

Data Processing Agreement Template

NeuroCluster Enterprise AI Platform

December 13, 2025

Data Processing Agreement (DPA)

NeuroCluster B.V.

Version: 1.0 Effective Date: January 1, 2025 Last Updated: December 13, 2025

1. Definitions

1.1 Definitions from GDPR

The terms "Personal Data", "Data Subject", "Processing", "Controller", "Processor", "Supervisory Authority", and "Data Breach" shall have the meanings set out in the GDPR (Regulation (EU) 2016/679).

1.2 Agreement-Specific Definitions

- "Customer"**: The legal entity that has entered into a services agreement with NeuroCluster.
- "Services"**: The AI agent platform, knowledge management, and related services provided by NeuroCluster as described in the Services Agreement.
- "Customer Data"**: All data, including Personal Data, submitted by Customer to the Services.
- "Sub-processor"**: Any third party engaged by NeuroCluster to process Customer Data.
- "Services Agreement"**: The master services agreement or terms of service between Customer and NeuroCluster.

2. Scope and Applicability

2.1 Scope

This Data Processing Agreement ("DPA") forms part of the Services Agreement between Customer (as "Controller") and NeuroCluster B.V. (as "Processor") and applies to the Processing of Personal Data by NeuroCluster on behalf of Customer in connection with the Services.

2.2 Hierarchy

In the event of any conflict between this DPA and the Services Agreement, this DPA shall prevail to the extent of the conflict.

2.3 Term

This DPA shall remain in effect for the duration of the Services Agreement or until all Personal Data is deleted or returned, whichever is later.

3. Data Processing

3.1 Roles and Responsibilities

- Customer acts as the Controller determining the purposes and means of Processing Personal Data.
- NeuroCluster acts as the Processor, processing Personal Data solely on behalf of and in accordance with Customer's documented instructions.
- NeuroCluster shall not process Personal Data for any purpose other than as instructed by Customer through the Services Agreement and this DPA.

3.2 Customer Instructions

- Customer's use of the Services constitutes Customer's complete and final instructions to NeuroCluster for the Processing of Personal Data.
- NeuroCluster shall promptly inform Customer if, in NeuroCluster's opinion, any instruction infringes Data Protection Laws.
- Additional instructions outside the scope of the Services require prior written agreement and may incur additional fees.

3.3 Nature and Purpose of Processing

| Category | Description | |-----|-----| | **Subject Matter** | Provision of AI agent platform, knowledge management, workflow automation, and related services | | **Duration** | For the term of the Services Agreement plus retention period | | **Nature of Processing** | Storage, analysis, retrieval, transformation, and deletion of Customer Data including Personal Data | | **Purpose** | To provide the Services as described in the Services Agreement | | **Types of Personal Data** | As determined by Customer, may include: names, email addresses, employee IDs, IP addresses, user activity logs, document content, chat transcripts | | **Categories of Data Subjects** | Customer's employees, contractors, customers, and end users |

4. Sub-Processors

4.1 Authorized Sub-Processors

Customer hereby provides general authorization for NeuroCluster to engage Sub-processors to process Personal Data, subject to the conditions in this Section.

4.2 Current Sub-Processors

NeuroCluster's current list of Sub-processors is available at:

<https://neurocluster.ai/trust/sub-processors>

Current Sub-processors include:

| Sub-processor | Service | Location | Purpose | |-----|-----|-----|-----| | AWS (Amazon Web Services) | Cloud infrastructure | EU (Frankfurt) | Infrastructure hosting | | Supabase Inc. | Database services | EU (self-hosted) | Database management | | Sentry | Error monitoring | USA (GDPR-compliant) | Error tracking | | Langfuse GmbH | LLM tracing | Germany | Observability |

4.3 New Sub-Processors

- NeuroCluster shall notify Customer at least 30 days before engaging any new Sub-processor.
- Notification shall be provided via email to Customer's designated contact and via the NeuroCluster admin console.
- Customer may object to the use of a new Sub-processor on reasonable data protection grounds within 30 days of notification.
- If Customer objects and NeuroCluster cannot accommodate the objection, either party may terminate the affected Services upon 30 days' written notice.

