

Privacy Policy for neurvance.com

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

Last updated: 12 August 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 42 83 92 18

This Privacy Policy explains how Neurvance collects, uses, stores, shares, transmits, licenses, sells where separately consented, 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 a provider or an optional data recipient acts as an independent controller for its own purposes.

Key point: Neurvance does not treat acceptance of the Terms of Use as consent to use personal User Content for optional AI training or to sell, license, or share personal data with third parties for their own commercial purposes. Those optional uses require a separate lawful basis and, where described below, separate consent.

1. Scope and who can use Neurvance

This Policy applies to account creation, mind maps, sticky notes, files and media, AI requests and outputs, web searches, generated images and charts, code-generation assistance, Study Analytics, subscriptions and credits, 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. 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, an uploaded file or image, or the entire mind map for an AI action.
- Grammar, rewriting, information, image, chart, code, flashcard, question-generation, and other AI features may send selected content to OpenAI or other external model providers.
- Deeper reasoning may be performed using a Neurvance AI model hosted on RunPod infrastructure in Illinois, United States, and may delegate sub-tasks to OpenAI or Anthropic.
- Web-search features may create and send search queries to Brave Search API.
- Mind maps, accounts, subscriptions, settings, consent records, and related application data may be stored through Supabase, while Heroku may process application requests and technical logs.
- Stripe or another payment provider may process billing data. Simply.com may provide domain, email, or related operational services.
- Study Analytics is off by default and, if enabled, records limited session timing information for personal study statistics.

Not every AI request sends the entire mind map. The amount sent depends on the feature and the selected or reasonably required context. However, a user can select or trigger processing of 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, settings, and preferences;
- email-login, authentication, verification, and security records;
- records showing acceptance of legal terms, age confirmation, and optional consent choices.

3.2 Mind-map and User Content data

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

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

3.3 AI request and AI Output data

- the AI action selected, such as grammar correction, information search, reasoning, image generation, chart creation, code generation, flashcards, or question generation;
- the selected note, selected notes, relevant context, uploaded material, 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, generated study material, and other AI 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.

3.7 Study Analytics data

If Study Analytics is enabled, Neurvance may collect session start times, session end times, active study duration, active days, and derived study-time statistics. Neurvance does not use Study Analytics to record the content of keystrokes, mouse movements, or activity outside Neurvance.

3.8 Optional AI-training and commercial-data-programme records

If you opt in, Neurvance records which optional consent you gave, the version of the notice, the date and time, the data categories and purposes covered, and withdrawal or preference changes. Eligible data included in an optional programme may be tagged or copied into controlled datasets for the consented purpose.

4. How users control what is sent to AI features

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, conversation state, 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, secure, and manage accounts;
- to store, display, synchronise, edit, share, and recover mind maps and workspace content;
- 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 AI Outputs, images, charts, code, search results, and study material;
- to provide Study Analytics when enabled;
- to operate subscriptions, credits, billing, payments, and account deletion workflows;
- to provide support and respond to privacy, legal, security, and deletion requests;
- to secure, debug, monitor, and improve the reliability and performance of the Service;
- to prevent fraud, abuse, policy violations, and security incidents;
- to comply with legal, tax, accounting, regulatory, and AI-governance obligations;
- to enforce the Terms of Use and protect Neurvance, users, and providers;
- where separately and validly consented, to use eligible User-Provided Data for Neurvance AI training and improvement;

- where separately and validly consented, to share, license, or sell eligible User-Provided Data to third parties for the specific commercial purposes disclosed before consent.

Neurvance does not use AI to make decisions about users that produce legal or similarly significant effects unless a future feature is introduced with the legally required information, safeguards, and legal basis.

6. Legal bases for processing

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

- **Contract:** processing needed to create an account, store a mind map, perform a requested AI action, provide a paid plan, or otherwise deliver the Service.
- **Legitimate interests:** security, fraud prevention, debugging, abuse prevention, service administration, limited reliability improvement, record keeping, and protection of legal rights, where those interests are not overridden by user rights.
- **Consent:** non-essential cookies, optional analytics or marketing, Study Analytics where consent is required, optional use of eligible User-Provided Data to train or improve Neurvance AI, and optional third-party commercial sharing, licensing, or sale where described in Section 10.
- **Legal obligation:** accounting, tax, lawful requests, regulatory compliance, disputes, and data-protection obligations.

Neurvance does not rely on acceptance of the Terms of Use as consent for optional AI training or third-party commercial data sale. Where consent is used, it must be obtained before that optional processing starts and recorded separately.

