Article 28 (3) General Data Protection Regulation (GDPR)
Controller-Processor Agreement
(Data Processing Agreement – Version 1.4)

Between

The Customer
The legal entity or individual that has accepted Infercom's Terms of Service at infercom.ai/termsconditions

- Controller -

and

Infercom SCS
Société en Commandite Simple incorporated under the laws of the Grand Duchy of Luxembourg
Registered address: 29 Boulevard Grande-Duchesse Charlotte, 1331 Luxembourg
RCS Luxembourg B298727

- Processor -

Preamble

(1) The Processor will process personal data on behalf of the Controller within the meaning of Article 4(8) and Article 28 of Regulation (EU) 2016/679 (GDPR). This Agreement governs the rights and obligations of the parties in connection with the processing of personal data.

(2) Insofar as the term "data processing" or "processing" (of data) is used in this Agreement, it has the meaning defined in Article 4(2) GDPR. The processing of personal data includes in particular the collection, storage, transmission, restriction, deletion as well as the anonymisation, pseudonymisation, encryption or other use of data.

(3) This Agreement supplements the service agreement between the parties (the "Service Agreement"; currently the terms available at https://www.infercom.ai/termsconditions). In the event of a conflict between this Agreement and the Service Agreement, this Agreement prevails with regard to the processing of personal data.

1. Subject matter and duration of the Agreement

(1) Subject matter

The Processor provides a high-performance "Inference-as-a-Service" platform on dedicated AI accelerator hardware hosted in the European Union (the "Service"). The Service allows the Controller to run open-source Artificial Intelligence models (e.g., gpt-oss-120b, DeepSeek) via an API for the purpose of generating text, code or other outputs based on Controller-provided inputs ("Prompts").

The Service is architected for European data sovereignty. Inference processing of Prompts and outputs takes place exclusively within the European Union. Any remote administration, support or other access from outside the EU/EEA is subject to Section 7a and the applicable transfer safeguards.

Models whose inference is not hosted within the EU/EEA ("Non-EU Models") are not covered by this Agreement. Their use requires a separate written addendum that sets out the sub-processors involved, the transfer mechanism under Chapter V GDPR and the associated safeguards.

(2) Duration

The duration of this Agreement corresponds to the duration of the Service Agreement. It ends automatically upon termination of the Service Agreement, without prejudice to obligations that by their nature continue to apply (in particular Sections 9, 11 and 15).

2. Concrete specification of the Agreement

(1) Nature and purpose of the processing

The nature and purpose of the processing of personal data by the Processor for the Controller are described in the Service Agreement. In more detail, the purpose of the Processor's tasks is to enable the Controller to use Large Language Models (LLMs) and AI acceleration hardware for its applications, products or internal workflows without managing physical infrastructure. Nature of the processing:

- **Transient inference:** processing is limited to the real-time ingestion of Prompts and inputs for the sole purpose of generating model outputs (inference).
- **No training:** the Processor does not use Prompts, inputs or outputs to train, retrain, fine-tune or otherwise improve models, and does not permit its sub-processors to do so.
- **No storage of content:** the Service is designed as a stateless inference engine. Prompts, inputs and outputs are processed in memory and are not written to persistent storage by the Processor after the response has been delivered. Personnel of the Processor do not have access to the content of Prompts or outputs in the ordinary course of operating the Service.
- **Place of processing:** inference processing of Prompts and outputs takes place exclusively in a Member State of the European Union or in another contracting state of the Agreement on the European Economic Area. The Processor does not route inference requests to infrastructure outside the EU/EEA, including for fallback, overflow or load-balancing purposes.
- **Remote access:** remote administration, monitoring and support of the platform by a sub-processor may take place from a third country, limited to account identifiers and technical metadata and only under the transfer safeguards set out in Section 7a. Any other transfer to a third country requires the prior consent of the Controller and may only take place if the conditions of Article 44 et seq. GDPR are met.

(2) Categories of data

The processing of personal data comprises the following categories of data:

a) **Content data:** personal data of any kind contained in Prompts, inputs, files and model outputs submitted to or generated through the Service. The categories are determined by the Controller's use case and may include special categories of personal data (Article 9 GDPR) where the Controller submits such data.

b) **Account and authentication data** of the Controller's users: name, business e-mail address, user and organisation identifiers, API keys and tokens, login timestamps, IP addresses and device/browser information.

c) **API request metadata and usage data:** timestamps, model used, token counts, request identifiers, response codes, latency and other technical log data.

d) **Communication and support data:** support requests, correspondence and the contact details of the persons involved, including descriptions of technical issues that may contain personal data.

e) **Contract and billing data:** contract details, subscription plan, usage-based billing records and payment references.

