

Privacy Policy for neurvance.com

Last updated: 06-07-2026

This Privacy Policy explains how Neurvance collects, uses, stores, shares, protects, and deletes personal data when you use neurvance.com, create an account, chat with AI models, vote, submit data, submit tools, use paid services, or otherwise interact with Neurvance.

Neurvance is operated by Adam Samer Daabas, a Danish sole proprietorship.

Data controller

Adam Samer Daabas / Neurvance

CVR: 46436024

Country: Denmark

Privacy contact: privacy@neurvance.com

Legal contact: legal@neurvance.com

General contact: adam@neurvance.com

Phone: +45 42839218

For this Privacy Policy, "Neurvance", "we", "us", and "our" refer to Adam Samer Daabas / Neurvance.

By using Neurvance, you acknowledge that your personal data will be processed as described in this Privacy Policy.

1. Who Can Use Neurvance

Neurvance is only for users who are at least 18 years old.

When you create an account or use the service, you may be asked to confirm that you are 18 or older.

Neurvance does not knowingly allow users under 18 to use the service. If we learn that a person under 18 has created an account or submitted personal data, we may delete or restrict the account and related data.

2. Personal Data We Collect

Neurvance may collect and process the following types of personal data.

2.1 Account data

When you create or use an account, we may collect:

1. your name;
2. your email address;
3. login verification data;

4. account creation date;
5. account status;
6. account settings;
7. confirmation that you are 18 or older;
8. records of your acceptance of Terms of Use, Privacy Policy, submission terms, or other required terms.

Neurvance uses email-based login with a one-time code. Neurvance does not use normal account passwords for this login method.

2.2 Chat data

When you chat with AI models on neurvance.com, we may collect:

1. your chat messages;
2. AI responses;
3. chat history;
4. timestamps;
5. account ID or user ID connected to the chat;
6. technical data needed to provide, debug, secure, or improve the chat service.

Chat data is linked to your user account so that you can access it and request deletion.

2.3 User submission data

When you submit data, files, datasets, prompts, tools, RAG systems, code, research, proposals, or other materials, we may collect:

1. your name;
2. your email address;
3. your account ID or user ID;
4. the submitted material;
5. the source link or original source of the submitted material;
6. license information;
7. public-domain or rights information;
8. confirmation that you accepted the relevant submission terms;
9. the time and date of submission;
10. the country connected to the submission where available;
11. review status;
12. approval or rejection status;
13. records of how the submission was used.

2.4 Voting and proposal data

When you vote or submit proposals, we may collect:

1. your vote;
2. proposal submissions;
3. voting timestamps;
4. account ID or user ID;
5. voting history;
6. proposal history;

7. moderation or review records.

Votes are visible to Neurvance internally. Votes are not intended to be publicly visible unless Neurvance clearly says otherwise.

2.5 Payment and subscription data

If you pay for Neurvance services, subscriptions, hosted AI access, API access, or other paid features, we may collect:

1. payment email;
2. subscription status;
3. invoice data;
4. payment history;
5. customer ID;
6. payment provider IDs;
7. plan type;
8. renewal status;
9. cancellation status;
10. refund records.

Neurvance uses Stripe for payments. Neurvance does not intentionally store full card numbers or full payment card details. Payment card details are handled by Stripe or another payment provider.

2.6 Technical, security, and log data

When you use Neurvance, we may collect technical and security data, including:

1. IP address;
2. server logs;
3. security logs;
4. login logs;
5. error logs;
6. abuse-prevention logs;
7. device-related technical information;
8. browser information;
9. timestamps;
10. request data;
11. system activity needed to operate, secure, debug, or protect the service.

2.7 Cookie and analytics data

Neurvance may use:

1. necessary cookies for login sessions and website functionality;
2. Google Analytics;
3. analytics cookies;
4. tracking or marketing cookies where enabled;
5. cookie consent records.

Where required by law, Neurvance will ask for consent before using non-essential analytics, tracking, or marketing cookies.

3. How We Use Personal Data

Neurvance may use personal data for the following purposes:

1. to create and manage user accounts;
2. to log users in using one-time email codes;
3. to provide AI chat services;
4. to store and show users their chat history;
5. to allow users to delete or request deletion of chat data;
6. to operate community voting;
7. to record votes and proposal history;
8. to review and manage user submissions;
9. to verify rights, licenses, and sources for submitted data;
10. to train, fine-tune, evaluate, document, or improve AI models using user-submitted training data where the user has submitted it for that purpose;
11. to provide paid services and subscriptions;
12. to process payments through Stripe;
13. to store payment status and invoice records;
14. to provide support;
15. to respond to legal, privacy, or deletion requests;
16. to moderate abuse, spam, illegal activity, manipulation, and harmful use;
17. to protect Neurvance, users, data, systems, and AI models;
18. to debug and improve technical reliability;
19. to produce internal records, transparency records, audit records, and safety records;
20. to comply with legal duties;
21. to enforce the Terms of Use;
22. to protect Neurvance's legal rights.