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.

Supabase: Accounts, database, mind-map storage, subscriptions, settings, consent records, logs, and backend services. Data may include account data, mind maps, settings, payment status, consent records, and application records. Processing location depends on Neurvance configuration and provider operations.

Heroku: Application and backend hosting, request routing, server operation, and logs. Data may include requests, technical metadata, logs, and data needed to run the application. Processing may occur outside Denmark or the EEA.

RunPod: Hosting and executing Neurvance AI models. Data may include selected notes or mind-map context, prompts, outputs where technically required, and request metadata. Neurvance currently uses RunPod infrastructure in Illinois, United States for deeper reasoning.

OpenAI: AI processing such as grammar, rewriting, information processing, image/chart-related generation, code generation, and other AI tasks. Data may include selected content, prompts, files or images, outputs, and technical request metadata.

Anthropic: Reasoning sub-tasks, code generation, and other model-assisted outputs. Data may include selected content, prompts, outputs, and technical request metadata.

Brave Search API: Web search and retrieval of public information. Data may include user-entered or generated search queries and request metadata.

Stripe: Payments, subscriptions, invoices, fraud prevention, and refunds. Data includes billing and transaction information.

Simply.com: Domain, email, and related operational services. Data may include email and technical service data where relevant.

Analytics providers, if enabled: Usage measurement and product analytics. Data may include cookie identifiers, events, device data, and usage data. Non-essential analytics are used only where enabled and where the required consent has been obtained.

7.1 Optional commercial data recipients

If you separately consent to third-party commercial data sharing, licensing, or sale, additional recipients may include specifically identified AI developers, research organisations, data or analytics companies, and technology companies. Before consent, Neurvance will identify the recipient or sufficiently specific recipient category, the data categories involved, the purpose, and whether the recipient acts as an independent controller or processor. Neurvance will not treat a vague reference to "partners" as sufficient notice for a new consent-based sale purpose.

8. Provider retention and provider model training

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

At the date of this Policy, OpenAI states that business/API data is not used to train its models by default unless the customer opts in, and standard abuse-monitoring logs may retain certain API content for up to 30 days subject to controls and exceptions. Anthropic states that commercial/API data is not used for model training without permission; retention depends on the model, feature, and configured controls and may include up to 30 days for some services or models. Brave states that standard Search API query records may be retained for up to 90 days for billing and troubleshooting, while zero-data-retention options may be available for some plans or configurations.

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

Neurvance does not opt OpenAI or Anthropic into provider model training with user data merely because a user has consented to Neurvance's own optional training programme. Any future decision to permit a third-party service provider to use data for its own model training would require the legal basis and notice applicable to that separate purpose.

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 may be hosted through RunPod infrastructure in Illinois, United States, and OpenAI, Anthropic, Brave, Heroku, Supabase, Stripe, Simply.com, optional commercial data recipients, 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 safeguards relevant to a transfer.

Laws in a destination country may differ from laws in Denmark or the EEA. Neurvance will not rely on a consent-based international-transfer derogation as a substitute for appropriate safeguards except where the legal conditions for such a derogation are actually met.

10. Optional use of User-Provided Data for AI training and commercial third-party use

This section is important: These optional purposes are not necessary to use the core Service and are not activated merely by accepting the Terms or Privacy Policy.

10.1 Separate consent for Neurvance AI training

Neurvance may offer a separate choice allowing eligible User-Provided Data to be used to train, fine-tune, evaluate, test, benchmark, and improve Neurvance AI models, safety systems, ranking systems, and related machine-learning features. The consent screen must state which data categories are included, the purpose, and any material retention or transfer information before the user opts in.

10.2 Separate consent for third-party sharing, licensing, or sale

Neurvance may offer a separate commercial-data choice allowing specified categories of eligible User-Provided Data to be shared, licensed, or sold to named third parties or sufficiently specific recipient categories for their own stated purposes, which may include AI training, model evaluation, research, product development, or analytics. These recipients may become independent data controllers and will be responsible for their own lawful basis, transparency, security, retention, and rights handling.

10.3 What may be eligible

Depending on the consent notice, eligible User-Provided Data may include mind-map text, notes, prompts written by the user, user-uploaded files or images, user-created labels and structure, search queries, selected feedback, or limited usage and Study Analytics data. Neurvance will apply data minimisation and will only include the categories covered by the active consent.

