

ai12z Privacy Policy

Effective Date: July 21, 2026 | Version 2.0

This Privacy Policy explains how ai12z, Inc. collects, uses, discloses, retains, and protects personal information when individuals visit our websites, communicate with us, create or administer an account, use ai12z services, or interact with an ai12z-powered experience.

1. Scope

This Privacy Policy applies to ai12z websites, including ai12z.com, account and administration portals, public demonstrations, trial experiences, customer and partner communications, marketing activities, and ai12z products and services that link to this Policy (collectively, the “Services”).

This Policy does not apply to third-party websites, applications, or services that have their own privacy policies, even when they are linked to or integrated with the Services.

2. Our Roles

When ai12z determines how information is used

ai12z acts as a business or data controller when it determines the purposes and means of processing personal information, such as information relating to website visitors, prospective customers, account administrators, billing contacts, support contacts, event participants, and marketing recipients.

When ai12z processes information for an enterprise customer

When ai12z processes Customer Content on behalf of an enterprise customer, the customer generally acts as the business or data controller and ai12z acts as its service provider or data processor. That processing is governed by the applicable Order Form, Master Subscription Agreement, and, where applicable, Data Processing Addendum. Individuals seeking to exercise rights regarding information controlled by an ai12z customer should generally contact that customer first.

3. Personal Information We Collect

The information we collect depends on how you interact with ai12z and the Services. We may collect the following categories of personal information:

- Contact and professional information, such as name, business email address, telephone number, employer, job title, and business contact details.
- Account and authentication information, such as username, organization, role, permissions, login records, and authentication identifiers.
- Subscription and transaction information, such as selected plan, invoices, payment status, billing address, tax information, and transaction identifiers. ai12z uses Stripe to process subscription transactions. Payment card and bank-account information is collected and processed directly by Stripe and is not stored in full by ai12z. ai12z may receive limited transaction details from Stripe, such as payment status, payment method type, billing details, and transaction identifiers.
- Customer Content and communications, such as prompts, questions, chatbot interactions, responses, uploaded files, knowledge-base materials, support requests, emails, comments, feedback, and other content submitted to the Services.
- Device, network, and usage information, such as IP address, browser type, operating system, device type, referring URLs, pages viewed, feature interactions, timestamps, session information, diagnostic logs, and security events.
- Cookie and similar technology information, such as cookie identifiers, local-storage identifiers, preferences, and analytics information.
- Integration and connector information, such as data made available through customer-authorized CRM, CMS, commerce, support, analytics, cloud-storage, or other third-party systems.
- Approximate location information derived from IP address or information you choose to provide.
- Other information you provide voluntarily or that we describe at the time of collection.

4. Sources of Personal Information

We may collect personal information:

- Directly from you when you contact us, create an account, request a demonstration, submit content, purchase a subscription, or use the Services.

- From your organization, account administrator, employer, partner, or an ai12z customer that authorizes your access.
- Automatically through the Services, cookies, logs, analytics tools, and security technologies.
- From customer-authorized integrations and third-party services.
- From service providers, business partners, public sources, and professional networking or marketing sources, where permitted by law.

5. How We Use Personal Information

We may use personal information to:

- Provide, administer, maintain, and support the Services.
- Create accounts, authenticate users, manage permissions, and secure access.
- Process subscriptions, invoices, payments, taxes, renewals, and related transactions.
- Operate AI-enabled features, search, digital assistants, reporting, analytics, integrations, and customer-configured workflows.
- Respond to inquiries, provide support, communicate service information, and manage customer and partner relationships.
- Monitor availability, troubleshoot errors, improve usability, measure performance, and maintain service reliability.
- Detect, investigate, prevent, and respond to fraud, abuse, security threats, prohibited conduct, and legal violations.
- Comply with contractual, legal, regulatory, tax, accounting, and reporting obligations.
- Establish, exercise, or defend legal claims and enforce agreements and policies.
- Send product news, event information, and marketing communications where permitted by law and subject to your communication preferences.
- Create aggregated or de-identified information for analytics, reporting, benchmarking, security, and product-performance improvement.

6. AI Model Training and Customer Content

ai12z does not use Customer Content to train, fine-tune, retrain, validate, or improve general-purpose, foundation, shared, or cross-customer artificial-intelligence or machine-learning models.

ai12z requires subprocessors used to provide the Services not to use Customer Content for those purposes. Any exception would require the customer's express prior written authorization.

