Persistent Flow Data Processing Agreement

Version 1.0 | November 2026 | Processor Terms under Article 28 GDPR

EFFECTIVE DATE: 10 NOVEMBER 2026

> Data Processing Agreement between **Persistent Flow AB** (Swedish corporate identity number 559586-0114), as processor, and each Organisation Customer, as controller, incorporated by reference into the Persistent Flow User Agreement.

1. PARTIES, BACKGROUND, AND ACCEPTANCE

This Data Processing Agreement ("DPA") is entered into between **Persistent Flow AB**, Swedish corporate identity number 559586-0114, Västra Finnbodavägen 9 D, 131 71 Nacka, Sweden ("Persistent Flow", "Processor"), and the Organisation Customer that has accepted the Persistent Flow User Agreement (the "User Agreement") ("Customer", "Controller"). Persistent Flow and Customer are each a "party" and together the "parties".

This DPA is incorporated into the User Agreement by reference, as set out in Section 10 of the User Agreement, and is accepted together with the User Agreement. If Customer and Persistent Flow have signed a separate data processing agreement for the Service, the signed agreement applies instead of this DPA.

This DPA sets out the terms required by Article 28(3) of the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") for the processing of personal data by Persistent Flow on behalf of Customer when providing the Service.

2. DEFINITIONS

Capitalised terms not defined in this DPA, such as Service, Workspace, Organisation Customer, Authorised User, Customer Content, Generated Output, External Service, and Order, have the meaning given to them in the User Agreement. The terms "controller", "processor", "data subject", "personal data", "processing", "personal data breach", and "supervisory authority" have the meaning given to them in the GDPR.

"Applicable Data Protection Law" means the GDPR, the Swedish Data Protection Act (lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning), and any other data protection laws of the European Union, the European Economic Area (EEA), or their member states that apply to the processing under this DPA.

"Customer Personal Data" means personal data contained in Customer Content and Generated Output within Customer's Workspaces that Persistent Flow processes on behalf of Customer when providing the Service.

"Sub-processor" means a third party engaged by Persistent Flow to process Customer Personal Data on behalf of Customer.

"Standard Contractual Clauses" or **"SCCs"** means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission in Commission Implementing Decision (EU) 2021/914, as amended or replaced from time to time.

"Restricted Transfer" means a transfer of Customer Personal Data to a country outside the EEA that is not subject to an adequacy decision under Article 45 GDPR.

3. SCOPE AND ROLES OF THE PARTIES

Customer is the controller of Customer Personal Data and Persistent Flow is the processor. Where Customer acts as a processor on behalf of a third party controller, Persistent Flow acts as Customer's sub-processor, and Customer is responsible for ensuring that its instructions are authorised by that controller.

This DPA does not apply to personal data that Persistent Flow processes as an independent controller, including account management, billing, security logging, support, and direct user communications, or to Personal Flows of individual users that are not administered by Customer. That processing is described in the Persistent Flow Privacy Policy.

4. SUBJECT MATTER, DURATION, NATURE, AND PURPOSE

The subject matter of the processing is the provision of the Service to Customer under the User Agreement. The processing continues for the term of the User Agreement and for the retrieval and deletion periods described in Section 13. The nature and purpose of the processing, the types of personal data, and the categories of data subjects are described in Annex I.

5. CUSTOMER OBLIGATIONS

Customer is responsible for complying with Applicable Data Protection Law as controller, including: (a) establishing a lawful basis for all Customer Personal Data submitted to or imported into the Service; (b) providing data subjects with the information required by Articles 13 and 14 GDPR; (c) ensuring that its instructions to Persistent Flow are lawful; (d) configuring Workspaces, access rights, and membership so that data is only available to those who should have access, taking into account that labels and tags inside a Workspace are not permission boundaries, as described in Section 6 of the User Agreement; and (e) verifying, before submitting special categories of personal data, that appropriate safeguards are in place, as required by Section 12 of the User Agreement.