(3) Categories of data subjects

a) Employees, contractors and other users of the Controller who use the Service or administer the Controller's account.

b) Customers, end users and other natural persons whose personal data the Controller processes through the Service, in particular persons referred to in Prompts, uploaded content or outputs.

c) Contact persons of the Controller for contractual, billing and support matters.

2a. Obligations of the Controller

(1) The Controller is responsible for ensuring that the processing of personal data through the Service is lawful. This includes ensuring a valid legal basis under Article 6 GDPR – and, where applicable, Article 9 GDPR – for any personal data submitted to the Service.

(2) The Controller shall ensure that any personal data included in Prompts or other inputs to the Service is processed lawfully and that data subjects have been informed in accordance with Articles 13 and 14 GDPR.

(3) The Controller determines whether and which personal data is submitted to the Service. Where the Controller submits special categories of personal data (Article 9 GDPR), the Controller shall ensure that this is permissible and shall inform the Processor where specific additional safeguards are required.

(4) The Controller shall use the Service only with EU-hosted models as designated in the Processor's service documentation, unless a separate addendum pursuant to Section 1(1) has been concluded for Non-EU Models.

(5) The Controller is solely responsible for compliance with Regulation (EU) 2024/1689 (AI Act) in its capacity as deployer of AI systems operated through the Service.

3. Technical and organisational measures

(1) The Processor has documented the technical and organisational measures implemented before the start of the processing in Annex 1 and has made them available to the Controller for examination. The documented measures form the basis of this Agreement. Insofar as an audit by the Controller reveals a need for changes, these shall be implemented by mutual agreement.

(2) The Processor shall ensure the security of processing in accordance with Article 28(3)(c) and Article 32 GDPR, in particular in connection with Article 5(1) and (2) GDPR. Overall, the measures to be taken are data security measures that ensure a level of protection appropriate to the risk in terms of the confidentiality, integrity, availability and resilience of the systems. The state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32(1) GDPR, shall be taken into account.

(3) The technical and organisational measures are subject to technical progress and further development. The Processor may implement alternative adequate measures, provided that the level of security of the agreed measures is not lowered. Significant changes shall be documented and communicated to the Controller.

4. Rectification, restriction and erasure of data

(1) The Controller is solely responsible for safeguarding the rights of data subjects.

(2) The Processor may not rectify, erase or restrict the processing of data processed on behalf of the Controller on its own initiative, but only in accordance with documented instructions from the Controller. Insofar as a data subject contacts the Processor directly in this regard, the Processor shall forward the request to the Controller without undue delay.

(3) Insofar as included in the scope of services, the Processor shall directly implement the deletion concept, the right to be forgotten, rectification, data portability and access in accordance with the documented instructions of the Controller. Owing to the transient processing of content data (Section 2(1)), such requests will as a rule relate to account, usage and support data only.

5. Quality assurance and other obligations of the Processor

(1) In addition to complying with the provisions of this Agreement, the Processor has statutory obligations under Articles 28 to 33 GDPR. In particular, it ensures compliance with the following requirements:

a) **Data protection officer.** The Processor has appointed an external data protection officer who performs his duties in accordance with Articles 38 and 39 GDPR: Mr Nick Neffgen, DEUDAT GmbH, Wiesbaden (Germany), nick.neffgen@deudat.de. The data protection officer performs an independent advisory and monitoring function; he is not the recipient of instructions under Section 10. A change of data protection officer shall be notified to the Controller without undue delay.

b) **Confidentiality** in accordance with Article 28(3)(b), Article 29 and Article 32(4) GDPR. The Processor shall only use employees and contractors who have been committed to confidentiality in text form and who have been familiarised beforehand with the data protection provisions relevant to them. The Processor and every person acting under its authority who has access to personal data may only process such data in accordance with the instructions of the Controller, including the powers granted in this Agreement, unless they are legally obliged to process it otherwise. The confidentiality commitments shall be evidenced to the Controller upon request.

c) The implementation of and compliance with all technical and organisational measures required for this Agreement in accordance with Article 28(3)(c) and Article 32 GDPR (Annex 1).

