Langfuse Data Processing Agreement (DPA)

Latest revision: September 9th, 2025

> **At a glance** — You (as *Controller*) remain in control of your data; Langfuse (as *Processor*) only uses it to run the Solution, keeps it secure under industry-standard TOMs, and allows you to delete it or deletes it when you ask us to or leave us. If we need new vendors or make material changes, we will let you know 30 days in advance.

Applicability Notice

This DPA is available for any Client of the Langfuse Cloud platform (EU Cloud at https://cloud.langfuse.com, US Cloud at https://us.cloud.langfuse.com, HIPAA Cloud at https://hipaa.cloud.langfuse.com) and any subscription tier (Hobby, Core, Pro, Teams, Enterprise). It forms part of and is incorporated by reference into the applicable Master Subscription Agreement or other agreement governing use of the Langfuse platform (the 'Main Contract').

Questions? Email support@langfuse.com

The current and past versions of this DPA are always available at https://langfuse.com/security/dpa

1. Preamble & Incorporation

This Data Processing Agreement (**'DPA'**) describes how Langfuse GmbH (**'Langfuse'**, **'we'**, **'us'**) processes Personal Data on behalf of the Client (**'you'**).

This DPA supplements and is incorporated by reference into Langfuse's Master Subscription Agreement ('**MSA**') or other agreement governing use of the Langfuse platform (collectively, the **'Main Contract'**).

It is intended to, inter alia, satisfy the requirements of:

- **Regulation (EU) 2016/679** (*EU GDPR*),
- the **UK GDPR** as defined in the UK Data Protection Act 2018, and
- the **California Consumer Privacy Act of 2018** (together with the California Privacy Rights Act of 2020, the *CCPA*)
- and **any other national data-protection laws** that implement or supplement the foregoing (collectively, **'Applicable Data-Protection Laws'**).

Applicability. This DPA applies to **all** Clients that Process Personal Data via the Solution. Sections on fees or cost-sharing apply only where you have a paid subscription.
Precedence. If there is a conflict between this DPA and the Main Contract, **this DPA controls** for data-protection matters.

2. Definitions

Capitalized terms not defined here have the meanings set out in the Main Contract or in the GDPR.

- **'Client'** – the legal entity accepting the Main Contract (regardless of subscription tier). Client's details (legal name, address, VAT/Tax ID) are captured during checkout and form part of the Main Contract.
- **'Solution'** – the hosted Langfuse platform and any associated support or professional service.

- **'Client Personal Data'** – the subset of 'Client Data' that constitutes personal data processed by Langfuse on behalf of Client via the Solution.
- **'EU Cloud' / 'US Cloud' /'HIPAA Cloud'** – the regional deployment selected by Client (cloud.langfuse.com (EU) or us.cloud.langfuse.com (US) or hipaa.cloud.langfuse.com (HIPAA - US)). **Client is responsible for selecting the deployment that satisfies its applicable data-protection obligations.**
- **'Affiliate'** - any entity that controls, is controlled by, or is under common control with a party.
- **'De-Identified Data'** means data that cannot reasonably identify a natural person, Client, or Client account, taking into account reasonable technical and organizational measures.
- **'Controller'** and **'Processor'** – have the meanings given in the Applicable Data-Protection Laws; Client is the Controller of Client Personal Data and Langfuse is the Processor.
- **'Applicable Data-Protection Laws'** – the EU GDPR, UK GDPR, CCPA, and any national laws that amend or replace them.

All other GDPR terms (Controller, Processor, etc.) shall have the meanings given in the GDPR.

---

3. Scope, Instructions & Responsibilities

Langfuse will Process Client Personal Data **only**:
(i) to provide, maintain, secure and support the Solution,
(ii) as documented in this DPA and the Main Contract, and
(iii) to comply with law or Client's documented instructions.

Processing continues for the term of the Main Contract **and** until deletion of Client Personal Data in accordance with Section 9 (*Deletion & Return*).

