# Privacy Policy

Last updated: 5 September 2025

Privacy Policy for California Residents
Privacy Policy for EU and UK Residents

## 1. Who we are

Jasnah Inc., a Delaware corporation, and its subsidiaries and affiliates ("us" or "we") respect your privacy and are committed to keeping your information secure. We are committed to protecting your privacy and complying with applicable data protection laws, including the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and relevant U.S. privacy regulations.

## 2. Scope & Audience

This Privacy Policy describes our practices with respect to information we collect from or about you when you use our private AI chat interface, applications, APIs, and related services (collectively, "**Services**").

This Privacy Policy is part of the Terms of Service applicable to your use of the Services. Please review this policy together with the **Terms of Service**, to understand all of your rights and obligations, and how we operate the Services.

All capitalized terms not otherwise defined in this privacy policy shall have the meanings ascribed to them in the **Terms of Service.**

**By using the Services you accept and agree to be bound and abide by this Privacy Policy and the Terms of Service.** If you do not want to agree to this privacy policy or the **Terms of Service**, you must not access or use the Services.

This Privacy Policy may change from time to time. Your continued use of the Services after we make changes is deemed to be acceptance of those changes, so please check the privacy policy periodically for updates.

## 3. Information We Collect

| Category | What We Collect | Why We Collect It | Retention & Protection |
|---|---|---|---|
| **Account Information** | Email address<br>OAuth authentication proofs (access / refresh tokens, signature nonces). | Create and secure your account; send essential service notices. | Encrypted in transit and at rest; deleted when you close your account. |

| | | | |
|---|---|---|---|
| **Chat Content** | Content uploaded to our private AI chat interface , which could contain personal data, including:<br>● text responses<br>● images<br>● prompts<br>● knowledge bases<br>● training utterances<br>● documents<br>● websites<br>and model outputs ("**Content**").<br>**Transition notice:** until the **history-encryption** rollout is complete (target week of 18 August 2025) Jasnah support engineers may, in rare support scenarios, view plaintext Content. Once live, Content will be stored only in ciphertext that is unreadable to Jasnah personnel. | Display optional chat history you choose to save. | Ciphertext stored inside an attested enclave; keys derived from your OAuth credentials.<br>No customer-managed keys (CMK) are stored;<br>Deleted immediately when you clear history or close your account. |
| **Technical Information** | Timestamp, request ID, endpoint, model version, latency, success code.<br>Browser user-agent, OS, time-zone offset, screen size.<br>Crash stack traces (server errors).<br>*We discard IP addresses after routing.* | Operate, secure, debug, and scale the Service. | Logs kept 30 days "hot" / 90 days archived, then purged. |
| **Usage & Billing Metadata** | Input/output token counts; model version; timestamp; conversation ID. | Calculate usage-based fees; enforce rate limits; compile aggregate statistics. | Collected inside the enclave; stored separately from Content. Retention currently **up to 12 months**. |
| **Attestation Artifacts** | Per-request CPU/GPU enclave quotes, container hash, policy digest, timestamp, account ID. | Provide cryptographic proof that **every** interaction ran inside a verified enclave. | Stored append-only for as long as your account (or associated chat history) exists; may be retained longer to preserve verifiability but for no longer than 12 months. |

| | | | |
|---|---|---|---|
| **Local Storage Keys** | Browser keys such as `auth_token`, `history_pref`, `theme`. | Keep you signed in; remember UI settings. | Reside only in your browser; you may clear them any time. |
| **Support & Communications** | Name, email, and the contents of messages you send us (email, Discord, in-app chat). | Respond to inquiries; improve support. | Retained up to 24 months unless legal obligations require longer. |

We do not store API keys in plaintext and do not keep chat content in our databases. Our infrastructure providers may process limited network metadata (e.g., IP addresses) to deliver the service.

**Retention.** Chat artifacts and derived metadata are retained for **up to 5 years** (or shorter per policy) then deleted or anonymised; payment records are kept as required by law. Admins can request earlier deletion where feasible.

**Sub-processors.** We use vetted providers under data-processing terms—for example **Stripe** (payments), **Supabase** (authentication/storage), and **hosting (e.g., Vercel/Cloud)**. A current list and regions appear in the **Privacy Policy for EU and UK Residents**

**Cookies and Similar Technologies.** We use only strictly necessary technologies to operate the Service (e.g., session cookies for authentication and CSRF protection). We do not use analytics, advertising cookies, or web beacons for tracking, and we do not permit third-party ad tech on the Service. Browser storage (e.g., local/session storage) is limited to essential settings. If this changes, we will update this notice and, where required, obtain consent.

## 4. "No PHI" (Default)

- Scope. The Service is not intended to collect or store Protected Health Information (PHI) under HIPAA.
- User instructions. Users must not input PHI. We apply technical and policy controls (e.g., redaction/filters) to reduce accidental PHI entry.
- If PHI is submitted. If PHI is inadvertently provided, it will be secured and handled per this policy. HIPAA obligations do not apply unless the HIPAA Addendum below is expressly enabled.

