Article 28 (3) General Data Protection Regulation (GDPR)
Controller-Processor Agreement

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 in the meaning of Article 4 (8) and Article 28 of Regulation (EU) 2016/679. 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 is taken as that defined in Article 4 (2) GDPR. The use of personal data includes in particular the collection, storage, transmission, blocking, deletion as well as the anonymization, pseudonymization, encryption or other use of data.

1. Subject matter and duration of the agreement

(1) Subject matter

The controller’s contract to the processor includes the following work and/or services:

☒ Infercom provides a high-performance, "Inference-as-a-Service" platform utilizing SambaNova Reconfigurable Dataflow Units (RDUs). The Service allows the Customer to deploy and run open-source Artificial Intelligence models (e.g., gtp-oss-120b, Deepseek) via an API for the purpose of generating text, code, or other outputs based on Customer-provided inputs ("Prompts"). The Service is architected for European Data Sovereignty. For EU-Hosted Models, all compute and data processing occur within the European Union. For models accessed through the Global Model Catalog, inference processing may occur outside the EU, subject to safeguards under Article 44 ff. GDPR.

(2) Duration

☒ The duration of this agreement corresponds to the duration of the service agreement.

2. Concrete specification of the agreement

(1) Nature and purpose of the processing of data

☒ The nature and purpose of the processing of personal data by the processor for the controller are described in concrete terms in the service agreement from https://www.infercom.ai/termsconditions

☒ A more detailed description of the subject matter of the agreement with regard to the nature and purpose of the processor's tasks is: to enable the Customer to utilize Large Language Models (LLMs) and AI acceleration hardware for their applications, products, or internal workflows without managing physical infrastructure.

- Nature of Processing:
  - Transient Inference: Processing is limited to the real-time ingestion of Customer Data (prompts/inputs) for the sole purpose of generating model outputs (inference).
  - No Training: The Provider explicitly does not use Customer Data to train, retrain, or improve foundational models (unless explicitly agreed otherwise in a separate specialized agreement).
  - No Storage: The Service is designed as a stateless inference engine; Customer Data sent for inference is processed in memory and is not written to persistent storage by the Provider after the response is generated.
  - For EU-Hosted Models, the provision of contractually agreed data processing takes place exclusively in a Member State of the European Union or in another Contractual State of the agreement on the European Economic Area. For models from the Global Model Catalog, Inference Data may be processed outside the EEA on SambaNova infrastructure. Any other transfer to a third country requires the prior consent of the controller and may only take place if the special conditions of Article 44 ff GDPR are met.

(2) Nature of data

☒ The processing of personal data contains the following types/categories (list/description of data categories)

☒ communication data (e.g. telephone, e-mail)

☒ contract data (contract relationship, product or contract interest)

☒ customer history ☒ contract settlement and payment data

(3) group of data subjects

☒ The group of data subjects affected by the processing includes (list/description of the categories of persons):

☒ employees of the controller ☒ subscribers

☒ interested parties

☒ sales representative

☒ contact partner

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 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) Where the Controller chooses to use models from the Global Model Catalog that process data outside the EEA, the Controller acknowledges this transfer. While the Processor ensures that appropriate safeguards (e.g., Standard Contractual Clauses) are in place with the respective sub-processors, the Controller remains responsible for assessing whether the use of such models is permissible for their specific data under their own data protection obligations and conducting any necessary risk assessments (e.g., Transfer Impact Assessments)**.**

(4) 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-organizational measures

(1) The processor has to document the implementation of the technical and organizational measures outlined in the run-up to the award of the contract and before the start of the processing, in particular with regard to the actual execution of the contract, and hand these over to the controller for examination. If accepted by the controller, the documented measures become the basis of the agreement. Insofar as an audit by the controller reveals a need for changes, these shall be implemented by mutual agreement.

(2) The processor has to deliver the security in accordance with Art. 28 sec. 3 c) and Art. 32 GDPR in particular in connection with Art. 5 sec. 1, paragraph 2 GDPR. Overall, the measures to be taken are data security measures and to ensure a level of protection in terms of the confidentiality, integrity, availability and resilience of the systems that is proportionate to the risk. The state of the art, the costs of implementation and the nature, scope and purposes of the processing, as well as the different probability 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 [see details in Annex 1].

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the processor is permitted to implement alternative adequate measures. The level of safety of the measures laid down shall not be lowered. Significant changes shall be documented.

4. Correction, restriction and deletion of data

(1) The controller is solely responsible for the protection of the rights concerned.

