Persistent Flow Privacy Policy

Version 1.0 | November 2026 | Privacy Notice under the GDPR

EFFECTIVE DATE: 10 NOVEMBER 2026

> This Privacy Policy explains how **Persistent Flow AB** (Swedish corporate identity number 559586-0114) collects and uses personal data when you use its websites and its managed memory, context layer, and AI integration services.

1. ABOUT THIS PRIVACY POLICY

This Privacy Policy describes how **Persistent Flow AB** ("Persistent Flow", "we", "us") processes personal data in connection with the Persistent Flow websites, accounts, applications, APIs, Model Context Protocol (MCP) interfaces, Personal Flows, shared Workspaces, and related services (collectively, the "Service"). It is provided in accordance with Articles 13 and 14 of the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") and the Swedish Data Protection Act (lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning).

Capitalised terms that are not defined in this Privacy Policy, such as Personal Flow, Workspace, Organisation Customer, Authorised User, Consumer, Customer Content, Generated Output, and External Service, have the meaning given to them in Section 2 of the Persistent Flow User Agreement (the "User Agreement"). This Privacy Policy explains our data practices. It does not replace the User Agreement or the Data Processing Agreement ("DPA") available at [https://www.persistentflow.com/dpa].

Data ownership is the core promise of the Service. You own your Customer Content and your Generated Output, as set out in Section 9 of the User Agreement. We process personal data only for the purposes described in this Privacy Policy, and we do not sell personal data.

2. WHO IS RESPONSIBLE FOR YOUR PERSONAL DATA

The controller for the processing described in this Privacy Policy is Persistent Flow AB, Swedish corporate identity number 559586-0114, Västra Finnbodavägen 9 D, 131 71 Nacka, Sweden. Web: https://www.persistentflow.com.

Contact for privacy matters: legal@persistentflow.com. Requests for erasure and administrative requests are handled via hello@persistentflow.com, as described in Section 14. Security incidents and suspected unauthorised access should be reported to security@persistentflow.com.

Data protection officer: Persistent Flow is not currently required to appoint a data protection officer under Article 37 GDPR, and has not done so. Our privacy contact point at legal@persistentflow.com handles all questions about how we process personal data. If we appoint a data protection officer in the future, we will update this Privacy Policy with their contact details.

3. OUR ROLES: CONTROLLER AND PROCESSOR

Persistent Flow processes personal data in two different roles, depending on whose data it is and why it is processed.

Persistent Flow as controller: We act as an independent controller for the processing of personal data that we need to run our business and the Service, including account management, billing, security logging, support, direct user communications, our websites and cookies, and any marketing, as described in Section 10 of the User Agreement

and in this Privacy Policy.

Personal Flows of individual users: When you use a Personal Flow as an individual, including as a Consumer, we act as controller for the personal data in your Customer Content and Generated Output that we process in order to provide the Service to you. We process this data only to provide, support, secure, and maintain the Service in accordance with your instructions and the User Agreement, and we do not use it for any other purpose of our own except as described in this Privacy Policy.

Persistent Flow as processor for Organisation Customers: When we process personal data within an Organisation Customer's Workspace on behalf of the Organisation Customer, we act as a processor under Article 28 GDPR, and the Organisation Customer is the controller. That processing is governed by the DPA, not by this Privacy Policy. If you are an Authorised User or another individual whose personal data appears in an Organisation Customer's Workspace, the Organisation Customer's own privacy information applies, and you should direct requests about that data to the Organisation Customer. If we receive such a request, we will forward it to the Organisation Customer where we can identify it. We still act as controller for the account, billing, security, and communication data of Authorised Users described in Section 4.

4. PERSONAL DATA WE PROCESS AND WHERE IT COMES FROM

Depending on how you use the Service, we process the following categories of personal data:

(a) Account and identity data: name, email address, username, password hash or single sign-on identifier, account settings, plan, role, and Workspace memberships.

(b) Billing and transaction data: billing name and address, company name and VAT number, invoices, plan and seat details, payment status, and limited payment card details (such as card type, last four digits, and expiry date) provided by our payment provider. We do not store full card numbers.

(c) Personal Flow content: prompts, documents, memories, notes, imported communications, uploaded files, decision logs, and other Customer Content you submit or import into your Personal Flow, and the Generated Output created from it. This content may include personal data about you and about other people.

(d) Technical, usage, and security data: IP address, device and browser information, log-in times, API and MCP request metadata, error logs, audit trails, security events, and aggregated service analytics about how features are used.

(e) Integration data: information about External Services you connect, such as the provider name, connection status, authentication tokens or API keys you supply, and limited metadata needed to route requests to and from those services.