d) Upon request, the Controller and the Processor shall cooperate with the supervisory authority in the performance of its tasks.

e) The Processor shall inform the Controller without undue delay of control actions and measures of the supervisory authority insofar as they relate to this Agreement. This also applies if a competent authority investigates the processing of personal data at the Processor in the context of administrative-offence or criminal proceedings.

f) If the Controller is subject to an inspection by the supervisory authority, administrative-offence or criminal proceedings, a liability claim of a data subject or a third party, or any other claim in connection with the processing by the Processor, the Processor shall support the Controller to the best of its ability.

g) The Processor regularly reviews its internal processes and the technical and organisational measures to ensure that the processing within its area of responsibility is carried out in accordance with applicable data protection law and that the rights of data subjects are protected.

h) The Processor shall demonstrate the technical and organisational measures taken to the Controller within the scope of the Controller's control rights under Section 8.

(2) The Processor shall support the Controller in fulfilling its duty to respond to requests from data subjects under Articles 12 to 23 GDPR. In particular, the Processor shall ensure that the information required for this purpose is provided to the Controller without undue delay so that the Controller can meet its obligations under Article 12(3) GDPR.

6. Remote work ("home office")

(1) The Processor operates as a remote-first organisation. Employees and contractors of the Processor who are entrusted with the processing of personal data for the Controller may process such data outside the Processor's business premises (remote work, including private households), provided that the requirements of this Section are met. Separate prior consent of the Controller is not required; the Controller may at any time request information on the remote-work arrangements.

(2) The Processor shall ensure that the contractually agreed technical and organisational measures (Annex 1) are also complied with in remote work. In particular, the Processor shall ensure that

a) only company-managed devices with full-disk encryption, automatic screen lock and current security updates are used;

b) access to systems processing personal data of the Controller requires multi-factor authentication and takes place via encrypted connections;

c) personal data of the Controller is not stored on local devices or private IT systems; where local storage is technically unavoidable, it is encrypted and deleted without undue delay;

d) private devices, private accounts and private cloud or messaging services are not used for processing personal data of the Controller; and

e) other persons in the household or surroundings cannot access personal data of the Controller (clear-desk and clear-screen rules, privacy during video and telephone calls).

Deviations from individual agreed technical and organisational measures shall be coordinated with the Controller in advance and approved in text form.

(3) The Processor shall ensure that effective control of the processing of personal data in remote work by the Controller (Section 8) remains possible. The personal rights of the employees and of other persons living in the respective household shall be adequately taken into account.

(4) As content data is processed transiently and not stored (Section 2(1)), remote work concerns account, usage, support and administrative data only.

(5) If employees of sub-processors work remotely, paragraphs 1 to 4 apply accordingly.

7. Engagement of sub-processors

(1) Sub-processing relationships within the meaning of this provision are those services that relate directly to the provision of the main service. This does not include ancillary services such as telecommunication services, postal or transport services, maintenance and user support or the disposal of data media, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems used by the Processor. However, the Processor is obliged to ensure data protection and data security of the Controller's data even in the case of outsourced ancillary services, by way of appropriate and legally compliant contractual agreements and control measures. The exclusion of ancillary services applies only insofar as the relevant provider does not process the Controller's personal data on behalf of the Processor. Where it does, the requirements applicable to sub-processors shall apply.

(2) The Processor may only commission sub-processors (other processors) with the prior express written or documented consent of the Controller. The Controller agrees to the commissioning of the following sub-processors under the condition of a contractual agreement in accordance with Article 28(2) to (4) GDPR:

Sub-processor	Address / country	Service and data concerned	Transfer safeguard
SambaNova Systems, Inc.	2460 North First Street, Suite 100, San Jose, CA 95131, United States	Managed operation and remote administration of the EU-hosted AI inference platform (SambaManaged); access to account identifiers (e-mail addresses) and API request metadata (timestamps, token usage) for operational monitoring, incident response and support escalation. Inference processing itself takes place on dedicated hardware in the EU (Munich, Germany); Prompts and outputs are not transferred to the United States.	Standard Contractual Clauses, Module Three (Section 7a)
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, D04 E5W5, Ireland	Internal business e-mail, calendar, document storage and collaboration (Gmail, Google Drive, Google Calendar); personal data may include customer-related correspondence handled by Infercom personnel.	– (EU)