Customer is responsible for the decision to enable any External Service, and for having an appropriate agreement with the provider of that External Service where required.

6. DOCUMENTED INSTRUCTIONS

Persistent Flow processes Customer Personal Data only on documented instructions from Customer, including with regard to transfers of personal data to a third country, unless required to do so by Union or member state law to which Persistent Flow is subject. In that case, Persistent Flow will inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

Customer's documented instructions consist of: (a) the User Agreement and this DPA; (b) Customer's configuration and use of the Service, including the actions of its administrators and Authorised Users; (c) the enabling of connections to External Services, which constitutes an instruction to transmit relevant data to those External Services, as set out in Section 13 of the User Agreement; and (d) any other reasonable written instructions given by Customer and accepted by Persistent Flow. Additional instructions that go beyond the agreed scope of the Service may be subject to agreement on fees.

Persistent Flow will immediately inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law. Persistent Flow is not required to carry out an instruction that it reasonably considers to be unlawful.

7. CONFIDENTIALITY OF PERSONNEL

Persistent Flow ensures that all persons authorised to process Customer Personal Data, including employees and contractors, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Access is limited to persons who need it to provide, support, secure, and maintain the Service.

8. SECURITY OF PROCESSING

Persistent Flow implements the technical and organisational measures described in Annex II, which are designed to ensure a level of security appropriate to the risk, as required by Article 32 GDPR. Customer acknowledges that the Service is provided in an early access phase, as described in Section 5 of the User Agreement, and that it has assessed the measures in Annex II as appropriate for the Customer Personal Data it submits.

Persistent Flow may update the measures in Annex II as the Service develops, provided that the overall level of protection is not materially reduced, consistent with Section 11 of the User Agreement.

9. SUB-PROCESSORS

General written authorisation: Customer gives Persistent Flow general written authorisation to engage Sub-processors. The Sub-processors engaged at the date of this DPA are listed in Annex III and at [https://www.persistentflow.com/subprocessors].

Sub-processor obligations: Persistent Flow imposes on each Sub-processor, by written contract, data protection obligations that provide at least the same level of protection as this DPA, in particular sufficient guarantees to implement appropriate technical and organisational measures. Persistent Flow remains fully liable to Customer for the performance of each Sub-processor's obligations, in accordance with Article 28(4) GDPR.

Notice of changes: Persistent Flow will notify Customer of any intended addition or replacement of a Sub-processor at least [thirty (30) days] before the new Sub-processor starts processing Customer Personal Data, by updating the list at [https://www.persistentflow.com/subprocessors] and by email to Customer's account administrators or by prominent notification in the Service. Where a replacement is urgently needed for security reasons or to keep the Service running, Persistent Flow may give shorter notice, and will then notify Customer as soon as possible.

Right to object: Customer may object to a new Sub-processor on reasonable grounds relating to data protection by notifying legal@persistentflow.com in writing within the notice period. The parties will discuss the objection in good faith. If Persistent Flow cannot reasonably accommodate the objection, Customer may, as its sole remedy, terminate the affected part of the Service by written notice before the new Sub-processor starts processing Customer Personal Data, and will receive a pro-rata refund of any prepaid fees for the unused part of the billing period. If Customer does not object within the notice period, the new Sub-processor is deemed accepted.

Default model inference provider: Persistent Flow contracts a provider to perform default model inference within the Service, currently Grunden AI AB in Sweden, and that provider is a Sub-processor listed in Annex III. Persistent Flow may replace this provider. Any replacement will perform inference within the EU/EEA, with the aim of keeping it in Sweden, and the notice and objection procedure in this section applies to the replacement.

External Services (bring your own provider): The Service is designed so that Customer uses its own account with AI model providers of its choice, for example OpenAI, Anthropic, or European providers such as Grunden AI or evroc. Persistent Flow has no contracts of its own with OpenAI or Anthropic. AI model providers that Customer uses with its own account or API key, and client tools such as Cursor, Slack, or Salesforce, are External Services and not Sub-processors of Persistent Flow. They receive data on Customer's instruction, as set out in Section 6, and process it under Customer's own terms with them.