(f) Support and communication data: messages you send to us, support tickets, feedback, notices sent under the User Agreement, and records of requests you make under this Privacy Policy.

(g) Website and cookie data: information collected through cookies and similar technologies when you visit our websites, as described in Section 18.

(h) Business contact data: names, roles, and contact details of administrators, billing contacts, and other representatives of Organisation Customers and prospective customers.

(i) Newsletter and marketing data: your email address, name if you provide it, marketing preferences, records of your consent and double opt-in confirmation, records of opt-out, and [basic open and click statistics, if used, to confirm], as described in Section 17.

Sources: We collect most personal data directly from you. We also receive personal data from an Organisation Customer that invites you to a Workspace, from authentication providers you use to sign in, from our payment provider, and from External Services you choose to connect to the Service. Personal Flow content may contain

personal data about other people that you choose to submit or import. If you submit personal data about others, you are responsible for having a lawful basis to do so.

5. PURPOSES AND LEGAL BASES

The table below sets out why we process personal data as controller and the legal basis under Article 6(1) GDPR for each purpose. Where we rely on legitimate interests, you have the right to object, as described in Section 13.

Purpose	Categories of personal data	Legal basis (Article 6(1) GDPR)
Creating and administering your account, authenticating you, and managing Workspace memberships	(a), (d), (e)	Performance of a contract (Article 6(1)(b))
Providing the Service, including storing, indexing, recalling, and creating Generated Output from your Personal Flow content	(c), (d), (e)	Performance of a contract (Article 6(1)(b))
Transmitting data to External Services that you enable	(c), (e)	Performance of a contract, based on your instruction (Article 6(1)(b))
Billing, payments, invoicing, and collection of fees	(a), (b), (h)	Performance of a contract (Article 6(1)(b))
Keeping accounting records as required by the Swedish Bookkeeping Act (bokföringslagen, 1999:1078)	(b)	Legal obligation (Article 6(1)(c))
Securing the Service, detecting and preventing fraud, abuse, and unauthorised access, and keeping security logs	(a), (d), (e)	Legitimate interests in protecting the Service, our users, and their data (Article 6(1)(f))
Providing support and handling your requests	(a), (d), (f)	Performance of a contract (Article 6(1)(b)), or legitimate interests in answering enquiries from non-customers (Article 6(1)(f))
Sending service messages, such as security alerts and notices of changes to terms, prices, or the Service	(a), (f)	Performance of a contract (Article 6(1)(b)) and legal obligation where notice is required by law (Article 6(1)(c))
Improving and developing the Service using aggregated service analytics, not Customer Content	(d)	Legitimate interests in improving our products (Article 6(1)(f))
Managing relationships with Organisation Customers and prospective customers	(h), (f)	Legitimate interests in running our business (Article 6(1)(f))
Operating our websites and using strictly necessary cookies	(d), (g)	Legitimate interests in providing a working and secure website (Article 6(1)(f))
Using non-essential cookies and analytics on our websites [if used, to confirm]	(g)	Consent (Article 6(1)(a))
Sending newsletters and product updates to people who have signed up	(i)	Consent (Article 6(1)(a))
Sending marketing about our own similar services by email to existing customers, where permitted by the Swedish Marketing Act [optional, to confirm]	(a), (i)	Legitimate interests in marketing our services, with a right to opt out at any time (Article 6(1)(f))
Keeping a minimal suppression record so that we do not email people who have unsubscribed	(i)	Legitimate interests in respecting your opt-out (Article 6(1)(f))

Purpose	Categories of personal data	Legal basis (Article 6(1) GDPR)
Handling notices of illegal content, appeals, and requests from authorities, and complying with other legal obligations	(a), (c), (d), (f)	Legal obligation (Article 6(1)(c))
Establishing, exercising, or defending legal claims	All relevant categories	Legitimate interests in protecting our legal rights (Article 6(1)(f))
Carrying out a merger, acquisition, or other transfer of our business as described in Section 22 of the User Agreement	All relevant categories	Legitimate interests in carrying out the transaction (Article 6(1)(f))
Training general-purpose foundational models, only if you have given affirmative, explicit written consent	(c)	Consent (Article 6(1)(a))

Special categories of personal data: We do not ask for special categories of personal data (Article 9 GDPR), and the Service is not intended as a repository for such data, as described in Section 12 of the User Agreement. If you choose to store such data in your Personal Flow, we process it only to provide the Service to you in accordance with your instructions, and you should only do so where you are comfortable with the safeguards described in this Privacy Policy. [Legal basis under Article 9(2) to be confirmed in legal review.]