Langfuse may use Solution-Generated Data (as defined in the MSA, i.e. data that cannot reasonably identify a natural person, Client, or Client account) to operate, analyze, and improve the Solution. Langfuse will not sell Client Personal Data to third parties and will not use Client Personal Data to train AI models or for advertising.

Processing on documented instructions. Langfuse will process Client Personal Data **solely on documented instructions from Client**, unless Union or Member-State law to which Langfuse is subject requires other processing; in such case Langfuse will inform Client of that legal requirement unless prohibited by law. If Langfuse reasonably believes an instruction infringes the GDPR or other Union-or Member-State data-protection rules, it will promptly notify Client and may suspend execution until the instruction is confirmed, modified or withdrawn.

Client responsibilities. Client is responsible for (a) ensuring that its instructions are lawful and that a valid legal basis exists for all Processing; (b) the accuracy, quality and legality of Client Personal Data; and (c) fulfilling controller obligations under Articles 33–36 GDPR.

---

4. Sub-Processors

1. **Authorised List.** The current list of authorised sub-processors for each instance of Langfuse is published at: https://langfuse.com/security/subprocessors
2. **Affiliates.** Client authorizes Langfuse to engage its Affiliates as sub-processors subject to written agreements imposing data-protection obligations no less protective than this DPA.
3. **Notification & Objection.** Langfuse will notify Client (via email) at least **30 days** before authorising a new sub-processor. Client may object on reasonable data-protection grounds within that period. If the parties cannot resolve an objection, Client's **sole and exclusive remedy** for such objection shall be to cancel the Main Contract - which it may do without notice period - in which

case Langfuse will provide a pro-rated refund of any prepaid fees covering the period after cancellation.

4. **Data-Transfer Mechanisms.** Transfers to sub-processors outside the EEA/UK/Switzerland will rely on an approved transfer mechanism (e.g. EU SCCs, UK IDTA, or participation in the EU–US Data Privacy Framework).

---

5. Security Measures

Langfuse will implement and maintain the technical and organisational measures ('TOMs') described in **Annex 2** (as updated from time to time). Material reductions will not be implemented without reasonable notice to Client.

Personnel confidentiality. All Langfuse employees and other recipients and subprocessor personnel who have access to Client Personal Data are bound by written confidentiality agreements or statutory duties of confidentiality **and receive regular privacy and security training appropriate to their role**.

Langfuse may update or modify the TOMs, without invoking Section 12, provided that such updates do not materially diminish the overall security of the Solution.

Langfuse maintains **ISO 27001** and **SOC 2 Type II** attestations. Further information on Langfuse's security posture & audit reports can be viewed or requested via https://langfuse.com/security.

---

6. Data Subject Rights & Regulatory Cooperation

Langfuse shall provide reasonable assistance (taking into account the nature of Processing and information available) for Client to respond to Data Subject requests or supervisory authority enquiries. Where possible, self-service functionality will be used. Additional assistance beyond self-service may be chargeable on a time-and-materials basis.

---

7. Security Incidents & Regulatory Support

Upon becoming aware of a Security Incident affecting Client Personal Data, Langfuse will notify Client **without undue delay** (and in no event later than 72 hours). Where required, Langfuse will provide information sufficient to allow Client to meet its regulatory obligations.
Langfuse will provide reasonable assistance (at Client's cost where such assistance is non-routine) for Client to notify data-protection authorities or affected data subjects (e.g. in accordance with Articles 33 and 34 GDPR).

---

8. Audits

Third-Party Reports. Annual SOC 2 (Type II) or ISO 27001 certificates shall ordinarily satisfy Client's audit rights to the extent permitted by Data Protection Laws.

