

## EUROPEAN ADDENDUM TO PRIVACY POLICY

Last updated: 5 September 2025

This Addendum to the [Privacy Policy](#) applies to you only if accessing the Services from within the confines of the European Economic Area (“EEA”), Switzerland or the United Kingdom. **THIS ADDENDUM TO THE PRIVACY POLICY DOES NOT APPLY TO ANY PERSON LOCATED WITHIN THE UNITED STATES OF AMERICA OR ANY OF ITS TERRITORIES, OR ANY COUNTRY OUTSIDE THE EEA, SWITZERLAND OR THE UNITED KINGDOM.**

Additional Information requirements pursuant to Art. 13 GDPR (EU General Data Protection Regulation):

This privacy policy addendum (the “**Privacy Policy European Addendum**”) applies solely to our and our service providers’ processing of the “personal data” (as such term is defined in the GDPR) of data subjects who are in the European Economic Area, where they use, browse or interact with, the Website, the Apps and the Tools.

It is important that you read this Privacy Policy European Addendum together with any other privacy policy, privacy notice or fair processing policy we and our service providers may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we and our service providers are using your data. This Privacy Policy European Addendum supplements other notices and privacy policies and is not intended to override them.

### Controllers

Jasnah Inc. is a controller with respect to the Services.

### Data Privacy Manager

We have appointed a data privacy manager who is responsible for overseeing questions in relation to this Privacy Policy European Addendum. If you have any questions about this Privacy Policy European Addendum, including any requests to exercise your legal rights, please contact the data privacy manager using the details set out below:

Full name of legal entity: Jasnah Inc.

Email address: [privacy@near.ai](mailto:privacy@near.ai)

### Changes to the Privacy Policy and your duty to inform us of changes

We keep the privacy policy under regular review.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

### The data we and our service providers collect about you

What	Type of Data	Purpose	Storage/Retention
------	--------------	---------	-------------------

<b>Account Information</b>	Email address 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.
<b>Content</b>	Inputs (e.g., text, files, model weights, data) and Outputs (model-generated results)	Display optional chat history you choose to save.	Ciphertext stored inside an attested enclave; keys derived from your OAuth credentials. No customer-managed keys (CMK) are stored; Deleted immediately when you clear history or close your account.
<b>Technical Information</b>	Timestamp, request ID, endpoint, model version, latency, success code. Browser user-agent, OS, time-zone offset, screen size. Crash stack traces (server errors). <i>We discard IP addresses after routing.</i>	Operate, secure, debug, and scale the Service.	Logs kept 30 days "hot" / 90 days archived, then purged.
<b>Usage &amp; Billing Metadata</b>	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 <b>up to 12 months..</b>
<b>Attestation Artifacts</b>	Per-request CPU/GPU enclave quotes, container hash, policy digest, timestamp, account ID.	Provide cryptographic proof that <b>every</b> 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.
<b>Local Storage Keys</b>	Browser keys such as <code>auth_token</code> , <code>history_pref</code> , <code>theme</code> .	Keep you signed in; remember UI settings.	Reside only in your browser; you may clear them any time.

<b>Support &amp; Communications</b>	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 and our service providers do not collect other categories of Special Data (as defined in the GDPR) about you such as details about your religious or philosophical beliefs, sex life, political opinions, trade union membership, genetic and biometric data, or information about criminal convictions and offences of European residents.

Please note that when using the Website, the Apps and the Tools, you may have the option to access, use or download third-party content. If you make use of such features of the Website, the Apps and the Tools, you will be accessing content offered by our and our service providers' third party vendors or third parties or are not affiliated with us or our service providers. We do not control what information they may collect from you to allow them to make their services available, such as Technical Data or Usage Data. This Privacy Policy European Addendum does not apply to collection or processing of your personal data by such parties.

We and our service providers may also collect, use and share aggregated data such as statistical or demographic data for any purpose. Aggregated data could be derived from your personal data but is not considered personal data in law as this data will **not** directly or indirectly reveal your identity. For example, we and our service providers may aggregate your Usage Data to calculate the percentage of users accessing a specific feature of the Website, the Apps and the Tools, or we and our service providers may collection anonymous registration data to calculate the number of individual users accessing the Website, the Apps and the Tools. However, if we or our service providers combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Policy European Addendum.

### **If you fail to provide personal data**

Where we and our service providers need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with the Website, the Apps and the Tools). In this case, we and our service providers may have to suspend your access to all or parts of the Website, the Apps and the Tools, as applicable, but we will endeavour to notify you if your access is suspended to such features.