10. ASSISTANCE WITH DATA SUBJECT REQUESTS

Taking into account the nature of the processing, Persistent Flow will assist Customer, by appropriate technical and organisational measures, insofar as this is possible, in fulfilling Customer's obligation to respond to requests from data subjects exercising their rights under Chapter III GDPR. The Service includes functions for export, rectification, and retirement of records, and irreversible erasure can be requested via an authenticated administrative request to hello@persistentflow.com, as described in Section 19 of the User Agreement.

If Persistent Flow receives a request directly from a data subject concerning Customer Personal Data, it will forward the request to Customer without undue delay where it can identify Customer, and will not respond to the request itself except to direct the data subject to Customer, unless Customer instructs otherwise or the law requires it.

11. ASSISTANCE WITH SECURITY, IMPACT ASSESSMENTS, AND CONSULTATION

Taking into account the nature of the processing and the information available to it, Persistent Flow will provide Customer with reasonable assistance in ensuring compliance with Articles 32 to 36 GDPR, including in relation to security of processing, data protection impact assessments, and prior consultation with a supervisory authority. Persistent Flow will primarily provide this assistance by making available documentation about the Service, including this DPA and its Annexes.

Persistent Flow may charge reasonable fees for assistance that goes beyond the documentation and functions it ordinarily makes available, except where the need for assistance results from Persistent Flow's breach of this DPA.

12. PERSONAL DATA BREACH NOTIFICATION

Persistent Flow will notify Customer without undue delay, [and where feasible within forty-eight (48) hours,] after becoming aware of a personal data breach affecting Customer Personal Data. The notification will be sent to Customer's account administrators and will, to the extent then known, describe: (a) the nature of the breach, including where possible the categories and approximate number of data subjects and records concerned; (b) the name and contact details of a contact point at Persistent Flow; (c) the likely consequences of the breach; and (d) the measures taken or proposed to address the breach and to mitigate its possible adverse effects. Where it is not possible to provide all information at the same time, it may be provided in phases without undue further delay.

Persistent Flow will take reasonable steps to contain and investigate the breach and will cooperate with Customer so that Customer can meet its obligations under Articles 33 and 34 GDPR. Customer is responsible for notifying the supervisory authority and data subjects where required. A notification under this section is not an acknowledgement of fault or liability. Customer should report suspected security incidents to security@persistentflow.com.

13. DELETION AND RETURN OF DATA

On termination or expiry of the User Agreement, switching to another provider, or discontinuation of the Service, Customer may export Customer Personal Data using the export functions described in Section 19 of the User Agreement, in structured machine-readable formats such as JSON, CSV, and PDF, without switching charges. The export functions remain available during a retrieval window of at least thirty (30) calendar days, as set out in Sections 19, 20, and 21 of the User Agreement. The return of data under this DPA takes place through these export functions.

After the retrieval window has ended, Persistent Flow will delete Customer Personal Data, including by cryptographic erasure, unless Union or member state law requires its storage. Copies held in encrypted backups are overwritten in the ordinary backup cycle within [thirty-five (35) days]. On written request, Persistent Flow will confirm the deletion in writing. Customer may also request irreversible erasure of a Workspace or data scope at any time during the term via an authenticated administrative request to hello@persistentflow.com.

In the event of insolvency or winding down of Persistent Flow, Section 22 of the User Agreement applies, and Customer Personal Data will, where practically possible, be made available for export before the Service is shut down and will then be deleted.

14. AUDITS AND INFORMATION

Persistent Flow will make available to Customer all information necessary to demonstrate compliance with Article 28 GDPR and this DPA, and will allow for and contribute to audits, including inspections, conducted by Customer or an independent auditor mandated by Customer, as follows.