(2) The processor may not correct, delete or restrict the processing of the data processed in the order without authorization, but only in accordance with documented instructions from the controller. Insofar

as a data subject contacts the processor directly in this regard, the processor will immediately forward this request to the controller.

(3) Insofar as the scope of services includes, the concept of deletion, the right to be forgotten, correction, data portability and information according to documented instructions of the controller shall be ensured directly by the processor.

5. Quality assurance and other obligations of the processor

(1) In addition to complying with the regulations of this agreement, the processor has legal obligations under Articles 28 to 33 GDPR. In particular, it ensures compliance with the following requirements:

a) ☒ Written appointment of a data protection officer who carries out his duties in accordance with Articles 38 and 39 GDPR.

The processor's appointed data protection officer is

Mr. Nick Neffgen, DPO, nick.neffgen@deudat.de

A change of data protection officer shall be notified to the controller without delay.

(b) Confidentiality in accordance with Art. 28 sec. 3 p. 2 b), 29, 32 (4) GDPR. The processor may only use employees who have been committed to maintain confidentiality and who have previously been familiarized with the provisions on data protection relevant to them in carrying out the work. The processor and every person subordinate to the processor who has access to personal data may only process this data in accordance with the instructions of the controller, including the powers granted in this agreement, unless they are legally obliged to process them. The obligation to confidentiality of the employees shall be proven to the controller upon request.

c) The implementation and compliance with all technical and organizational measures required for this agreement in accordance with Article 28 (3) p. 2 lit. c, 32 GDPR [details in Appendix 1].

(d) On request the controller and the processor work together with the supervisory authority in the performance of their tasks.

(e) The immediate notification of the controller about control actions and measures of the supervisory authority, as far as they relate to this agreement. This also applies if a competent authority investigates the processing of personal data during processing at the processor's premises within the framework of an administrative offense or criminal proceedings.

(f) If the controller is exposed to a control by the supervisory authority, an administrative offense or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the processing at the processor, the processor shall support the controller to the best of his ability.

(g) The processor regularly checks the internal processes, as well as the technical and organizational measures to ensure that the processing in his area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the rights of the data subject are protected.

h) Verifiability of the technical and organizational measures taken vis-à-vis the controller within the scope of his control powers according to Section 8 of this contract.

(2) The processor is obliged to support the controller in his duty to process requests from data subjects in accordance with Art. 12-23 GDPR. In particular, the processor shall ensure that the information required in this respect is immediately given to the controller so that he can meet his obligations under Art. 12 Par. 3 GDPR.

6. “Home-Office” – Regulation

(1) The processor may, with the prior consent of the controller, allow its employees who are entrusted with the processing of personal data for the controller to process personal data in private households ("home office"). The consent of the controller shall be given in text form (e.g. email).

(2) The processor shall ensure that compliance with the contractually agreed technical and organizational measures is also guaranteed in the "home office" of the processor's employees. Deviations from individual contractually agreed technical and organizational measures shall be coordinated with the controller in advance and approved by in writing.

(3) In particular, the controller shall ensure that, when processing personal data in “home office”, the storage locations are configured in such a way, that storage of data on local IT systems that are used in the “home office” is prohibited. If this is not possible, the processor shall ensure that the local storage is encrypted and that other people in the household do not have access to this data.

(4) The processor is obliged to ensure that an effective control of the processing of personal data in "home office" by the controller is possible. The personal rights of the employees and other people living in the respective household shall be adequately taken into account.

(5) If employees of sub-processors are to be employed in "home office", the provisions of paragraphs 1 to 4 apply accordingly.

7. Engagement of sub-processors

1) Sub-processing relationships within the meaning of this regulation are those services that relate directly to the provision of the main service. This does not include ancillary services e.g. telecommunication services, postal / transport services, maintenance and user service 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, that the processor uses.

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, to take appropriate and legally compliant contractual agreements and control measures.

(2) The processor may only commission sub-processors (other processors) with the prior express written or documented consent of the controller.

☐ Sub-processing is not permitted.

