Neurvance Cube 1.0 - Data Protection Addendum

Effective date: 20 September 2026

This Cube Data Protection Addendum ("DPA") forms part of the agreement between Neurvance and each Customer using Neurvance Cube.

1. Purpose

This DPA governs personal-data processing connected with Cube.

It also sets mandatory requirements for Customers implementing Cube on websites and online shops.

2. Roles of the parties

The parties acknowledge that data-protection roles depend on the processing purpose.

Customer-controlled processing

Where Neurvance processes personal data solely to provide Cube functionality on the documented instructions of the Customer, Customer acts as controller and Neurvance acts as processor to the extent required by GDPR.

Neurvance-controlled processing

Neurvance acts as an independent controller where Neurvance determines its own processing purpose, including where legally applicable:

- security and abuse prevention;
- legal compliance;
- Neurvance's consented product improvement;
- consented AI/model development;
- statistical research;
- anonymisation; and
- creation of Neurvance's own aggregated products.

Where Neurvance relies on visitor consent for its own processing purpose, the Customer must ensure that Neurvance and the relevant purpose are clearly disclosed when consent is obtained.

Joint processing

If a specific implementation results in Customer and Neurvance jointly determining the purposes and essential means of a processing activity, the parties will cooperate in implementing any additional arrangement required by GDPR Article 26.

Neither party may use contractual terminology to avoid a controller role imposed on it by applicable law.

3. Processing details

Data subjects

Primarily visitors and customers of Customer websites using Cube.

Types of personal data

Data may include:

- pseudonymous visitor ID;
- session ID;
- event or sample numbers;
- timestamps;
- mouse movement speed;
- mouse click counts;

- cursor-position information;
- time on site;
- weekday;
- products viewed;
- product-view counts;
- products clicked;
- product-click counts;
- purchase status;
- products purchased;
- purchase quantities;
- products and colours displayed;
- cart contents;
- weather context;
- previous purchase date;
- previous purchased item; and
- information derived from these fields.

Derived information

Derived information may include:

- purchase probability;
- estimated purchase quantity;
- behavioural classification;
- statistical matching;
- statistical averages;
- product recommendations;
- layout recommendations; and
- colour recommendations.

Nature of processing

Processing may include:

- collection;
- transmission;
- storage;
- organisation;
- statistical analysis;
- aggregation;
- matching;
- prediction;
- model inference;
- model training where separately authorised;
- pseudonymisation;
- anonymisation; and
- deletion.

Duration

Processing continues for the duration of the Cube agreement and for any limited additional period necessary for deletion, anonymisation, security, legal compliance or other lawful purposes.

Genuinely anonymous information may survive termination.

4. Documented instructions

Where Neurvance acts as processor, Neurvance will process personal data only on documented instructions from Customer unless processing is required by applicable law.

The Cube agreement, Customer configuration and this DPA constitute documented instructions.

Neurvance will notify Customer if, in Neurvance's reasonable view, an instruction infringes applicable data-protection law, unless Neurvance is legally prohibited from doing so.

Neurvance may refuse an unlawful instruction.

5. Confidentiality

Neurvance will ensure that persons authorised to process Customer personal data are subject to appropriate confidentiality obligations.

6. Security

Neurvance will maintain technical and organisational measures appropriate to the nature, scope, context and risks of Cube processing.

Measures will be reviewed as appropriate and may include controls relating to:

- authentication and access management;
- least-privilege access;
- encryption in transit;
- credential and secret management;
- system logging;
- backup and recovery;
- vulnerability management;
- incident response;
- separation of access;
- pseudonymisation;
- aggregation; and
- data minimisation.

Customer remains responsible for the security of its own website, consent system, API credentials and integration.

7. No normal Customer access to raw visitor data

Cube is designed so Customers do not require routine access to raw behavioural records for individual visitors.

Customer will ordinarily receive recommendations, predictions and aggregated outputs.

Neurvance is not required to provide Customer with an unrestricted raw visitor-data dashboard or bulk visitor-data export merely because Customer uses Cube.

This does not prevent access or cooperation where necessary to:

- comply with data-subject rights;
- meet controller obligations;
- respond to a regulator;
- investigate a security incident;
- comply with law; or
- meet another mandatory GDPR requirement.

