Privacy Policy

Effective: 6 October 2025

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.

For consumer Services, Jasnah Inc. is the controller of your personal information. For enterprise tenants, Jasnah acts as a processor under a DPA, processing personal data solely on the customer’s documented instructions. If you have questions about the processing of your personal data that we process on behalf of enterprise customers, please contact the relevant customer with your questions.

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**”).

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.

The Services may contain links or other connections to other third-party websites, platforms, products, services or applications that are independent of our Services. The information collection practices and privacy policies of these third parties may differ from ours. We provide links to you only as a convenience, and the inclusion of any link does not imply affiliation, endorsement or adoption by Ascend of any site or any information contained therein.

3. Information We Collect

Information we collect and the purposes for which we collect it include the following:

Category	**What We Collect**
Account Information	Email address OAuth authentication proofs (access / refresh tokens, signature nonces).

Chat Content	Content uploaded to our private AI chat interface , which could contain personal data, including: ● text responses ● images ● prompts ● knowledge bases ● documents ● websites and model outputs ("**Content**").
Technical Information	Timestamp, request ID, endpoint, model version, latency, success code. Browser user-agent, OS, time-zone offset, screen size. Crash stack traces (server errors).
Usage & Billing Metadata	Input/output token counts; model version; timestamp; session ID or request ID; .
Attestation Artifacts	Per-request CPU/GPU enclave quotes, container hash, policy digest, timestamp, account ID.
Local Storage Keys	Browser keys such as `auth_token`, `history_pref`, `theme`.
Support & Communications	Name, email, and the contents of messages you send us (email, Discord, in-app chat).
Analytics events (GA4)	Audience measurement/performance

Our infrastructure providers may process limited network metadata (e.g., IP addresses) to deliver the service.

Data we collect automatically

In addition to data we collect directly from you, we may automatically collect certain information about the computer or devices (including mobile devices or tablets) you use to access the Services. As described further below, we may collect and analyze information such as (a) IP addresses, general location information (e.g. inferred from a IP address), unique device identifiers, IMEI and TCP/IP address, and other information about your computer or device(s), browser types, browser language, operating system, mobile device carrier information, the state or country from which you accessed the Services; and (b) information related to the ways in which you interact with the Services, such as: referring and exit web pages and URLs, platform type, the number of clicks, domain names, landing pages, pages and content viewed and the order of those pages, statistical information about the use of the Services, the amount of time spent on particular pages, the date and time you used the Services, the frequency of your use of the Services, error logs, and other similar information. As described below, we may use third-party analytics providers and technologies, including cookies and similar tools, to assist in collecting this information.

We may also collect data about your use of the Services through the use of Internet server logs, cookies and/or tracking pixels. A web server log is a file where website activity is stored. A cookie is a small text file that is placed on your computer when you visit a website, that enables us to: (i) recognize your computer; (ii) store your preferences and settings; (iii) understand the web pages of the Services you have visited; (iv), enhance your user experience by delivering content specific to your interests; (v) perform searches and analytics; and (vi) assist with security administrative functions. Tracking pixels (sometimes referred to as web beacons or clear GIFs) are tiny electronic tags with a unique identifier embedded in websites, online ads and/or email, and that are designed to provide usage information, measure popularity of the Services, and to access user cookies.

We may also collect your approximate location based on IP address.

Do Not Track. There is no uniform or consistent standard or definition for responding to, processing, or communicating Do Not Track signals. At this time, the Services do not function differently based on a user's Do Not Track signal. For more information on Do Not Track signals, see All About Do Not Track.

Analytics & Online Tracking (**Google Analytics)**

As of the effective date of this Policy, we do not permit third-party advertising or cross-context behavioral advertising on the Service.

What we use and why. We use Google Analytics (GA) to measure and improve Service performance (e.g., which pages/screens are used, stability, and load times). To prevent Google Analytics from using your information for analytics, you may install the Google Analytics Opt-out Browser Add-on by clicking here.

Data collected via analytics. Depending on your settings, GA may collect: device/browser information, GA cookie/SDK identifiers, pages/screens viewed, events and their parameters (e.g., clicks, errors), session duration and engagement time, referrer and campaign parameters, approximate location (country/city), and audience membership we define (e.g., new vs. returning users).