## 5. HIPAA Addendum (If Enabled for Designated Workspaces/Customer)

- When this applies. This Addendum applies only where [Company] acts as a Covered Entity or Business Associate and a Business Associate Agreement (BAA) is in place for designated workflows.
- Permitted uses/disclosures. We will use or disclose PHI only as permitted by HIPAA and the BAA, including for Treatment, Payment, and Health Care Operations (TPO), or as otherwise authorized by the individual or required by law.

- Safeguards. We implement administrative, physical, and technical safeguards (access controls, encryption, audit logging, minimum-necessary, workforce training) appropriate to the risk and as required by HIPAA. Where supported, **confidential computing** provides enclave-based protection during processing of PHI; HIPAA safeguards (access controls, encryption, audit logging, minimum-necessary) continue to apply.

- Subcontractors. Any subcontractor that creates, receives, maintains, or transmits PHI on our behalf will agree in writing to HIPAA-compliant obligations.

- Breach notification. We will investigate potential Security Incidents and provide Breach notices in accordance with HIPAA and the BAA.

- Individual rights. We will support the Covered Entity's obligations to provide access,amendment, and accounting of disclosures of PHI, as applicable.

- Return/Destruction. Upon termination or request, we will return or destroy PHI consistent with HIPAA and the BAA, unless infeasible (in which case protections continue).

## 6. How We Use Personal Data We Collect

We use the personal and usage information we collect for the following purposes, and we ensure that each use of your data has a lawful basis (such as your consent, our legitimate interests in improving our Services, or performing a contract with you):

- **Account & Auth -** (name, email, workspace/user IDs, authentication records)

- **Aggregate statistics –** use de-identified metrics (never plaintext Content) to improve performance

- **Billing & administration –** meter token usage and process payments, no full card numbers

- **Content (your prompts and outputs) -** ephemeral by default; stored only if your organization enables storage (e.g., saved history or RAG)

- **Legal compliance –** comply with applicable laws and enforce our Terms

- **Operational Metadata (timestamps, usage measures, request IDs, IP/agent) -** to operate, secure, bill, and comply

- **Security & integrity –** detect fraud or abuse, enforce rate limits, and verify Trusted Execution Environment (TEE) integrity via per-request attestation

- **Security/Audit Logs -** access events, admin actions, enclave attestations

- **Service Delivery -** authenticate you, route requests, generate responses, and (optionally) store your chat history

- **Support:** - respond to questions, bug reports, or feedback you submit.

**We never** train, retrain, or fine-tune models on your Content, nor do we run automated content scanning or sell personal information.

## 7. Legal Bases

We process personal data for these reasons (GDPR refs in brackets):

- **Contractual necessity (Art. 6(1)(b))** To set up and run your account, provide the chat service (including search/RAG and file uploads), support you, and apply your settings. If you don't provide the data we need for these functions, some features won't work.

- **Legal obligation (Art. 6(1)(c))** To comply with laws—e.g., security and audit requirements, keeping certain records, responding to lawful requests, and fulfilling data-rights requests.

- **Legitimate interests (Art. 6(1)(f))** To keep the service **secure and reliable** (logging, threat detection, abuse prevention), to **measure and improve** performance and guardrails (without training foundation models on your content), to run **light product analytics**, and to **defend legal claims**.
  We balance these interests against your rights and minimise data. **You can object at any time**—see "Your Rights."

- **Consent (Art. 6(1)(a))** Only for optional features or communications, such as **saved chat history** beyond the default, **personalised suggestions**, **voice input/transcription**, or **marketing emails**. You can **withdraw consent at any time** in settings or by contacting us. Withdrawal doesn't affect past processing; we'll stop the feature going forward.

- **Special categories (Art. 9).** The Service isn't meant for special-category or criminal-convictions data. Please don't input it unless necessary and permitted. If such data is processed, we'll rely on a valid Art. 9(2) condition (e.g., **explicit consent**, **legal claims**, or **employment-law**) or delete it.

**Controller/processor roles.**

For internal deployments, **Jasnah Inc.** is the **controller**. If we operate the Service for another group entity or customer, we act as **processor** under a DPA and they determine the legal basis.

**Equivalent laws.**
"GDPR" includes the **UK GDPR**. Where local law uses different terms (e.g., Switzerland's **FADP**), we rely on the closest equivalent (consent, legitimate/overriding interests, or legal obligation).

You may withdraw consent at any time via in-product settings or by contacting us. No advertising networks, data brokers, or social-media platforms receive your data.

**8. Use of Content; No Training.**

We do not use your Content (Inputs or Outputs) to train, retrain, or fine-tune our models. We process Content only to provide and secure the Services, troubleshoot issues, comply with law, and enforce our Terms. We do not sell personal information.

**9. Processing Model (Confidential Computing).**

Prompts and outputs are encrypted in transit and at rest. During inference, they are decrypted only inside an attested hardware enclave (e.g., Intel® TDX) designed to prevent access by our personnel and cloud operators. We may retain Operational Metadata (e.g., timestamps, usage volumes, IP address/user agent) for billing, abuse prevention, and compliance. We do not retain plaintext Content outside the enclave unless you or your organization enables storage (e.g., saved chat history or RAG indexes) or we are legally required to preserve it.