Documentation first: Customer agrees that audit requests will first be addressed through written documentation, such as this DPA and its Annexes, security documentation, answers to reasonable security questionnaires, and summaries of third-party audits or certifications where available.

On-site audits: If Customer reasonably considers that the documentation is not sufficient to demonstrate compliance, Customer may carry out an audit, including an inspection, on giving at least [thirty (30) days'] written notice. Audits will be carried out during normal business hours, without unreasonable disruption to Persistent Flow's business, and in a way that protects the confidentiality and security of other customers' data. The auditor must be bound by confidentiality and must not be a competitor of Persistent Flow. Customer bears its own costs and reimburses Persistent Flow's reasonable costs for the audit.

Frequency: Audits may take place at most once in any twelve (12) month period, unless an audit is required by a supervisory authority or follows a personal data breach affecting Customer Personal Data. Audits of Sub-processors are carried out through the information Persistent Flow receives from them, unless the law requires otherwise.

15. INTERNATIONAL TRANSFERS

Core primary storage is hosted in Sweden by Cleura AB. Default model inference is currently performed in Sweden by Grunden AI AB, and will remain within the EU/EEA if the inference provider is replaced, with the aim of keeping it in Sweden. Selected authentication, telemetry, and integration Sub-processors may process limited metadata outside the EEA, as described in Section 11 of the User Agreement and in Annex III. Persistent Flow will only make or permit a Restricted Transfer of Customer Personal Data in compliance with Chapter V GDPR, for example on the basis of the EU-U.S. Data Privacy Framework for certified recipients, or of the SCCs.

SCCs incorporated where needed: Where a Restricted Transfer takes place between Customer and Persistent Flow, the SCCs are incorporated into this DPA by reference, using Module Two (controller to processor) or Module Three (processor to processor) as applicable, or Module Four (processor to controller) where Customer is located outside the EEA. For this purpose: (a) the optional docking clause in Clause 7 applies; (b) Option 2 of Clause 9 (general written authorisation) applies with the notice period set out in Section 9; (c) the optional wording in Clause 11 does not apply; (d) the competent supervisory authority under Clause 13 is the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten, IMY); (e) the governing law under Clause 17 and the courts under Clause 18 are those of Sweden; and (f) Annexes I to III of this DPA complete the annexes to the SCCs. Where Persistent Flow engages a Sub-processor that makes a Restricted Transfer, Persistent Flow will put in place the SCCs or another valid transfer mechanism with that Sub-processor.

Transfers to External Services that Customer enables take place on Customer's instruction, and Customer is responsible for ensuring that a valid transfer mechanism exists for such transfers.

16. LIABILITY

Each party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability in the User Agreement, including Sections 25 and 27, to the extent permitted by Article 82 GDPR and other Applicable Data Protection Law. Liability under this DPA and the User Agreement is counted together and is not cumulative. Nothing in this DPA limits the rights of data subjects under Article 82 GDPR, or liability that cannot be limited under applicable law, including liability for intentional misconduct or gross negligence.

17. DURATION AND SURVIVAL

This DPA applies from the date the User Agreement is accepted and remains in force for as long as Persistent Flow processes Customer Personal Data on behalf of Customer, including during the retrieval window and deletion periods described in Section 13. If the User Agreement is assigned or transferred under Section 22 of the User Agreement, this DPA is transferred together with it and with Customer Personal Data.

18. ORDER OF PRECEDENCE

In the event of a conflict, the following order of precedence applies: (a) the SCCs, where incorporated under Section 15; (b) this DPA; and (c) the User Agreement and any Order, as set out in Section 33 of the User Agreement. In matters of personal data processing, this DPA prevails over the User Agreement and any Order, unless a signed agreement expressly states that it overrides this DPA.

19. CHANGES TO THIS DPA

Persistent Flow may update this DPA in accordance with Section 31 of the User Agreement, or where required to comply with Applicable Data Protection Law, decisions of a supervisory authority, or changes to the SCCs. Changes will not reduce the overall level of protection of Customer Personal Data, unless the change is required by law.