Sub-processor	Address / country	Service and data concerned	Transfer safeguard
Pipedrive OÜ	Mustamäe tee 3a, 10615 Tallinn, Estonia	Customer relationship management (CRM); storage of contact data, deal information and customer-related communications for sales and account management.	– (EU)
Stripe Payments Europe Limited	1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Ireland	Payment processing and billing; processing of payment card data and transaction records for platform subscription and usage-based billing.	– (EU)
TECLIB SAS	231 Rue Saint-Honoré, 75001 Paris, France	GLPI IT support ticketing: storage and management of support requests, which may include contact data and descriptions of technical issues submitted by or on behalf of the Controller's users.	– (EU)

The addition or replacement of sub-processors is permitted to the extent that:

- the Processor notifies the Controller of the intended change in writing or in text form (e.g., by e-mail to the Controller's designated contact and via the sub-processor list published at infercom.ai/dpa) at least 14 days before the change takes effect, providing the information necessary to assess the change;
- **the Controller does not object to the intended change on reasonable data-protection grounds in writing or in text form within 14 days of receipt of the notification (if no objection is raised within this period, the change is deemed approved);** and
- a contractual agreement in accordance with Article 28(2) to (4) GDPR is in place with the sub-processor.

(3) The transfer of personal data of the Controller to a sub-processor and the sub-processor's first activity are only permitted once all requirements for sub-processing are met.

(4) The Processor shall ensure that the provisions agreed in this Agreement and any additional instructions of the Controller also apply to the sub-processor, and that the sub-processor complies with them.

(5) If the sub-processor provides the agreed service outside the EU/EEA, or accesses personal data from outside the EU/EEA, the Processor shall ensure admissibility under data protection law by taking appropriate measures in accordance with Section 7a. The same applies if service providers within the meaning of paragraph 1 sentence 2 are used.

(6) Further outsourcing by a sub-processor requires the prior information and consent of the Controller (at least in text form); all contractual obligations in the processing chain shall also be imposed on the further sub-processor. The further sub-processors engaged by SambaNova Systems, Inc. as at the date of this Agreement are listed in Annex III of the sub-processing agreement between the Processor and SambaNova Systems, Inc. and are made available to the Controller upon request; the Controller's consent under paragraph 2 extends to them.

(7) The Processor shall carry out regular checks on its sub-processors. These checks shall be documented and made available to the Controller upon request.

7a. International data transfers

(1) Inference processing of Prompts and outputs takes place exclusively within the EU/EEA (Section 2(1)). The Processor shall not route inference requests to infrastructure outside the EU/EEA, including for fallback, overflow or load-balancing purposes.

(2) The Processor shall ensure that any transfer of personal data to a third country – including remote access to personal data from a third country – is carried out in compliance with Chapter V GDPR (Articles 44 to 49).

(3) For the remote administration and support access of SambaNova Systems, Inc. (United States) to account identifiers and technical metadata, the Processor relies on the Standard Contractual Clauses pursuant to Commission Implementing Decision (EU) 2021/914, Module Three (transfer processor to processor), concluded between the Processor and SambaNova Systems, Inc. Where a sub-processor is certified under the EU-U.S. Data Privacy Framework, the Processor may rely on that certification in addition.

(4) The Processor conducts and maintains a Transfer Impact Assessment for transfers to third countries and makes it available to the Controller upon request.

(5) Supplementary measures for the SambaNova sub-processing relationship include: no transfer of content data (Prompts and outputs are processed in the EU and not persistently stored); limitation of remote access to account identifiers and technical metadata; encryption in transit and at rest; strict role-based access controls and multi-factor authentication for remote operations; logging of all remote access; and contractual obligations of the sub-processor to review and challenge disclosure requests by third-country public authorities and to inform the Processor (Clauses 14 and 15 of the Standard Contractual Clauses).

(6) Upon request, the Processor shall provide the Controller with a list of the countries from which personal data may be accessed and a description of the applicable access rules and safeguards.

8. Controller's control rights

(1) The Controller has the right to carry out inspections in consultation with the Processor or to have them carried out by inspectors to be named in the individual case. Inspections shall generally be announced 14 days in advance, unless an unannounced inspection is necessary to avoid compromising the purpose of the inspection. Inspections shall be carried out during normal business hours, without unreasonable disruption of the Processor's operations and subject to appropriate confidentiality obligations.