8. Customer consent obligation

Customer must obtain legally valid consent before enabling non-essential Cube tracking where consent is required.

Customer must ensure that:

- tracking is blocked before consent;
- consent is affirmative;
- boxes or toggles are not pre-selected;
- refusal is available;
- separate purposes are separated where required;
- withdrawal is available;
- consent records can be demonstrated;
- the visitor receives required information before consenting; and
- withdrawal is respected technically.

Customer must not represent to Cube that consent exists unless it actually exists.

9. Mandatory Cube disclosures

Before activating Cube, the Customer must clearly tell visitors, in appropriate language, that Cube may collect behavioural information.

The disclosure must cover, at minimum:

- pseudonymous identifiers;
- interaction and click behaviour;
- mouse or cursor behaviour;
- time spent;
- products viewed and clicked;
- purchase activity;
- cart contents where applicable;
- relevant contextual information supplied by the shop;
- profiling/purchase probability;
- recommendations;
- Neurvance as a recipient or provider; and
- links to further privacy information.

Where enabled, the notice must additionally disclose AI/model training and anonymous commercial aggregate use.

10. Minimum consent design

A compliant implementation should provide materially separate choices similar to the following.

Option 1 - Cube analytics and personalisation

Cube analytics & personalisation

Allow this shop and Neurvance Cube to use pseudonymous information about how you use the shop, such as clicks, mouse/cursor behaviour, time on the site, products viewed or purchased and cart activity, to analyse shopping behaviour and provide product, layout and similar recommendations.

Default: OFF

Option 2 - AI improvement

Neurvance AI improvement

Allow Neurvance to use the consented Cube information to develop, train, test, evaluate and improve AI and machine-learning systems used for e-commerce recommendations, behavioural analytics and related optimisation, including models Neurvance develops for commercial customers.

Default: OFF

Option 3 - Anonymous commercial insights

Anonymous aggregate insights

Allow Neurvance to use the consented information to create anonymized statistical datasets, benchmarks and commercial insights. Once genuinely anonymized, these may be retained, shared, licensed or sold and will no longer identify you.

Default: OFF

A Customer may adapt the wording to its interface and applicable law, but must not materially weaken the disclosure.

11. Accept and reject controls

Where required by applicable law, the first consent layer must give the visitor an effective choice.

A Customer must not design Cube consent so that:

- accepting is automatic;
- rejecting is hidden without justification;
- continuing to browse equals consent;
- scrolling equals consent;

- inactivity equals consent; or
- withdrawing consent is materially harder than giving it.

12. Failure to obtain consent

Failure to comply with Sections 8-11 constitutes a material breach.

Neurvance may immediately:

- block Cube tracking;
- disable Customer API access;
- suspend the Customer;
- terminate Cube access; or
- require remediation.

Repeated or intentional bypassing of consent controls may result in permanent termination.

13. Special-category data

Customer must not intentionally send special-category personal data to Cube unless expressly authorised in writing and legally permitted.

Customer must consider whether product information could itself reveal sensitive characteristics.

For example, purchase information may become sensitive depending on the product or context.

Customer is responsible for preventing prohibited fields from being transmitted through its integration.

14. Direct identifiers

Unless agreed otherwise, Customer must not intentionally transmit:

- customer names;
- email addresses;
- phone numbers;
- delivery addresses;
- payment-card information;
- account passwords; or
- government identification numbers.

Cube identifiers should be pseudonymous wherever reasonably possible.

15. Data-subject rights

Each party will reasonably assist the other where necessary to respond to valid requests relating to:

- access;
- correction;
- deletion;
- restriction;
- portability;
- objection;
- consent withdrawal; and
- qualifying automated decision-making.

Because Cube generally uses pseudonymous identifiers, Customer may need to provide the relevant identifier or session information needed to locate a record.

Neither party is required to collect additional identifying information solely to identify an otherwise unidentifiable person where GDPR does not require it.

16. Deletion and anonymisation

Where Neurvance acts as processor, at the end of the relevant processing services Neurvance will delete or return personal data as required by GDPR and the Customer's lawful instructions, unless applicable law requires retention.

