Data Processing Agreement

Contract for the processing of personal data on behalf of a controller pursuant to Art. 28 GDPR

between

_____

_____

- hereinafter referred to as the "**Client**" -

and

Langfuse GmbH, Gethsemanestr. 4, 10437, Berlin, Germany - ("**Langfuse**")

- hereinafter referred to as "**Contractor**" -

1. **Subject matter of the contract**

   As part of the provision of services under the contract for the use of the Langfuse platform (hereinafter referred to as the "Main Contract"), it is necessary for the Contractor to handle personal data for which the Client acts as data controller within the meaning of data protection regulations (hereinafter referred to as "**Client Data**"). This contract specifies the rights and obligations of the parties under data protection law in connection with the Contractor's handling of Client Data for the performance of the Main Contract.

2. **Scope of the assignment**

   (1) The contractor processes the client data on behalf of and in accordance with the instructions of the client within the meaning of Art. 28 GDPR (commissioned processing). The client remains the controller within the meaning of data protection law.

   (1) The Contractor shall process the Client Data in the manner, to the extent and for the purpose specified in Annex 1 to this Agreement; the processing shall concern the types of personal data and categories of data subjects specified therein. The duration of the processing corresponds to the term of the main contract.

   (2) The Contractor reserves the right to anonymize or aggregate the Client Data so that it is no longer possible to identify individual data subjects and to use it in this form for the purpose of needs-based design, further development and optimization as well as the provision of the service agreed in accordance with the main contract. The parties agree that anonymized or aggregated client data in accordance with the above provision shall no longer be considered client data within the meaning of this agreement.

   (3) The Contractor may process and use the Client's data for its own purposes under its own responsibility within the scope of what is permitted under data protection law if this is permitted by a statutory authorization provision or a declaration of consent by the data subject. This contract does not apply to such data processing.

   (4) The processing of the Client Data by the Contractor shall generally take place within the European Union or in another state party to the Agreement on the European Economic Area (EEA). The Contractor is nevertheless permitted to process Client Data outside the EEA in compliance with the provisions of this contract if it informs the Client in advance of the place of data processing and the requirements of Art. 44-48 GDPR are met or an exception pursuant to Art. 49 GDPR applies.

3. **Authority of the client to issue instructions**

   (1) The Contractor shall process the Client Data in accordance with the Client's instructions, unless the Contractor is legally obliged to process the data otherwise. In the latter case, the Contractor shall notify

the Client of these legal requirements prior to processing, unless the law in question prohibits such notification due to an important public interest.

(1) The Client's instructions are in principle conclusively defined and documented in the provisions of this contract. Individual instructions that deviate from the provisions of this contract or impose additional requirements shall require the prior consent of the Contractor and shall be made in accordance with the amendment procedure set out in the main contract, in which the instruction shall be documented and the assumption of any additional costs incurred by the Contractor as a result shall be regulated by the Client.

(2) The Contractor warrants that it processes the Client Data in accordance with the Client's instructions. If the Contractor is of the opinion that an instruction of the Client violates this Agreement or the applicable data protection law, it shall be entitled, after notifying the Client accordingly, to suspend the execution of the instruction until the Client confirms the instruction. The parties agree that the sole responsibility for processing the client data in accordance with the instructions lies with the client.

4. **Responsibility of the client**

(1) The client is solely responsible for the lawfulness of the processing of the client data and for safeguarding the rights of the data subjects in the relationship between the parties. Should third parties assert claims against the Contractor due to the processing of Client Data in accordance with this contract, the Client shall indemnify the Contractor against all such claims upon first request.

(2) The Client shall be responsible for making the Client Data available to the Contractor in good time for the provision of services under the main contract and shall be responsible for the quality of the Client Data. The Client must inform the Contractor immediately and in full if it discovers errors or irregularities with regard to data protection regulations or its instructions when checking the Contractor's order results.

(3) Upon request, the Client shall provide the Contractor with the information specified in Art. 30 (2) GDPR, unless the Contractor has this information itself.