4. Legal Bases for Processing

Where GDPR or similar data protection law applies, Neurvance relies on one or more legal bases for processing personal data.

4.1 Contract

We process some personal data because it is necessary to provide the service you requested, including:

1. account creation;
2. email login;
3. AI chat access;
4. subscriptions;
5. hosted AI services;
6. payment-related account features;
7. user dashboard features;
8. voting and proposal features.

4.2 Consent

We may rely on consent for:

1. non-essential cookies;
2. analytics cookies where consent is required;
3. marketing cookies where consent is required;
4. optional data submissions;
5. optional public attribution;
6. optional use of submitted data for AI training, fine-tuning, research, evaluation, or documentation where consent is used as the legal basis.

You may withdraw consent where consent is the legal basis. Withdrawal of consent does not make earlier processing unlawful.

4.3 Legal obligation

We may process data where necessary to comply with legal duties, including:

1. accounting;
2. tax;
3. fraud prevention;
4. legal requests;
5. dispute handling;
6. data protection requests;
7. security obligations.

4.4 Legitimate interests

We may process data where necessary for legitimate interests, including:

1. security;
2. abuse prevention;
3. fraud prevention;
4. service operation;
5. debugging;
6. product improvement;
7. moderation;
8. protection against legal claims;
9. keeping records of votes, proposals, submissions, model releases, and safety decisions;
10. protecting Neurvance, users, data, and infrastructure.

Where we rely on legitimate interests, we consider whether your rights and freedoms override those interests.

5. AI Chat Privacy

Neurvance stores AI chat messages so users can access their chat history and so Neurvance can operate, secure, debug, and moderate the service.

Private AI chats are linked to the user account.

Private AI chats may be visible to Neurvance team members. Users should not share sensitive personal information, confidential information, medical information, legal secrets, financial secrets, passwords, private keys, or other sensitive information in AI chats.

Neurvance does not use private AI chats to train or fine-tune AI models unless Neurvance clearly changes this Privacy Policy and obtains a valid legal basis where required.

If Neurvance changes its approach in the future and wants to use private chats for AI training or fine-tuning, Neurvance will update this Privacy Policy before doing so. Neurvance will only use chats collected after such a change, unless it has a valid legal basis to do otherwise.

User-submitted training data is separate from private AI chats.

6. User-Submitted Training Data

Users may submit data, files, datasets, prompts, tools, RAG systems, code, research, or other materials for AI training, fine-tuning, evaluation, research, documentation, or community review.

Before submitting training data or related materials, users may be required to accept specific submission terms and confirm that they have the legal right to submit the material.

When you submit training data, Neurvance may store:

1. your real name;
2. your email address;
3. your user ID;
4. the submitted data;
5. the original source link;
6. license information;
7. proof of rights where available;
8. timestamp;
9. country information where available;
10. confirmation that you accepted the relevant terms;
11. records of how the submission was reviewed and used.

Accepted submissions may be publicly credited using the user's real first and last name, if the user has agreed to this.

Users may request removal of their public name or credit at any time.

Removing public credit does not necessarily remove the underlying submitted material from models, datasets, backups, audit records, safety records, forks, downloads, logs, or systems already created using the submission.

7. Model and Dataset Backups

Neurvance may keep backups of models, datasets, pre-model versions, training records, fine-tuning records, evaluation records, source records, and related documentation.

Neurvance may keep model and dataset backups for at least 30 days.

Neurvance may keep certain model, dataset, source, license, and audit records for longer where needed for:

1. copyright review;
2. license review;
3. safety review;
4. legal compliance;
5. dispute handling;
6. auditability;
7. security;
8. model rollback;
9. research integrity;
10. proving what data was or was not used.

Some data may be difficult or impossible to fully remove from already-trained or fine-tuned model weights, released models, forks, public downloads, backups, research notes, logs, or derivative systems.

Where personal data is involved, Neurvance will handle deletion and restriction requests according to applicable data protection law.

8. Voting Privacy

Neurvance stores voting records and proposal records to operate community voting and maintain governance history.

Votes are visible internally to Neurvance. Votes are not intended to be publicly visible unless Neurvance clearly says otherwise.

If a vote has already passed or affected a decision, the user may request removal or anonymisation of their name or personal identifiers, but Neurvance may keep the vote itself as part of the governance record.

This means the historical vote result may remain, but the personal name or account details connected to it may be removed or anonymised where legally required and technically practical.

