

FLUENCE PRIVACY POLICY

Last updated: 21 October 2026

Fluence DAO, a Swiss association ("Fluence," "we," "us," or "our"), is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard personal information when you access or use fluence.network, fluence.ai, and fluence.cloud, including all subdomains of each (collectively, the "Site"), our Compute Services, including on-demand CPU and GPU resources, our AI Model API Service, and related applications, consoles, APIs, and services (collectively, the "Services"). The AI Model API Service enables access to artificial intelligence models through APIs and related interfaces. This Policy describes our practices and your choices; it does not itself constitute your consent to processing that requires consent.

Fluence is the controller of personal information it processes for its own account administration, billing, security, support, and marketing purposes. When a customer submits personal information for processing through the Services and determines the purposes of that processing, the customer may be the controller and Fluence may act as a processor on the customer's instructions. Any applicable data-processing agreement governs that processing. This Policy does not replace such an agreement or a customer's responsibility to provide notices and obtain permissions for information about other people.

1. Information We Collect

A. Information You Provide to Us

When you register for an account, use our Services, or communicate with us, you may provide us with personal information, which may include:

- **Contact and Profile Information:** Your name, email address, postal address, telephone number, profile photo, and account preferences, where provided.
- **Account Credentials:** Login credentials, sign-in and verification information, session information, API-key identifiers, permissions, and security settings.
- **Payment Information:** Payment details collected and processed by our payment providers, and billing addresses, tax information, transaction records, payment status, and limited payment-method information received by Fluence.
- **User Content:** Information, data, code, prompts, files, images, tool-call context, workload configurations, and other materials you submit or process through the Services, together with generated responses and other results. This content may include personal information about you or other people.
- **Support Information:** Messages, emails, attachments, and relevant account or usage information supplied in connection with support requests.

B. Information Collected Automatically

When you use our Site and Services, we automatically collect certain information about your device and usage:

- **Device Information:** IP address, browser type, operating system, device identifiers, and mobile network information.
- **Usage Data:** Pages visited, links clicked, feature interactions, request identifiers and timestamps, models and providers used, resource consumption, token or other usage counts, charges, performance information, errors, and security-event records.
- **Cookies and Similar Technologies:** Cookies, tags, and related technologies used for service operation, analytics, advertising measurement, and related purposes described in Section 7.

C. Information from Third Parties

We may also receive information from authentication services, payment providers, Compute Providers, Model Providers, business partners, or social media services you choose to connect. This may include authentication results, payment and fraud signals, usage records, and results needed to provide the Services. We use this information for the purposes described in this Policy.

2. How We Use Your Information

We use the information we collect for various purposes, including to:

- **Provide and Maintain Services:** Deliver Compute Services and the AI Model API Service, provision resources, process model requests and return results, manage your account, process transactions, provide support, and communicate with you about the Services.
- **Apply Your Preferences:** Configure the Services according to your settings, permissions, and supported feature choices.
- **Improve Our Services:** Analyze operational and usage information, diagnose problems, and improve the functionality and performance of our Site and Services.
- **Security:** Protect accounts and the Services, detect fraud and abuse, enforce usage limits, and perform applicable security checks. Content-protection features may inspect request context, model responses, and tool-call information.
- **Marketing and Communications:** Send you information about promotions, updates, or other offerings, provided you have given consent where required by law.
- **Legal Obligations:** Comply with applicable laws, regulations, and legal processes, and enforce our Terms of Use.

Customer content is processed to fulfill requests and provide applicable support and security features. The general service-improvement purposes above do not authorize unrelated model training on customer request content. Model Providers' content-retention and training practices may differ by provider, model, and service configuration. Any no-training or zero-retention commitment applies within the scope expressly stated for the relevant Service and settings.

Where the EU or UK GDPR applies, our legal bases depend on the processing: performance of a contract for requested services and account administration; legal obligations for required financial, tax, and regulatory records; legitimate interests in operating, securing, supporting, and improving the Services where those interests are not overridden by your rights; and consent for processing that requires it. A legitimate-interest basis does not replace consent required for advertising or other tracking technologies. You may withdraw consent as described in Section 6.

3. How We Share Your Information

We may share your information with:

- **Service Providers:** Vendors and contractors that perform services on our behalf, including hosting, storage, authentication, payment processing, email delivery, analytics, and customer support.
- **Compute Providers:** Providers supplying computing resources may receive workload content, resource configurations, and other information needed to provision, operate, and support the Compute Services you request.
- **Model Providers:** Providers supplying models or related processing receive the request content and technical information needed to process requests and return results. This may include providers selected by

Fluence on your behalf and their underlying service providers, subject to applicable service settings and commitments.

- **AI Support and Security Providers:** Automated support and certain content-protection features use third-party AI services, including OpenRouter and the providers serving those features. Those services receive the relevant support messages, account context, or request and response content needed for the feature. Authorized support personnel may also access support conversations.
- **Analytics and Advertising Partners:** Partners may receive website interaction information, online identifiers, and conversion data for the purposes and subject to the choices described in Section 7.
- **Legal and Regulatory Authorities:** When required by law, regulation, or legal process, we may disclose your information to law enforcement, government authorities, or as otherwise required by applicable law.
- **Business Transfers:** In the event of a merger, acquisition, or sale of assets, your information may be transferred as part of the transaction, subject to appropriate safeguards.
- **With Your Consent:** We may share your information with your consent or at your direction.

Compute Providers and Model Providers are collectively referred to as “Providers.” Depending on the service and contractual arrangement, a recipient may process information on our or your instructions or for purposes governed by its own applicable terms and privacy notice. Provider terms do not reduce Fluence’s express privacy commitments or your rights under applicable law. Contact us for information about providers involved in the Services you use.

