DATA PROCESSING AGREEMENT

This Data Processing Agreement, including its Schedules, (the "**DPA**") forms a part of the Enterprise Access Agreement or other written or electronic agreement between OpenRouter, Inc. ("**OpenRouter**") and _____ ("**Customer**") for the purchase of the Service (the "**Agreement**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates, if and to the extent OpenRouter processes Personal Data (defined below) for which such Affiliates qualify as the Controller (defined below).

In the course of providing the Service to Customer pursuant to the Agreement, OpenRouter may Process (defined below) Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

1. DEFINITIONS

a. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with, another entity.

b. "**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws, and (b) is permitted to use the Service pursuant to the Agreement.

c. **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, as amended by the California Privacy Rights Act, and their implementing regulations.

d. **"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.

e. "**Data Protection Impact Assessment**" or "**DPIA**" means an assessment of the impact of the Processing operations on the protection of Personal Data, as described in the GDPR.

f. **"Data Protection Laws"** means all applicable laws and regulations of the European Union, the European Economic Area and their member states (the "**EEA**"), Switzerland, the United Kingdom and the United States applicable to the Processing of Personal Data under the Agreement, including the GDPR and CCPA.

g. **"Data Subject"** means the identified or identifiable person to whom Personal Data relates.

h. "**GDPR**" means (a) the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**EU GDPR**") and (b) the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**").

i. "**International Data Transfer**" means any transfer of Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom;

j. **"Personal Data"** means any information relating to an identified or identifiable natural person where such data is Customer Data.

k. **"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

l. **"Processor"** means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

m. "**Public Authority**" means a government agency or law enforcement authority, including judicial authorities.

n. **"Standard Contractual Clauses"** means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by EC Commission Implementing Decision of 4 June 2021, as currently set out at http://data.europa.eu/eli/dec_impl/2021/914/oj.

o. **"Subprocessor"** means any Processor engaged by OpenRouter or an Affiliate of OpenRouter engaged in the Processing of Personal Data.

p. "**UK Addendum**" means the International Data Transfer Addendum to the Standard Contractual Clauses issued by the UK Information Commissioner's Office, in force as of 21 March 2022, available at https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf. ~~https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.~~

2. PROCESSING OF PERSONAL DATA

a. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is a Controller, and OpenRouter is a Processor.

b. Customer's Processing of Personal Data. Customer shall use the Service to Process Personal Data in accordance with the applicable requirements of Data Protection Laws. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer is responsible for reviewing the data handling terms set forth in AI Model Terms and configuring Customer's account accordingly.

c. OpenRouter's Processing of Personal Data. OpenRouter shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Authorized Users in their use of the Service; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

d. Details of the Processing. The subject-matter of Processing of Personal Data by OpenRouter is the performance of the Service pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS. OpenRouter shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". OpenRouter shall not respond to a

Data Subject Request itself, except that Customer authorizes OpenRouter to redirect the Data Subject Request as necessary to allow Customer to respond directly. Taking into account the nature of the Processing, OpenRouter shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Service, does not have the ability to address a Data Subject Request, OpenRouter shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent OpenRouter is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from OpenRouter's provision of such assistance.

4. OPENROUTER PERSONNEL

a. Confidentiality. OpenRouter shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. OpenRouter shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

b. Reliability. OpenRouter shall take commercially reasonable steps to ensure the reliability of any OpenRouter personnel engaged in the Processing of Personal Data.

c. Limitation of Access. OpenRouter shall ensure that OpenRouter's access to Personal Data is limited to those personnel performing the Service in accordance with the Agreement.

5. SUBPROCESSORS

a. Appointment of Subprocessors. Customer acknowledges and agrees that (a) OpenRouter's Affiliates may be retained as Subprocessors; and (b) OpenRouter and OpenRouter's Affiliates respectively may engage third-party Subprocessors in connection with the provision of the Service. Prior to providing any access to Personal Data, OpenRouter or a OpenRouter Affiliate has entered into a written agreement with each Subprocessor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Service provided by such Subprocessor.