This does not require Neurvance to delete:

- data Neurvance independently processes as controller where a lawful basis remains;
- records legally required for security or compliance;
- information already genuinely anonymized; or
- genuinely anonymous statistical information that can no longer be linked to a data subject.

17. AI-training processing

Neurvance must not treat the Customer's general Cube subscription as visitor consent to Neurvance's independent AI training.

Where AI/model-development processing relies on consent, the relevant consent must cover that purpose.

Neurvance may use appropriately consented data to:

- train;
- fine-tune;
- test;
- validate;
- evaluate;
- benchmark; and
- improve

AI and machine-learning models relating to e-commerce, behavioural analytics, recommendations and associated optimisation.

Materially unrelated AI-training purposes require an appropriate separate legal basis.

18. Anonymous-data rights

Once information has been genuinely anonymized, Neurvance may use it independently.

Neurvance may:

- retain it;
- combine it;
- analyse it;
- train models using it;
- commercialise it;
- license it;
- disclose it;
- publish statistics derived from it; and
- sell it.

Customer receives no ownership interest in Neurvance's anonymous aggregate dataset merely because Customer's visitors contributed to statistical aggregates.

Customer may not require Neurvance to reconstruct or remove an individual's contribution from a dataset that is genuinely anonymous and no longer permits identification of that individual.

19. No sale of pseudonymous visitor data

For avoidance of doubt, the commercialisation rights in Section 18 apply to genuinely anonymized information.

They do not authorise Neurvance to sell visitor-level pseudonymous records as though pseudonymisation alone made them anonymous.

20. Subprocessors

Customer provides general authorisation for Neurvance to use subprocessors reasonably necessary to operate Cube.

Neurvance will impose appropriate data-protection obligations on subprocessors.

Where required by GDPR, Neurvance will provide reasonable notice of material new subprocessors so Customer can raise legitimate data-protection objections.

Neurvance remains responsible for its processor obligations regarding subprocessors as required by GDPR.

21. International transfers

Where personal data is transferred outside the EEA and GDPR requires a transfer safeguard, Neurvance will use an appropriate lawful mechanism such as:

- an adequacy decision;
- Standard Contractual Clauses; or
- another permitted safeguard.

22. Security incidents

Where Neurvance acts as processor, Neurvance will notify Customer without undue delay after becoming aware of a qualifying personal-data breach affecting Customer data.

Neurvance will provide reasonably available information necessary for Customer to assess its notification obligations.

Neurvance's notification of an incident does not constitute an admission of liability.

23. DPIAs and regulator cooperation

Taking into account the nature of processing and information available to Neurvance, Neurvance will provide reasonable assistance with:

- data-protection impact assessments;
- prior consultations; and
- regulator enquiries

where required by GDPR and relating to Neurvance's processing.

Customer remains responsible for determining whether its overall use of Cube requires a DPIA.

24. Audits and compliance information

Where Neurvance acts as processor, Neurvance will make information reasonably necessary to demonstrate compliance with applicable Article 28 obligations available to Customer.

Audits must:

- have reasonable advance notice;
- avoid unnecessary disruption;
- protect Neurvance and other customers' confidential information;
- be proportionate to the processing risk; and
- use independent auditors where reasonably appropriate.

Neurvance may satisfy audit requirements through appropriate independent reports or documentation where sufficient.

25. Records of processing

Each party is responsible for maintaining records of processing required for the processing activities for which that party is responsible.

Customer must maintain appropriate documentation of its Cube implementation and consent process.

26. Changes in purpose

Customer must not use Cube data for a materially new incompatible purpose without first establishing the required legal basis and transparency.

Neurvance will do the same for processing for which Neurvance acts as controller.

27. Order of precedence

If this DPA conflicts with the Cube Terms regarding personal-data protection, this DPA controls.

If mandatory data-protection law conflicts with this DPA, mandatory law controls.

28. Termination

This DPA remains effective for as long as either party processes personal data subject to it.

Provisions concerning confidentiality, data protection, anonymous information, audits, liability and other clauses intended by their nature to survive will continue where applicable.

29. Contact

Neurvance

CVR: 46436024

Denmark

Privacy: **privacy@neurvance.com**

Legal: **legal@neurvance.com**