Privacy Policy

What Momor collects, why, who receives it, how long it is kept and what you control, across Momor Search, Momor Workflows and Momor Gateway.

Last updated November 7, 2026 Version 2 · current

IN SHORT

- Momor keeps what it needs to do what you ask, and this page says what that is and for how long.
- Momor does not sell or share your information, show ads, or train models on what you give it.
- In Momor Search, saved conversations stay until you delete them, and incognito conversations are deleted 30 minutes after their last activity. In an organization, runs and chats are kept as long as the organization's retention setting says.
- What Momor learns about you stays in your own user graph. Only you see it, and you can correct or remove anything in it.
- Everyone has the same rights over their information, wherever they live.

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

1. Who this policy covers

Momor.ai LLC ("Momor") runs momor.ai, the installed Momor app, Momor's APIs and MCP addresses, and the products offered through them: Momor Search, Momor Workflows (including Chat) and Momor Gateway. This policy explains how Momor handles personal information about the people who use them and the people who contact Momor.

Momor applies the principles of the EU General Data Protection Regulation to everyone who uses it, wherever they live.

In an organization. When you use Momor in an organization, the organization decides what its workflows, Chat and Gateway calls process, and Momor processes that data for the organization under the Data Processing Addendum. The organization's own privacy notice governs that data, so ask the organization about it. This policy still covers your sign-in, your user graph, and what Momor keeps about you itself.

2. What Momor collects

2.1 Your sign-in

- Your email address, name, profile picture, language and time zone.
- If you sign in with Google or Apple: your name, email address, confirmation that the address is verified, and the identifier of your Google or Apple account. Momor never receives your password from them.
- Your sign-in methods and two-factor settings, and your sessions: device, browser, approximate location from your IP address, and when each was last active.
- The codes and links Momor emails you to sign in or to confirm a change.

2.2 Momor Search

- **Your questions and conversations:** what you ask, the steps Search took, the sources it used and its answers, kept as each conversation's record.
- **Files you attach:** images, audio, video, PDF, Word, text and data files.
- **Location:** your approximate location from your IP address when a question needs it, or, if you allow it, your device's location, which stays on your device until a question needs it. The location sent with a question is kept with that conversation.
- **Your preferences,** such as answer style, safe search, how Search may use your location, what you mainly use Search for, and any note you give Search about yourself.

- **Voice input:** when you dictate a question, your browser's own speech recognition turns your voice into text, and Momor receives only the text. The browser's maker handles the audio under its own terms: Google in Chrome, Apple in Safari, Microsoft in Edge.
- **A record of each model call** made for your searches: the models, the provider that answered, tokens, cost and timing, for billing and your usage page. The record holds no question or answer.
- **What Momor learns about you** (section 3).

2.3 In an organization

- Your membership: your role, who invited you, when you joined and last signed in, your usage and any spending cap.
- The administrative actions you take, recorded in the organization's audit log with the time and your IP address.
- Accounts you connect for your own runs, such as your mail, calendar or files. Momor keeps their credentials encrypted.
- Your work in the organization: the chats you have, the runs you start and the questions you answer. This belongs to the organization (section 1).

2.4 Momor Gateway and keys

- The name, creator, limits and use of each API key and run key.
- A record of each Gateway call: the key or person that made it, the models asked for, the provider and model that answered, the attempts, tokens, cost and timing. Momor does not keep the prompts, messages, files or answers of Gateway calls.
- Provider keys your organization saves, which are stored encrypted and never shown again, to anyone.

2.5 Providers

If your organization applies to serve models through Momor Gateway: its company details and contacts, the models and prices it serves, its endpoint and the credential for it (stored encrypted), its data policy, and its test and health results. Stripe holds your payout account's identity, bank and tax details; Momor never sees them.

2.6 Payments

Stripe processes payments and payouts. Momor keeps the references Stripe returns for your customer record and each payment, your receipts and credit history, and, for an organization, its billing name, address and tax ID. Momor never sees or stores your full card number.

2.7 When you contact Momor

If you email Momor or use the contact form: your name, email address, organization, role, industry, how you'd like to work with Momor, and your message.

2.8 Collected automatically

- **Technical data:** your IP address, browser and device type, the pages and features you use, response times and errors. Momor's telemetry derives your approximate city from your IP address, then shortens the address before storing it.
- **A session identifier:** a random identifier for each browser tab, used to connect that tab's requests when diagnosing a problem. It is never used to follow you across other sites.
- **Usage data you choose to share:** if you turn on "Share anonymous usage data" in Search's settings, anonymous data about how the app is used. Never what you asked.