### **How is your personal data collected?**

We and our service providers use different methods to collect data from and about you including through:

**Direct interactions.** You may give us and our service providers your identity, contact data, commercial data, and special data by registering for an account, as part of the employment process, requesting or obtaining access to the Services and Website, or by corresponding with us or our service providers through any means.

**Automated technologies or interactions.** For a description of cookies and other Tracking Technologies used as part of the Services and Website, please visit the [Cookie Policy](#).

**Third parties or publicly available sources.** We and our service providers receive personal data about you from various third parties and public sources as set out below:

- Identity Data from your Account Information and Support and Communication Information, this includes your name and email address.
- Technical Information, Usage & Billing Metadata when you choose to use or access third-party websites and services linked or otherwise made available on or through the Services and Website.

### **How we and our service providers use your personal data**

We will only use your personal data that we collect when the law allows us to. Most commonly, we and our service providers will use your personal data in the following circumstances:

- Where we and our service providers make available the Services and Website to you, and provide you with products and services relating to the same.
- Where it is necessary for our and our service providers' legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we and our service providers need to comply with a legal obligation.
- Generally, we and our service providers do not rely on consent as a legal basis for processing your personal data. You have the right to withdraw consent to marketing at any time by contacting us or through the "unsubscribe" feature in any marketing communication we or our service providers may send you.

### **Purposes for which we and our service providers will use your personal data**

We have set out below, in a table format, a description of all the ways we, and our service providers on our behalf, plan to use your personal data that we each collect through any of the foregoing means, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we and our service providers may process your personal data for more than one lawful ground depending on the specific purpose for which we and our service providers are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

<b>Purpose/Activity</b>	<b>Type of data</b>	<b>Lawful basis for processing including basis of legitimate interest</b>
To provide the Website To provide the Services	Account Information Technical Information Usage & Billing Metadata Support & Communications Information	Performance of a contract with you. Necessary to comply with a legal obligation. Necessary for legitimate interests (to keep our records updated and to study how users use the Services and the Website).
To manage our and our service providers' relationship with you, which may include: Notifying you about changes to our relationship. Enabling you to interact with us or our third-party vendors. Responding to requests from you. Updating your personal data that relates to our relationship.	Account Information Technical Information Usage & Billing Metadata Support & Communications Information	Performance of a contract with you. Necessary to comply with a legal obligation. Necessary for legitimate interests (to keep our records updated and to study how users use the Services and Website).

To administer and protect our business, the Services and Website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data, identity verification, fraud prevention, cybersecurity monitoring).	Account Information Technical Information Usage & Billing Metadata	Necessary for legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or corporate event). Necessary to comply with a legal obligation.
To deliver relevant Services and Website content.	Account Information Technical Information Usage & Billing Metadata Support & Communications Information	Necessary for legitimate interests (to study how users use the Services and Website, to develop them, to grow our business, and to inform our and our service providers' marketing strategies).
To use data analytics to improve the Services and Website, products/services available on or through the Services and Website, marketing efforts, customer relationships and experiences, and identify potential users.	Account Information Technical Information Usage & Billing Metadata Support & Communications Information	Necessary for legitimate interests (to define types of users for the Service and Website, to keep the Services and Website updated and relevant, to grow our business, and to inform our and our service providers' marketing strategies).
To make suggestions and recommendations to you about products or services that may be of interest to you.	Account Information Technical Information Usage & Billing Metadata Support & Communications Information	Necessary for legitimate interests (to develop our and our service providers' respective products/services and to grow our business).

## Marketing

We to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. We have established the following personal data control mechanisms:

### Promotional offers from us and our service providers

We and our service providers may use your Account Information, Technical Information, Usage & Billing Metadata, and Support & Communications Information to form a view on what we and our service providers think you may want or need, or what may be of interest to you (which we each may use for marketing purposes and may share with our respective third-party vendors).

You will receive marketing communications from us and our service providers if you have requested information from either of us or purchased services from either of us, and you have not opted out of receiving that marketing.

### Third-party marketing

We will get your express opt-in consent before sharing your personal data with any third party for their own marketing purposes.

### Opting out

You can ask to stop receiving marketing messages at any time by following the opt-out links on any marketing message sent to you by us or by our service providers on our behalf.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us and our service providers as a result of a service purchase or other transactions.

### **Cookies on the Website**

For a description of cookies and other Tracking Technologies used on the Website, please visit the **Cookie Policy**.

Note that you may not be able to refuse all data collection even by setting your browser cookies settings, and that some collection of Technical and Usage Data may continue.

