

Privacy Policy

Effective Date: April 14, 2026

mAlvn, LLC | 3368 100th St, Urbandale, IA 50322

1. Introduction

mAlvn, LLC ("mAlvn," "we," "us," or "our"), an Iowa limited liability company located at 3368 100th St, Urbandale, IA 50322, is committed to protecting your privacy. This Privacy Policy describes how we collect, use, disclose, retain, and protect your personal information when you use the mAlvn Developer Platform, including our APIs, SDKs, Developer Portal, documentation, and related services (collectively, the "Service").

By accessing or using the Service, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with our data practices, please do not use the Service.

This Privacy Policy is incorporated into and forms part of our Terms of Service.

2. Information We Collect

2.1 Information You Provide Directly

- **Account Information:** Name, email address, phone number, company name, job title, and password when you create an account or join an organization.
- **Profile Information:** Display name, avatar, timezone preferences, and other optional profile details you choose to provide.
- **Organization Information:** Organization name, billing email, logo, data classification settings, and data residency preferences.
- **Billing Information:** Payment method details, billing address, and transaction history. Payment card information is processed by our third-party payment processor and is not stored on our servers.
- **Communications:** Information you provide when you contact us for support, submit feedback, or participate in surveys.
- **Waitlist and Access Request Information:** Name, email, company, role, investment focus, and other information submitted through waitlist or access request forms.

2.2 Information Collected Automatically

- **API Usage Data:** API request metadata including endpoints accessed, request timestamps, response times, HTTP status codes, tokens consumed, and error details. We do not log the content of API request or response bodies.
- **Authentication Data:** Login timestamps, session information, IP addresses, and authentication failure records for security monitoring.

- **Device and Browser Information:** Browser type, operating system, device identifiers, screen resolution, and language preferences.
- **Usage Analytics:** Pages visited, features used, click patterns, navigation paths, and session duration within the Developer Portal.
- **Log Data:** Server logs containing IP addresses, access times, requested URLs, referral URLs, and system error information.
- **Webhook Delivery Data:** Delivery timestamps, response codes, and retry information for webhooks you configure.

2.3 Information from Third Parties

- **Authentication Providers:** If you sign in through a third-party authentication provider, we receive your name, email address, and profile information as authorized by you.
- **LLM Providers:** We receive usage metrics and model performance data from large language model providers used in the Service. We do not share your raw prompts or content with these providers beyond what is necessary for processing.

3. How We Use Your Information

We use the information we collect for the following purposes:

- **Providing the Service:** To create and manage your account, process API requests, deliver the Developer Portal, and provide customer support.
- **Billing and Payments:** To process subscriptions, track usage against plan quotas, generate invoices, and manage payment transactions.
- **Security and Fraud Prevention:** To detect and prevent unauthorized access, abuse, fraud, and other security threats, including monitoring API key usage and authentication patterns.
- **Service Improvement:** To analyze usage patterns, identify bugs, optimize performance, and develop new features.
- **Communications:** To send transactional notifications (account verification, password resets, billing alerts, API key expiration warnings), and, with your consent, marketing communications about new features and updates.
- **Compliance:** To comply with legal obligations, respond to lawful requests, enforce our Terms of Service, and maintain audit trails as required by applicable regulations.
- **Analytics and Reporting:** To generate aggregated, de-identified analytics about platform usage for internal business purposes.

4. Legal Basis for Processing

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

- **Contract Performance:** Processing necessary to perform our contract with you (the Terms of Service), including account management, API access, and billing.
- **Legitimate Interests:** Processing necessary for our legitimate business interests, such as security, fraud prevention, service improvement, and analytics, provided these interests are not overridden by your rights.

- **Consent:** Processing based on your explicit consent, such as marketing communications and optional analytics. You may withdraw consent at any time.
- **Legal Obligations:** Processing necessary to comply with applicable laws and regulations, including tax reporting, audit requirements, and responding to lawful government requests.