☒ The controller agrees to the commissioning of the following sub-processor(s) under the condition of a contractual agreement in accordance with Art. 28 Paragraph 2-4 GDPR:

Company sub-processors	Address/Country	Performance
SambaNova Systems Inc.	2200 Geng Road, Suite 100, Palo Alto, CA 94303 /United States	Managed operation and remote administration of the AI inference platform (SambaManaged); access to account identifiers (email addresses) and API request metadata (timestamps, token usage) for operational monitoring, incident response, and support escalation; AI inference processing for models served via the Global Model Catalog
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, D04 E5W5, Ireland	Internal business email, calendar, document storage and collaboration (Gmail, Google Drive, Google Calendar); personal data may include customer-related correspondence handled by Infercom personnel
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 pipeline management
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
TECLIB SAS	231 Rue Saint-Honoré, 75001 Paris, France	GLPI - IT support ticketing system; storage and management of customer support requests, which may include contact data and descriptions of technical issues submitted by or on behalf of the Controller's users

☒ the change of the existing sub-processor

are permitted to the extent that:

- the processor notifies the controller of such outsourcing to sub-processors a reasonable time in advance in writing or in text form, and
- **the controller does not raise an objection to the planned outsourcing in writing or in text form within 14 days after receipt of the notification (if no objection is raised within this period, the change is deemed approved), and**
- a contractual agreement in accordance with Art. 28 Paragraph 2-4 GDPR is used.

(3) The transfer of personal data of the controller to the sub-processor and its initial activity are only permitted if all the requirements for sub-processing are met.

(4) The processor shall ensure that the provisions agreed in this contract and any additional instructions from the controller also apply to the sub-processor.

(5) If the sub-processor provides the agreed service outside of the EU / EEA, the processor shall ensure admissibility under data protection law by taking appropriate measures. The same applies if service providers within the meaning of paragraph 1 sentence 2 are to be used.

(6) Further outsourcing by the sub-processor requires the express information and consent of the controller (at least in text form); all contractual regulations in the contractual chain shall also be imposed on the further sub-processor.

(7) The processor carries out regular checks on the sub-processors. These controls are to be documented and made available to the controller upon request.

7a. International Data Transfers

(1) The Processor shall ensure that any transfer of personal data to a third country is carried out in compliance with Chapter V of the GDPR (Articles 44-49).

(2) For transfers to sub-processors in the United States, the parties rely on:

- the EU-US Data Privacy Framework (where the sub-processor is certified); and/or

- Standard Contractual Clauses pursuant to Commission Implementing Decision (EU) 2021/914 as a supplementary or fallback mechanism.

(3) The Processor shall conduct and maintain a Transfer Impact Assessment for transfers to third countries and make this available to the Controller upon request.

(4) Supplementary measures for the SambaNova sub-processing relationship include: encryption in transit and at rest, strict access controls for remote operations, logging of all access, and contractual limits on disclosure to third-country authorities.

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 individual cases. These inspections shall generally be announced 14 days in advance, unless an unannounced inspection appears necessary to avoid compromising the purpose of the inspection.

(2) The processor ensures that the controller can convince himself of the compliance with the obligations of the processor according to Art. 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 organizational measures.

(3) Evidence of such measures, which do not only relate to the specific processing, can be provided by:

> ☒ current certificates, reports or report excerpts from independent bodies (e.g. auditors, auditors, own data protection officer, IT security department, data protection auditors, quality auditors);

(4) In particular, the processor shall be obliged to ensure, by means of contractual arrangements, that the control powers and rights of the contracting entity and supervisory authorities also apply to the sub-

processor. It is also to be contractually stipulated, that the sub-processor shall tolerate these control measures and any on-site checks to be notified at least 14 days in advance.

(5) The controller has the right to check the complete and contractual return and deletion of the data to the processor, in accordance with clause 11 of this Agreement. This may also be done by inspecting the data processing systems at the processor's premises. The on-site inspection is to be announced by the controller within a reasonable period of time.

9. Notification of breaches by the processor

(1) The processor supports the controller in complying with the obligations relating to the security of personal data specified in Articles 32 to 36 of the GDPR, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. These include:

a. ensuring an appropriate level of protection through technical and organizational measures, that take into account the circumstances and purposes of the processing, as well as the forecasted probability and severity of a possible violation of the law due to security gaps and enable the immediate detection of relevant violations.

b. the obligation to notify the controller without undue delay and within 48 hours of any breach of data protection regulations or of the contractual agreements made and / or the instructions issued by the controller in the course of the processing of data by him or other persons involved in the processing. The notification of the processor to the controller shall, in particular, include the information in accordance with Article 33, paragraphs a) to d).

c. the obligation to support the controller within the scope of his obligation to provide information to data subjects and to provide him with all relevant information in this context without delay

d. the support of the controller in its data protection impact assessment

e. the assistance of the controller in the context of prior consultations with the supervisory authority.