b. List of Current Authorized Subprocessors and Notification of New Subprocessors. The current list of authorized Subprocessors that may be engaged in Processing Personal Data, including a description of their authorized processing activities and countries of location, is listed in Schedule 3 (Current List of Authorized Subprocessors). Customer hereby consents to these Subprocessors, their locations and processing activities as it pertains to their Personal Data. Customer can send an email at support@openrouter.ai to subscribe to notifications of new Subprocessors, and if Customer subscribes, excluding processing by AI Model Providers, OpenRouter shall provide thirty (30) days notification of a new Subprocessor(s) before authorizing any new Subprocessor(s) to Process Personal Data in connection with the provision of the applicable Service. Customer may configure in Customer's account settings to exclude Processing by certain AI Model Providers.

c. Objection Right for New Subprocessors. Customer may object to OpenRouter's use of a new Subprocessor by notifying OpenRouter promptly in writing within thirty (30) days of receipt of OpenRouter's notice in accordance with the mechanism set out in section 5(b). If Customer objects to a new Subprocessor as permitted in the preceding sentence, OpenRouter will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially reasonable change to

Customer's configuration or use of the Service to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If OpenRouter is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) with respect only to the aspects of the Service which cannot be provided by OpenRouter without the use of the objected-to new Subprocessor by providing written notice to OpenRouter. OpenRouter will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Service, without imposing a penalty for such termination on Customer.

d. Liability. OpenRouter shall be liable for the acts and omissions of its Subprocessors to the same extent OpenRouter would be liable if performing the services of each Subprocessor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

6. AUDIT. Upon reasonable request and at Customer's sole expense, OpenRouter will make available to Customer all information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by a Public Authority or reasonably requested, no more than once a year by Customer and performed by an independent auditor as agreed upon by Customer and OpenRouter. The foregoing shall only extend to those documents and facilities relevant and material to the Processing of Personal Data, and shall be conducted during normal business hours and in a manner that causes minimal disruption. OpenRouter will inform Customer if OpenRouter believes that Customer's instruction under this Section infringes Data Protection Laws. OpenRouter may suspend the audit or inspection, or withhold requested information until OpenRouter has modified or confirmed the lawfulness of the instructions in writing.

7. DATA SECURITY AND INCIDENT NOTIFICATION. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, OpenRouter will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures listed in Schedule 2. In addition, OpenRouter maintains security incident management policies and procedures and shall notify Customer without undue delay, and in any case, within seventy-two (72) hours after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by OpenRouter or its Subprocessors (a "**Customer Data Incident**"). OpenRouter shall make reasonable efforts to identify the cause of such Customer Data Incident and take such steps as OpenRouter deems necessary and reasonable to remediate the cause of such a Customer Data Incident to the extent the remediation is within OpenRouter's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Authorized Users.

8. GOVERNMENT ACCESS REQUESTS. In its role as a Processor, OpenRouter shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary to safeguard national security, defense and public security. If OpenRouter receives a legally binding request to access Personal Data from a Public Authority, OpenRouter shall, unless otherwise legally prohibited, promptly notify Customer including a summary of the nature of the request. To the extent OpenRouter is prohibited by law from

providing such notification, OpenRouter shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable OpenRouter to communicate as much information as possible, as soon as possible. Further, OpenRouter shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Notwithstanding the above, (a) Customer acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) this DPA shall not require OpenRouter to pursue action or inaction that could result in civil or criminal penalty for OpenRouter such as contempt of court. In the event OpenRouter does not or cannot challenge the request, OpenRouter shall notify Customer, as soon as possible, following the access by the government authority, and provide Customer with relevant details of the same, unless and to the extent legally prohibited to do so.

9. RETURN AND DELETION OF CUSTOMER DATA. OpenRouter shall return or delete Personal Data in accordance with the procedures and timeframes specified in the Agreement. Until Personal Data is deleted or returned, OpenRouter shall continue to comply with this DPA and its Schedules.

10. DATA PROTECTION IMPACT ASSESSMENT. If Customer is required under Data Protection Laws to conduct a Data Protection Impact Assessment, OpenRouter will, upon written request, use commercially reasonable efforts to assist, to the extent Customer does not otherwise have access to the relevant information, including reasonable assistance with any cooperation or prior consultation with supervisory authorities.