4. How We Use Personal Data We Collect

We use the personal and usage information for the various purposes, including the following:

- **Account & Authorization -** provide access to and administer your account**Analytics –** allow us and our analytics partners (e.g., Google) to understand how our users use our Services so that we can measure and improve the Services
- **Billing & administration –** meter token usage and process payments, no full card numbers
- **Communicate with you** – including to keep you posted on purchases, Services updates, changes to our terms and policies, and provide you with content we think will be of interest to you
- **Legal compliance –** comply with applicable laws and enforce our Terms
- **Operate and deliver the Services -** authenticate you, route requests, generate responses, (optionally) store your chat history, and otherwise provide and operate the Services you requested
- **Security & integrity –** detect fraud or abuse, enforce rate limits, and verify Trusted Execution Environment (TEE) integrity via per-request attestation
- **Support:** - respond to questions, bug reports, or feedback you submit.

We may combine the information we collect from other sources (such as your interactions with us on social media) with the other information we collect from and about you and use such combined information in accordance with this Policy. We may also de-identify information we collect so the information cannot reasonably identify you or your device, or we may collect information that is already in de-identified form. Our use and disclosure of de-identified information is not subject to any restrictions under this Privacy Policy, and we may use and disclose it to others for any purpose, without limitation.

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

5. How We Disclose Personal Data We Collect

We may disclose your information to the following entities:

- **Affiliates:** In accordance with applicable legal requirements and depending on our contracts with you, we may disclose information among our various entities for the business purposes as discussed above and in this Privacy Policy.
- **Vendors:** We engage vendors to perform business purposes, as described above, on our behalf and may disclose information to them to enable them to assist us with such business purposes, including analytics, hosting, transaction and payment processing, fraud prevention, and other services. Service providers may use such information for their operational purposes in order to provide their services to us.
- **Analytics:** As described above, we may disclose or make available some of your information to analytics partners to provide analytics services.
- **Law Enforcement, Regulators, Anti-fraud Coalitions, Attorneys and similar organizations:** We disclose the information we collect, as appropriate, to these third parties when we have a good faith belief that such disclosure is necessary to protect and enforce the legal rights, privacy, and safety of ourselves and our users; protect against possible fraud, misuse or misappropriation of our Services, or illegal activity; respond to requests from government and other authorities; protect our intellectual property rights and the integrity of our Services, and otherwise comply with legal process.
- **Business transactions:** In the event that we or any affiliate is involved in a merger, acquisition, or transfer of control, bankruptcy, reorganization or sale of some or all assets, we may sell or transfer the information described in this Policy as part of that transaction or diligence associated with or in contemplation of such matters.
- **Others with your consent:** We may disclose your information when we have on your consent to do so

6. Legal Bases

The laws in some jurisdictions require companies to tell you about the legal grounds they rely on to process your information. To the extent those laws apply, our legal bases are as follows:

- **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** or **legal claims**) or delete it.

7. 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.

8. International Transfers

Whenever we transfer your personal data out of the European Economic Area ("**EEA**"), Switzerland and the United Kingdom we will endeavour to ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

- Where we use certain vendors, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

Please contact us if you want further information on the specific mechanism used when transferring your personal data outside your jurisdiction.

9. Security Measures

We implement technical and organisational measures 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 strive to practise data minimisation and configurable retention, and we take steps to 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.

Although we work to protect the security of your account and other data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure.

10. 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** in accordance with our retention procedures, unless a particular retention 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.

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.

11. 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. Specifically, your local laws (including applicable laws in the EU, UK, Switzerland, and United States (including California, Connecticut, Colorado, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Montana, Minnesota, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Virginia, Tennessee, and Texas, as well as similar U.S. state laws)) may permit you to request that we:

- provide access to and/or a copy of certain information we hold about you
- update information which is out of date or incorrect
- delete certain information that we are holding about you
- restrict the way that we process and disclose certain of your information

- prevent the processing of your information for direct-marketing purposes (including any direct marketing processing based on profiling)
- opt out of the processing of your information for automated processing that results in legal or similarly significant effects (if relevant)

Your local laws may also permit you to revoke your consent to the processing of your information for certain purposes.