(4) If the Contractor is obliged vis-à-vis a government agency or a person to provide information about the processing of Client Data or to cooperate with these agencies in any other way, the Client shall be obliged to support the Contractor upon first request in providing such information or fulfilling other obligations to cooperate.

5. **Requirements for personnel**

The contractor shall oblige all persons who process client data to maintain confidentiality with regard to the processing of client data.

6. **Safety of processing**

(1) The Contractor shall take appropriate technical and organizational measures in accordance with Art. 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing of the Client Data as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, to ensure a level of security for the Client Data appropriate to the risk.

(2) The contractor is permitted to change or adapt technical and organizational measures during the term of the contract as long as they continue to meet the legal requirements.

7. **Use of further processors**

(1) The Client hereby grants the Contractor general authorization to involve further processors with regard to the processing of Client data. The other processors involved at the time of the conclusion of the contract are listed in **Annex 2**.

(2) The Contractor shall inform the Client of any intended changes with regard to the involvement or replacement of additional processors. In individual cases, the Client shall have the right to object to the commissioning of a potential additional processor. An objection may only be raised by the client for good cause to be proven to the contractor. If the client does not raise an objection within 14 days of receipt of the notification, its right of objection to the corresponding assignment shall expire. If the Client raises an objection, the Contractor shall be entitled to terminate the main contract and this contract jointly with a notice period of 30 days.

(3) The contract between the Contractor and the additional processor must impose the same obligations on the latter as are imposed on the Contractor by virtue of this contract. The parties agree that this requirement is met if the contract has a level of protection corresponding to this contract or if the obligations set out in Art. 28 para. 3 GDPR are imposed on the additional processor.

(4) Subject to compliance with the requirements of Section 2 (5) of this Agreement, the provisions of this Section 7 shall also apply if another processor in a third country is involved. In this case, the Contractor shall agree with the additional processor the EU standard contractual clauses for the transfer of personal data to processors in third countries of June 4, 2021, Module 3. The Client agrees to cooperate to the extent necessary in fulfilling the requirements of Art. 49 GDPR.

8. **Rights of the data subjects**

(1) The Contractor shall support the Client with technical and organizational measures within the scope of what is reasonable in order to comply with its obligation to respond to requests to exercise the rights of data subjects to which they are entitled.

(2) If a data subject asserts a request to exercise their rights directly against the Contractor, the Contractor shall forward this request to the Client in a timely manner.

(3) The Contractor shall provide the Client with information about the stored Client Data, the recipients of Client Data to whom the Contractor passes it on in accordance with the order and the purpose of the storage, unless the Client has this information itself or can obtain it itself.

(4) The Contractor shall enable the Client to correct, delete or restrict the further processing of Client data within the scope of what is reasonable and necessary against reimbursement of the expenses and costs incurred by the Contractor as a result, or to carry out the correction, blocking or restriction of further processing itself at the request of the Client if and to the extent that this is impossible for the Client itself.

(5) Insofar as the data subject has a right to data portability vis-à-vis the Client with regard to the Client Data in accordance with Art. 20 GDPR, the Contractor shall support the Client in providing the Client Data in a common and machine-readable format within the scope of what is reasonable and necessary against reimbursement of the expenses and costs incurred by the Contractor in this respect, if the Client cannot obtain the data in any other way.

9. **Notification and support obligations of the contractor**

(1) Insofar as the Client is subject to a statutory reporting or notification obligation due to a breach of the protection of Client Data (in particular pursuant to Art. 33, 34 GDPR), the Contractor shall inform the Client promptly of any reportable events in its area of responsibility. The Contractor shall support the Client in the fulfillment of the reporting and notification obligations at the Client's request within the scope of what is reasonable and necessary against reimbursement of the expenses and costs incurred by the Contractor to be proven.

(2) The Contractor shall support the Client, to the extent reasonable and necessary, in any data protection impact assessments to be carried out by the Client and any subsequent consultations with the supervisory authorities pursuant to Art. 35, 36 GDPR against reimbursement of the expenses and costs to be proven to the Contractor as a result.

10. **Data deletion**

(1) The Contractor shall delete the Client Data after termination of this contract, unless the Contractor is legally obliged to continue storing the Client Data.

