Data Processing Addendum

How Momor processes personal data for organizations that use Momor Workflows, Chat and Momor Gateway: roles, instructions, providers, security and deletion.

Last updated November 2, 2026 Version 1 · current

IN SHORT

- Your organization decides what its data is for. Momor processes it only to provide the Service and as your settings instruct.
- Momor never trains models on your organization's data and never sells it.
- The providers that can receive your data follow your organization's routing settings, and the list of Momor's providers is published.
- What Momor learns about a member personally is the member's, never your organization's.
- Delete runs, set retention or delete the organization, and the data goes.

A summary only. The full text below is what applies.

1. Scope

This Data Processing Addendum ("DPA") is part of Momor's Business Terms and applies to every organization that uses Momor Workflows, Chat or Momor Gateway (the "organization"). It covers the personal data in organization data that Momor processes for the organization. Where this DPA conflicts with the Terms on the processing of personal data, this DPA wins. An agreement Momor signs with the organization wins over both.

"Organization data" means what the organization, its members, its API keys and run keys, and its connections put into the Service, and what the Service produces from it: requests and

messages, files, runs and their records, Chat conversations, the organization's knowledge graph, data from connected tools, the content of Gateway calls while Momor handles them, and telemetry the organization exports.

2. Roles

- **The organization is the controller** of organization data. It decides what it is processed for, and it is responsible for having a lawful basis for it and for telling the people it concerns.
- **Momor is the processor** of organization data. It processes it only for the organization, as this DPA describes.
- **Momor is the controller** of the data it needs to run the Service and its relationship with the organization: members' sign-ins, billing and usage records, security and abuse prevention, and each member's user graph. A member's user graph holds what Momor learns about that member; it belongs to the member, follows them between their own accounts, and is never shown to the organization. The organization decides whether its members' own words can become its knowledge.

3. Instructions

Momor processes organization data only to provide the Service under the Terms, and as the organization instructs through its use of the Service and its settings, including:

- which workflows run, and what they read, call and write;
- whether runs may be temporary, how long runs are kept, and what the knowledge graph may learn;
- which models and providers calls may reach, whether calls run under zero data retention, and which providers are excluded by region or because they train on prompts;
- whether Chat may search the web;
- whether telemetry is exported, and whether it includes message content;
- which tool servers and accounts are connected.

Momor also processes organization data where the law requires it, and then tells the organization first unless the law forbids it. Momor tells the organization if it believes an instruction breaks the law.

Momor never sells organization data, never uses it for advertising, and never uses it to train models.

4. Momor's people

- Everyone at Momor who can reach organization data is bound by confidentiality.
- Momor's staff reach organization data only with the organization's consent, for a limited time, and every access is logged.
- Secrets, such as provider keys, connection credentials and telemetry headers, are never shown to anyone, including Momor's staff.

5. Security

Momor keeps appropriate technical and organizational measures in place, including:

- encryption of organization data in transit and at rest;
- write-only, encrypted secrets, which need a fresh confirmation to add or replace and are recorded in the audit log;
- separation of each organization's data in the data layer, before any model sees it;
- access limited to what each person and service needs;
- an audit log of the organization's administrative actions, and a log of every staff action;
- telemetry that shortens IP addresses before storing them, and Gateway records that hold metadata only.

6. Subprocessors

- The organization authorizes Momor to use subprocessors to provide the Service. The current list is on the Subprocessors page.
- Momor gives at least 30 days' notice before adding or replacing a subprocessor. The organization may object on reasonable data protection grounds within that time; if Momor cannot meet the objection, the organization may stop using the affected part of the Service.
- Momor binds each subprocessor to data protection terms at least as protective as this DPA, and remains responsible for it.
- **Model providers.** On Momor's supply, the provider serving a call is Momor's subprocessor, chosen within the organization's routing settings. Each provider's data policy is shown in the catalog. Some of Momor's own features, such as file conversion and keeping the knowledge graph, always run on Momor's supply.
- **The organization's own choices.** A call on the organization's own provider key goes to that provider under the organization's own agreement with it, and a tool server or assistant the organization connects receives data under its own terms. Those providers are the organization's, not Momor's subprocessors.

7. Helping the organization

- **People's requests.** Momor gives the organization tools to find, delete and set retention for organization data, and helps it answer requests from people exercising their data protection rights. If someone asks Momor directly about organization data, Momor passes the request to the organization.
- **Assessments.** Momor gives reasonable help with data protection impact assessments and consultations with regulators that concern the Service.
- **Evidence.** Momor answers reasonable questions about its processing and provides the information needed to show it keeps this DPA, once a year or after a breach.

8. Breaches

If Momor learns of a breach of security that affects organization data, it tells the organization's owners without undue delay, and within 72 hours where it can, with what is known: what happened, the data and people affected, the likely consequences, and what Momor has done and will do. Momor updates the organization as it learns more.

9. Deletion

- Runs are deleted when the organization deletes them, and when they pass its retention setting. Temporary runs are deleted 30 minutes after their last activity.
- Deleting a run deletes its record and what that run found. Facts the knowledge graph learned from it remain, without the run as their source, until the organization removes them.
- Files uploaded to a run are deleted 30 minutes after upload; what Momor read from them stays with the run.
- Momor does not keep the content of Gateway calls. File conversions on Gateway calls are kept for up to a day.
- When the organization is deleted, Momor deletes its organization data, keeping only the billing and usage records the law requires. Deleted data leaves Momor's backups within 7 days.

10. Where data is processed

Momor stores and processes organization data in the United States. Model providers may process it in the regions the organization's routing settings allow.

11. Liability and term

This DPA lasts as long as Momor processes organization data. The limits on liability in the Business Terms apply to it.

12. Contact

Privacy and data protection: privacy@momor.ai
Security: security@momor.ai

Momor.ai LLC
2501 Chatham Rd, Ste N
Springfield, IL 62704

Questions about this document: privacy@momor.ai