5. How We Share Your Information

We do not sell your personal information. We may share your information in the following circumstances:

- **Service Providers:** With trusted third-party vendors who assist us in operating the Service, including cloud hosting providers, payment processors, email delivery services, and analytics providers. These providers are contractually obligated to protect your information and may only use it to provide services to us.
- **LLM Processing:** With large language model providers to the extent necessary for AI agent execution. Our PrivateDataGateway architecture ensures that raw secrets and sensitive data are separated from the data sent to LLM providers. We contractually require these providers to not use your data for training purposes.
- **Within Your Organization:** With other members of your mAlvn organization to the extent necessary for collaborative use of the Service, as determined by your organization's administrator settings.
- **Legal Requirements:** When required by law, regulation, legal process, or governmental request, or when we believe disclosure is necessary to protect our rights, your safety, or the safety of others.
- **Business Transfers:** In connection with a merger, acquisition, reorganization, bankruptcy, or sale of all or a portion of our assets, your information may be transferred as part of such transaction.
- **With Your Consent:** In any other circumstance where you have provided explicit consent to share your information.

6. Data Security

We implement comprehensive technical and organizational security measures to protect your information against unauthorized access, alteration, disclosure, or destruction. These measures include:

- **Encryption:** All data is encrypted in transit using TLS 1.2 or higher. Sensitive data at rest is encrypted using AES-256 encryption. Highly confidential data is protected with column-level transparent column encryption (TCE) using pgsodium.
- **Access Controls:** Role-based access controls with principle of least privilege, row-level security policies on all database tables, and multi-factor authentication support.
- **Privacy Architecture:** Our PrivateDataGateway separates raw secrets and credentials from AI model processing layers. The PrivateDataShield provides an additional boundary that redacts private data before agent invocations.

- **Audit Trails:** Comprehensive audit logging of all administrative actions, API access, and data modifications with tamper-evident recording and seven (7) year retention for compliance purposes.
- **Data Hashing:** SHA-256 hashing is applied to sensitive identifiers where appropriate to support data minimization principles.
- **Infrastructure Security:** The Service is hosted on secure cloud infrastructure with regular vulnerability scanning, penetration testing, and security patching.
- **Incident Response:** We maintain an incident response plan and will notify affected users of any data breach in accordance with applicable law, including Iowa Code Chapter 715C (Iowa Personal Information Security Breach Protection Act).

While we take reasonable measures to protect your information, no method of transmission over the Internet or electronic storage is completely secure, and we cannot guarantee absolute security.

7. Data Retention

We retain your personal information for as long as necessary to fulfill the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law. Specific retention periods include:

- **Account Data:** Retained for the duration of your account and for thirty (30) days after account deletion to allow for data export and recovery.
- **API Usage Logs:** Retained for ninety (90) days for operational purposes, then aggregated and de-identified for long-term analytics.
- **Audit Trail Records:** Retained for seven (7) years to support compliance with regulatory requirements (regulatory readiness and internal governance requirements).
- **Billing Records:** Retained for the period required by applicable tax laws, typically seven (7) years.
- **Security Logs:** Retained for one (1) year for security investigation purposes.
- **Marketing Consent Records:** Retained for the duration of consent and for three (3) years after withdrawal for compliance documentation.

When personal information is no longer needed, we securely delete or anonymize it in accordance with our data retention policies.

8. Your Rights and Choices

Depending on your jurisdiction, you may have the following rights regarding your personal information:

- **Access:** Request a copy of the personal information we hold about you.
- **Correction:** Request correction of inaccurate or incomplete personal information.
- **Deletion:** Request deletion of your personal information, subject to certain exceptions.
- **Data Portability:** Request your personal information in a structured, commonly used, machine-readable format.
- **Consent Withdrawal:** Withdraw consent for data processing where consent is the legal basis.

- **Marketing Opt-Out:** Unsubscribe from marketing communications at any time.
- **Memory Purge:** Request deletion of AI memory data associated with your sessions, projects, or organization.