(2) Documentation that serves as proof of the orderly and proper processing of client data may be retained by the contractor even after the end of the contract.

11. **Verifications and checks**

(1) The Contractor shall provide the Client, at the Client's request, with all necessary information available to the Contractor to prove compliance with its obligations under this contract.

(2) The Client is entitled to review the Contractor with regard to compliance with the provisions of this contract, in particular the implementation of the technical and organizational measures, including through inspections.

(3) In order to carry out inspections in accordance with Section 11.2, the Client shall be entitled to enter the Contractor's business premises where Client Data is processed during normal business hours (Mondays to Fridays from 10 a.m. to 6 p.m.) at its own expense, without disrupting operations and subject to strict confidentiality of the Contractor's business and trade secrets, after giving timely advance notice in accordance with Section 11.5.

(4) The Contractor is entitled, at its own discretion, taking into account the Client's legal obligations, not to disclose information that is sensitive with regard to the Contractor's business or if the Contractor would violate legal or other contractual regulations by disclosing it. The Client is not entitled to obtain access to data or information about other clients of the Contractor, to information regarding costs, to quality inspection and contract management reports and to any other confidential data of the Contractor that is not directly relevant to the agreed inspection purposes.

(5) The client must inform the contractor in good time (generally at least two weeks in advance) of all circumstances relating to the performance of the inspection. The Client may carry out one inspection per calendar year. Further inspections shall be carried out against reimbursement of costs and after consultation with the Contractor.

(6) If the Client commissions a third party to carry out the inspection, the Client shall obligate the third party in writing in the same way as the Client is obligated to the Contractor under this Section 11 of this Agreement. In addition, the Client shall oblige the third party to maintain confidentiality and secrecy, unless the third party is subject to a professional obligation of confidentiality. At the request of the Contractor, the Client shall immediately submit to the Contractor the obligation agreements with the third party. The Client may not commission a competitor of the Contractor with the inspection.

(7) At the Contractor's discretion, proof of compliance with the obligations under this contract may also be provided by the submission of a suitable, current certificate or report from an independent body (e.g. auditor, internal audit, data protection officer, IT security department, data protection auditors or quality auditors (e.g. SOC2 Type 2 or ISO 27001) or a suitable certification by IT security or data protection audit - e.g. in accordance with BSI basic protection ("audit report") - instead of an inspection.SOC2 Type 2 or ISO 27001)) or a suitable certification through an IT security or data protection audit - e.g. in accordance with BSI basic protection - ("audit report"), if the audit report enables the client to reasonably satisfy itself of compliance with the contractual obligations.

12. **Contract duration and termination**

The term and termination of this contract are governed by the provisions on the term and termination of the main contract. Termination of the main contract shall automatically result in termination of this contract. Isolated termination of this contract is excluded

13. **Liability**

(1) The exclusions and limitations of liability under the main contract shall apply to the Contractor's liability under this contract. Insofar as third parties assert claims against the Contractor which have their cause

in a culpable breach by the Client of this contract or of one of its obligations as the controller under data protection law, the Client shall indemnify the Contractor against these claims upon first request.

(2) The Client undertakes to indemnify the Contractor on first demand against any fines imposed on the Contractor to the extent that the Client bears a share of the responsibility for the infringement sanctioned by the fine.

14. **Final provisions**

(1) Should individual provisions of this contract be or become invalid or contain a loophole, the remaining provisions shall remain unaffected. The parties undertake to replace the invalid provision with a legally permissible provision that comes closest to the purpose of the invalid provision and meets the requirements of Art. 28 GDPR.

(2) In the event of contradictions between this contract and other agreements between the parties, in particular the main contract, the provisions of this contract shall take precedence.