Additional audits. Only if required by authority or material issue or if the reports referenced in Section 8.1 do not provide sufficient evidence of Langfuse's compliance with this DPA, Langfuse shall make available to Client all information reasonably necessary to demonstrate such compliance and, at Client's cost, allow for and contribute to audits—including on-site inspections—conducted by Client or its appointed

independent auditor, in each case solely and strictly scoped to assess compliance with this DPA. Any such audit shall be subject to (i) at least 30 days' prior written notice, (ii) reasonable confidentiality and security safeguards imposed by Langfuse, and (iii) a limit of one on-site audit in any rolling 12-month period unless a material breach is reasonably suspected or as otherwise required by a competent supervisory authority.

---

9. Deletion & Return of Data

Deletion requests during the Term. Where the Solution includes self-service deletion or data-redaction features, Client shall use those features to delete Client Personal Data. Langfuse-assisted deletion during the Term may be provided where such service is not available.

Deletion after termination. No later than **30 days** following termination of the Main Contract (or earlier upon written request), Langfuse will delete or return (and thereafter delete) Client Personal Data, unless retention is required by law.

Notwithstanding the foregoing, Langfuse may retain copies of Client Personal Data **(a)** in secure back-up archives that are isolated from active systems and retained in the ordinary course of business and **(b)** as strictly necessary for the establishment, exercise or defence of legal claims or to demonstrate compliance with this DPA.

---

10. International Transfers

Langfuse will implement an appropriate transfer mechanism for each transfer, including the EU SCCs (Decision 2021/914) using Module 2 and/or Module 3 as applicable; the UK IDTA/Addendum; and the Swiss addendum. Where Langfuse relies on the EU-US Data Privacy Framework, it will maintain self-certification and, if DPF ceases to apply, the SCCs (with relevant addenda) will automatically govern.

Data processed in the **EU Cloud** remains within the EEA (or equivalent adequacy jurisdictions) by default. Where Langfuse or its Affiliates must access or process such data from outside the EEA (for example, to deliver follow-the-sun support), it shall do so only under a valid transfer mechanism compliant with Chapter V GDPR and, where required by Article 46 GDPR, will inform Client in advance.

Data processed in the **US Cloud** is primarily hosted in the United States; Langfuse relies on the EU Standard Contractual Clauses (Module 2 and/or 3) and/or the EU–US Data Privacy Framework for such transfers.

Data processed in **HIPAA Cloud**: PHI is hosted in a dedicated, HIPAA-compliant environment in the United States. Transfers rely on the same mechanisms as the US Cloud, supplemented by the Langfuse HIPAA Business Associate Agreement (BAA).

---

11. Main Contract Governance

Indemnity & Liability: Each party's aggregate liability and indemnities relating to Processing are governed by the Main Contract.

Governing Law: The governing law and forum/venue for any dispute arising out of or relating to this DPA are the same as those specified in the Main Contract (currently either California, San Francisco courts, or Berlin, Germany courts, as applicable under the Main Contract), excluding its conflict-of-laws rules.

Precedence: If there is a conflict on the same subject matter: (1) for PHI, the BAA controls; (2) for Personal Data (excluding PHI), the DPA controls; otherwise, the MSA controls. Where information qualifies as both PHI and Personal Data, the BAA controls and the DPA applies only where not inconsistent with the BAA.

Termination: This DPA is coterminous with the Main Contract and may be terminated only in accordance with the Main Contract (except where expressly provided herein, including Section 4). Upon expiry or termination, Processor will Process Client Personal Data solely to wind down the Solutions and to return/delete data per Section 9; Sections 5, 7–9, and 11 (and any provisions intended to survive) survive to the extent applicable.

---

12. Changes to this DPA

Langfuse may modify this DPA from time to time to reflect changes in applicable law, new Solutions or practices and/ or updated transfer clauses.

Langfuse will provide at least 30 days' notice (via email) of any modification. Continued use of the Solution after the notice period constitutes acceptance. Client's sole and exclusive remedy if it objects to a modification is to cancel the Solution before the effective date, and Langfuse will refund any prepaid fees that relate to the period after cancellation.