To exercise any of these rights, please contact us at hello@maivn.io. We will respond to your request within thirty (30) days.

9. Cookies and Tracking Technologies

We use cookies and similar tracking technologies to operate and improve the Service:

- **Essential Cookies:** Required for the Service to function, including session management, authentication, and security tokens. These cannot be disabled.
- **Analytics Cookies:** Used to understand how users interact with the Developer Portal, identify popular features, and detect usability issues. These are only set with your consent.
- **Preference Cookies:** Used to remember your settings and preferences, such as theme selection and dashboard layout.

We do not use third-party advertising cookies or tracking pixels. We do not participate in cross-site tracking or interest-based advertising.

10. Children's Privacy

The Service is not directed to individuals under the age of 18. We do not knowingly collect personal information from children under 18. If we learn that we have collected personal information from a child under 18, we will promptly delete such information. If you believe we have collected information from a child under 18, please contact us immediately at hello@maivn.io.

11. International Data Transfers

mAlvn is based in the United States, and the Service is hosted on infrastructure located primarily in the United States. If you access the Service from outside the United States, your information may be transferred to, stored, and processed in the United States or other countries where our service providers operate.

We take steps to ensure that international data transfers are conducted in compliance with applicable data protection laws. Where required, we implement appropriate safeguards such as standard contractual clauses or rely on other lawful transfer mechanisms.

12. Iowa-Specific Provisions

As an Iowa-based company, we comply with applicable Iowa data protection and privacy laws, including:

- **Iowa Consumer Data Protection Act (Iowa Code Chapter 715D):** Iowa residents who qualify as consumers under this Act have the right to: confirm whether we are processing their personal data; access their personal data; delete their personal data; obtain a copy of their personal data in a portable format; and opt out of the processing of their personal data for

targeted advertising, the sale of personal data, or profiling. We do not sell personal data or use it for targeted advertising.

- **Iowa Personal Information Security Breach Protection Act (Iowa Code Chapter 715C):** In the event of a security breach involving your personal information, we will notify you and the Iowa Attorney General as required by law, without unreasonable delay.

To exercise your rights under Iowa law, please contact us at hello@maivn.io. We will respond to your request within ninety (90) days as required by the Iowa Consumer Data Protection Act. We will not discriminate against you for exercising your privacy rights.

13. California Residents

If you are a California resident, you may have additional rights under the CCPA and CPRA, including:

- The right to know what personal information we collect, use, disclose, and sell;
- The right to request deletion of your personal information;
- The right to opt out of the sale or sharing of your personal information;
- The right to non-discrimination for exercising your privacy rights;
- The right to correct inaccurate personal information;
- The right to limit the use of sensitive personal information.

We do not sell personal information as defined under the CCPA/CPRA. To exercise your California privacy rights, please contact us at hello@maivn.io.

14. European Economic Area, United Kingdom, and Switzerland

If you are located in the EEA, UK, or Switzerland, you may have additional rights under the GDPR, including:

- The right to lodge a complaint with your local data protection authority;
- The right to restrict processing of your personal data;
- The right to object to processing based on legitimate interests;
- The right to data portability in a structured, commonly used format;
- The right not to be subject to automated decision-making, including profiling.

For the purposes of GDPR, mAlvn, LLC is the data controller. To exercise your rights or for any data protection inquiries, please contact us at hello@maivn.io.

15. Do Not Track

Some web browsers transmit "Do Not Track" (DNT) signals. Because there is no uniform standard for interpreting DNT signals, the Service does not currently respond to DNT signals. However, we do not engage in cross-site tracking or interest-based advertising.

16. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or other factors. We will notify you of material changes by posting the updated policy on this page with a revised "Effective Date" and, for users with accounts, by sending notice via email or through the Developer Portal.

Your continued use of the Service after the effective date of any changes constitutes your acceptance of the updated Privacy Policy.

17. Contact Us

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

mAlvn, LLC
3368 100th St
Urbandale, IA 50322
United States
Email: hello@maivn.io