_____ San Francisco, _____ 2024

(Signature of client)

Clemens Rawert
Managing Director, Langfuse GmbH
Contractor

Attachments:

Appendix 1: Purpose, type and scope of data processing, type of data and categories of data subjects

Appendix 2: Other processors

Appendix 3: Technical and organizational measures

Appendix 1: Purpose, type and scope of data processing, type of data and categories of data subjects

Purpose of data processing:

The purpose of data processing is the contractual provision of the Langfuse platform

Scope of data processing:

Type of data:

- Names, email addresses of employees and other users of the client
- Communication content stored by the client on the platform

(collectively referred to as "client data")

Categories of data subjects:

- Employees and other users of the client (collectively referred to as "users")
- Individuals to whom communication content refers stored by the client on the platform refer

(collectively referred to as "data subjects of the client")

Appendix 2: Further processors

/

Annex 2: List of authorized Subprocessors *(In case of any discrepancy or inconsistency between the German version and its translation, the German version shall prevail and be considered legally binding. The translation is provided for convenience and informational purposes only. It is important to refer to the original German version for any legal interpretations or implications).*

Company	**Purpose / Purpose**	**Art der Daten / Type of Data**	**Categories of data subjects / Categories of data subjects**	**Ort der Verarbeitung / Location of data processing**
Supabase, Inc.	Database Services/Database services	Client data / Client Data	Betroffene Personen des Auftraggeber / Affected individuals of the client	EU
Vercel Inc.	Application Hosting / Hosting services	Client data / Client Data	Betroffene Personen des Auftraggeber / Affected individuals of the client	EU
Amazon Web Services, Inc.	Application Hosting / Hosting services	Client data / Client Data	Betroffene Personen des Auftraggeber / Affected individuals of the client	EU
Clickhouse Inc.	Application Hosting / Hosting services	Client data / Client Data	Betroffene Personen des Auftraggeber / Affected individuals of the client	EU
Google LLC	Application Hosting / Hosting services	Client data / Client Data	Betroffene Personen des Auftraggeber / Affected individuals of the client	EU
Posthog, Inc.	Product metrics / Product metrics	Client data / Client Data	Betroffene Personen des Auftraggeber / Affected individuals of the client	EU
Betterstack, Inc.	Application logs / Application logging for internal use	Client data / Client Data	Betroffene Personen des Auftraggeber / Affected individuals of the client	EU
Cloudflare, Inc.	Application security & data storage / Web Application Security and file storage	Client data / Client Data	Betroffene Personen des Auftraggeber / Affected individuals of the client	EU / US
Functional Software, Inc. d/b/a Sentry	Anwendungsüberwachung / Application monitoring for internal use	Client data / Client Data	Betroffene Personen des Auftraggeber / Affected individuals of the client	US

Appendix 3: Technical and Organizational Measures implemented by the Processor

The present document supplements chapter 11 of the Data Processing Agreement (DPA) between Client and Contractor pursuant to Art 28 GDPR (EU General Data Protection Regulation).

The technical and organizational measures are implemented by Langfuse in accordance with Art 32 GDPR. They are continuously improved by Langfuse according to feasibility and state of the art - not least also in terms of the active pursuing of both, ISO 27001 and SOC 2 Type II certifications - and brought to a higher level of security and protection.

1. confidentiality

1.1 Physical Access Control: *Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.*	
Technical Measures	**Organizational Measures**
Doors with knob outside	Physical Security Policy
Locking systems	Visitor's book and protocol
Lockable storage containers	Visitors accompanied by employees
	Information Security Policy
1.2 Logical Access Control: *Measures suitable for preventing data processing systems from being used by unauthorized persons.*	
Technical Measures	**Organizational Measures**
Login with username and strong password or SSO where available	User permission management
Encryption of devices	Creating user profiles
Enforced MFA where applicable	Information Security Policy
Automatic desktop lock	
1.3 Authorization Control: *Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.*	
Technical Measures	**Organizational Measures**
Logging of access to applications, specifically when entering, changing, and deleting data	Information Security Policy
SSH encrypted access	Minimum number of administrators
Certified SSL encryption	Management of user rights by administrators
1.4 Separation Control: *Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.*	
Technical Measures	**Organizational Measures**
Separation of productive and test environment	Control via authorization concept
Multi-tenancy of relevant applications	Determination of database rights
	Information Security Policy
	Data Protection Policy
1.5 Pseudonymization: *The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.*	
Technical Measures	**Organizational Measures**