10.4 What is not included

AI-generated Outputs are not used by Neurvance as training data and are not sold or licensed by Neurvance as a dataset to third parties under this programme. The programme also does not authorise use of passwords, private keys, full payment-card data, government identification documents, data about minors, or special-category personal data. Personal data about another person is not covered by a user's consent unless Neurvance has a separate lawful basis for that person's data.

10.5 Consent must be voluntary and granular

Where Neurvance relies on consent, the user must have a genuine choice. Consent is requested through a clear affirmative action, is kept separate from acceptance of mandatory Terms, and can be refused without losing the core Service. Separate purposes are presented separately. Neurvance keeps records needed to demonstrate the consent that was given.

10.6 Withdrawal and effect of withdrawal

A user may withdraw a consent at any time through available settings or by contacting privacy@neurvance.com. Withdrawal is intended to be as easy as giving consent. It stops future processing based on that consent and does not affect the lawfulness of processing completed before withdrawal.

Where personal data has already been included in a model or transferred to an independent recipient, Neurvance will take the deletion, restriction, unlearning/retraining, recipient-notification, or other remediation steps required by applicable law and technically applicable to the situation. Neurvance will not describe data as anonymous unless it has assessed that the data or model no longer permits individuals to be identified by means reasonably likely to be used.

10.7 New purposes require new notice and, where required, new consent

Neurvance will not use an old optional consent as blanket permission for materially different data categories, recipients, or purposes. A materially new optional use will be explained before it starts and a new legal basis or consent will be obtained where required.

11. Sharing and disclosure outside the optional commercial programme

Neurvance may disclose personal data outside the optional commercial programme:

- to service 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 and required notices;
- at the user's direction or with another valid legal basis.

Service-provider processing needed to deliver Neurvance is different from the optional commercial sale or licensing described in Section 10.

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 relevant content, subject to legal, security, backup, fraud-prevention, and dispute requirements.

The Service may use a 30-day account-deletion grace period during which signing back in can cancel a pending deletion. After the applicable grace period, Neurvance aims to remove or anonymise relevant data from active Neurvance systems within a reasonable period, normally within 30 days, unless a longer period is necessary or legally required. Copies may remain temporarily in provider backups until overwritten under normal backup cycles.

12.2 AI requests and AI Outputs

AI requests and AI 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.

12.3 Study Analytics

Study Analytics history may be kept while enabled or until the user deletes it, subject to limited backup, security, or legal requirements. Users can disable Study Analytics and delete their study history through available controls.

12.4 Optional training and commercial-data datasets

Before optional training or commercial data sharing starts, the applicable consent notice will state the material retention criteria for the raw personal data used for that purpose. Neurvance will keep identifiable or pseudonymised source data only as long as necessary for the consented purpose and legal obligations, and will periodically review whether continued retention is necessary. Data that has been irreversibly anonymised so that it is no longer personal data may be retained longer.

12.5 Logs and payment records

Technical and security logs are normally retained for a limited period and 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 non-essential analytics or marketing technologies only where enabled and where the required consent has been obtained. Users will be offered a way to accept, reject, or manage non-essential cookies where required.

Study Analytics is a product feature for personal study statistics and is kept separate from advertising or marketing analytics. It is off until enabled and can be turned off or deleted in the product.

14. Security and data protection by design

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

For optional training and commercial-data programmes, Neurvance will apply measures appropriate to the risk, such as data minimisation, access controls, filtering, pseudonymisation or anonymisation where appropriate, purpose separation, and review of recipient safeguards. Where processing is likely to result in a high risk to people's rights and freedoms, Neurvance will assess whether a data-protection impact assessment is required before processing begins.

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. Your data-protection 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 at any time where processing is based on consent;
- object to certain processing based on legitimate interests;
- 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 selected content to the provider used for that action. Optional AI training and commercial-data sale do not apply to another person's personal data merely because a user uploaded it.

18. EU AI Act and other AI regulation

The EU AI Act applies different obligations depending on whether Neurvance acts as a provider or deployer of a particular AI system or model and on the system's risk classification. Neurvance will assess and implement applicable obligations, including AI literacy, transparency, documentation, copyright, general-purpose AI, or other provider/deployer requirements where they apply. The AI Act does not replace GDPR obligations when personal data is processed.

19. 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.

20. 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, business changes, or operational needs.

Material changes will be communicated where reasonably practical or legally required. Updating this Policy does not itself create valid consent for a new optional training or third-party commercial-data purpose. Where a new consent is required, Neurvance will ask for it before the new processing begins.

21. Contact

- Privacy and data-protection requests: privacy@neurvance.com
- Legal questions: legal@neurvance.com
- General questions: adam@neurvance.com