

Data Processing Agreement

Version 1.1. Effective: 28 October 2026.

This Data Processing Agreement (“DPA”) is made between **Negbeta Limited**, a company registered in England and Wales (company number 14318349), registered office 71-75 Shelton Street, Covent Garden, London WC2H 9JQ, United Kingdom (“Negbeta”), and the customer that uses the Service under the Agreement (the “Customer”). It forms part of the Agreement, under which Negbeta provides the Customer with access to its inference API (the “Service”). “Agreement” means the written agreement under which the Customer accesses the Service or, if there is none, Negbeta’s Inference API Terms at <https://negbeta.com/inference/terms> as accepted by the Customer’s use of the Service.

A copy of this DPA countersigned by Negbeta is available on request at info@negbeta.com.

1. Definitions

1.1 “Data Protection Laws” means, as applicable: the UK GDPR and the Data Protection Act 2018 (as amended, including by the Data (Use and Access) Act 2025); Regulation (EU) 2016/679 (the “EU GDPR”) and the national laws implementing or supplementing it; and any other data protection law that applies to the processing under this DPA.

1.2 “Controller”, “Processor”, “Data Subject”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” have the meanings given in the UK GDPR or the EU GDPR, as applicable.

1.3 “Customer Personal Data” means Personal Data that Negbeta processes on behalf of the Customer in providing the Service, as described in Annex 1, part A. It does not include Service Data.

1.4 “Subprocessor” means a third party engaged by Negbeta that processes Customer Personal Data.

1.5 “Service Data” means the operational metadata described in Annex 1, part B, which Negbeta generates and keeps to operate, secure and bill the Service.

1.6 “SCCs” means the standard contractual clauses approved by the European Commission in Implementing Decision (EU) 2021/914. “UK Addendum” means the International Data Transfer Addendum to the SCCs, and “IDTA” the International Data Transfer Agreement, each issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018.

2. Roles

2.1 For Customer Personal Data, the Customer is the Controller or a Processor acting for its own customers, and Negbeta is a Processor (where the Customer is a Controller) or a sub-processor (where the Customer is a Processor).

2.2 Where the Customer is a Processor, the Customer warrants that its instructions, including the appointment of Negbeta, are authorised by the relevant Controller, and the Customer remains the sole point of contact for that Controller.

2.3 Negbeta is an independent Controller of Service Data and processes it only for the purposes in Annex 1, part B, as described in its inference privacy policy (<https://negbeta.com/inference/privacy>). Service Data never includes request content. Negbeta does not use Service Data to identify any Data Subject, does not combine it with other data for that purpose, and does not use it for advertising, profiling or training. Negbeta discloses Service Data only to the service providers named in Annex 3 as processing it, or where the law requires.

2.4 The Customer: (a) is responsible for the lawfulness of its instructions, including the lawful basis for the processing and any notice or consent its end users require; (b) warrants that this DPA satisfies its own obligations to any Controller for which it acts, and does not pass on to Negbeta obligations beyond this DPA without Negbeta’s written agreement; (c) sends special categories of Personal Data, Personal Data of children, or data subject to sector rules (for example health or payment data) only where lawful, and accepts that Negbeta cannot see or filter request content; (d) keeps its API keys confidential and is responsible for all requests sent with them; and (e) is Negbeta’s sole counterparty under this DPA: no Controller for which the Customer acts, and no other third party, has rights under

this DPA except as the SCCs require, and the Contracts (Rights of Third Parties) Act 1999 does not apply.

3. Instructions

3.1 Negbeta processes Customer Personal Data only on the Customer's documented instructions, which are: to receive requests through the API, generate the response and return it, and the other processing described in Annex 1, part A. Each API request is an instruction to process its content to produce that response.

3.2 Negbeta informs the Customer without delay if it believes an instruction infringes Data Protection Laws, and may suspend the affected processing until the instruction is confirmed or changed.

3.3 Negbeta does not use Customer Personal Data for any other purpose. In particular, Negbeta does not use request content (prompts, images, completions) to train, fine-tune or evaluate any model, does not sell it and does not share it except with the Subprocessors in Annex 3. Generating Service Data from a request is part of providing the Service.