3. What Momor knows about you: your user graph

To make its answers fit you, Momor keeps a graph of facts about you: what you tell it about yourself, your preferences, such as how you like answers given, and what your conversations and work suggest about you, which is marked as inferred.

- It is built from your saved Search conversations and your work in organizations. Incognito conversations and temporary runs add nothing to it.
- Every fact keeps the source it came from.
- Only you see it. It follows you between your own accounts: Momor reads it in your own work in an organization too, so answers fit you there, but the organization never sees it.
- You can see it, correct any fact in it, or have Momor forget a fact.
- It is deleted in full when your sign-in is deleted, which happens when you delete your last account.
- In Momor Search, what you say never becomes Momor's knowledge about the world. Search learns about the world only from the sources it reads.
- In an organization, what you tell your runs also becomes the organization's knowledge, unless the organization turns that off.

4. Why Momor uses it

What Momor does	Legal basis
Provide your accounts and the products you use, including saved conversations, runs, your user graph and the notifications they need	Performing its agreement with you
Take payments and keep billing and tax records	Performing its agreement with you; legal obligation
Keep the Service secure, prevent fraud and abuse, enforce limits and fix problems	Legitimate interests
Use your device's location	Your consent, given in your browser or device
Receive anonymous usage data	Your consent
Send product updates	Your consent

What Momor does	Legal basis
Answer you when you contact Momor	Legitimate interests
Comply with the law and respond to lawful requests	Legal obligation
Process an organization's data for it	The organization's instructions, under the Data Processing Addendum

Security emails, such as a sign-in from a new device or a change to your email address, are part of keeping your account safe and cannot be turned off.

5. What Momor never does

- Sell or share personal information, as California law defines those words, or under any other law.
- Show ads, or give your information to advertisers or data brokers.
- Build profiles of you for marketing, or follow you across other websites.
- Train models on your questions, files, conversations or work.

Momor Search and Momor's own features never send your content to a model provider that trains on it. In an organization, each provider's data policy is shown in Momor's catalog, and the organization can keep its calls away from providers that train on prompts and to providers in the countries it chooses.

6. Who receives it

Momor gives personal information only to the companies that help run the Service, for that work, and as section 13 describes. They may use it only to provide their service.

- **Model providers** receive what a request needs: the question, the conversation so far, files and tool results. Which providers can receive an organization's calls follows the

organization's routing settings, and a call on an organization's own provider key goes to that provider under the organization's agreement with it.

- **Search and data providers,** for web search, maps, weather, markets and similar, receive the search terms, place names or coordinates Momor sends them to answer a question, and, to find your approximate location, your IP address.
- **Tool servers** an organization or person connects receive what their workflows send them.
- **Infrastructure providers** host Momor's servers, databases, file storage and telemetry in the United States.
- **Stripe** processes payments and provider payouts.
- **An email provider** sends Momor's emails.
- **Google and Apple,** if you sign in with them.
- **Your organization** receives the work you do in it and its audit log of your administrative actions. It never receives your user graph.
- **AI assistants** that you or your organization connect to Momor's MCP address receive the workflow results they ask for, under their own providers' terms.

Information from Google. If you connect a Google account, Momor's use and transfer of information received from Google APIs follows the Google API Services User Data Policy, including its Limited Use requirements.

The companies Momor uses

- **Hosting and network:** Render and Microsoft Azure host Momor's servers and databases; Cloudflare stores files and carries traffic to Momor's servers.
- **Telemetry:** Better Stack, New Relic and Microsoft Azure Application Insights.
- **Email:** Twilio SendGrid and Resend.
- **Payments:** Stripe.
- **Sign-in:** Google and Apple.

- **Model providers:** Anthropic, DeepInfra, Fireworks AI, Google (Gemini API and Vertex AI), Groq, Microsoft (Azure OpenAI), Mistral AI, Moonshot AI, OpenAI, Together AI and TypeSafe, and the providers approved to serve models through Momor Gateway, each shown in Momor's model catalog.
- **Search and data providers:** Serper, SerpApi, Jina AI, Wikipedia, Wolfram Alpha, Google (Translation and Books), Unsplash, OpenWeather, Open-Meteo, WeatherAPI.com, Mapbox, HERE, OpenStreetMap, ip-api, Finnhub, Deezer, Free Dictionary API and MedlinePlus.