20. GOVERNING LAW AND JURISDICTION

This DPA is governed by the substantive laws of Sweden, without regard to conflict of law principles. Any dispute arising out of or in connection with this DPA shall be submitted to the exclusive jurisdiction of the Stockholm District Court (Stockholms tingsrätt) as the court of first instance, consistent with Section 34 of the User Agreement. Where the SCCs apply, disputes under the SCCs are governed by the SCCs.

21. CONTACT DETAILS

Persistent Flow AB | Reg. No: 559586-0114 | Västra Finnbodavägen 9 D, 131 71 Nacka, Sweden

Data protection and legal: legal@persistentflow.com | Security incidents: security@persistentflow.com | Erasure & Admin: hello@persistentflow.com | Web: https://www.persistentflow.com

ANNEX I: DESCRIPTION OF THE PROCESSING

Item	Description
Controller	Customer, as identified in its account and Order. Contact: the account administrators registered in the Service.
Processor	Persistent Flow AB, 559586-0114, Västra Finnbodavägen 9 D, 131 71 Nacka, Sweden. Contact: legal@persistentflow.com.
Categories of data subjects	Authorised Users; Customer's employees, contractors, and representatives; and Customer's clients, business contacts, meeting participants, and other individuals whose personal data appears in Customer Content, for example in imported emails, messages, documents, meeting notes, or CRM records.
Categories of personal data	Identification and contact details (such as name, email address, phone number, job title, and employer); content of communications, documents, notes, memories, and decision logs; information about work activities, opinions, and decisions recorded in Customer Content; Generated Output relating to individuals, such as summaries, recalled facts, context graphs, and synthetic personas or "Soul" profiles; user identifiers, provenance data, and audit trails linked to Workspace activity; and integration metadata needed to route data to and from External Services.
Special categories of personal data	Not intended. Customer must not submit special categories of personal data (Article 9 GDPR) or data relating to criminal convictions (Article 10 GDPR) unless it has verified in advance that appropriate safeguards are in place, as required by Section 12 of the User Agreement. If such data is submitted, it is protected by the measures in Annex II.
Frequency of processing	Continuous, for as long as Customer uses the Service.
Nature of the processing	Hosting, storage, encryption, indexing, embedding, entity extraction, search and recall, AI model inference and generation of output, transmission to External Services as instructed by Customer, backup, export, and deletion.
Purpose of the processing	Providing, supporting, securing, and maintaining the Service for Customer in accordance with the User Agreement and Customer's documented instructions.
Retention	For the term of the User Agreement or until Customer deletes the data or requests erasure, followed by a retrieval window of at least thirty (30) calendar days, after which the data is deleted. Encrypted backups are overwritten within [thirty-five (35) days], as described in Section 13.
Transfers to Sub-processors	As listed in Annex III, for the purposes and in the locations stated there.
Competent supervisory authority	Integritetsskyddsmyndigheten (IMY), Sweden, www.imy.se.

ANNEX II: TECHNICAL AND ORGANISATIONAL MEASURES

Persistent Flow is a young company and the Service is in an early access phase. The measures below describe what the Service is designed to do at the date of this DPA. They will be strengthened as the company and the Service grow, and they may change as described in Section 8. Persistent Flow does not currently hold third-party security certifications [to confirm].

Encryption at rest: Memory bodies are designed to be encrypted at rest using tenant-specific cryptographic keys. Search indices, entity graphs, and metadata may use distinct indexing safeguards to allow contextual recall. Cryptographic erasure is used as part of deletion.

Encryption in transit: Data transmitted between users, the Service, Sub-processors, and External Services is designed to be protected using TLS encryption [version to confirm, for example TLS 1.2 or higher].