**10. Limited Exceptions to Access.**

In rare cases, we may access Content if: (i) you or your organization request support; (ii) required by applicable law or valid legal process; or (iii) necessary to investigate abuse affecting the security or integrity of the Services. Such access is time-bound, logged, and minimised, and, where lawful, we will provide notice.

## 11. International Transfers

In case of transfers of personal data outside the European Economic Area, the United Kingdom or Switzerland, we rely on appropriate transfer mechanisms and are compliant with the EU-US, UK-US and/or Swiss-US Data Privacy Framework self-certification program operated by the US Department of Commerce. Please refer to **Privacy Policy for EU and UK Residents** for more information.

## 12. Security Measures

We implement appropriate technical and organisational measures—aligned with industry standards and GDPR Article 32—with a **confidential-computing–first** design. **Content is encrypted in transit and at rest and decrypted only within an attested hardware enclave** (e.g., Intel® TDX) verified via **remote attestation**; by default, plaintext Content is **not retained outside the enclave**. We maintain layered controls for data confidentiality, integrity, and availability (e.g., modern encryption in transit and at rest, strong identity and access management with SSO/MFA/RBAC, network and application hardening, continuous monitoring and audit logging, least-privilege/time-bound access, and tested incident-response and business-continuity procedures). We practise data minimisation and configurable retention, and we regularly assess our controls through independent reviews and penetration testing. Where we use third-party service providers or model APIs, they operate under written data-processing terms (including no-training commitments where applicable) and are subject to appropriate security and privacy due diligence.

## 13. Data Retention

We retain personal information only for as long as needed to **provide and secure** the Services, or as required to **comply with law**. When data is no longer necessary for these purposes, we **delete, de-identify, or aggregate** it within **60 days**, unless a longer period is required by law or a valid legal hold applies.

If you have an account with us, we retain your information while the account is active and as needed to perform our contractual obligations, deliver the Services, comply with legal obligations, resolve disputes, preserve legal rights, and enforce our agreements. Once no longer necessary, we will delete, de-identify, or aggregate the information to the extent possible.

**Enclave processing (Content).** By default, **prompts and outputs ("Content") are processed inside an attested hardware enclave and are not retained in plaintext outside the enclave**. If you or your organization **enable storage** (e.g., saved chat history or RAG indexing), encrypted copies of Content and derived artifacts may be retained according to the settings below.

**Customer controls.** Depending on your Services plan, you may **configure retention** for end-user information and apply different settings to **messages, files, or other types of Customer Data**. Customer deletions and retention changes may result in the deletion and/or de-identification of related personal information.

**Default retention schedule**

| Data type | Default retention | Deletion trigger |
|---|---|---|
| Account data (profile, auth records, workspace settings) | Life of account | Account closure (plus up to [60] days for deletion workflows) |

| | | |
|---|---|---|
| Content (plaintext) processed inside enclave | Ephemeral (not stored outside enclave by default) | Not retained post-processing (unless storage is enabled or required by law) |
| Chat Content (ciphertext) stored outside enclave (if storage enabled by organisation) | Up to 5 years (configurable) | Admin “clear history,” workspace policy expiry, or account deletion |
| Derived artifacts (embeddings, RAG indexes) (if enabled) | Up to 5 years (configurable) | Re-indexing, admin deletion, or account deletion |
| Usage & billing metadata (timestamps, request IDs, usage volumes, IP/agent) | Life of account (minimum 12 months for reconciliation) | Policy expiry or account deletion (subject to legal recordkeeping) |
| Logs & diagnostics (security/app/service logs) | 30 / 90 days rolling purge (per log class) | Rolling purge; extended retention for investigations/legal holds |
| Attestation artifacts (enclave measurements/evidence) | Life of account (may extend for audit/compliance) | Account deletion or end of audit/legal hold |
| Backups | Up to 35 days (rolling) | Scheduled expiry; accelerated purge on validated deletion request where feasible |

**Legal holds & exceptions.** We may preserve limited records where necessary to comply with law, legal process, or enforce our rights. Preservation lasts only as long as required and is logged.

## 14. Your Rights

You may have rights to access, correct, delete, or port your data, and to object or restrict certain processing. Exercise these through in-product settings or by emailing privacy@near.ai. We may require identity verification.

## 15. Minors

You must be 13+ to use the Services; if under 18, you need parental/guardian consent. Certain features (e.g., paid plans, API) may require 18+. We may adjust eligibility thresholds where required by law.

## 16. Changes to This Privacy Policy

It is our policy to post any changes made to the privacy policy on this page. When changes are made, we will post a revised version on our Website with the last updated and effective date posted on the top of this page.

## 17. Contact Information

To ask questions or comment about this privacy policy and our privacy practices, please direct such inquiries to:

E-mail: privacy@near.ai