3.4 Where processing is required by law, Negbeta informs the Customer before processing unless the law prohibits it.

3.5 If a public authority asks Negbeta for Customer Personal Data, Negbeta informs the Customer unless the law prohibits it, limits disclosure to what the law requires, and challenges a request it reasonably considers unlawful. Negbeta holds no request content, so there is normally nothing to disclose.

4. Confidentiality

Negbeta ensures that every person authorised to process Customer Personal Data is bound by confidentiality.

5. Security

5.1 Negbeta implements the technical and organisational measures in Annex 2, appropriate to the risk, taking into account Article 32 of the UK GDPR and EU GDPR.

5.2 Negbeta may update the measures, provided the overall level of protection is not reduced.

6. Personal Data Breaches

6.1 Negbeta notifies the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data, or affecting Service Data relating to the Customer, by email to the security contact the Customer has given Negbeta or, if none, to the Customer's usual contact for the Service (GDPR Art. 33(2)). Negbeta becomes aware of a breach when it has a reasonable degree of certainty that one has occurred; unsuccessful attempts (for example blocked scans or rejected requests) are not breaches.

6.2 The notice describes, as far as then known: the nature of the breach, the categories and approximate numbers of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed. Information not available at first is provided in phases.

6.3 Negbeta takes reasonable steps to contain and remedy the breach and cooperates with the Customer's notifications to Supervisory Authorities and Data Subjects. Notice of a breach is not an admission of fault.

7. Subprocessors

7.1 The Customer gives general authorisation for Negbeta to engage Subprocessors. The Subprocessors at the date of this DPA are listed in Annex 3.

7.2 Negbeta informs the Customer by email of any intended addition or replacement of a Subprocessor before it takes effect, at least 7 days in advance, so that the Customer can object (GDPR Art. 28(2)). Moving processing between locations of an existing Subprocessor is governed by clause 11.1, not by

this clause. The Customer may object on reasonable data protection grounds within that period; if the parties cannot resolve the objection, the Customer may stop using the Service, and Negbeta refunds any prepaid amounts for the unused period.

7.3 Negbeta enters into a written contract with each Subprocessor that imposes data protection obligations materially no less protective of Customer Personal Data than those in this DPA, including appropriate technical and organisational measures. Negbeta remains liable to the Customer for the performance of each Subprocessor's obligations.

8. Data Subject requests and assistance

8.1 Negbeta stores no request content and no names or email addresses of end users, so it normally cannot identify a Data Subject. Negbeta forwards to the Customer any Data Subject request it receives that concerns Customer Personal Data, and does not answer it except on the Customer's instructions. Negbeta answers requests that concern only Service Data itself, and informs the Customer where such a request also concerns the Customer.

8.2 Where a Data Subject request can be matched to Service Data (for example by a request ID returned in the X-Request-Id header), Negbeta helps the Customer respond.

8.3 Taking into account the nature of the processing and the information available to it, Negbeta assists the Customer with its obligations under Articles 32 to 36 of the GDPR (security, breach notification, data protection impact assessments and prior consultations), using the information in this DPA and its Annexes (GDPR Art. 28(3)(f)). Assistance beyond that information, or beyond 8 hours in any 12 months, is charged at Negbeta's reasonable rates, except assistance with a Personal Data Breach caused by Negbeta.

9. Deletion and return

9.1 Request content is not retained after the response is complete, apart from the prompt cache of model state described in Annex 2, which is evicted in the ordinary course and cleared when the server restarts. After termination, Negbeta restarts the affected model servers within 14 days on request, which clears it.

9.2 On termination of the Agreement, Negbeta revokes the Customer's API keys. Service Data is deleted by its retention schedule (Annex 1, part B); Negbeta may keep Service Data for longer only as needed to resolve a billing dispute, defend a legal claim or investigate abuse.

9.3 There is no Customer Personal Data to return, as none is stored.

9.4 On request, Negbeta confirms in writing that it holds no Customer Personal Data.

10. Audits

10.1 Negbeta makes available the information needed to demonstrate compliance with this DPA: this DPA and its Annexes, its published privacy and data policies, written answers to a reasonable security questionnaire (at most one full questionnaire in any 12 months, plus updates after a Personal Data Breach or a material change), and further information a Supervisory Authority requires.