Neurvance may keep voting records where necessary for fraud prevention, abuse prevention, security, transparency, dispute handling, or protection of Neurvance.

9. Payments and Stripe

Neurvance uses Stripe to process payments.

Stripe may process payment card information, billing information, fraud-prevention data, and transaction data according to Stripe's own terms and privacy policy.

Neurvance does not intentionally store full payment card numbers or full card security codes.

Neurvance may store payment-related records in Supabase or other systems, including:

1. payment email;
2. subscription status;
3. invoice records;
4. payment history;
5. customer ID;
6. Stripe customer ID;
7. plan type;
8. renewal status;
9. cancellation status;
10. refund status.

Payment and accounting records may be kept for as long as required by tax, accounting, fraud-prevention, legal, or dispute-handling obligations.

10. Cookies, Analytics, and Tracking

Neurvance may use cookies and similar technologies.

10.1 Necessary cookies

Neurvance may use necessary cookies or similar technologies for:

1. login sessions;
2. account security;
3. remembering user settings;
4. keeping the website functional;
5. fraud prevention;
6. abuse prevention.

Necessary cookies may be used without consent where allowed by law.

10.2 Analytics and marketing cookies

Neurvance may use Google Analytics and may use analytics, tracking, or marketing cookies.

Where required by law, Neurvance will ask for consent before using non-essential analytics, tracking, or marketing cookies.

Users should be able to accept, reject, or manage non-essential cookies where required by law.

Neurvance may use cookie consent records to remember user choices.

11. Third-Party Service Providers

Neurvance may use third-party providers to operate the service.

These may include:

1. **Supabase** for database, user data, account data, voting data, payment records, logs, and related backend storage;
2. **Heroku** for website hosting, backend hosting, server operation, and related logs;
3. **RunPod** for AI model hosting, AI backend, GPU processing, and AI model execution;
4. **Stripe** for payments, subscriptions, invoices, and payment processing;
5. **Google Analytics** for analytics;
6. **Simply.com** for domain and email services;
7. other providers that Neurvance may use in the future for hosting, email, security, storage, analytics, payments, support, or infrastructure.

Neurvance may change service providers over time.

Where third-party service providers process personal data for Neurvance, Neurvance will aim to use appropriate agreements and safeguards where required by law.

Third-party providers may also process some data according to their own privacy policies where they act as independent controllers.

12. International Data Transfers

Neurvance is based in Denmark, but some service providers may process data outside Denmark, the EU, or the EEA.

This may happen because Neurvance uses providers such as Stripe, Supabase, RunPod, Heroku, Google Analytics, Simply.com, or other infrastructure providers.

Neurvance will try to use European servers where practical, especially for AI model storage and GPU processing through RunPod.

However, if European servers are unavailable, technically unsuitable, too unstable, or not practical, data may be processed in other countries.

Where required by law, Neurvance will use appropriate safeguards for international transfers, such as standard contractual clauses, adequacy decisions, provider transfer safeguards, or other lawful transfer mechanisms.

13. Security

Neurvance aims to use reasonable technical and organisational measures to protect personal data against unauthorised access, loss, misuse, alteration, destruction, or disclosure.

Security measures may include:

1. access controls;
2. account-based access;
3. limited internal access where practical;
4. logging;
5. abuse detection;
6. database security settings;
7. provider security features;
8. backups;
9. deletion processes;
10. review of suspicious activity.

However, no website, AI system, database, server, cloud provider, or online service can be guaranteed to be perfectly secure.

Users are responsible for using Neurvance safely and should not submit sensitive information unless necessary.

14. Server Logs and Security Logs

Neurvance may keep server logs, IP addresses, security logs, login logs, and technical logs for security, debugging, abuse prevention, fraud prevention, and service operation.

Security and technical logs are normally kept for up to 30 days.

Neurvance may keep logs for longer if needed for:

1. legal compliance;
 2. security incidents;
 3. fraud prevention;
 4. abuse investigations;
 5. payment disputes;
 6. technical investigations;
 7. protection of Neurvance;
 8. protection of users;
 9. legal claims.
-

15. How Long We Keep Personal Data

Neurvance keeps personal data for as long as necessary for the purposes described in this Privacy Policy, unless a longer period is required or allowed by law.

15.1 Account data

Account data may be kept while your account exists.

If you delete your account or request deletion, Neurvance will aim to delete or anonymise relevant personal data within 30 days, unless a longer period is required for legal, accounting, security, fraud-prevention, backup, dispute, or operational reasons.

15.2 Chat data

Chat data may be stored until you delete it, request deletion, or Neurvance deletes it for storage optimisation, moderation, technical, legal, or operational reasons.

If you request deletion of chat data, Neurvance will aim to remove it within 30 days, unless a longer period is required for legal, security, abuse-prevention, backup, dispute, or operational reasons.