4. Data Retention and Security

A. Data Retention

We retain your personal information only for as long as is necessary to fulfill the purposes for which it was collected, to comply with legal obligations, resolve disputes, and enforce our agreements.

- **AI Model API Content:** We process request and response content to fulfill requests, including in transient memory. Routine API request telemetry does not include prompt or response bodies. Features involving files, caches, or other stored content, where available, may have different retention arrangements described for the relevant feature or Provider.
- **Account and Operational Records:** Account information, usage and billing records, security events, and diagnostic metadata are retained as needed to operate your account, reconcile charges, investigate incidents, resolve disputes, and meet legal obligations. Some diagnostic records may be archived. Account closure does not necessarily remove records retained for these purposes.
- **Support Records:** Support conversations are stored separately from ordinary API request telemetry to handle requests and maintain support continuity. Closing an account removes its stored support conversations from the application. Related emails, accounting records, or records retained for legal or security purposes may remain subject to their applicable retention requirements.
- **Hosted Workloads and Stored Files:** Retention and deletion depend on the resources, configurations, storage features, and Provider arrangements used. Resource deletion, account closure, and any backup retention should be assessed under the applicable service terms and data-processing arrangements.

Where zero data retention (“ZDR”) is required for an AI Model API request, we select eligible Providers according to that requirement and restrict features that are incompatible with it. ZDR concerns request-content retention; it does not eliminate account, billing, or security metadata and does not establish a processing-location restriction. Support conversations follow the separate practices above. Tool-call protection is unavailable with ZDR where the classifier’s retention requirements have not been verified. The relevant service documentation explains available controls and their scope.

B. Data Security

We implement commercially reasonable technical, administrative, and physical security measures designed to protect your information from unauthorized access, disclosure, alteration, and destruction. However, no security system is impenetrable, and we cannot guarantee the absolute security of your data.

5. International Data Transfers

Your information may be transferred to and processed in countries outside your country of residence. Locations depend on the Services, resources, and Providers involved and may include Germany, the United States, and other countries in which relevant providers operate. A selected compute region does not necessarily determine the location of account administration, support, billing, or other processing. ZDR is not a data-residency guarantee.

International transfers are subject to applicable data-protection requirements. Where a transfer requires a specific legal mechanism, that mechanism must be permitted by applicable law, such as an adequacy decision, approved contractual safeguards, or an available statutory exception. Where explicit consent is relied on for a particular transfer, it must be obtained separately with the information required by law. Merely using the Services does not constitute that consent. Contact us for the destination countries and transfer safeguards applicable to your Services and information about obtaining a copy of relevant safeguards.

6. Your Rights and Choices

Depending on your location and applicable law, you may have certain rights regarding your personal information, including:

- **Access:** Request access to the personal information we hold about you.
- **Correction:** Request that we correct any inaccurate or incomplete information.
- **Deletion:** Request that we delete your personal information, subject to certain legal obligations.
- **Objection and Restriction:** Request that we restrict or object to our processing of your information.
- **Data Portability:** Request the transfer of your personal information to another party.
- **Opt-Out:** Manage your preferences for receiving marketing communications. You can opt out by following the unsubscribe instructions provided in such communications or by contacting us directly.
- **Withdrawal of Consent:** Withdraw consent for processing based on consent, without affecting the lawfulness of processing before withdrawal.
- **Complaints:** Complain to a competent data-protection authority, including the Swiss Federal Data Protection and Information Commissioner or an authority in your jurisdiction, where applicable.

To exercise these rights, please contact us using the details in Section 10. We may request information proportionate to what is needed to verify your identity and will respond within the time required by applicable law. If we process information on behalf of a customer, we may refer your request to that customer or assist it in responding. Rights may be subject to exceptions required or permitted by law.

7. Cookies and Tracking Technologies

We use cookies, web beacons, tags, and similar technologies for authentication and security, service operation, analytics, advertising measurement, and retargeting. Necessary technologies support requested functions such as signing in. Analytics and advertising technologies serve different purposes and may collect information about browsing activities over time and across websites.

On relevant marketing pages, we use Google Analytics and X advertising tags. These providers may receive IP addresses, browser or device information, cookie or other online identifiers, page and interaction information,

and conversion events. Analytics events may also include campaign attribution, session identifiers, and email-domain information. Some conversion and usage events are sent from our servers, so browser cookie controls may not prevent all related processing.

Where applicable law requires consent for non-essential tracking, prior consent is required; acceptance of this Policy or continued browsing does not supply it. You may manage cookies through your browser and use relevant provider privacy or opt-out controls. Disabling necessary cookies may affect functionality. Contact us about tracking choices or to withdraw consent for processing that relies on consent. Marketing-message preferences are separate from necessary account and service communications.

8. Children's Privacy

Our Services are not directed to children under the age of 13. We do not knowingly collect personal information from children under 13. If you are a parent or guardian and believe your child has provided us with personal information, please contact us immediately, and we will take steps to delete such information from our records.

The AI Model API Service is intended for users aged 18 or over, as stated in our Terms of Use. Parental permission does not override that requirement. The age requirements for other Services remain subject to their applicable terms. If we learn that personal information has been collected in violation of applicable age restrictions or law, we will take appropriate steps to address the account and delete the information unless retention is legally required.

9. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices, Services, or legal requirements. We will revise the “Last updated” date above and post the revised Policy on the Site. We will provide additional notice of material changes, and obtain consent for changed processing, where required by applicable law. Changes to this Policy do not by themselves provide consent for processing that requires it.

10. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us at:

Fluence DAO, a Swiss association. Email: hello@fluence.network