4.4 Sub-Processor Obligations

- NeuroCluster shall impose data protection obligations on Sub-processors that are no less protective than those in this DPA.
 - NeuroCluster remains liable for the acts and omissions of its Sub-processors.
-

5. Data Subject Rights

5.1 Assistance with Data Subject Requests

NeuroCluster shall, to the extent legally permitted, promptly notify Customer if NeuroCluster receives a request from a Data Subject to exercise their rights under Data Protection Laws.

5.2 Customer Responsibility

Customer is responsible for responding to Data Subject requests. NeuroCluster shall provide reasonable assistance to Customer in responding to such requests, including by:

- Providing Customer with the ability to access, correct, and delete Personal Data through the Services interface
- Providing Customer with the ability to export Personal Data in a machine-readable format
- Assisting with data portability requests
- Providing documentation of Processing activities upon request

5.3 Fees

Assistance beyond what is available through the standard Services interface may be subject to reasonable fees based on the complexity and time required.

6. Security Measures

6.1 Technical and Organizational Measures

NeuroCluster shall implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

6.2 Security Measures

Current security measures include:

Organizational Measures:

- Security policies and procedures
- Employee security training (annual)
- Background checks for employees with access to Personal Data
- Confidentiality obligations for all employees
- Security incident response procedures
- Regular security audits and assessments

Technical Measures:

- Encryption in transit (TLS 1.3)
- Encryption at rest (AES-256)
- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- Network segmentation and firewalls
- Intrusion detection and prevention systems (IDS/IPS)
- Regular security patching and updates
- Automated backup and disaster recovery
- Vulnerability scanning and penetration testing (annually)
- Audit logging and monitoring

6.3 Security Documentation

NeuroCluster's current security documentation, including SOC 2 Type II report and ISO 27001 certificate, is available upon request to qualified security personnel under NDA.

7. Data Breaches

7.1 Notification

NeuroCluster shall notify Customer without undue delay and in any event within 72 hours of becoming aware of a Data Breach affecting Customer Data.

7.2 Notification Contents

Notification shall include:

- Description of the nature of the Data Breach
- Categories and approximate number of Data Subjects affected

- Categories and approximate number of Personal Data records affected
- Likely consequences of the Data Breach
- Measures taken or proposed to address the Data Breach
- Contact point for more information

7.3 Investigation and Remediation

NeuroCluster shall:

- Investigate the Data Breach and provide Customer with detailed information
 - Take reasonable measures to mitigate the effects of the Data Breach
 - Cooperate with Customer in any investigation or notification to Supervisory Authorities or Data Subjects
 - Document all Data Breaches and make documentation available to Customer upon request
-

8. Audits and Compliance

8.1 Audit Rights

Customer may, upon reasonable notice and during normal business hours, audit NeuroCluster's compliance with this DPA, subject to the following:

- Audits may be conducted no more than once per year, unless required by a Supervisory Authority
- Customer shall provide at least 30 days' written notice
- Audits shall be conducted by Customer or an independent third-party auditor under NDA
- Audits shall not unreasonably interfere with NeuroCluster's operations
- Customer shall bear all costs of the audit

8.2 Compliance Certifications

In lieu of an audit, NeuroCluster may provide Customer with:

- SOC 2 Type II report (annual)
- ISO 27001 certificate (current)
- EU AI Act compliance assessment (when applicable)
- Self-assessment questionnaires or compliance documentation

8.3 Remediation

If an audit reveals non-compliance with this DPA, NeuroCluster shall remediate the non-compliance within a reasonable timeframe agreed with Customer.