Also, note that we and our service providers use the following analytics service providers, who also collect Technical and Usage Data based on your use of the Services and Website. The analytics providers listed below are independent controllers of that data, and use it for their own purposes. You specifically grant your consent to such data collection and usage.

Service provider	Privacy Policy
Stripe	<a href="https://stripe.com/gb/privacy">https://stripe.com/gb/privacy</a>
Supabase	<a href="https://supabase.com/privacy">https://supabase.com/privacy</a>
Vercel	<a href="https://vercel.com/legal/privacy-policy">https://vercel.com/legal/privacy-policy</a>

### **Change of purpose**

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider its usage necessary for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please submit a request to [privacy@near.ai](mailto:privacy@near.ai)

If we or our service providers need to use your personal data for an unrelated purpose, we will notify you and explain the legal basis permitting such use.

Please note that we and our service providers may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

### **Disclosures of your personal data**

We and our service providers may share your personal data for the purposes of providing services to you, engaging in marketing activities, and making the Services and Website available to you, including the following:

- Internal Third Parties as set out in the Glossary.
- External Third Parties as set out in the Glossary.

Third parties to whom we and our service providers may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we or our service providers may seek to acquire other businesses or

merge with them. If a change happens to our or our service providers' business, then the new owners may use your personal data according to their own privacy practices.

We contract with third-party vendors to require that they do not use your personal data for their own purposes and to authorize them to process your personal data for specified purposes and in accordance with our instructions.

### **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 or our service providers 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](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).
- Where we or our service providers 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](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.

### **Data security**

We have in place security measures intended to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

### **Data retention**

We have implemented measures intended to ensure that we will not retain your personal data longer than is necessary to fulfil the purposes it was collected for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Note, however, that if we or our service providers have a legitimate interest in retaining the data, or if we are required to do so by applicable law, we will retain the data in accordance with our respective data retention plans and policies.

In some circumstances we and our service providers may choose to anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we and our service providers may use this information indefinitely without further notice to you.

### **Your legal rights**

Under certain circumstances, you have rights under data protection laws in relation to your personal data. You may: (1) request access to your personal data; (2) request correction of your personal data; (3) request erasure of your personal data; (4) object to processing of your personal data; (5) request restriction of processing your personal data; (6) request transfer of your personal data; or (7) right to withdraw consent by contacting [privacy@near.ai](mailto:privacy@near.ai).

### **No fee usually required**

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

### **What we and our service providers may need from you**

We and our service providers may need to request specific information from you to help confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights), including your: name and email address (if applicable), and an email to be used for future communication. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We and our service providers may also contact you to ask you for further information in relation to your request to speed up our response.

### **Time limit to respond**

We try to respond to all legitimate requests within one month. Occasionally it could take longer than a month if your request is particularly complex or you have made a number of requests. In this case, we or our service providers will notify you and keep you updated.

### **Glossary**

**Legitimate Interest** means the interest of our business in conducting and managing the business and enabling us and our service providers to give you the best service/product and the best and most secure experience that we can offer. We make sure to consider and balance any potential impact on you (both positive and negative) and your rights before processing your personal data for such legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we or our service providers have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess such legitimate interests against any potential impact on you in respect of specific activities by submitting a request to [privacy@near.ai](mailto:privacy@near.ai).

**Performance of Contract** means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

**Comply with a legal obligation** means processing your personal data where it is necessary for compliance with a legal obligation that we or our service providers are subject to.

## **THIRD PARTIES**

### **Internal Third Parties**

Affiliates of Jasnah Inc.

### **External Third Parties**

Service providers acting as processors. A list of such parties is available upon reasonable request.

Third-party service providers which collect data as set forth in this policy and are each an independent controller of such data, including:

Stripe Inc.

Supabase Inc.

Vercel Inc.



Regulators and other authorities acting as processors or joint controllers based in the United States who require reporting of processing activities in certain circumstances.

## **YOUR LEGAL RIGHTS**

You have the right to:

**Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

**Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we and our service providers may need to verify the accuracy of the new data you provide.

**Request erasure** of your personal data. This enables you to request deletion or removal of personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we and our service providers may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

**Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate compelling legitimate grounds for our and our service providers’ processing of your information which override your rights and freedoms.

**Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- If you want us to establish the data’s accuracy.
- Where our use of the data is unlawful but you do not want to erase it.
- Where you need us to hold the data even if we no longer require it, as you need it to establish, exercise or defend legal claims.
- You have objected to our use of your data but such data is necessary to verify whether we have overriding legitimate grounds to use it.

**Request the transfer** of your personal data to you or to a third party. We or will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us or our service providers to use or where we used the information to perform a contract with you.

**Withdraw consent** at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we and our service providers may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.