

Privacy Policy for neurvance.com

Privacy information for the Neurvance mind-map platform and its AI features

Last updated: 30 July 2026

Operator	Adam Samer Daabas / Neurvance
CVR	46436024
Country	Denmark
Legal email	legal@neurvance.com
Privacy email	privacy@neurvance.com
General email	adam@neurvance.com
Phone	+45 42839218

This Privacy Policy explains how Neurvance collects, uses, stores, shares, transmits, protects, and deletes personal data when you use neurvance.com and the Neurvance mind-map application.

Neurvance is the data controller for the personal data described in this Policy unless another provider acts as an independent controller for its own purposes.

1. Scope and who can use Neurvance

This Policy applies to account creation, mind maps, sticky notes, AI requests and outputs, web searches, generated images and charts, code-generation assistance, payments, support, and technical use of the Service.

Neurvance is intended only for people who are at least 18 years old. Neurvance does not knowingly provide accounts to children.

2. Important summary of AI data flows

Neurvance is an AI-assisted mind-map product. Its core AI features require server-side processing and, in many cases, transmission of selected content to providers outside Neurvance.

- You may choose one note, several notes, relevant connected context, or the entire mind map for an AI action.
- Grammar, rewriting, information, image, chart, and code features may send selected content to OpenAI or other external model providers.
- Deeper reasoning is performed using a Neurvance AI model hosted on RunPod infrastructure in Illinois, United States, and may also delegate sub-tasks to OpenAI or Anthropic.
- Web-search features may create and send search queries to Brave Search API.
- Mind maps, accounts, and related application data may be stored through Supabase, while Heroku may process application requests and technical logs.

Not every AI request sends the entire mind map. The amount sent depends on the feature and the content selected by the user. However, a user can choose the entire mind map, in which case all selected content may be transmitted for processing.

3. Personal data we collect

3.1 Account data

- name and email address;
- account identifier, creation date, status, plan, and settings;
- email-login or verification records;
- records showing acceptance of legal terms and age confirmation.

3.2 Mind-map and sticky-note data

- mind-map titles, sticky notes, node labels, descriptions, links, relationships, and structure;
- text, ideas, prompts, comments, and other content entered by the user;
- files, images, or other material uploaded to or connected with a mind map;

- creation and modification timestamps, ownership, permissions, and deletion status.

3.3 AI request and output data

- the action selected, such as grammar correction, information search, reasoning, image generation, chart creation, or code generation;
- the selected note, selected notes, relevant context, or entire mind map sent with the request;
- instructions, prompts, model settings, files, images, and technical metadata needed to perform the request;
- AI responses, generated code, generated images, search summaries, and other outputs;
- timestamps, model/provider used, request status, error information, token or credit usage, and safety or moderation results.

3.4 Search data

- search queries entered by the user or generated from selected notes;
- search results, source references, snippets, and timestamps;
- information needed to troubleshoot search requests and calculate usage.

3.5 Payment and subscription data

- billing name and email, customer identifier, subscription or plan status;
- payment history, invoice information, credit balance, renewal and cancellation status;
- limited payment metadata received from Stripe or another payment provider.

Neurvance does not intentionally store full card numbers or card-security codes. Those details are handled by the payment provider.

3.6 Technical, security, and cookie data

- IP address, server and application logs, login records, timestamps, request identifiers, and error logs;
- browser, device, operating-system, and network-related information;
- security, fraud-prevention, abuse-prevention, and moderation records;
- necessary cookies, session data, consent records, and analytics data where enabled.

4. How users control what is sent

Before or when activating an AI action, the user chooses or causes the application to select the content to be processed. Depending on the feature, this may be a single sticky note, multiple notes, connected context, an uploaded file or image, or the entire mind map.

Neurvance may add limited technical context needed to complete the request, such as the action name, note relationships, instructions, formatting requirements, or conversation state. Neurvance does not intentionally send unrelated mind maps to an AI provider.

Users should review their selection before activating an AI feature and should remove personal, confidential, or sensitive information that is not necessary for the request.

5. How we use personal data

- to create, authenticate, and manage accounts;
- to store, display, synchronise, and edit mind maps and sticky notes;
- to perform AI actions selected by the user;
- to route requests between Neurvance, RunPod, OpenAI, Anthropic, Brave Search API, or other providers;
- to generate, store, and return outputs, images, charts, code, and search results;
- to operate subscriptions, credits, billing, and payments;
- to provide support and respond to privacy, legal, and deletion requests;
- to secure, debug, monitor, and improve the reliability of the Service;
- to prevent fraud, abuse, policy violations, and security incidents;
- to comply with legal, tax, accounting, and regulatory obligations;
- to enforce the Terms of Use and protect Neurvance, users, and providers.