11. AUTHORIZED AFFILIATES

a. Contractual Relationship. The parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate agrees to be bound by the Customer's obligations under this DPA, if and to the extent that Customer Processes Personal Data on the behalf of such Authorized Affiliates, thus qualifying them as the "Controller."

b. Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with OpenRouter under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

c. Rights of Authorized Affiliates. Where Customer enters into this DPA on behalf of an Authorized Affiliate, such Authorized Affiliate shall, to the extent required under applicable Data Protection Laws, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

i. Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against OpenRouter directly by itself, the parties agree that (x) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (y) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together.

ii. The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on OpenRouter and its Subprocessors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

12. LIMITATION OF LIABILITY. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement.

13. INTERNATIONAL DATA TRANSFERS

a. Authorization. Customer hereby authorizes OpenRouter to carry out International Data Transfers with respect to Personal Data in accordance with Data Protection Laws.

b. EEA Transfers. To the extent required under Data Protection Laws for the International Data Transfer of Personal Data originating in the EEA from Customer to OpenRouter, by signing this DPA, Customer and OpenRouter hereby enter into Module 2 (Controller to Processor) of the Standard Contractual Clauses, which are hereby incorporated by reference and completed as follows: the "data exporter" is Customer; the "data importer" is OpenRouter; Clause 9(a) option 2 is implemented and the time period therein is specified as thirty 30 days; the optional redress clause in Clause 11(a) is struck; Clause 17 option 1 is implemented and the governing law is the law of Ireland; the court in Clause 18(b) are the Courts of Dublin, Ireland; Annex 1 and 2 of the Standard Contractual Clauses are Schedule 1 and Schedule 2 to this DPA respectively. To the extent that there is any conflict between the terms of this DPA, the Agreement, and the terms of the Standard Contractual Clauses, the terms of the following documents will prevail (in order of precedence): (i) the Standard Contractual Clauses; (ii) this DPA; and (iii) the Agreement.

c. United Kingdom Transfers. The UK Addendum will be applicable to any International Data Transfers originating in the United Kingdom and is completed as follows: for the purpose of table 1 of part 1, the exporter is Customer and the importer is OpenRouter and the table is deemed to be completed with the information set out in Schedule 1. For the purpose of table 2 of part 1, the "Approved EU SCCs" which the UK Addendum is appended to are the Standard Contractual Clauses incorporated into this DPA and completed as set out in the foregoing paragraph. For the purpose of table 3 of part 1, the information requested in Annex 1 and 2 of the Standard Contractual Clauses is provided in Schedule 1 and Schedule 2 to this DPA respectively and the list of Subprocessors is attached as Schedule 3. For the purpose of table 4 of part 1, the importer may end the UK Addendum as set out in section 19 of the UK Addendum.

d. Switzerland Transfers. If there is an International Data Transfer subject to Data Protection Laws of Switzerland, then the Standard Contractual Clauses will apply to such International Data Transfer with the following modifications: the competent supervisory authority in Annex I.C under Clause 13 will be the Federal Data Protection and Information Commissioner; references to a "Member State" and "EU Member State" will not be read to prevent Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland); and references to

"GDPR" in the Standard Contractual Clauses will be understood as references to Data Protection Laws of Switzerland.

e. Change in Data Protection Laws. If OpenRouter's compliance with Data Protection Laws applicable to International Data Transfers is affected by circumstances outside of OpenRouter's control, including circumstances affecting the validity of an applicable legal instrument, OpenRouter and Customer will work together in good faith to reasonably resolve such non-compliance.

14. MISCELLANEOUS. This DPA may only be modified by a written amendment by OpenRouter with notice given to the Customer. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

The parties' authorized signatories have duly executed this DPA:

OPENROUTER, INC.	**CUSTOMER**
Signed:	Signed:
Name:	Name:
Title:	Title:
Date:	Date:

SCHEDULE 1

DETAILS OF PROCESSING

A. LIST OF PARTIES

Name of Data Importer:	OpenRouter, Inc.
Address:	169 Madison Ave #2404, New York NY 10016
Contact person's name, position, and contact details:	[Contact Information]
Activities relevant to the data transferred under these Clauses:	See Schedule 1(B) below and the Agreement.
Signature and date:	This Schedule 1 shall automatically be deemed executed when the DPA is executed by OpenRouter.
Role (controller/processor):	Processor

Name of Data Exporter:	The party identified as the "Customer" in the Agreement.
Address:	Reference is made to the Agreement.
Contact person's name, position, and contact details:	Reference is made to the Agreement.
Activities relevant to the data transferred under these Clauses:	See Schedule 1(B) below and the Agreement.
Signature and date:	This Schedule 1 shall automatically be deemed executed when the DPA is executed by Customer.
Role (controller/processor):	Controller