---

13. Notices

Method of notice. All legal notices under this DPA are to be sent (i) to Client at the primary email address associated with the account used to subscribe to the Solution, and (ii) to Langfuse at legal@langfuse.com. Notices are deemed received when the sending server records transmission. Notices are governed by the Main Contract's notice clause.

Execution

Acceptance & execution. *This DPA is incorporated into the Main Contract and becomes effective upon the Parties' execution of the Main Contract or an Order Form (including via a legally valid electronic signature or click-accept). The Parties agree that such execution constitutes execution of Annex I.A of the EU SCCs (Decision (EU) 2021/914) and of the UK and Swiss addenda included in Annex 4, with the selections and Annexes completed herein. No additional signatures are required.*

Optional countersignature. *Upon Client's written request, Langfuse will provide a countersigned copy of this DPA for record-keeping. The effectiveness of this DPA and the SCCs does not depend on a separate signature.*

Annex 1 – Details of Processing

Item	Description
Purpose of processing	Contractual provision of the Langfuse platform
Scope of processing	Processing necessary to provide, secure, support, maintain and improve the Solution
Types of personal data	Names, email addresses and other identifiers of Client's users; Application content, prompts/outputs, traces, logs and identifiers provided by Client (collectively 'Client Personal Data')
Categories of data subjects	Client's employees and other users ('users'); Individuals referenced in communication content ('data subjects of the Client')
Special Categories / Sensitive Data.	Client will not submit Special Categories of Personal Data (GDPR Arts. 9–10) or Sensitive Personal Information under CPRA/CCPA to non-HIPAA environments. For HIPAA workloads, PHI may be processed only in the HIPAA Cloud under the BAA. Any exception must be expressly agreed in writing and appropriately configured.

Annex 2 – Technical and Organisational Measures (TOMs) implemented by Langfuse

The present document supplements Section 5 of this DPA and fulfils inter alia Article 32 GDPR, UK GDPR Art 32 and Cal. Civ. Code § 1798.81.5.

TOMs:

1. **Confidentiality**

1.1 **Physical Access Control** – preventing unauthorised persons from gaining access to data-processing systems.

Technical Measures

- Locking systems
- Lockable storage containers

Organisational Measures

- Physical Security Policy
- Visitors accompanied by employees
- Information Security Policy

1.2 **Logical Access Control** – preventing data-processing systems from being used by unauthorised persons.

Technical Measures

- Login with username and strong password or SSO where available
- Encryption of devices
- Enforced MFA where applicable
- Automatic desktop lock

Organisational Measures

- User-permission management
- Creating user profiles
- Information Security Policy

1.3 **Authorisation Control** – ensuring users can only access data subject to their authorisation and cannot read, copy, modify or remove Personal Data without permission.

Technical Measures

- Logging of access to applications (entering, changing, deleting data)
- SSH-encrypted access
- TLS encryption in transit

Organisational Measures

- Minimum number of administrators
- Management of user rights by administrators
- Information Security Policy

1.4 **Separation Control** – ensuring data collected for different purposes is processed separately.

Technical Measures

- Separation of production and test environments
- Multi-tenancy of relevant applications

Organisational Measures

- Control via authorisation concept
- Determination of database rights
- Information Security & Data-Protection Policies

1.5 **Pseudonymisation** – processing Personal Data so it can no longer be attributed to a specific data subject without additional information.

Technical Measures

- Separation of allocation data in encrypted systems
- Pseudonymised log files at Client request

Organisational Measures

- Internal instruction to anonymise/pseudonymise where possible
- Information Security & Data-Protection Policies

---

2. **Integrity**

2.1 **Transfer Control** – ensuring Personal Data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or transport/storage on media.