(2) The processor may claim remuneration for support services, that are not included in the service description or cannot be tracked back to misconduct on the part of the processor.

10. Authority of the controller to issue instructions

(1) The processor processes personal data exclusively within the framework of the agreements made and / or in compliance with any additional instructions given by the controller. Excluded from this are statutory regulations that may oblige the processor to process the data otherwise. In such a case, the processor will inform the controller of these legal requirements prior to processing, unless the relevant law prohibits such communication because of an important public interest. The purpose, type and scope of the data processing are otherwise based exclusively on this agreement and / or the instructions of the controller. The processor is prohibited from processing data that deviates from this unless the controller has given his written consent.

(2) Verbal instructions are immediately confirmed by the controller (at least in text form).

The processor shall designate the person(s) to the controller who is / are entitled to receive instructions from the controller.

Persons entitled to receive instructions from the controller are:

Mr. Nick Neffgen, DPO, nick.neffgen@deudat.de

In the event of a change or long-term absence of the contact person, the controller shall be informed immediately in writing of the successor or the representative.

(3) The processor shall inform the controller immediately if he is of the opinion, that an instruction violates data protection regulations. The processor is entitled to suspend the implementation of the relevant instruction until it is confirmed or changed 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. Exception to this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data, that are necessary with regard to compliance with statutory retention requirements.

(2) After completion of the contractually agreed work or earlier upon request by the controller – at the latest upon termination of the service agreement – the processor shall hand over to the controller all documents, processed and usage results drawn up and data relating to the contractual relationship to the controller or, with prior consent, destroy them in accordance with data protection. The same applies to test and scrap material. The log of the deletion shall be submitted on request.

(3) Documentation, that serves as evidence of orderly and proper data processing must be stored by the processor beyond the end of the contract in accordance with the respective retention periods. He can hand them over to the controller at the end of the contract.

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

- Inference Data (Prompts and Outputs): Not retained; processed transiently and discarded after response delivery.

- API request metadata and logs: Retained for up to 90 days for operational and billing purposes.

- Authentication logs: Retained for up to 12 months for security purposes.

- Billing records: Retained in accordance with applicable tax and commercial law.

(5) Upon termination of the service agreement, all personal data 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 right of retention by the processor 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.

(2) The competent supervisory authority is the Commission nationale pour la protection des données (CNPD), Luxembourg.

(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 property of the controller be endangered by third-party measures, such as seizure or confiscation or other events, the processor shall notify the controller without delay. The processor points out to the third party, that the responsibility and ownership of the data rest exclusively with the controller.

(2) Amendments and additions to this additional agreement and all of its components shall require a written agreement.

(3) Should one or more clauses of this agreement be ineffective, this shall not affect the validity of the rest of the 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 organizational measures

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

☒ **Access control**

No unauthorized access to data processing systems, e.g .: magnetic or chip cards, keys, electric door openers, plant security or porters, alarm systems, video systems.

The following measures exist for access control:

- Access Control Systems: Biometric scanners, electronic key cards, 24/7 video surveillance
- Alarm System: Integrated alarm system for perimeter security
- Video Surveillance: 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 certain keys
- Visitor Management: Visitor book/log, visitor ID cards, escorted visit

☒ **System access control**

No unauthorized system use, e.g .: (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers.

The following measures exist for system access control:

- Secure Passwords: Password policy requiring strong, complex passwords
- Two-Factor Authentication (2FA): Mandatory 2FA for administrative access and API access
- Multi-Factor Authentication: Activation of multi-factor authentication for all users
- API Security: API access secured via encrypted tokens
- Central Password Management: Centralized password assignment and management
- Anti-Virus Protection: Anti-virus software on servers and clients
- Firewall: High-grade firewalls for network protection
- Intrusion Detection Systems: Systems to detect unauthorized access attempts
- VPN for Remote Access: Virtual Private Network for secure remote connections
- Mobile Device Policy: Policy for secure use of mobile devices
- Clean Desk Policy: Policy requiring clean desks when leaving workstations

☒ **Data access control**

No unauthorized reading, copying, changing or removing within the system, e.g .: authorization concepts and needs-based access rights, logging of accesses.