B. DESCRIPTION OF PROCESSING/ TRANSFER

Categories of Data Subjects whose Personal Data is transferred	Customer's employees and contractors who are Authorized Users.
Categories of Personal Data transferred	Name, contact information, online identifiers (including without limitation, IP address and timestamps), account/user IDs, any information provided by Authorized Users in unstructured data, and other information necessary to provide the Service under the Agreement.
Sensitive data transferred (if applicable) and applied restrictions or safeguards	No sensitive data is processed under the Agreement.
Frequency of Transfer	Continuous for the duration of the Agreement.
Nature and purpose(s) of the data transfer and Processing	OpenRouter will process Personal Data as necessary to provide the Service under the Agreement.
Retention period (or, if not possible to	Personal Data will be retained for as long as

determine, the criterial used to deter- mine the period)	necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Data Protection Laws.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing	OpenRouter will restrict the onward Subprocessor's access to Personal Data only to what is strictly necessary to provide the Service, and OpenRouter will prohibit the Subprocessor from Processing the Personal Data for any other purpose.
Identify the competent supervisory authority/ies in accordance with Clause 13	Where the EU GDPR applies, the competent supervisory authority shall be designated in accordance with Clause 13 of the EU SCCs. Where the UK GDPR applies, the UK Information Commissioner's Office.

SCHEDULE 2
OpenRouter Security Practices

Information Security Team
An internal OpenRouter group is responsible for enforcing the information and operational security policies, including those in this Schedule. This group currently consists of the CTO, Head of Security, engineers and other security personnel. The team may be contacted at support@openrouter.ai.

Security Controls
OpenRouter will implement and maintain appropriate technical and organizational measures designed to protect Customer Data against accidental or unlawful destruction, loss, alteration, and unauthorized disclosure of or access to Customer Data processed or transmitted through the Service. Security controls include the following:

1. SOC 2 Type II control framework.
2. TLS 1.2+ encryption in transit; AES 256 at rest.
3. Google Cloud Platform hosting in US regions; data at rest is region restricted.
4. Cloudflare WAF, rate limiting and DDoS mitigation.
5. Role based access; MFA; least privilege.
6. Centralised logging via Datadog; immutable audit logs.
7. Quarterly vulnerability scans; annual external penetration test (scheduled Q3 2025).
8. Incident response plan in place; breach notifications <72 h.
9. Business continuity with replicated backups; tested restores.
10. Annual security and privacy training; pre employment background checks.

Incident Management
OpenRouter will maintain incident management policies and procedures designed to promptly investigate, identify, and remediate unauthorized disclosure of Customer Data. In the event of any confirmed or reasonably suspected unauthorized disclosure of Customer Data resulting from a breach of OpenRouter's security obligations, OpenRouter will promptly notify Customer. Upon request from a Customer, OpenRouter will communicate the status and post-mortem details of such an incident.

Data Deletion
Customer may request deletion of Customer Data at any time by emailing support@openrouter.ai. OpenRouter deletes Customer Data from the [datastores] and backups within X business days of request and supplies notification of completion via email.

Personnel Practices
All employees with access to technical resources are required to complete security training. When an employee's work relationship with OpenRouter is ending or ends, OpenRouter's operations team revokes access to any proprietary technical systems.

Schedule 3

Current List of Authorized Sub processors

Entity Name	Sub-processing Activities	Corporate Location
Cloudflare Inc.	Edge & CDN	USA
Google Cloud Platform	Hosting & Compute	USA / global
Google Cloud Natural Language API	NLP Categorisation	USA
Vercel Inc.	Hosting (frontend)	USA
ClickHouse Cloud (ClickHouse Inc.)	Database	USA
Supabase Inc.	Database & Auth	USA
Clerk Inc.	Authentication	USA
Stripe Inc.	Payments	USA
Coinbase Commerce	Payments (crypto)	USA
Datadog Inc.	Monitoring & Logs	USA
Customer.io	Messaging	USA
Hex Technologies Inc.	Analytics & Notebooks	USA
AI Model Providers, listed at https://openrouter.ai/docs/features/privacy-and-logging	Large language model providers	Various