In case of pseudonymization: separation of the allocation data and storage in separate system (encrypted)	Internal instruction to anonymize/pseudonymize personal data as far as possible in the event of disclosure or even after the statutory deletion period has expired
Log files are pseudonymized at the request of the client	Information Security Policy
	Data Protection Policy

2. integrity

2.1 Transfer Control: *Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.*	
Technical Measures	**Organizational Measures**
Logging of access and retrievals	Survey of regular retrieval and transmission processes
Provision via encrypted connections such as sftp, https and secure cloudstores	Transmission in anonymized or pseudonymized form
	Information Security Policy
	Data Protection Policy
2.2 Input Control: *Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).*	
Technical Measures	**Organizational Measures**
Manual or automated control of the logs (according to internal specifications)	Traceability of data entry, modification and deletion through individual user names (not user groups)
	Assignment of rights to enter, change and delete data on the basis of an authorization concept
	Clear responsibilities for deletions
	Information Security Policy

3. availability and resilience

3.1 Availability Control: *Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).*	
Technical Measures	**Organizational Measures**
Hosting in certified data centers by reputable cloud providers (e.g. Supabase/Vercel which run on AWS)	Backup concept
	Existence of a business continuity and disaster recovery plan
	Information Security Policy

3.1 Recoverability Control: *Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.*	
Technical Measures	**Organizational Measures**
Backup monitoring and reporting	Recovery concept
Restorability from automation tools	Control of the backup process
Backup concept according to criticality and customer specifications	Regular testing of data recovery and logging of results
	Existence of a business continuity and disaster recovery plan
	Information Security Policy

4 Procedures for Regular Review, Assessment and Evaluation

4.1 Data protection management	
Technical Measures	**Organizational Measures**
Central documentation of data protection regulations with access for employees	Privacy officer appointed
A review of the effectiveness of the TOMs is carried out at least annually and TOMs are updated	Staff trained and obliged to confidentiality/data secrecy
	Regular awareness trainings at least annually
	Processes regarding information obligations according to Art 13 and 14 GDPR established
	Formalized process for requests for information from data subjects is in place
	Data protection established as part of corporate risk management
4.2 Incident Response Management: *Support for security breach response and data breach process.*	
Technical Measures	**Organizational Measures**
Use of Google Workspace firewall and regular updating	Documented process for detecting and reporting security incidents / data breaches (also with regard to reporting obligation to supervisory authority)
Use of Google Workspace spam filter and regular updating	Formalized procedure for handling security incidents
Use of Google Workspace virus scanner and regular updating	Involvement of Privacy Officer and CTO in security incidents and data breaches
	Documentation of security incidents and data breaches via ticket system
	A formal process for following up on security incidents and data breaches
	Information Security Policy
	Data Protection Policy
4.3 Data Protection by Design and by Default: *Measures pursuant to Art 25 GDPR that comply with the*	

principles of data protection by design and by default.	
Technical Measures	**Organizational Measures**
No more personal data is collected than is necessary for the respective purpose	Data Protection Policy (includes principles "privacy by design / by default")
Use of data protection-friendly default settings in standard and individual software	
4.4 Order Control (Outsourcing, Subcontractors and Order Processing): *Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.*	
Technical Measures	**Organizational Measures**
Monitoring of remote access by external parties, e.g. in the context of remote support	Selection of contractors under due diligence aspects (especially with regard to data protection and data security)
Monitoring of subcontractors according to the principles and with the technologies according to the preceding chapters 1, 2	Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses
	Agreement on effective control rights over the contractor
	Ensuring the destruction of data after termination of the contract

5 Organization and Data Protection at Langfuse

In its policies, Langfuse has set itself the goal, among other things, of providing its customers with the products and services to be delivered at the highest possible level of information security in compliance with the law.

Employees are continuously informed and trained in the area of data protection. In addition, all employees are contractually bound to data secrecy and confidentiality. External parties who may come into contact with personal data in the course of their work for Langfuse are obligated to maintain secrecy and confidentiality as well as to comply with data protection and data secrecy by means of anNDA (Non-Disclosure Agreement) before they begin their work.