Neurvance does not use AI to make decisions about users that produce legal or similarly significant effects.

6. Legal bases for processing

Where the GDPR applies, Neurvance relies on one or more of the following legal bases:

- Contract: processing needed to create an account, store a mind map, perform a requested AI action, provide a paid plan, or deliver the Service.
- Legitimate interests: security, fraud prevention, debugging, abuse prevention, service administration, record keeping, and protection of legal rights, where those interests are not overridden by user rights.
- Consent: non-essential cookies, optional analytics or marketing, and optional uses that are clearly presented as consent-based.
- Legal obligation: accounting, tax, lawful requests, regulatory compliance, disputes, and data-protection obligations.

7. Service providers and data recipients

Neurvance uses service providers to operate the Service. The exact provider and model may depend on the feature, availability, cost, account configuration, and user request.

Provider	Purpose	Data that may be sent	Location / note
Supabase	Accounts, database, mind-map storage, subscriptions, logs, and backend services	Account data, mind maps, settings, payment status, and application records	Processing location depends on Neurvance configuration and provider operations
Heroku	Application and backend hosting, request routing, server operation, and logs	Requests, technical metadata, logs, and data needed to run the application	May involve processing outside Denmark or the EEA
RunPod	Hosting and executing Neurvance's own reasoning AI model	Selected notes or mind-map context, prompts, outputs, and technical metadata	Illinois, United States
OpenAI	Grammar, rewriting, information processing, image or chart-related generation, code generation, and other AI tasks	Selected content, prompts, files or images, outputs, and technical request metadata	May involve United States or other configured regions
Anthropic	Complex reasoning sub-tasks, code generation, and other model-assisted outputs	Selected content, prompts, outputs, and technical request metadata	May involve United States or other provider locations
Brave Search API	Web search and retrieval of public information	Search queries entered by the user or derived from selected content, plus request metadata	Brave Software Inc. is located in the United States
Stripe	Payments, subscriptions, invoices, fraud prevention, and refunds	Billing and transaction information	Processed under Stripe's own terms and privacy information
Simply.com	Domain, email, and related operational services	Email and technical service data where relevant	Provider processing locations may vary
Analytics providers, if enabled	Usage measurement and product analytics	Cookie identifiers, events, device and usage data	Non-essential analytics are used only where enabled and consent is obtained when required

8. Provider retention and model training

Neurvance does not promise that external providers operate with zero data retention. Provider practices may change, and providers may retain data for security, abuse prevention, legal compliance, billing, troubleshooting, or service operation.

At the date of this Policy, OpenAI states that API data is not used to train its models by default unless the customer opts in, and that standard abuse-monitoring logs may retain prompts and outputs for up to 30 days, subject to endpoint settings and exceptions. Anthropic states that inputs and outputs from its commercial API are not used for model training by default and are normally deleted from its backend within 30 days, subject to agreed controls, policy-enforcement, or legal exceptions.

At the date of this Policy, Brave states that search queries submitted through a Brave Search API customer account may be retained for up to 90 days for billing and troubleshooting, subject to legal obligations. Neurvance therefore advises users not to put unnecessary personal or confidential information into search queries.

Provider retention may continue even after a user deletes the corresponding item from Neurvance, because Neurvance cannot directly erase data from every provider log. Neurvance will use available deletion and data-control options where appropriate and technically possible.

9. International data transfers

Neurvance is based in Denmark, but personal data may be processed outside Denmark and outside the EU or EEA. In particular, Neurvance's reasoning model is hosted through RunPod infrastructure in Illinois, United States, and OpenAI, Anthropic, Brave, Heroku, Supabase, Stripe, or their subprocessors may process data in the United States or other countries.

Where required, Neurvance will rely on an applicable adequacy decision, the European Commission's Standard Contractual Clauses, contractual and technical safeguards, or another lawful transfer mechanism. Users may contact privacy@neurvance.com for information about the safeguards relevant to a transfer.

Laws in a destination country may differ from laws in Denmark or the EEA. No international transfer mechanism can eliminate every risk associated with foreign processing or government access.

10. Use of data for AI training

Neurvance does not use private mind maps, sticky notes, AI requests, or outputs to train or fine-tune Neurvance or third-party AI models by default.

If Neurvance introduces an optional training, feedback, or research programme, it will clearly explain the data involved and obtain consent or another valid legal basis where required. A change allowing broader training use will be reflected in an updated Privacy Policy before the new use begins.