Technical Measures

- Logging of access and retrievals
- Provision via encrypted connections (SFTP, HTTPS, secure cloud stores)
- Transmission in anonymised or pseudonymised form

Organisational Measures

- Survey of regular retrieval and transmission processes
- Information Security & Data-Protection Policies

2.2 **Input Control** – ability to verify whether and by whom Personal Data has been entered, modified or removed.

Technical Measures

- Manual or automated control of logs
- Traceability through individual user names (not groups)

Organisational Measures

- Assignment of rights based on an authorisation concept
- Clear responsibilities for deletions
- Information Security Policy

---

3. **Availability and Resilience**

3.1 **Availability Control** – protecting Personal Data against accidental destruction or loss.

Technical Measures

- Hosting in certified data centres by reputable cloud providers (e.g. AWS)
- Backup concept

Organisational Measures

- Business continuity and disaster-recovery plan
- Information Security Policy

3.2 **Recoverability Control** – rapid restoration of availability and access after an incident.

Technical Measures

- Backup monitoring and reporting
- Automated restoration tools
- Regular recovery tests with logged results

Organisational Measures

- Recovery concept aligned to data criticality and Client specs
- Information Security Policy

---

4. **Regular Review, Assessment and Evaluation**

4.1 **Data-Protection Management**

- Central documentation of data-protection regulations accessible to employees
- Privacy Officer appointed
- Annual review of TOMs and updates
- Staff trained and bound to confidentiality
- Regular awareness trainings
- Processes for information obligations (Art 13/14 GDPR)
- Formal DSAR process
- Data protection in corporate risk management

4.2 **Incident Response Management**

- email security gateway, anti-malware, and filtering controls with regular updates
- Documented incident-response process covering authority notifications
- Formalised procedure for handling incidents
- Involvement of Privacy Officer and CTO
- Ticket-based documentation and follow-up of incidents

4.3 **Data Protection by Design and Default**

- No more Personal Data collected than necessary
- Privacy-friendly default settings in software

4.4 **Order Control (Sub-Processors)**

- Vendor due-diligence and DPAs/SCCs in place
- Monitoring of subcontractors
- Audit rights over contractors
- Secure deletion of data after contract end

---

5. **Organisation and Staff**

- Information-security as a core corporate objective
- Employees bound to confidentiality and data secrecy
- External parties subject to NDA before work commences

Annex 3 – Subprocessors

A current list of Langfuse's subprocessors for each Langfuse instance can be found at https://langfuse.com/security/subprocessors.

A version history of this page can be found at:
https://github.com/langfuse/langfuse-docs/commits/main/pages/security/subprocessors.mdx

Please refer to Section 4 of this DPA for further information on subprocessing.

Annex 4 – International Transfer Pack (EU SCCs + UK & Swiss Addenda)

4.1 Incorporation and Application of EU SCCs

(a) Incorporation. The Parties incorporate by reference the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries under the GDPR, set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the 'EU SCCs'), as if set out in full. The SCCs' text is not modified except to select modules/options and complete annexes.

(b) When they apply. The EU SCCs apply only to the extent Client Personal Data is transferred from the EEA (or otherwise subject to the GDPR) to a country without an adequacy decision, including remote access to such data from such country, in connection with the Solution.

(c) Modules selected.

- **Module 2 (Controller → Processor):** Selected where Client (as controller/data exporter) transfers to Langfuse (as processor/data importer) outside the EEA.
- **Module 3 (Processor → Sub-processor):** Selected for transfers from Langfuse (as processor/data exporter) to its sub-processors (data importers) outside the EEA.

(d) Options and clause selections.

- **Clause 7 (Docking clause):** Included.
- **Clause 9(a) (Use of sub-processors):** Option 2 (General written authorisation); notice period: 30 days (aligns with Section 4).
- **Clause 13 (Supervisory authority):** As determined by Clause 13 for the data exporter.
- **Clause 17 (Governing law):** German law.
- **Clause 18 (Forum and jurisdiction):** Courts of Berlin, Germany, without prejudice to data subjects' rights under the SCCs.