The following measures exist for data access control:

- Needs-Based Access Rights: Authorization based on principle of least privilege
- Authorization Concept: Formal authorization concept defining access levels
- Logging of Access: Comprehensive logging of all data accesses
- User Permission Management: Centralized management of user permissions

☒ **Separation**
Separate processing of data collected for different purposes, e.g. Multi-tenancy, sandboxing

The following measures exist for separation:

- Multi-Tenancy: Separate data processing environments per customer
- Sandboxing: Hardware-level sandboxing within RDUs to prevent cross-customer data leakage
- Physical Separation: Physical separation of data processing environments
- Authorization-Based Separation: Definition of authorization concepts for data separation.

☒ **Pseudonymization & Encryption (Art. 32 Para. 1 lit. a) GDPR; Art. 25 para. 1 GDPR)**
The processing of personal data in such a way that the data can no longer be assigned to a specific data subject without the use of additional information, provided that this additional information is stored separately and is subject to appropriate technical and organizational measures

The following measures exist for Pseudonymization & Encryption:

- 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
- Pseudonymization: Processing of personal data so it cannot be assigned to specific data subject without additional information
- Electronic Signature: Use of electronic signatures for data integrity.

☒ **Organizational Measures**
The following measures exist for Organization:

- Key Control: Physical key management and control procedures
- Reception/Porter: Staffed reception for visitor management
- Visitor Log: Maintaining visitor books and logs
- Employee/Visitor ID Cards: Mandatory ID card usage for all personnel
- Escorted Visits: Visitors accompanied by authorized employees
- Global Data Privacy Policy: Organization-wide data privacy policy
- Delete/Destroy Policy: Policy for secure deletion and destruction of data

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

☒ **Transfer control**

No unauthorized reading, copying, changing or removing during electronic transmission or transport, e.g. encryption, virtual private networks (VPN), electronic signature

The following measures exist for transfer control:

- TLS Encryption: TLS 1.2 or higher for all API calls and data transmission
- VPN Tunnels: VPN for secure data transmission
- Electronic Signature: Use of 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, e.g.: logging, document management.

The following measures exist for data entry control:

- API Call Logging: Logs of all API calls to track data processing activities
- Administrative Change Logs: Logging of administrative changes to track modifications
- Audit Trail: Comprehensive logging of who entered, changed or removed data.

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

☒ **Availability control (Art. 32 Para. 1 lit. c) GDPR)**
Protection against accidental or willful destruction or loss, e.g.: backup strategy (online / offline; on-site / off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans

The following measures exist for availability control:

- High-Grade Firewalls: Enterprise-grade firewall protection
- Redundant UPS: Uninterruptible power supplies for continuous operation
- Virus Protection: Comprehensive antivirus and anti-malware protection
- DDoS Protection: Protection against distributed denial-of-service attacks
- Backup Strategy: Online and offline backups, on-site and off-site storage
- Grafana Reporting: Real-time monitoring and reporting dashboards
- Incident Reporting Channels: Defined channels for reporting security incidents
- Emergency Plans: Documented emergency response procedures

☒ Rapid recovery (Art. 32 Para. 1 lit. c) GDPR)

The following measures exist for a rapid recovery:

- Automated Failover: Automated failover mechanisms for high availability
- Incident Response Plan: Documented incident response plan for immediate action
- Service Restoration: Procedures to restore inference services immediately

4. Procedure for regular review, assessment and evaluation (Art. 32 Paragraph 1 lit.d GDPR; Art. 25 Paragraph 1 GDPR)

The following measures exist for procedure for regular review, assessment and evaluation

☒ **Data protection management**

- Data Protection Management: Continuous management and oversight of data protection measures
- Privacy-Friendly Defaults: Data protection-friendly default settings (Art. 25 Para. 2 GDPR)
- Regular Assessments: Periodic review and assessment of technical and organizational measures

☒ **Incident-Response-Management**

- Incident Response Plan: Documented procedures for responding to security incidents
- Breach Notification: Procedures for notifying supervisory authorities and data subjects in case of breaches
- Post-Incident Reviews: Reviews and lessons learned after security incidents

☒ **Data protection-friendly default settings (Art. 25 Para. 2 GDPR)**

☒ **Contract control**
No order processing within the meaning of Art. 28 GDPR without corresponding instructions from the client, e.g .: clear contract drafting, formalized order management, strict selection of the service provider, obligation to provide prior conviction, follow-up controls.

- All sub-processors, including SambaNova Systems Inc., are bound by contractual agreements that mirror the data protection standards of this DPA
- Sub-Processor Agreements: All sub-processors bound by contractual agreements mirroring data protection standards
- Vendor Due Diligence: Regular assessment and due diligence of processors and sub-processors
- Contract Control: Contractual controls ensuring compliance with data protection requirements