This section does not prevent Neurvance or its providers from using limited technical, security, moderation, or aggregated data for fraud prevention, abuse prevention, system reliability, billing, or legal compliance.

11. Sharing and disclosure

Neurvance may disclose personal data:

- to the providers described above as necessary to deliver the Service;
- to professional advisers, insurers, auditors, or contractors under confidentiality and data-protection obligations;
- to authorities or other parties where required by law or reasonably necessary to protect rights, safety, security, or prevent fraud;
- in connection with a merger, sale, restructuring, investment, or transfer of all or part of the business, subject to appropriate safeguards;
- at the user's direction or with the user's consent.

Neurvance does not sell personal data to advertisers.

12. How long we keep data

12.1 Account and mind-map data

Account data and mind maps may be stored while the account remains active or until the user deletes the relevant content, subject to legal, security, backup, fraud-prevention, and dispute requirements.

When a user deletes an account or requests deletion, Neurvance aims to remove or anonymise relevant data from active Neurvance systems within 30 days unless a longer period is necessary or legally required. Copies may remain temporarily in provider backups until they are overwritten under normal backup cycles.

12.2 AI requests and outputs

AI requests and outputs may be stored in the user's mind map or history until deleted, or may be retained for a shorter period if the feature is designed as temporary processing. Neurvance may retain limited request metadata, safety records, and billing records for security, support, cost control, disputes, and legal compliance.

External providers may retain prompts, outputs, queries, or logs for the periods described in Section 8 or in their current terms. Deletion from Neurvance does not necessarily cause immediate deletion from provider logs.

12.3 Logs and payment records

Technical and security logs are normally retained for up to 30 days, but may be kept longer where necessary to investigate an incident, prevent abuse or fraud, resolve a dispute, protect the Service, or comply with law.

Payment, invoice, tax, and accounting records may be retained for the periods required by Danish accounting and tax law and for fraud-prevention or dispute purposes.

13. Cookies and analytics

Neurvance may use necessary cookies or similar technologies for login, sessions, security, user preferences, fraud prevention, and core website functionality. Necessary cookies may be used without consent where permitted by law.

Neurvance may use analytics or marketing technologies only where enabled. Where consent is required, users will be offered a way to accept, reject, or manage non-essential cookies.

14. Security

Neurvance uses reasonable technical and organisational measures intended to protect personal data, such as access controls, account-based permissions, provider security features, logging, secure transmission, backups, and review of suspicious activity.

No online service, cloud provider, AI model, or database can be guaranteed to be perfectly secure. Users should avoid entering unnecessary sensitive information and should protect access to their email and account.

15. User rights

Where the GDPR applies, users may have the right to:

- access personal data and receive information about processing;
- correct inaccurate or incomplete personal data;
- request deletion of personal data;
- restrict or object to certain processing;
- receive certain data in a portable format;
- withdraw consent where processing is based on consent;
- complain to a competent data-protection authority.

To exercise a right, contact privacy@neurvance.com. Neurvance may request information needed to verify identity and may limit a request where law permits or requires continued processing.

16. Deletion requests

Users may delete content through available product controls or contact privacy@neurvance.com. Neurvance aims to respond to privacy requests within one month, subject to lawful extensions for complex or numerous requests.

Some information may be retained where necessary for accounting, tax, security, fraud prevention, legal claims, provider logs, backup integrity, or compliance. Neurvance will explain applicable limitations where required.

17. Information about other people and sensitive data

Users should not include another person's personal data unless they have a lawful basis and have provided any required notice. Users should avoid submitting health data, passwords, private keys, financial secrets, privileged legal material, confidential business information, identity documents, information about minors, or other special-category data unless it is necessary and lawful.

Because selected content may be sent to external AI or search providers, users should treat every activated AI action as a potential disclosure of the selected content to the provider used for that action.

18. Complaints

Users in Denmark may complain to Datatilsynet, the Danish Data Protection Agency. Users in another EU or EEA country may also have the right to complain to their local supervisory authority. Neurvance asks users to contact privacy@neurvance.com first so that it can try to resolve the concern.

19. Changes to this Privacy Policy

Neurvance may update this Policy because of legal changes, new models, new providers, new features, changes to server locations, changes in data use, security requirements, or business and operational changes.

Material changes will be communicated where reasonably practical or legally required. If Neurvance changes its approach to using private mind-map content for model training, the Policy will be updated before the new use begins and a valid legal basis will be obtained where required.

20. Contact

Privacy and data-protection requests: privacy@neurvance.com

Legal questions: legal@neurvance.com

General questions: adam@neurvance.com