Access control: Access to Customer Personal Data is enforced at the Workspace level, with administrative roles and membership controls. Internal access to production systems is limited to authorised personnel on a need-to-know basis, using individual accounts and [multi-factor authentication, to confirm]. Access rights are reviewed [regularly, frequency to confirm].

Tenant separation: Customer Content is designed to be logically separated by tenant and Workspace, using tenant-specific keys.

Logging and monitoring: Security-relevant events, administrative actions, and access to production systems are designed to be logged, and logs are kept for [12 months] to support investigation of incidents.

Backups and availability: Customer Content is backed up [frequency to confirm] in encrypted form, with backups stored in Sweden by Persistent Flow's hosting Sub-processor Cleura AB [to confirm]. Backups are overwritten within [thirty-five (35) days]. Restore procedures are [tested periodically, to confirm].

Incident response: Persistent Flow maintains a procedure for detecting, assessing, containing, and documenting security incidents and personal data breaches, and for notifying Customer as described in Section 12. Incidents can be reported to security@persistentflow.com.

Staff confidentiality and training: All personnel and contractors with access to Customer Personal Data are bound by written confidentiality obligations and receive instructions on data protection and security.

Secure development and vulnerability management: Changes to the Service are reviewed before release, dependencies are kept up to date, and security vulnerabilities are prioritised and fixed based on risk.

Data minimisation: Persistent Flow processes Customer Personal Data only as needed to provide the Service, and uses aggregated service analytics, not Customer Content, to improve the Service. Customer Content is not used to train general-purpose foundational models without Customer's affirmative, explicit written consent.

Sub-processor management: Sub-processors are selected based on their ability to provide sufficient guarantees, and are bound by written data protection terms as described in Section 9.

Physical security: Physical security of data centres is provided by Persistent Flow's hosting Sub-processors, as described in their security documentation.

ANNEX III: LIST OF SUB-PROCESSORS

Status: The first two rows are confirmed Sub-processors. Rows marked EXAMPLE ROW are placeholders that must be confirmed before they apply, and no provider in such a row is confirmed as engaged. The current and binding list is published at [https://www.persistentflow.com/subprocessors].

Provider	Purpose	Location	Transfer mechanism
Cleura AB (reg. no. 556630-7806), Sweden	Core primary storage, compute, and encrypted backups	Sweden	Not applicable (no transfer outside the EEA)
Grunden AI AB (reg. no. 559341-9129), Sweden	Default model inference, current provider. A replacement will remain within the EU/EEA, with the aim of Sweden, and is notified under Section 9	Sweden	Not applicable (no transfer outside the EEA)
[Authentication provider, to confirm] (EXAMPLE ROW)	User sign-in and single sign-on	[to confirm]	[SCCs or EU-U.S. Data Privacy Framework, to confirm]
[Cloudflare, Inc., if used, to confirm] (EXAMPLE ROW)	Content delivery, DNS, and protection against network attacks	[Global network, to confirm]	[EU-U.S. Data Privacy Framework and SCCs, to confirm]
[Email provider, to confirm] (EXAMPLE ROW)	Transactional and service emails	[to confirm]	[to confirm]
[Newsletter email provider, to confirm] (EXAMPLE ROW)	Sending newsletters. Processes subscriber data for which Persistent Flow is controller, listed for transparency	[to confirm]	[to confirm]
[Telemetry and error monitoring provider, to confirm] (EXAMPLE ROW)	Error logs and limited usage metadata	[to confirm]	[to confirm]
[Support tool, to confirm] (EXAMPLE ROW)	Handling of support requests	[to confirm]	[to confirm]
[Payment provider, to confirm] (EXAMPLE ROW)	Payment processing for billing. Processes billing data for which Persistent Flow is controller, listed for transparency	[to confirm]	[to confirm]

AI model providers that Customer uses with its own account or API key (for example OpenAI, Anthropic, Grunden AI, or evroc) and other External Services are not Sub-processors and are therefore not listed here, as described in Section 9. Persistent Flow has no contracts of its own with OpenAI or Anthropic.