(e) Transfer risk assessments and supplementary measures. The Parties will perform and document transfer impact assessments as required by Clause 14 and implement supplementary measures where necessary.

4.2 EU SCCs – Annex I (completed)

A. List of Parties

- **Data exporter:** the Client as identified in the Main Contract, including its legal name, registered address and contact details as recorded therein; role: Controller (and/or Processor for onward transfers as applicable).
- **Data importer:** Langfuse GmbH, Gethsemanestr. 4, 10437 Berlin, Germany; privacy@langfuse.com; legal@langfuse.com; role: Processor.

(Additional Langfuse entities and/or sub-processors may accede pursuant to Clause 7 by executing an accession; no further Client action is required.)

B. Description of Transfer

- **Categories of data subjects:** Client's users; individuals referenced in application content/logs ('data subjects of the Client').

- **Categories of personal data:** As described in Annex 1 (e.g., names, email addresses, identifiers; application content, prompts/outputs, traces, logs and identifiers provided by Client).

- **Special category/sensitive data:** Not intended for non-HIPAA environments. For HIPAA workloads, PHI may be processed only in the HIPAA Cloud under the BAA.

- **Frequency & nature:** Continuous and as necessary to provide, secure, support, maintain and improve the Solution (hosting, storage, retrieval, transmission, display, computation, logs/monitoring, backup/DR, support).

- **Purpose:** Contractual provision of the Langfuse platform.

- **Retention:** For the term of the Main Contract and until deletion/return per Section 9 (or as required by law).

- **Subject matter & duration:** As above and coterminous with the Main Contract and post-termination wind-down/deletion period.

C. Competent Supervisory Authority

As determined by Clause 13 of the EU SCCs for the data exporter.

4.3 EU SCCs – Annex II (Technical and Organisational Measures)

The TOMs in Annex 2 are incorporated here by reference as Annex II to the EU SCCs.

4.4 EU SCCs – Annex III (List of Sub-processors)

The sub-processors in Annex 3 are incorporated here by reference as Annex III to the EU SCCs.

4.5 UK Addendum (UK GDPR)

For restricted transfers under the UK GDPR, the Parties incorporate by reference the UK Information Commissioner's International Data Transfer Addendum to the EU SCCs (Version B1.0, in force 21 March 2022) (the 'UK Addendum'). The UK Addendum varies the EU SCCs only as required by UK law.

- **Table 1 (Parties):** Exporter = the Client as identified in the Main Contract; Importer = Langfuse GmbH, Gethsemanestr. 4, 10437 Berlin, Germany.

- **Table 2 (Selected SCCs):** EU SCCs (Decision (EU) 2021/914), Module 2 and/or Module 3; Docking clause included; Clause 9 Option 2 with 30 days; Clause 17 = German law; Clause 18 = courts of Berlin, Germany.

- **Table 3 (Appendix Information):** Mirrors Annex 1–3 of this DPA.

- **Table 4 (Ending the UK Addendum):** Mandatory clauses apply; no bespoke amendments.

By executing the Main Contract or an Order Form (including via a legally valid e-signature or click-accept), the Parties are deemed to have executed the UK Addendum. No additional signatures are required.

4.6 Swiss Addendum (FADP)

For transfers subject to Swiss data protection law, the Parties agree the EU SCCs are adapted as follows (the 'Swiss Addendum'):

1. References to the 'GDPR' include the FADP where applicable; references to 'Member State' include Switzerland; references to the 'supervisory authority' include the FDPIC.

2. For Swiss-subject transfers, Clauses 17–18 are governed by Swiss law and the courts of Zurich, Switzerland, without prejudice to data subjects' rights.

3. Swiss data subjects may exercise third-party beneficiary rights in Switzerland under the SCCs as adapted.

By executing the Main Contract or an Order Form (including via a legally valid e-signature or click-accept), the Parties are deemed to have executed the Swiss Addendum. No additional signatures are required.