(2) The Processor shall ensure that the Controller can satisfy itself of the Processor's compliance with its obligations under Article 28 GDPR. The Processor undertakes to provide the Controller with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

(3) Evidence of measures that do not relate solely to the specific processing may be provided by current certificates, reports or report extracts from independent bodies (e.g., auditors, data protection officer, IT security department, data protection or quality auditors) or by suitable certifications (e.g., ISO/IEC 27001).

(4) In particular, the Processor shall ensure by contractual arrangements that the control rights of the Controller and of the supervisory authorities also apply to the sub-processors. It shall also be contractually stipulated that the sub-processor shall tolerate these control measures and any on-site inspections announced at least 14 days in advance.

(5) The Controller has the right to verify the complete and contractual return and deletion of data by the Processor in accordance with Section 11. This may also be done by inspecting the data processing systems at the Processor's premises. Such an on-site inspection shall be announced by the Controller within a reasonable period.

9. Notification of personal data breaches and support obligations

(1) The Processor supports the Controller in complying with the obligations relating to the security of personal data, breach notification, data protection impact assessments and prior consultations set out in Articles 32 to 36 GDPR. This includes:

a) ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the forecast likelihood and severity of a possible infringement due to security vulnerabilities, and that enable the immediate detection of relevant infringements;

b) the obligation to notify the Controller of any personal data breach concerning the Controller's data **without undue delay and at the latest within 48 hours after becoming aware of it**. The notification shall contain at least the information referred to in Article 33(3)(a) to (d) GDPR insofar as it is available; where not all information is available at that time, the Processor shall make an initial notification within the deadline with the information then available and provide further information in phases without undue delay. The same applies to breaches of the provisions of this Agreement or of the Controller's instructions in the course of the processing by the Processor or by other persons involved in the processing. Personal data breaches at sub-processors are deemed to be breaches at the Processor for the purposes of this Section;

c) the obligation to support the Controller within the scope of its duty to inform data subjects and to provide the Controller with all relevant information in this context without undue delay;

d) supporting the Controller in its data protection impact assessments;

e) supporting the Controller in the context of prior consultations with the supervisory authority.

(2) The support owed under Article 28(3)(e) and (f) GDPR and under this Section shall be provided free of charge insofar as it forms part of the Service, is required by law or is caused by the conduct of the Processor or its sub-processors. Breach notifications under paragraph 1(b) are always free of charge. The Processor may claim reasonable remuneration only for additional support services that are requested by the Controller, go beyond the scope described above and are not attributable to the Processor's conduct; such remuneration shall be agreed in advance.

10. Authority of the Controller to issue instructions

(1) The Processor processes personal data exclusively within the framework of the agreements made and in compliance with any additional documented instructions of the Controller. Excluded from this are provisions of Union or Member State law that oblige the Processor to process the data otherwise; in such a case, the Processor shall inform the Controller of these legal requirements prior to processing, unless the relevant law prohibits such information on important grounds of public interest. The purpose, type and scope of the data processing are otherwise based exclusively on this Agreement and the instructions of the Controller. The Processor is prohibited from processing data in deviation from this unless the Controller has consented in writing or in text form.

(2) Instructions shall be given in writing or in text form (e.g., e-mail); instructions may also be given via the configuration options of the Service. Verbal instructions shall be confirmed by the Controller without undue delay, at least in text form.

The Processor designates the following person(s) as authorised to receive instructions from the Controller:

Altug Eker, Managing Director, Infercom SCS, aeker@infercom.ai

The data protection officer (Section 5(1)(a)) is not authorised to receive or issue instructions.

The Controller's instructions are given by the persons authorised for the Controller's account on cloud.infercom.ai, or by any other person the Controller names in text form.

In the event of a change or long-term absence of a contact person, the other party shall be informed without undue delay in text form of the successor or representative.

(3) The Processor shall inform the Controller without undue delay if it is of the opinion that an instruction infringes data protection law. The Processor is entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller.

11. Deletion and return of personal data

(1) Copies or duplicates of the data shall not be made without the knowledge of the Controller. Exceptions are backup copies insofar as they are necessary to ensure proper data processing, and data that must be retained to comply with statutory retention obligations.

(2) After completion of the contractually agreed work, or earlier upon request of the Controller – at the latest upon termination of the Service Agreement – the Processor shall, at the Controller's choice, hand over to the Controller all documents, processing and usage results and data relating to the contractual relationship that have come into its possession, or destroy them in a manner compliant with data protection law. The same applies to test and scrap material. The deletion log shall be submitted upon request.