10.2 Where that is not sufficient, or a Supervisory Authority requires it, the Customer (or an independent auditor bound by confidentiality and not a competitor of Negbeta) may audit Negbeta's compliance with this DPA on at least 30 days' written notice, at the Customer's cost, at most once in any 12 months unless there has been a Personal Data Breach, there are indications of non-compliance, or a Supervisory Authority requires it (GDPR Art. 28(3)(h); SCCs clause 8.9). Audits are conducted remotely, by review of documents and configuration and by interview or screen-sharing session with Negbeta; they do not include physical access to Subprocessors' data centres, for which the Subprocessors' own certifications and reports apply. Negbeta provides up to 8 hours of assistance per audit at no charge and may charge its reasonable rates beyond that. Audit findings are confidential, and the Customer shares them with Negbeta.

11. International transfers

11.1 Location. Negbeta's API gateway and its Service Data database run in the European Union, on Nebius servers. Inference takes place in the European Union and, for some models, in the United States, on the Subprocessors' servers listed in Annex 3; where the Customer asks for UK capacity, inference for the Customer takes place in the United Kingdom.

- a. EU commitment: where the Customer has asked in writing for EU-only processing (including by email at onboarding), Negbeta processes the Customer's request content and Service Data only on servers located in the EEA, unless the Customer agrees otherwise in writing. Those servers may be rented from Subprocessors established outside the EEA (today Runpod, Inc. and Vast.ai, Inc.), which can access them remotely; that access is covered by the transfer mechanisms in clause 11.5. Where the Customer also asks in writing for Subprocessors established in the EEA only, Negbeta serves the Customer only from Nebius servers in the EEA, and the Customer accepts that fewer models or less capacity may then be available. The Customer must not describe the Service to its users as hosted in the EEA or the UK (for example with an EU label, badge or region for Negbeta's endpoint) unless it has asked Negbeta in writing for processing there under this clause.
- b. Otherwise, the Customer authorises Negbeta to process Customer Personal Data in the EEA, the United Kingdom and the United States, on the servers of the Subprocessors in Annex 3, and to move processing between those locations without notice. Negbeta informs the Customer by email at least 7 days (as in clause 7.2) before processing Customer Personal Data in any other country, and lists every location in use on its subprocessor list (Annex 3 as updated, published in section 6 of <https://negbeta.com/inference/privacy>).
- c. A location outside the EEA and the UK (today, the United States) is used only with a transfer mechanism under this clause 11, and this clause is the Customer's documented instruction for such transfers (GDPR Art. 28(3)(a)).

11.2 EU to UK. Negbeta is established in the United Kingdom and operates the Service from there (remote administrative access). Transfers from the EEA to Negbeta in the United Kingdom rely on the European Commission's adequacy decision for the United Kingdom, as in force from time to time. If that decision ceases to apply, the parties' transfers are governed by the SCCs, Module 2 (controller to processor) or Module 3 (processor to processor) as applicable, which are then incorporated by reference with: clause 7 (docking) included; clause 9 option 2 (general authorisation, with the notice period in clause 7.2 of this DPA); clause 11 optional language omitted; clause 17 option 1, the law of Ireland; clause 18, the courts of Ireland; Annexes as in this DPA.

11.3 UK to EEA. Transfers from the UK to the EEA rely on the UK's adequacy regulations for the EEA.

11.4 Customers in other countries. Where the Customer is outside the UK and EEA, the Customer is responsible for the lawfulness of its transfer of Customer Personal Data to Negbeta. For the return of responses and any other Customer Personal Data by Negbeta to a Customer in a country without a UK adequacy decision, to the extent Chapter V of the UK GDPR or EU GDPR applies to that return, the parties agree the SCCs, Module 4 (processor to controller), as amended by the UK Addendum (clause 11.7) where the UK GDPR applies, incorporated by reference with clause 17 the law of Ireland, clause 18 the courts of Ireland and the Annexes to this DPA.

11.5 Subprocessors in the United States. Runpod, Inc. and Vast.ai, Inc. (Annex 3) are established in the United States and run GPU servers for some models in the European Union and the United States. Negbeta sends them Customer Personal Data (request content, held in server memory while a request runs) only under the UK Addendum to the SCCs (or the IDTA) and, where Negbeta's processing is subject to the EU GDPR, the SCCs, in each case in the module incorporated in the Subprocessor's data processing agreement with Negbeta: for Vast.ai, the data processing agreement that forms part of its Terms of Service (<https://vast.ai/data-processing-agreement>); for RunPod, its data processing agreement (<https://www.runpod.io/legal/data-processing-agreement>), signed by Negbeta. Where a Subprocessor is certified under the EU-US Data Privacy Framework and its UK Extension, that certification is an additional basis. Negbeta sends no Customer Personal Data to a Subprocessor before its data processing agreement is in force.