9. International Data Transfers

9.1 Data Residency

Customer may select the geographic region for data storage:

- **EU Region:** All Customer Data stored in EU data centers (Frankfurt, Amsterdam)
- **US Region:** All Customer Data stored in US data centers (US East, US West)
- **On-Premise:** Customer's own infrastructure (no data leaves Customer's environment)

9.2 EU to Non-EU Transfers

For transfers of Personal Data from the EU to countries not recognized by the European Commission as providing adequate protection:

- NeuroCluster shall rely on Standard Contractual Clauses (SCCs) as adopted by the European Commission
- The SCCs are incorporated into this DPA by reference and are available at:
<https://neurocluster.ai/trust/sccs>
- NeuroCluster shall implement supplementary measures as necessary to ensure adequate protection

9.3 UK and Switzerland

For transfers from the UK or Switzerland, NeuroCluster shall comply with UK GDPR and Swiss Federal Act on Data Protection (FADP), including use of UK and Swiss SCCs as applicable.

10. Data Return and Deletion

10.1 Return of Data

Upon termination or expiration of the Services Agreement, NeuroCluster shall:

- Provide Customer with the ability to export all Customer Data in a machine-readable format (JSON, CSV) for 30 days
- Notify Customer 30 days before the end of the export period

10.2 Deletion

After the export period:

- NeuroCluster shall delete or irreversibly anonymize all Customer Data, including backups, within 90 days
- NeuroCluster shall provide Customer with a certificate of deletion upon request
- NeuroCluster may retain Customer Data to the extent required by applicable law (e.g., audit logs for compliance)

10.3 Exceptions

NeuroCluster is not required to delete:

- Customer Data that is anonymized or aggregated such that it cannot be re-identified
 - Customer Data retained in accordance with legal or regulatory obligations
 - Customer Data in archived backups, which shall be deleted in accordance with NeuroCluster's backup retention policy (maximum 7 years)
-

11. Liability and Indemnification

11.1 Liability Cap

Each party's total aggregate liability arising out of or related to this DPA shall be subject to the limitations of liability set forth in the Services Agreement.

11.2 Indemnification

NeuroCluster shall indemnify and hold harmless Customer from and against any third-party claims, losses, damages, or costs arising from NeuroCluster's breach of this DPA, except to the extent caused by Customer's breach or instructions.

12. General Provisions

12.1 Governing Law

This DPA shall be governed by the laws of the Netherlands, without regard to conflict of law principles.

12.2 Amendments

NeuroCluster may amend this DPA to comply with changes in Data Protection Laws. Material amendments shall require Customer consent or provide termination rights.

12.3 Severability

If any provision of this DPA is held invalid or unenforceable, the remainder shall continue in full force and effect.

12.4 Order of Precedence

In the event of conflict between documents, the order of precedence shall be:

- This DPA
 - Services Agreement
 - Terms of Service
-

13. Contact Information

Data Protection Officer:

- **Name:** Dr. Elena Vermeer
- **Email:** dpo@neurocluster.ai
- **Address:** NeuroCluster B.V., Herengracht 450, 1017 CA Amsterdam, Netherlands
- **Phone:** +31 20 123 4567

Security Contact:

- **Email:** security@neurocluster.ai
 - **PGP Key:** Available at <https://neurocluster.ai/security.asc>
-

ANNEX I: Standard Contractual Clauses

[The European Commission's Standard Contractual Clauses for data transfers from the EU to non-EU countries are incorporated by reference and available at:
<https://neurocluster.ai/trust/sccs>]

ANNEX II: Technical and Organizational Measures

Detailed technical and organizational security measures are documented in NeuroCluster's Security Whitepaper, available at: <https://neurocluster.ai/trust/security-whitepaper.pdf>

Signature Block

CUSTOMER:

[illegible]

Name: ___________________

[illegible][illegible]

NEUROCLUSTER B.V.:

[illegible][illegible][illegible][illegible]

END OF DATA PROCESSING AGREEMENT

For questions about this DPA, please contact our Data Protection Officer at dpo@neurocluster.ai