(3) Documentation serving as evidence of proper data processing shall be retained by the Processor beyond the end of the contract in accordance with the respective retention periods. The Processor may hand it over to the Controller at the end of the contract.

(4) The following retention periods apply to personal data processed under this Agreement:

- Content data (Prompts, inputs and outputs): not retained; processed transiently and discarded after delivery of the response.
- API request metadata and logs: retained for up to 90 days for operational and security purposes.
- Authentication logs: retained for up to 12 months for security purposes.
- Support data: retained for the duration of the Service Agreement and deleted in accordance with paragraph 5.
- Billing records: retained in accordance with applicable tax and commercial law.

(5) Upon termination of the Service Agreement, all personal data processed on behalf of the Controller shall be deleted within 30 days, unless retention is required by applicable law. The Processor shall confirm deletion in writing upon request.

12. Right of retention

The parties agree that the Processor's right of retention is excluded with regard to the processed data and the associated data carriers.

13. Liability

The liability rules under Article 82 GDPR apply.

14. Governing law and jurisdiction

(1) This Agreement shall be governed by and construed in accordance with the laws of the Grand Duchy of Luxembourg, without prejudice to the mandatory provisions of the GDPR and of the data protection law applicable to the Controller.

(2) The supervisory authority competent for the Processor is the Commission nationale pour la protection des données (CNPD), Luxembourg. The competence of the supervisory authority of the Controller remains unaffected.

(3) Any disputes arising from this Agreement shall be subject to the exclusive jurisdiction of the courts of Luxembourg City.

15. Miscellaneous

(1) Should the Controller's data be endangered by third-party measures such as seizure or confiscation, insolvency or composition proceedings or other events, the Processor shall notify the Controller without undue delay. The Processor shall inform the third party that the responsibility for and ownership of the data rest exclusively with the Controller.

(2) Amendments and additions to this Agreement and all of its components require an agreement in writing or in text form, which may also be concluded electronically, and an express reference to the fact that it is an amendment or addition to this Agreement. Updates of the sub-processor list under Section 7(2) and of Annex 1 under Section 3(3) are made in accordance with those provisions.

(3) Should one or more provisions of this Agreement be invalid, this shall not affect the validity of the remaining provisions.

(4) Annex 1 (Technical and organisational measures) forms an integral part of this Agreement.

This Agreement is incorporated by reference into Infercom's Terms of Service available at infercom.ai/termsconditions. By accepting the Terms of Service, the Controller agrees to be bound by this Agreement. No separate signature is required.

Annex 1 – Technical and organisational measures

The Processor implements the following technical and organisational measures pursuant to Article 32 GDPR. Measures relating to physical security and data-centre operations are provided by the Processor's infrastructure sub-processor at the EU data centre on which the Service is operated; measures relating to the Processor's own organisation apply to its remote-first operation. Content data (Prompts and outputs) is processed transiently and not persistently stored (Section 2(1)).

1. Confidentiality (Art. 32(1)(b) GDPR)

Physical access control – *No unauthorised physical access to data processing systems.*

- Access control systems: biometric scanners, electronic key cards, 24/7 video surveillance
- Alarm system: integrated alarm system for perimeter security
- Video surveillance of all entrances and critical areas
- Chip card / transponder systems: electronic access control using chip cards
- Security locks: high-security locks on all access points
- Server room access: server rooms can only be entered with specific keys
- Visitor management: visitor log, visitor ID cards, escorted visits

System access control – *No unauthorised use of systems.*

- Secure passwords: password policy requiring strong, complex passwords
- Two-factor authentication: mandatory 2FA for administrative access and API access
- Multi-factor authentication for all users
- API security: API access secured via encrypted tokens
- Central password management: centralised password assignment and management
- Anti-virus protection on servers and clients
- Firewalls: high-grade firewalls for network protection
- Intrusion detection systems to detect unauthorised access attempts
- VPN for remote access: encrypted connections for remote work
- Mobile device policy for the secure use of mobile devices
- Clean desk policy when leaving workstations

Data access control – *No unauthorised reading, copying, modification or removal within the system.*

- Needs-based access rights: authorisation based on the principle of least privilege
- Authorisation concept: formal authorisation concept defining access levels
- Logging of access: comprehensive logging of data access
- User permission management: centralised management of user permissions

Separation – *Separate processing of data collected for different purposes.*

- Multi-tenancy: separate data processing environments per customer
- Sandboxing: hardware-level sandboxing within the AI accelerators to prevent cross-customer data leakage
- Physical separation of data processing environments
- Authorisation-based separation: authorisation concepts for data separation