These mechanisms apply whether the server is in the EU or the US, because both companies can access their servers from the United States. In selecting these Subprocessors, Negbeta took into account that request content is held only in server memory for the duration of the request (and in the prompt cache, Annex 2) and travels only over encrypted connections.

11.6 Other Subprocessors. Cloudflare's network may carry requests through locations outside the EEA and UK in transit (Annex 3). Cloudflare, Inc. is established in the United States and certified under the EU-US Data Privacy Framework and its UK Extension; its customer data processing addendum also incorporates the SCCs and the UK Addendum (clause 6, <https://www.cloudflare.com/cloudflare-customer-dpa/>).

11.7 UK Addendum. Where this DPA incorporates the UK Addendum, it is version B1.0 issued under section 119A of the Data Protection Act 2018 (or any version that replaces it), with: Table 1, the parties' details in this DPA; Table 2, the SCCs with the modules and options set out in this clause 11; Table 3, the Annexes of this DPA; Table 4, neither party may end it when the approved Addendum changes. As its Part 2 provides (Sections 12(c) and 15(m) and (n)), it is governed by the laws of England and Wales and disputes go to the courts of England and Wales.

12. Liability and order of precedence

12.1 Nothing in this DPA limits liability that cannot be limited by law, or either party's liability to Data Subjects under Article 82 of the UK GDPR or EU GDPR. Subject to that, as between the parties and regardless of any higher limit in the Agreement, each party's total aggregate liability arising out of or in connection with this DPA (including under the SCCs, whether in contract, tort, breach of statutory duty or otherwise) is limited to the greater of (a) the fees paid by the Customer under the Agreement in the 12 months before the event giving rise to the claim and (b) GBP 100; and neither party is liable for indirect or consequential loss, or loss of profit, revenue or business. A party that pays compensation to a Data Subject for damage caused by the other party may recover from that party the part of the compensation corresponding to its responsibility, subject to this clause.

12.2 If this DPA conflicts with the Agreement on data protection, this DPA prevails. If the SCCs apply and conflict with this DPA, the SCCs prevail. Annexes 2 and 3 may be updated as clauses 5.2, 7.2 and 11.1(b) allow; otherwise this DPA is amended only in writing.

13. Term and law

13.1 This DPA lasts as long as Negbeta processes Customer Personal Data.

13.2 This DPA is governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction, except (a) where the Agreement is governed by the law of an EEA member state or another part of the United Kingdom, that law and its courts apply, and (b) where the SCCs or the UK Addendum require otherwise.

13.3 The Customer accepts this DPA by using the Service under the Agreement; no signature is needed.

13.4 Clauses 9, 12 and 13 survive termination.

14. US state privacy laws

To the extent Customer Personal Data is subject to the California Consumer Privacy Act (as amended) or a similar US state privacy law, Negbeta acts as a "service provider", "contractor" or "processor" under that law. Negbeta (a) processes Customer Personal Data only for the business purpose of providing the Service as described in Annex 1 and for no commercial purpose of its own; (b) does not sell or share it, retain, use or disclose it outside the direct business relationship with the Customer, or combine it with personal information from any other source, except as the law permits a service provider; (c) complies with the obligations that law places on service providers and provides the same level of privacy protection as it requires; (d) notifies the Customer if it can no longer meet those obligations; (e) allows the Customer to take reasonable and appropriate steps under clause 10 to ensure that Negbeta uses the data consistently with the Customer's obligations, and to stop and

remediate unauthorised use; and (f) certifies that it understands these restrictions. Terms used in this clause have the meanings given in the applicable law.