This commitment does not prevent ai12z from using aggregated or de-identified operational information that does not identify a customer or individual to operate, secure, analyze, and improve the performance, reliability, and functionality of the Services. Voluntary feedback may also be used to improve ai12z products, provided it does not include Customer Content or confidential information.

7. Cookies and Similar Technologies

We and our service providers may use cookies, local storage, pixels, tags, and similar technologies to operate the Services, remember preferences, authenticate users, maintain security, understand usage, and, where applicable, support communications and marketing.

We may use the following categories of technologies:

- Essential technologies required for security, authentication, navigation, and core functionality.
- Preference technologies that remember settings and choices.
- Analytics technologies that help us understand traffic, usage, and performance.
- Marketing technologies, if enabled, that help measure campaigns or deliver relevant communications.

You can manage certain cookie choices through available cookie controls and browser settings. Blocking some technologies may affect functionality. Where required, we honor legally recognized opt-out preference signals, such as the Global Privacy Control, for applicable processing.

ai12z uses a cookie-consent manager to provide information about cookies and similar technologies and, where required by law, to obtain consent before non-essential technologies are activated. You may review or change your choices through the cookie-preference controls available on the Website. Additional details about specific technologies may be provided in a separate Cookie Policy.

8. How We Disclose Personal Information

We may disclose personal information to the following categories of recipients for the purposes described in this Policy:

- Cloud hosting, infrastructure, database, storage, content-delivery, and network providers.
- AI model, inference, search, speech, and related technology providers used to deliver customer-requested functionality.
- Authentication, identity, security, fraud-prevention, monitoring, logging, and incident-response providers.
- Service providers that support our operations, including Stripe for subscription payment processing, as well as invoicing providers, banks, tax and accounting providers.
- Email, customer-support, CRM, communications, analytics, event, and marketing providers.
- Professional advisers, auditors, insurers, and legal counsel.
- Customer-authorized third-party applications and integrations.
- Government authorities, courts, regulators, law enforcement, or other parties when disclosure is required by law or reasonably necessary to protect rights, security, or safety.
- Potential or actual acquirers, investors, lenders, or successors in connection with a merger, financing, acquisition, reorganization, bankruptcy, or sale of assets, subject to appropriate confidentiality protections.

Service providers may process personal information only for authorized purposes and subject to contractual obligations appropriate to their role.

9. Sale, Sharing, and Targeted Advertising

ai12z does not sell personal information or share personal information for cross-context behavioral advertising, as those terms are defined under applicable privacy laws. ai12z does not use or disclose Customer Content for targeted advertising.

We periodically review our website tags, analytics configurations, and marketing technologies to confirm that they remain consistent with this statement. If our practices change, we will update this Policy and provide any legally required opt-out mechanism.

10. Customer-Directed Integrations

If you or your organization connects the Services to a third-party system, ai12z may receive information from and send information to that system according to the permissions, configuration, and instructions selected by you or your organization. Third-party services are governed by their own terms and privacy practices. In enterprise environments, an administrator may control or disconnect integrations.

11. Data Retention

We retain personal information only for as long as reasonably necessary for the purposes described in this Policy, including to provide the Services, maintain security, comply with legal and contractual obligations, resolve disputes, and enforce agreements.

Retention periods vary based on the type of information, the customer's configuration and instructions, the status of an account or subscription, legal and accounting requirements, and operational or security needs. Customer Content is retained and deleted in accordance with the applicable enterprise agreement, Order Form, Data Processing Addendum, and customer configuration.

We generally retain website inquiries and sales-contact records for up to three years after the last meaningful interaction; account and organization records for the duration of the account or customer relationship and, where needed for contracts, disputes, accounting, or legal compliance, for up to seven years afterward; subscription, invoice, tax, and transaction records for seven years; support records for three years after closure; general application logs for approximately twelve months; security and audit logs for up to twenty-four months; and marketing contact records until opt-out or for up to three years after the last engagement. Consent, unsubscribe, and suppression records may be retained as long as reasonably necessary to demonstrate compliance. Customer Content is retained during the subscription and ordinarily made available for export for thirty days after termination, subject to the applicable agreement, customer configuration, legal requirements, and backup cycles. Backup copies are generally maintained on a rolling basis for up to ninety days.

12. Data Security

ai12z uses reasonable administrative, technical, and organizational safeguards designed to protect personal information against unauthorized access, acquisition, disclosure, alteration, loss, or destruction. Safeguards may include access controls, authentication, encryption, monitoring, employee confidentiality obligations, security policies, and incident-response procedures.