Pseudonymisation and encryption (Art. 32(1)(a), Art. 25(1) GDPR) – *Processing of personal data in such a way that it can no longer be attributed to a specific data subject without additional information kept separately.*

- Encryption in transit: all customer data encrypted in transit using TLS 1.2 or higher
- In-memory processing: stateless engine processes data in memory without persistence
- Pseudonymisation of personal data where the purpose of processing allows

- Electronic signatures for data integrity where applicable

Organisational measures – *Organisational safeguards supporting confidentiality.*

- Key control: physical key management and control procedures
- Staffed reception for visitor management at the data centre
- Visitor log
- Employee / visitor ID cards
- Escorted visits: visitors accompanied by authorised employees
- Global data privacy policy: organisation-wide data protection policy
- Delete / destroy policy: policy for the secure deletion and destruction of data

2. Integrity (Art. 32(1)(b) GDPR)

Transfer control – *No unauthorised reading, copying, modification or removal during electronic transmission or transport.*

- TLS encryption: TLS 1.2 or higher for all API calls and data transmission
- VPN tunnels for secure data transmission
- Electronic signatures for document integrity

Data entry control – *Determination of whether and by whom personal data has been entered, changed or removed in data processing systems.*

- API call logging: logs of all API calls to track processing activities
- Administrative change logs: logging of administrative changes
- Audit trail: comprehensive logging of who entered, changed or removed data

3. Availability and resilience (Art. 32(1)(b) and (c) GDPR)

Availability control – *Protection against accidental or wilful destruction or loss.*

- High-grade firewalls: enterprise-grade firewall protection
- Redundant UPS: uninterruptible power supplies for continuous operation
- Virus protection: comprehensive anti-virus and anti-malware protection
- DDoS protection against distributed denial-of-service attacks
- Backup strategy: online and offline backups, on-site and off-site storage
- Monitoring: real-time monitoring and reporting dashboards (Grafana)
- Incident reporting channels: defined channels for reporting security incidents
- Emergency plans: documented emergency response procedures

Rapid recovery – *Ability to restore availability and access to personal data in a timely manner.*

- Automated failover mechanisms for high availability
- Incident response plan: documented plan for immediate action
- Service restoration: procedures to restore inference services promptly

4. Procedures for regular review, assessment and evaluation (Art. 32(1)(d), Art. 25(1) GDPR)

Data protection management – *Continuous management and oversight of data protection measures.*

- Data protection management: continuous oversight of data protection measures; external data protection officer appointed
- Privacy-friendly defaults: data protection-friendly default settings (Art. 25(2) GDPR)
- Regular assessments: periodic review and assessment of the technical and organisational measures

Incident response management – *Procedures for handling security incidents and personal data breaches.*

- Incident response plan: documented procedures for responding to security incidents
- Breach notification: procedures for notifying the Controller (Section 9), supervisory authorities and data subjects
- Post-incident reviews: reviews and lessons learned after security incidents

Contract control – *No processing within the meaning of Art. 28 GDPR without corresponding instructions from the Controller.*

- All sub-processors, including SambaNova Systems, Inc., are bound by contractual agreements that mirror the data protection standards of this Agreement
- Vendor due diligence: regular assessment and due diligence of processors and sub-processors
- Contract control: contractual controls ensuring compliance with data protection requirements

Document history

Version	Date	Changes
1.3	4 March 2026	Previous version (infercom.ai/dpa).
1.4	24 September 2026	Scope clarified: inference exclusively on EU-hosted infrastructure; Non-EU Models only by separate addendum (§ 1, § 2, § 2a, § 7a). Categories of data and data subjects specified for the Service (§ 2(2), (3)). Data protection officer no longer named as recipient of instructions; operational contact designated (§ 5(1)(a), § 10(2)). Remote-work clause: consent requirement replaced by binding standards; drafting error corrected (§ 6). Ancillary services clarified; sub-processor list updated to the current configuration; further sub-processors of the infrastructure provider referenced (§ 7). International transfers: Standard Contractual Clauses (Module Three) for the infrastructure provider's remote access; no fallback routing outside the EU; information on access countries on request (§ 7a). Breach notification within 48 hours with phased follow-up; support obligations free of charge, remuneration clause clarified (§ 9). Editorial corrections throughout.