Annex 1: Description of the processing

A. Customer Personal Data (Negbeta as Processor or sub-processor)

Item	Description
Subject matter and purpose	Generating model responses (text, reasoning, tool calls) to API requests sent by the Customer
Nature	Receiving, holding in memory, passing to a model server over an encrypted private network, processing by a large language model, returning the output; prompt caching of model state to speed up continuing conversations (Annex 2); conversation fingerprints in the gateway's memory (one-way hashes of the beginnings of recent conversations, not text, dropped 5 minutes after a conversation goes idle and when the gateway restarts)
Duration	For each request, until the response is complete; model state in the prompt cache until evicted (no fixed time) or the server restarts
Categories of Data Subjects	The Customer's end users, and any person mentioned in request content
Categories of Personal Data	Whatever the Customer's end users put in prompts, system prompts, images, tool definitions and tool results, and the model's output derived from them
Special categories	Not intended; see clause 2.4(c)
Retention	Not stored
Location	Gateway: the European Union (Nebius). Inference: the European Union (Nebius; RunPod and Vast.ai servers in the EU) and, for some models, the United States (RunPod and Vast.ai); United Kingdom only on the Customer's request. Servers in the EEA only for EU-labelled or EU-only Customers (clause 11.1(a))

For the SCCs and the UK Addendum: the parties are as in the opening paragraph, with the Customer's details as given in the Agreement or to Negbeta, Negbeta's contact info@negbeta.com, and the Customer's acceptance under clause 13.3 in place of signature and date (Annex I.A); part A of this Annex is Annex I.B (frequency of transfer: continuous, with each API request); the competent supervisory authority is the one determined by clause 13 of the SCCs (Annex I.C); Annex 2 is Annex II; Annex 3 is Annex III.

B. Service Data (Negbeta as Controller, clause 2.3; listed for transparency)

Per request: identifiers (our request ID, the caller's request ID if sent, the model server's response ID), a SHA-256 prefix of the API key, timings, token counts (input, cached input, output, reasoning), sampling settings, counts of messages per role, tools, stop sequences and images, image sizes, tool-call validity counts, a sanitised error message (at most 300 characters, quoted text removed), a one-way routing hash, the connecting client's IP address, country, user agent and Cloudflare ray ID. The connecting client is normally the Customer's servers. Purposes: billing and reconciliation with the Customer, running and monitoring the Service, measuring quality, and investigating abuse and security incidents. Stored in the European Union (Nebius), where Negbeta's own monitoring dashboards and alerts also run, on the same server. Retention: 180 days; raw IP and user agent 30 days. Full field list: <https://negbeta.com/inference/data-policy>.

Annex 2: Technical and organisational measures

How the Service is built: Cloudflare's network edge passes requests through an encrypted tunnel to Negbeta's gateway on a CPU server in the European Union, which also holds the Service Data database; the gateway sends each request over a private encrypted network to a GPU server that runs the model, and returns the response the same way.

Area	Measure
Zero data retention of content	Prompts, system prompts, images, tool definitions, tool results and completions exist only in server memory (on the gateway and the GPU server) while the request runs. They are never written to the database or any log, and never used for training
Prompt cache	To speed up continuing conversations, the GPU server keeps the model's internal representation of recent prompt beginnings (not text) in temporary storage on the same server: today its GPU memory and, on some servers, its main memory, never its disk. If Negbeta adds an encrypted local-disk tier on the same server, it gives notice under clause 5.2, and the cache stays under the same rules. It is reused only for a request that starts with exactly the same content, evicted as new requests arrive and cleared when the server restarts. Images: at most 512 MB of model encodings in memory, same rules. The cache on a server is shared across customers; a cache hit returns no content and is possible only for a request that already contains the identical beginning
Data minimisation	Request parameters are stored as an allowlist of numbers and counts; stop sequences, tool names and arguments only as counts or hashes; error messages sanitised before storage; model-server rejections stored as type, length and keyed hash only
Log redaction	No log line on the gateway or model servers contains request content. Tested by sending marker text in every request field, including malformed requests, and searching every log, the database and the servers' files
Log retention	Service logs (start-up and error events with request IDs, no content) are deleted after 14 days on every server Negbeta administers
Service Data retention	Automatic deletion by database time-to-live: 180 days, 30 days for raw IP and user agent and for non-inference request records; if the database was stopped, expired rows are deleted within a day of restart
Encryption in transit	TLS from the client to Cloudflare; Cloudflare Tunnel (encrypted, outbound-only from our server) from Cloudflare to the gateway; WireGuard (end-to-end encrypted) from the gateway to the GPU servers and from the operator's devices to the monitoring dashboards
Private networking and exposure	Only SSH (key-only, password login off) is open inbound on the gateway server; the API, admin API, database and monitoring dashboards listen only on its loopback interface (the dashboards are published only on the private network); only the public API hostname is routed through the tunnel, and admin paths are not reachable publicly. Model servers are not reachable from the internet: they listen only on the private network, network access rules allow only the gateway to reach the model port, and each model server requires its own key
Encryption at rest	The gateway server's and Nebius GPU servers' disks are encrypted at rest by Nebius (AES-256, keys managed by Nebius). The Service Data database has no additional application-level encryption; it holds no request content
Authentication	Bearer API key per Customer (64 random characters after a fixed prefix), stored only on the gateway server and Negbeta's administrative workstation with owner-only file permissions, never logged (only a SHA-256 prefix); revocable in about 1 second
Access control	Only Negbeta's authorised operators, with SSH keys only; database users with passwords, and a read-only role with query limits for monitoring
Rented GPU servers	GPU servers rented from GPU cloud and marketplace providers (Runpod, Inc.; Vast.ai, Inc.), in the EU and the US. They hold request content in memory only, and no Service Data database and no Customer API keys. The provider, and on a marketplace the host that operates the server, have physical and administrative access to it. Used under the providers' data processing agreements and the SCCs (clause 11.5)
Isolation	Separate API keys and traffic labels per Customer; no Customer can read another's data (the API has no read endpoints for stored data)
Availability and resilience	Immediate 429 with Retry-After at capacity instead of queueing; drain before restart (no dropped requests); zero-downtime gateway restarts; automatic health checks take a failing model server out of rotation; servers rebuilt from version-controlled configuration