7. How long Momor keeps it

Information	How long
Saved Search conversations, with what Momor read from their files and the location sent with them	Until you delete the conversation or your Search account
Incognito conversations	Deleted 30 minutes after their last activity
Files attached to a question or a run	The file itself, 30 minutes; what Momor read from it stays with its conversation or run
Your user graph	Until you remove a fact, or your sign-in is deleted
Your sign-in, profile and preferences	Until your last account is deleted
Sign-in codes and links	10 minutes
Sign-in sessions	30 days from their last use
An organization's runs and chats	As the organization's retention setting says, or until it deletes them or the organization
An organization's knowledge	Until the organization removes it or is deleted
Converted files, kept so the same file is not converted twice	Up to 1 day

Information	How long
Payment, credit and usage records, including Gateway call records	7 years
Telemetry and server logs	30 days
Messages sent through the contact form	For as long as needed to answer and follow up

Deleted information leaves Momor's backups within 7 days.

8. Your choices and your rights

In the product, you can delete conversations, search in incognito, correct or forget what Momor knows about you, stop sharing your device's location, turn usage data and product update emails on or off, and delete your accounts.

Your rights. Wherever you live, you can ask Momor to:

- tell you what information it holds about you and give you a copy;
- correct information that is wrong;
- delete your information;
- give you your information in a machine-readable format;
- stop or limit using your information for a purpose, where you object to it;
- withdraw a consent you gave.

Email privacy@momor.ai from the address you sign in with. Momor may need to confirm it is you, answers within 30 days, and does not charge for it. If Momor declines a request, it says why, and you can appeal by replying with "Appeal" in the subject within 45 days. A request about data Momor holds for an organization is passed to that organization, and Momor helps it answer.

Using these rights never changes the price or quality of the Service you receive. Momor does not sell or share personal information, so a Global Privacy Control signal has nothing to turn off; Momor treats it as such a request anyway.

If you are unhappy with how Momor handled your information, you can complain to the data protection authority where you live.

9. Cookies and storage on your device

- **Momor's public pages and docs** set no cookies.
- **When you sign in,** Momor sets one strictly necessary cookie, `__Host-session`, which keeps you signed in for up to 30 days from your last visit and is checked against your account at least every 30 minutes. It is encrypted, HttpOnly, Secure and SameSite=Strict, is sent only to Momor, and is never used for advertising or tracking. A Google or Apple sign-in also uses short-lived cookies while it is in progress.
- **On your device,** Momor stores your preferences, your device location if you choose to remember it, the tab's session identifier, answers to the questions Search suggests for up to a day, unsaved workflow drafts and, in the installed app, recent conversations and images for offline reading, which you can clear in the app's settings.

10. Security

- Information is encrypted in transit and at rest.
- Secrets, such as provider keys, connection credentials and telemetry headers, are encrypted, write-only and never shown again, to anyone, including Momor's staff. Adding or replacing one needs a fresh confirmation that it is you, and is recorded in the audit log.
- Each organization's data is kept apart in the data layer, before any model sees it.
- If a security breach puts your information at risk, Momor tells you without undue delay and within 72 hours of learning of it where it can, with what happened, what was affected, what Momor did and what you can do.

11. Momor's staff

- Momor's staff do not read your conversations or your user graph.
- Staff reach an organization's data only with that organization's consent, for a limited time, and every access is logged.
- Staff see the account details support and billing need, such as memberships, sign-in methods, last sign-in and balances.
- Every staff action on an account is recorded with who took it, when and why.

12. Age

Momor is only for people aged 18 or over. If Momor learns that someone under 18 has an account, it deletes the account and its information.

13. Legal requests and business changes

- Momor discloses information to authorities only when the law requires it, discloses the minimum necessary, and tells you first unless the law forbids it.
- Momor reports child sexual abuse material to the National Center for Missing & Exploited Children as the law requires.
- If Momor is merged with or acquired by another company, it tells you before your information becomes subject to a different privacy policy.

14. Where your information is kept

Momor's servers, databases and file storage are in the United States. If you use Momor from another country, your information is transferred to the United States.

The model, search and data providers a request reaches may process it in other countries; Mistral AI, for example, processes requests in the European Union.

- **In Momor Search,** Momor chooses which provider serves each request.
- **In an organization,** its routing settings decide, and the organization, or a single call, can keep calls to providers in the countries it chooses.

15. Changes to this policy

Momor may update this policy. For a material change, Momor gives at least 30 days' notice by email or in the product before it takes effect.

16. Contact

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

- Privacy questions and requests: privacy@momor.ai
- Security: security@momor.ai
- Support: support@momor.ai
- Legal notices: legal@momor.ai

Questions about this document: privacy@momor.ai