Oregon and Minnesota residents can request a list of the specific third parties, other than natural persons, to which we have disclosed information.

As provided in applicable law, you also have the right to not be discriminated against for exercising your rights

Please note that certain information may be exempt from such requests under applicable law. For example, we need certain information in order to provide the Services to you. We will take reasonable steps to verify your identity before fulfilling your request.

You may be able to designate an authorized agent to make requests on your behalf. In order for an authorized agent to be verified, you must provide the authorized agent with signed, written permission to make such requests or a power of attorney. We may also follow up with you to verify your identity before processing the authorized agent's request as permitted by applicable law.

If you are a resident of Virginia, Minnesota, Montana, Oregon, Tennessee, Texas, Iowa, Indiana, Kentucky, Maryland, Nebraska, New Hampshire, New Jersey, Rhode Island, Delaware, Colorado, or Connecticut, and we deny your information request, you have the right to appeal our denial. You can exercise this right by contacting us at the contact information provided below. Your description must include your full name and the email address used for your account with us, along with a copy of the denial notice you received from us.

If you are using the Services as a customer's end-user, please contact that customer to exercise your rights.

Notice of Right to Opt Out of Sales of Personal Information and Processing/Sharing of Personal Information for Targeted Advertising Purposes.

Depending on your jurisdiction (including residents of California, Colorado, Connecticut, Delaware, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas, Utah, and Virginia), you may also have the right to opt out of "sales" of your information and "sharing" or processing of your information for targeted advertising.

As of the Effective Date of this Policy, we do not sell or share your information in exchange for money or in ways that enable recipients of your data to use it for their own purposes. For example, our analytics providers, such as Google, are configured to only use data on our behalf.

We also do not knowingly sell the personal information of minors under 16 years of age without legally-required affirmative authorization.

Please note that if you have a legally-recognized browser-based opt out preference signal turned on via your device browser, we recognize such preference in accordance with applicable law.

Marketing. We may contact you with the latest Services announcements, promotions, and information about upcoming events in accordance with applicable law. To opt out of marketing, please follow the unsubscribe instructions in the marketing communication or email us using the contact information below. Please note that it may take some time, consistent with applicable law, to process your request. Also,

please note that your opt out will only apply to the specific entity that sent you a marketing communication.

12. 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. EEA users must be 16+ (or the local digital consent age).

If we become aware that we have collected data without legally valid parental consent from children under an age where such consent is required in connection with such Services, we will take reasonable steps to delete it as soon as possible.

13. California Privacy Rights Notice

This section describes how we collect, use, and share Personal Information of California residents in our capacity as a Business under the California Consumer Privacy Act ("CCPA"), and such residents' rights with respect to that Personal Information.

For purposes of this section, the terms "Personal Information," "Sensitive Personal Information," and "Business" have the respective meanings given in the CCPA, but Personal Information does not include information exempted from the scope of the CCPA. In some cases, we may provide a different privacy notice to certain categories of California residents, such as job applicants and employees/personnel, in which case that notice will apply instead of this section.
Throughout this Privacy Policy, we discuss in detail the specific pieces of personal information and sensitive personal information we collect, the sources of that information, and how we disclose it. Under the CCPA, we also have to provide you with (1) the "categories" of personal information and sensitive personal information we collect and disclose for business or commercial purposes (as "categories" are defined by the CCPA); (2) the categories of other parties to whom we (a) disclose such information for a business purpose, (b) "share" information for "cross-context behavioral advertising," and/or (c) "sell" such information.

The terms "sale" and "share" have the meanings given to such terms in the CCPA, and not the common meanings of these terms in conversational English. Under the CCPA, "sharing" is defined as the targeting of advertising to a consumer based on that consumer's personal information obtained from the consumer's activity across websites, and "selling" is defined as the disclosure of personal information to third parties in exchange for monetary or other valuable consideration. We don't "sell" or "share" information, as such terms are defined in the CCPA. Please see the following chart for the rest of this information, which is also described throughout this Privacy Policy.