6. HOW LONG WE KEEP PERSONAL DATA

We keep personal data only for as long as it is needed for the purposes described in Section 5, or for as long as the law requires. Periods shown in brackets are provisional and will be confirmed before this Privacy Policy takes effect.

Category	Retention period
Account and identity data	For as long as your account is active. After closure or erasure of your account, deleted within [30 days], subject to the retrieval window described below and any legal retention duty.
Personal Flow content and Generated Output	For as long as your account is active, or until you request erasure. Retired records are excluded from active recall but necessary audit trails are kept, as described in Section 19 of the User Agreement. After termination, switching, or discontinuation, you have a retrieval window of at least 30 calendar days to export your data, after which it is permanently deleted. Encrypted backup copies are overwritten within [35 days] after deletion.
Billing and accounting records	Seven (7) years after the end of the calendar year in which the financial year ended, as required by the Swedish Bookkeeping Act.
Security and audit logs	[12 months] from the date of the event, or longer where needed to investigate a specific security incident or legal claim.
Technical and usage data, website server logs	[90 days]. Aggregated service analytics that no longer identify any person may be kept for longer.
Integration data (tokens and connection metadata)	Until you disconnect the External Service or your account is closed. Tokens are deleted or revoked when the connection is removed.
Support and communication data	[24 months] after the support case or communication is closed.
Records of privacy and erasure requests	[36 months] after the request was handled, to show that we complied.
Business contact data	For as long as the business relationship continues and [24 months] thereafter.

Category	Retention period
Newsletter and marketing data	Until you unsubscribe or withdraw your consent, after which your address is removed from the mailing list without undue delay. Open and click statistics, if used, are kept for [12 months]. A minimal suppression record (your email address and the date of opt-out) is kept for as long as needed to honour your opt-out.
Cookie data	As set out in the cookie information described in Section 18.
Data needed for legal claims	For as long as needed to establish, exercise, or defend the claim, up to the applicable limitation period.

7. AI PROCESSING AND NO GENERAL MODEL TRAINING

The Service uses AI models to process your Customer Content, for example to index and search it, extract facts and entities, build context graphs, summarise documents and meetings, and generate responses and other Generated Output. This processing happens automatically when you use the relevant features, and it is necessary to provide the Service you have asked for.

Default model inference provided by Persistent Flow is currently performed by our inference provider Grunden AI AB, in Sweden. If we replace our inference provider, default model inference will remain within the EU/EEA, and our aim is to keep it in Sweden.

Your own AI provider: The Service is designed so that you can use your own account with an AI model provider of your choice, for example OpenAI, Anthropic, or European providers such as Grunden AI or evroc. Persistent Flow does not have its own contracts with OpenAI or Anthropic. A provider that you use with your own account is an External Service, and the relevant Customer Content is sent to that provider at your instruction, as described in Section 8.

No general model training: We do not use Customer Content or Generated Output to train general-purpose foundational models without your affirmative, explicit written consent, as set out in Section 9 of the User Agreement. If you give such consent, you may withdraw it at any time with effect for the future. We do not use Customer Content to build advertising profiles.

Accuracy: Generated Output, including summaries, recalled facts, and synthetic personas or "Soul" profiles, is a computational approximation and may contain errors. Section 14 of the User Agreement explains why Generated Output should be reviewed by a human before you rely on it. You may ask us to rectify inaccurate personal data, as described in Section 13.

8. EXTERNAL SERVICES YOU ENABLE

When you enable a connection to an External Service, such as an external AI model, an MCP host application, or a client tool like Cursor, Slack, or Salesforce, this constitutes your instruction to transmit the relevant data to that External Service, as described in Section 13 of the User Agreement. This also applies to AI model providers that you use with your own account or API key, such as OpenAI, Anthropic, Grunden AI, or evroc. Such providers are not our service providers or sub-processors. The provider of the External Service processes that data under its own terms and privacy policy, which you should review. We do not control, and are not responsible for, the security, model training policies, retention, or location of processing of independent External Services.

You can stop the transmission of data to an External Service at any time by disconnecting it in your account settings. Data that has already been sent to the External Service is handled in accordance with that provider's terms.

9. WHO WE SHARE PERSONAL DATA WITH

We do not sell personal data, and we do not share it with third parties for their own marketing. We share personal data only with the following categories of recipients, and only to the extent necessary:

(a) Service providers acting on our behalf: providers of hosting, storage and backups, default model inference, authentication, content delivery and network security, email delivery, telemetry and error monitoring, customer support tools, newsletter delivery, and payment processing. Our hosting and storage provider is Cleura AB (Sweden), and our current default model inference provider is Grunden AI AB (Sweden). These providers process personal data on our instructions under written agreements. The current list of sub-processors is available at [https://www.persistentflow.com/subprocessors].