Area	Measure
Patching	Security-only unattended upgrades; pinned container images and model weights
Monitoring	Per-request metrics and dashboards, self-hosted on the gateway server (read-only database user with query limits; no third-party monitoring service); alert rules emailed to the operator; health checks on every model server; an external availability probe every 2 minutes
Testing	Conformance and correctness test suites before each release
Incident response	A written incident procedure covering detection, triage, containment, notice to the Customer under clause 6, notice to the Supervisory Authority where Negbeta is Controller, and a record of every breach; available on request. Contact: info@negbeta.com

Annex 3: Subprocessors

Name	Purpose	Data	Location	Transfer mechanism
Nebius B.V., Burgerweeshuispad 101, 1076 ER Amsterdam, the Netherlands	Compute: the CPU server that runs the gateway, the Service Data database and the tunnel endpoint; GPU servers; disks	Request content in memory while it passes through the gateway or runs on a Nebius GPU server; Service Data on disk	European Union. United Kingdom only on request	None needed (EEA). UK to EEA: UK adequacy regulations. Nebius data processing agreement: https://docs.nebius.com/legal/dpa
Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA	Network edge: TLS, encrypted tunnel to the gateway, DNS; answers model-list requests itself	Request content in transit only, not stored; records of requests to the model list and home page (not Customer Personal Data; see the data policy)	Global network; a request enters at the Cloudflare location nearest the client	EU-US Data Privacy Framework and UK Extension; SCCs and UK Addendum in Cloudflare's data processing addendum (clause 11.6)
Runpod, Inc., 1351 Fairview Blvd, Ste A 1134, Delran, NJ 08075, USA	GPU cloud provider: GPU compute for some models	Request content in GPU and host memory only, while a request runs, plus the prompt cache; never stored; no Service Data	European Union and United States	UK Addendum and SCCs in RunPod's data processing agreement (clause 11.5)
Vast.ai, Inc., 6600 Sunset Blvd, Ste 256, Los Angeles, CA 90028, USA	GPU marketplace: GPU compute for some models; each server is operated by an independent host engaged through Vast.ai, which also has physical and administrative access to it	As RunPod	European Union and United States	UK Addendum and SCCs in the data processing agreement that forms part of Vast.ai's Terms of Service (clause 11.5)

Not Subprocessors (no access to Customer Personal Data): internet carriers, and the encrypted private-network service between Negbeta's servers (Tailscale Inc.; traffic end-to-end encrypted with WireGuard, Tailnet Lock being enabled on 28 October 2026), transmit only data they cannot read. Zoho carries business email with the Customer's staff (Negbeta is Controller of those contact details; no API traffic). Model hubs, container registries and package mirrors supply software only. Details on request.