clauses) and, where applicable, the EU-U.S. Data Privacy Framework
- **Data Processing:** USA