(b) External Services you enable: providers of External Services that you choose to connect, as described in Section 8.

(c) Organisation Customers: if you are an Authorised User, the Organisation Customer that administers your Workspace and its administrators, who can see your membership and your contributions to the Workspace.

(d) Professional advisors: lawyers, auditors, accountants, and insurers, under a duty of confidentiality.

(e) Authorities and courts: public authorities, courts, and law enforcement, where we are required by law to disclose personal data, or where disclosure is necessary to establish, exercise, or defend legal claims.

(f) Successors and acquirers: a buyer, successor, or affiliate in connection with a merger, acquisition, sale of assets, or reorganisation, as described in Section 22 of the User Agreement. In that case, the data protection commitments in this Privacy Policy transfer together with your data.

10. WHERE PERSONAL DATA IS PROCESSED AND INTERNATIONAL TRANSFERS

Core primary storage of Customer Content 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 providers may process limited metadata in other jurisdictions, including outside the European Economic Area (EEA), as described in Section 11 of the User Agreement.

When personal data is transferred to a country outside the EEA, we ensure that the transfer is protected by an appropriate safeguard under Chapter V GDPR, such as: (a) an adequacy decision of the European Commission, including the EU-U.S. Data Privacy Framework for recipients in the United States that are certified under it; or (b) the Standard Contractual Clauses adopted by the European Commission (Commission Implementing Decision (EU) 2021/914), together with supplementary measures where needed. You can request a copy of the relevant safeguards by contacting legal@persistentflow.com.

When you enable an External Service, data may be transferred to the location where that provider processes it, at your instruction and under that provider's own terms.

11. AUTOMATED DECISION-MAKING

We do not make decisions based solely on automated processing, including profiling, that produce legal effects concerning you or similarly significantly affect you, within the meaning of Article 22 GDPR. The AI features of the Service generate content and suggestions for you, but they do not make decisions about you.

We use automated security measures, such as rate limits and detection of suspicious log-in activity, which may temporarily restrict access to protect the Service. If you believe such a measure has affected you incorrectly, you can contact security@persistentflow.com and the matter will be reviewed by a person.

12. HOW WE PROTECT PERSONAL DATA

We use technical and organisational measures designed to protect personal data against unauthorised access, loss, and alteration. Memory bodies are designed to be encrypted at rest using tenant-specific cryptographic keys, data in transit is designed to be protected using TLS encryption, and access to production systems is restricted to authorised personnel who need it for their work and who are bound by confidentiality. Section 11 of the User Agreement describes our security architecture and hosting boundaries in more detail.

Persistent Flow is a young company, and the Service is currently provided in an early access phase, as described in Section 5 of the User Agreement. We work continuously to make the Service as safe as we reasonably can, and our security measures and certifications will expand as the company grows. No system is completely secure, and we recommend that you keep your own copies of important Customer Content. If a personal data breach is likely to result in a high risk to your rights and freedoms, we will inform you without undue delay, as required by Article 34 GDPR.

13. YOUR RIGHTS

Under the GDPR you have the following rights regarding personal data for which we are controller:

Right of access (Article 15): You may ask whether we process personal data about you and receive a copy of it, together with information about how it is processed.

Right to rectification (Article 16): You may ask us to correct inaccurate personal data and to complete incomplete personal data.

Right to erasure (Article 17): You may ask us to erase your personal data, for example where it is no longer needed or where you withdraw your consent. Erasure may be limited where we must keep data by law, such as accounting records.

Right to restriction (Article 18): You may ask us to restrict processing, for example while we check the accuracy of data or assess an objection.

Right to data portability (Article 20): You may receive personal data you have provided to us in a structured, commonly used, and machine-readable format, and transmit it to another controller. The export functions described in Section 19 of the User Agreement allow you to export your Customer Content and Generated Output in formats such as JSON, CSV, and PDF.

Right to object (Article 21): You may object at any time to processing based on our legitimate interests, on grounds relating to your particular situation. You may always object to direct marketing, and we will then stop using your data for that purpose.

Right to withdraw consent (Article 7(3)): Where processing is based on your consent, you may withdraw it at any time. This does not affect the lawfulness of processing carried out before the withdrawal.

14. HOW TO EXERCISE YOUR RIGHTS

You can exercise your rights by contacting legal@persistentflow.com. Requests for irreversible deletion or erasure of an account or a data scope must be submitted via an authenticated request to hello@persistentflow.com, because self-service irreversible deletion is not supported in the user interface at this time, as described in Section 19 of the User Agreement. Many rights can also be exercised directly in the Service, for example by editing account details, exporting data, or retiring records.