Category of Personal Information	**How We Use this Personal Information**	**Categories of Parties to Whom We Disclose Personal Information**
Contact information (such as information associated with your account, like your email address)	Provide the Services; communicate with you; personalize the Services; analyze, troubleshoot, maintain, and improve the Services; marketing; enforce agreements; security/fraud prevention; to comply with our legal obligations; business transfers; as authorized by you	Affiliates and subsidiaries; vendors; analytics providers; as directed by you (e.g. exhibitors at conferences and events)

Content of communications through the private AI chat interface (such as text, photos/images, prompts, knowledge bases, documents, websites, and outputs)	Provide the Services; communicate with you;; analyze, troubleshoot, maintain, and improve the Services; marketing; enforce agreements; security/fraud prevention; to comply with our legal obligations; business transfers; as authorized by you	Affiliates and subsidiaries; vendors.
Device and online information (such as mobile device content, IP address, browsing history, and usage information)	Provide the Services; communicate with you; personalize the Services; analyze, troubleshoot, maintain, and improve the Services; marketing; enforce agreements; security/fraud prevention; to comply with our legal obligations; business transfers; as authorized by you	Affiliates and subsidiaries; vendors; analytics providers; as directed by you
Commercial information, such as transactions with us	Provide the Services; communicate with you; personalize the Services; analyze, troubleshoot, maintain, and improve the Services; marketing; enforce agreements; security/fraud prevention; to comply with our legal obligations; business transfers; as authorized by you	Affiliates and subsidiaries; vendors; analytics providers; as directed by you
Username and password to access your account	Provide the Services; analyze, troubleshoot, maintain, and improve the Services; enforce agreements; security/fraud prevention; to comply with our legal obligations; business transfers; as authorized by you	Affiliates and subsidiaries; vendors
General geolocation (e.g., inferred from IP address)	Provide the Services; analyze, troubleshoot, maintain, and improve the Services; enforce agreements; security/fraud prevention; to comply with our legal obligations; business transfers; as authorized by you	Affiliates and subsidiaries; vendors
Inferences we draw from information about you and other information (any other information you choose to provide directly to us)	Provide the Services; communicate with you; personalize the Services; analyze, troubleshoot, maintain, and improve the Services; marketing; enforce agreements; security/fraud prevention; to comply with our legal obligations; business transfers; as authorized by you	Affiliates and subsidiaries; vendors; analytics providers; as directed by you

The CCPA sets forth certain obligations for businesses that "sell" personal information or "share" personal information for cross-context behavioral advertising purposes. Under the CCPA, "sale" and "sharing" are defined such that they may include allowing third parties to receive certain information for advertising purposes. Please review the "Notice of Right to Opt Out of Sales of Personal Information and Processing/Sharing of Personal Information for Targeted Advertising Purposes" for information on opting out of "sales" or "sharing" of your personal information. We do not knowingly sell or share the personal information of minors under 16 years of age.

California residents may make certain requests about their personal information under the CCPA as set forth in the "Your Rights" section above.

If we ever offer any financial incentives in exchange for your personal information, we will provide you with appropriate information about such incentives.

We collect a username and password that enables access to your account. This information is considered sensitive personal information under the CCPA. We do not process such information for a purpose that would require us to provide a “right to limit” under the CCPA.

Please see the “Data Retention” section below for information about how long we maintain your Personal Information.

Shine the Light: California law permits customers who are California residents to request certain information once per year regarding our disclosure of “personal information” (as that term is defined under applicable California law) to third parties for such third parties’ direct marketing purposes. To request such information, please contact us at privacy@near.ai.

Colorado Residents

The Colorado Privacy Act requires us to provide additional information on how we process “personal data,” as that term is defined by the Colorado Privacy Act. Please see the chart above to see those additional details.

Nevada Residents

If you are a resident of Nevada, you have the right to opt-out of the sale of certain personal information to unaffiliated parties. We do not sell your information as sales are defined under the Nevada law.

14. Changes to This Privacy Policy

This Privacy Policy may change from time to time. 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. 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.

15. 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