



Privacy Policy

How Delphyr handles your personal data when
you use the Delphyr LLM directly as an individual
end user

Delphyr B.V.

IJsbaanpad 2, 1076 CV Amsterdam, the Netherlands

privacy@delphyr.ai

Last updated: 15 June 2026

Privacy Policy

Last updated: 15 June 2026

At Delphyr B.V., we value your trust and take privacy seriously. When you use our large language model (LLM) as an individual end user, you should know exactly how your personal data is handled. This privacy statement explains our practices clearly and transparently.

This privacy statement applies specifically to the use of the Delphyr LLM in situations where **you access our services directly as an individual**.

When you interact with the Delphyr LLM, you are engaging with an AI system, **not a human**. This means all outputs, such as responses to your prompts, are generated by artificial intelligence. Outputs may contain inaccuracies. Use your own judgment when relying on them.

Who we are

Delphyr B.V. is a company based in Amsterdam, the Netherlands. You'll find us at IJsbaanpad 2, 1076CV Amsterdam.

We develop and operate the Delphyr LLM, a general-purpose AI model as defined under the EU AI Act. When you use our LLM directly, we are responsible for how your personal data is handled. In legal terms, this means Delphyr acts as the **data controller**.

If you have any questions about this privacy statement or the way we process your personal data, feel free to contact us at: **privacy@delphyr.ai**. We've also appointed a Data Protection Officer (DPO) to help oversee data protection at Delphyr. You can reach our DPO via the same address: **privacy@delphyr.ai**.

What personal data we process

When you use the Delphyr LLM Services directly as an end user, we may collect and process the following categories of personal data. The data we collect depends on how you interact with the services and which features you use.

1. Personal data you provide to us

- **Account information:** When you create an account, we collect your full name, email address and profile picture.



- **User input and generated output:** We collect the content you input into the LLM (such as prompts, questions, uploaded files) and the output generated by the system in response for observability, logging, evaluation and feedback. Depending on what you submit, this may include personal or sensitive information. You are responsible for what you choose to input.
- **Communication information:** If you contact us directly, we may collect the contents of your messages and related contact details to respond or provide support.

2. Personal data we collect automatically

- **Technical usage data:** This includes session metadata (e.g. timestamps, duration), browser type, language preferences, device type, screen resolution, and referring pages.
- **Log data:** Information such as your IP address, time of access, user actions within the service, error reports, and application status at the time of an issue.
- **Device and connection information:** We collect information about the device you use, including operating system, browser version, and network details (such as internet service provider and connection speed).
- **Usage information:** How you interact with the service (e.g. features used, number of prompts submitted, settings selected) to understand how the platform is used and to improve performance.
- **Cookie data:** As described in **Use of cookies**, we use cookies and similar technologies to support essential features, analyze performance, and (only if consented) personalize experiences.

Why we process your data

We process your personal data to operate, secure, and improve the Delphyr LLM Services. Specifically, we use your data for the following purposes:

- **To provide and maintain the service:** This includes enabling you to access and use the Delphyr LLM, process your inputs and generate outputs, maintain your account, and deliver core functionality across devices.
- **To respond to your requests and communicate with you:** We use your information to provide user support, notify you about service updates or changes, and respond to inquiries you send us.



- **To improve the service and understand how it's used:** We may analyze de-identified or aggregated usage patterns and technical performance data to help us debug issues, optimize system performance, and make the experience more reliable and intuitive. Your user input is **not** used to further train our model.
- **To detect and prevent abuse or misuse:** We process personal data to prevent fraud, misuse of the service, violations of our terms or policies, and to protect Delphyr, our users, and third parties from harm.
- **To meet legal obligations:** We may process personal data to comply with applicable laws and regulations, including tax, regulatory, audit, and security requirements.

Do note our system is not designed to make decisions with legal, clinical or similarly significant effects.

Legal grounds for processing

We process your personal data based on the following legal grounds:

- **Performance of a contract:** To provide you with access to the Delphyr LLM, generate responses, maintain your account, and respond to support requests.
- **Consent:** For optional features like tracking cookies. We only process your data if you've given explicit permission.
- **Legitimate interests:** To ensure the reliability, security, and performance of our services, prevent fraud or abuse, improve functionality based on anonymized usage data, and resolve user complaints, provided these interests do not override your privacy rights. For each processing activity based on legitimate interest, we have carried out a balancing test. For more information about this assessment, you can contact us at **privacy@delphyr.ai**.
- **Legal obligations:** To comply with laws and regulations, such as tax or audit requirements, to ensure system security, or to respond to lawful requests from public authorities or regulators.