We may ask you to verify your identity before we act on a request, to protect your data from unauthorised access. We respond to requests without undue delay and in any event within one (1) month of receipt. This period may be extended by two (2) further months where necessary, taking into account the complexity and number of requests, in which case we will tell you why. Requests are free of charge, unless they are manifestly unfounded or excessive.

If your request concerns personal data in an Organisation Customer's Workspace, please contact the Organisation Customer, which is the controller for that data. We will assist the Organisation Customer in responding, as set out in the DPA.

15. COMPLAINTS TO THE SUPERVISORY AUTHORITY

If you are unhappy with how we process your personal data, please contact us first at legal@persistentflow.com, and we will try to resolve the matter. You also have the right to lodge a complaint with a supervisory authority. In Sweden, the supervisory authority is the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten, IMY), www.imy.se, Box 8114, 104 20 Stockholm. You may also lodge a complaint in the EU or EEA member state where you live or work, or where the alleged infringement took place.

16. CHILDREN

The Service is not intended for children under 16 years of age, as set out in Section 3 of the User Agreement. Individuals under 16 may only access the Service within an authorised, supervised educational deployment governed by a separate written institutional agreement. Users aged 16 or 17 must have parental or guardian consent where required by applicable local law. If we learn that we have collected personal data from a child under 16 outside such a deployment, we will delete it without undue delay. Please contact legal@persistentflow.com if you believe this has happened.

17. NEWSLETTERS AND MARKETING

We send newsletters and product updates by email to people who have asked to receive them. We do not sell or share your email address with third parties for their own marketing.

Consent: You sign up for our newsletter by actively opting in, for example by ticking a box that is not pre-ticked or by entering your email address in a sign-up form. Our legal basis is your consent (Article 6(1)(a) GDPR). We use double opt-in, which means that you receive an email asking you to confirm your subscription before we send you any newsletters [to confirm].

Unsubscribing: Every newsletter contains an unsubscribe link. You can withdraw your consent at any time, free of charge, by using that link or by contacting hello@persistentflow.com. When you unsubscribe, your address is removed from the mailing list without undue delay. We keep a minimal suppression record, consisting of your email address and the date of the opt-out, only so that we can make sure you do not receive further newsletters.

Existing customers [optional, to confirm]: Under the Swedish Marketing Act (marknadsföringslagen, 2008:486), we may send customers who have given us their email address in connection with a purchase marketing about our own similar products and services, without separate consent. In that case, you are clearly given the opportunity to object when your address is collected and in every message, and you can opt out at any time. Our legal basis is legitimate interests (Article 6(1)(f) GDPR).

Statistics [if used, to confirm]: Our newsletters may contain basic statistics on whether an email was opened and which links were clicked, so that we can understand which content is useful. Such statistics are only collected from subscribers who have been informed of this when signing up, and are kept for [12 months].

Newsletter provider: Newsletters are sent through an email service provider that processes your data on our behalf [provider to confirm]. The provider is listed at [https://www.persistentflow.com/subprocessors].

18. COOKIES AND SIMILAR TECHNOLOGIES

Our websites use cookies and similar technologies. Strictly necessary cookies are used to keep you signed in, to remember your settings, and to protect the Service against abuse. These cookies are needed for the website and the Service to work and do not require consent under the Swedish Electronic Communications Act (lag (2022:482)

om elektronisk kommunikation).

[To confirm: whether any analytics, performance, or marketing cookies or similar tools are used. If so, they will only be set after you have given consent through our cookie banner, and you can withdraw your consent at any time. A list of the cookies used, their purpose, provider, and lifetime will be made available at [https://www.persistentflow.com/cookies].]

19. WHETHER YOU MUST PROVIDE PERSONAL DATA

You are not required by law to provide personal data to us. However, certain personal data, such as your name, email address, and, for paid plans, billing details, is necessary to enter into and perform the User Agreement. If you do not provide it, we cannot create an account for you or provide the Service. Signing up for newsletters and accepting non-essential cookies is always voluntary.

20. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time, for example when the Service changes or when we engage new types of service providers. The version number and effective date at the top of this Privacy Policy show when it was last updated. If we make material changes, we will notify you by email or by prominent notification in the Service before the changes take effect. Where a change requires your consent under applicable law, we will ask for it.

21. CONTACT DETAILS

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

Privacy and legal requests: legal@persistentflow.com | Security: security@persistentflow.com | Erasure & Admin: hello@persistentflow.com | Web: https://www.persistentflow.com