No method of transmission or storage is completely secure, and we cannot guarantee absolute security. Where required by law, ai12z will provide notices concerning qualifying personal-data incidents.

13. International Data Transfers

ai12z is based in the United States, and personal information may be processed in the United States and other countries where ai12z or its service providers operate. Those countries may have privacy laws that differ from the laws where you live.

Where required, ai12z uses appropriate safeguards for international transfers, which may include contractual protections approved by relevant authorities. Enterprise transfer arrangements may also be addressed in the applicable Data Processing Addendum.

14. Your Privacy Rights

Depending on where you live and subject to applicable law, you may have rights to:

- Know or access personal information we process about you.
- Correct inaccurate personal information.
- Delete personal information.
- Obtain a portable copy of certain personal information.
- Restrict or object to certain processing.
- Withdraw consent where processing is based on consent.
- Opt out of certain sales, sharing, targeted advertising, or profiling.
- Appeal a decision concerning a privacy request.
- Receive equal service and not be discriminated against for exercising privacy rights.
- Complain to a privacy or data-protection regulator.

To submit a request, contact compliance@ai12z.com. We may need to verify your identity and authority before completing a request. You may use an authorized agent where permitted by law. We may deny or limit a request where permitted by law, such as when information is needed to provide requested services, protect security, comply with legal obligations, preserve evidence, or exercise legal rights.

When ai12z processes information on behalf of an enterprise customer, we may direct your request to that customer or assist the customer in responding.

15. Additional Information for California and Other U.S. State Residents

Residents of certain U.S. states may have additional rights regarding personal information, including rights to know, access, correct, delete, obtain portability, opt out of certain sale, sharing, targeted advertising, or profiling, and appeal denied requests.

For purposes of applicable state privacy laws, the categories of personal information collected, sources, purposes, and categories of recipients are described in Sections 3 through 9 of this Policy. ai12z does not use or disclose sensitive personal information for purposes requiring a right to limit unless otherwise disclosed at collection.

Whether a particular state privacy law applies depends on statutory thresholds and the circumstances of the processing. Regardless of whether ai12z is legally required to provide a particular right in every jurisdiction, we will make reasonable efforts to honor verified requests for access, correction, deletion, and portability, subject to applicable exceptions and operational feasibility.

16. Additional Information for the EEA, United Kingdom, and Switzerland

Where European data-protection law applies and ai12z acts as controller, ai12z generally relies on one or more of the following legal bases: performance of a contract; legitimate interests in operating, securing, supporting, and improving the Services and managing business relationships; compliance with legal obligations; and consent where required.

You may have rights of access, correction, deletion, restriction, portability, objection, and withdrawal of consent. You may also lodge a complaint with your local supervisory authority. Where ai12z processes personal data on behalf of an enterprise customer, that customer is generally responsible for identifying the applicable legal basis and responding to individual requests.

ai12z has not appointed a Data Protection Officer. Privacy inquiries may be directed to compliance@ai12z.com. If applicable law requires ai12z to appoint a representative in the European Economic Area or United Kingdom, this Policy will be updated with the representative's contact information.

17. Children's Privacy

The ai12z website and general Services are not directed to children under 13, and ai12z does not knowingly collect personal information directly from children under 13 without legally valid authorization. If we learn that we collected such information in violation of applicable law, we will take appropriate steps to delete it.

Enterprise customers are responsible for obtaining required permissions and implementing appropriate safeguards when deploying ai12z services in schools, youth programs, or other contexts involving minors.

18. Marketing Communications

You may opt out of marketing emails by using the unsubscribe link in the message or contacting us. Even after opting out of marketing messages, you may continue to receive transactional, service, account, security, and legal communications.

19. Third-Party Links and Services

The Services may contain links to third-party websites or services. ai12z does not control and is not responsible for their privacy, security, or content. Review the privacy policies of third-party services before providing information to them.

20. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. We will post the revised Policy with an updated effective date and provide additional notice of material changes where required or appropriate. Material changes generally apply prospectively. We will obtain consent where required by law.

21. Contact Us

Questions, privacy requests, or concerns may be directed to:

ai12z, Inc.

Email: compliance@ai12z.com

Telephone: (978) 415-9612

Legal mailing address: 867 Boylston Street, 5th Floor #1011, Boston, Massachusetts 02116, United States