Who we share data with

To run and maintain our services, we share your personal data with the following parties:



- **Nebius (cloud infrastructure):** Nebius provides the cloud infrastructure we use to host and run the Delphyr LLM. As a processor, Nebius processes personal data strictly on our behalf and under our instructions. They are contractually bound to comply with the GDPR, including confidentiality, data protection, and security requirements. They are located in the Netherlands, France and Finland.
- **Public authorities:** We may disclose your personal data to government bodies, regulators, or law enforcement if we are legally required to do so for example, in response to a court order or to comply with tax, audit, or security obligations.

We do **not** share your data with third parties for marketing, analytics, advertising, or profiling. We also do **not** sell personal data under any circumstances.

Data transfers outside the EEA

Delphyr, nor its subprocessors, do not transfer data outside the European Economic Area (EEA). If, in the future, any subprocessors or services require such transfers, we ensure appropriate safeguards are in place, such as Standard Contractual Clauses.

For more information about these safeguards, feel free to contact us at privacy@delphyr.ai.

Use of cookies

Our web application uses:

- **Functional cookies:** for core functionality (e.g. login session, preferences).
- **Analytical cookies:** to measure and improve performance (anonymous data).
- **Tracking cookies:** only with your consent, to personalize content or understand user behavior.

You can manage or withdraw consent through your browser preferences at any time.

How long we keep your data

We store your personal data only for as long as necessary to fulfill the purposes for which it was collected, unless a longer retention period is required by law. We apply data minimisation by limiting storage to what is strictly necessary. Do note that inputs and outputs are not retained by default.

Details about specific retention periods are available upon request.



Your rights under the GDPR

As a user, you have several rights under the GDPR. You can:

- Access the personal data we process about you.
- Correct inaccurate or outdated information.
- Request deletion of your data.
- Restrict or object to certain types of processing.
- Request your data in a portable format.
- Withdraw your consent at any time (for processing based on consent).

To exercise any of these rights, contact us at **privacy@delphyr.ai**. We respond within one month.

We are committed to respecting your rights, even when personal data has been processed by an AI system. We take appropriate measures to fulfill requests such as erasure or restriction and assess whether outputs can be unlinked or suppressed. If you'd like to know more about how we handle this in practice, feel free to contact us.

Filing a complaint

If you believe we are not handling your data appropriately, you can contact us. You also have the right to file a complaint with the Dutch Data Protection Authority: **autoriteitpersoonsgegevens.nl**

Children's data

Our services are not intended for use by children under the age of 18. We do not knowingly collect or process personal data from individuals in this age group.

Automated decision-making

We do not make decisions that have a legal or similarly significant effect on you based solely on automated processing. While our platform may use AI or algorithms to generate insights or support decision-making, any final actions are taken by you.



We do not use your data to train our AI models. However, we may analyze how the AI performs for example, when outputs are clearly incorrect or unexpected, in order to improve the quality and reliability of the service. This quality review process is strictly limited to internal analytics and performance monitoring, not for model training or external use. Any such analysis is carried out in a way that respects your privacy and complies with data protection requirements.

How we protect your data

We design our systems with privacy and security in mind (also known as Privacy by Design). This means collecting only what's needed, isolating sensitive data, and actively managing risks such as bias or unintended memorisation.

We apply the following safeguards:

- **Encryption** of data in transit and at rest.
- **Strict access controls** to limit who can access your data.
- **Security monitoring and logging** to detect issues early.
- **Regular testing**, including penetration tests and AI-specific checks.
- **Internal policies** aligned with ISO 27001, NEN 7510, and MDR.
- **Confidentiality obligations** for all Delphyr personnel.

To ensure safe and transparent AI use:

- We monitor the LLM's performance to detect anomalies or misuse.
- We do **not** build user profiles or track individuals beyond what's needed for service integrity.
- All AI-generated content (text, images, audio, video) is marked or made detectable using watermarks, metadata tags, or visible labels.
- We regularly test the model to reduce bias and improve fairness in its outputs.
- We audit the system to monitor AI-specific risks and welcome user feedback via **privacy@delphyr.ai**.

Changes to this statement

This statement may be updated from time to time. Substantive changes will be communicated via email. You can always find the latest version on our website: **delphyr.ai/privacy-policy**