15.3 User-submitted training data

Submitted training data, source links, license records, proof of rights, acceptance records, timestamps, and usage records may be kept long-term where needed for copyright review, license review, model safety, auditability, legal compliance, dispute handling, and proving what data was used.

Where the submitted material contains personal data, Neurvance will handle deletion, restriction, objection, and other rights requests according to applicable data protection law.

Neurvance may refuse or limit deletion of certain submission records where deletion would seriously affect legal defence, copyright review, safety review, audit records, or the integrity of model and dataset records, unless applicable law requires deletion.

15.4 Voting records

Voting records may be kept as governance records.

If you request deletion, Neurvance may remove or anonymise your personal identifiers, but may keep the vote itself where needed to preserve the integrity of past voting results.

15.5 Payment records

Payment and invoice records may be kept for as long as required by accounting, tax, fraud-prevention, legal, or dispute-handling obligations.

15.6 Logs

Server logs and security logs are normally kept for up to 30 days unless longer retention is needed for legal, security, abuse-prevention, fraud-prevention, or dispute reasons.

16. Deletion Requests

Users may request deletion of their personal data by contacting:

privacy@neurvance.com

Neurvance aims to respond to deletion requests and other privacy requests within 30 days.

Some requests may take longer if they are complex, legally sensitive, technically difficult, or require identity verification.

Neurvance may keep some data where necessary for:

1. legal compliance;
2. accounting;
3. tax;
4. fraud prevention;
5. abuse prevention;
6. security;
7. payment disputes;
8. backup systems;
9. legal claims;
10. copyright review;
11. model safety;
12. audit records;
13. proving what data was used in training or fine-tuning.

Deletion from active systems may not always immediately remove data from backups, logs, released models, downloaded models, forks, model weights, research records, or third-party systems.

Where required by law, Neurvance will delete, restrict, anonymise, or otherwise handle personal data according to applicable data protection law.

17. Your Rights

Where GDPR or similar data protection law applies, you may have the following rights:

1. the right to access your personal data;
2. the right to correct inaccurate personal data;
3. the right to request deletion of personal data;
4. the right to restrict processing;
5. the right to object to processing;
6. the right to data portability;
7. the right to withdraw consent where processing is based on consent;
8. the right to complain to a data protection authority.

To exercise your rights, contact:

privacy@neurvance.com

Neurvance may need to verify your identity before fulfilling a request.

Some rights may be limited where Neurvance has legal grounds to keep or continue processing data.

18. Complaints

If you are located in Denmark, you may complain to the Danish Data Protection Agency.

Danish Data Protection Agency
Website: datatilsynet.dk

If you are located in another EU or EEA country, you may also have the right to complain to your local data protection authority.

Neurvance asks that you contact privacy@neurvance.com first so we can try to resolve the issue.

19. Public Attribution and Removal of Names

If you submit accepted data, tools, research, prompts, RAG systems, code, or other community contributions, Neurvance may publicly credit you using your real first and last name where you have agreed to this.

You may request removal of your public name or credit at any time by contacting:

privacy@neurvance.com

Neurvance will aim to remove public credit where technically and legally practical.

Removing public credit does not necessarily remove the underlying contribution, submitted data, training effect, dataset record, source record, model record, backup, log, or released material.

20. Sensitive Information

Users should not submit sensitive information to Neurvance unless it is necessary and lawful.

This includes:

1. health information;
2. financial secrets;
3. legal secrets;
4. passwords;
5. private keys;
6. confidential business information;
7. personal identification documents;
8. private messages from other people;
9. information about minors;
10. special category personal data under GDPR.

AI chats may be visible to Neurvance team members. Users should not treat AI chats as confidential legal, medical, psychological, financial, or emergency advice channels.

21. Changes to This Privacy Policy

Neurvance may update this Privacy Policy from time to time.

Neurvance may update it because of:

1. legal changes;
2. new features;
3. new providers;
4. new AI systems;
5. new payment systems;
6. changes in data use;
7. security needs;
8. operational changes;
9. changes to training or fine-tuning practices.

If Neurvance makes material changes, Neurvance will aim to provide reasonable notice where practical.

If Neurvance ever wants to use private AI chats for training or fine-tuning, Neurvance will update this Privacy Policy before doing so and will only use data according to a valid legal basis.

Continued use of Neurvance after changes become effective means you acknowledge the updated Privacy Policy.

22. Contact

For privacy requests, deletion requests, access requests, correction requests, or questions about this Privacy Policy, contact:

privacy@neurvance.com

For legal questions:

legal@neurvance.com

For general contact:

adam@neurvance.com

Neurvance
Adam Samer Daabas
CVR: 46436024
Denmark
Phone: +45 42839218