DATA PROTECTION ADDENDUM

FOR ENTERPRISE PLATFORM SERVICES

Effective as of JAN 5, 2026

This Data Processing Addendum ("**DPA**") forms part of the Software License Agreement (“SLA”, as Schedule C), the Terms of Agreement for Enterprise Platform Services ("TOA"), Data License Agreement (“DLA”), and/or other agreement governing the use of the Licensor's enterprise platform services (collectively, the "Agreement") entered by and between you ("you", "your", "Customer", "Client", "Licensee"), and Nerturbo AG ("the Licensor", "provider", "Nerturbo").

This DPA sets out the terms that apply with regard to the Processing of Personal Data (as defined below) by the Licensor, on behalf of Customer, in the course of providing the Licensed Software and Enterprise Platform services to Customer under the Agreement.

All capitalized terms not defined herein will have the meaning outlined in the Software License Agreement.

By accessing the graph.swiss website or Enterprise Platform, utilizing the Service (e.g., Graph.Swiss AI Chat, Enterprise Dashboard, API), or signing the SLA/DLA, you accept this DPA, you agree to be bound by this DPA and you represent and warrant that you have full authority to bind the Customer to this DPA.

1 DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.1 "Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws and Regulations, and (b) is permitted to use the Service pursuant to the Agreement between the Customer and the Licensor and is not a "Customer" as defined under the Agreement.

1.2 "Authorized User" or "End User" means any individual authorized or otherwise enabled by Customer to use the Service through Customer's account, including employees or contractors who have a right to access the proprietary information of the Licensee as defined in the TOA.

1.3 "Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

1.4 "Customer Data" or "Internal Data" means what is defined in the Agreement as "Customer Data" or "Internal Data", including data submitted via API, enterprise dashboard interface, or direct ingestions from Customer sources.

1.5 "Data Protection Laws" means all privacy and data protection laws and regulations applicable to the processing of personal data under the Agreement in the jurisdiction(s) specified in the Software License Agreement.

1.6 "Data Subject" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.7 "Deployment options" means the different deployment models the Licensor is currently offering.

1.8 "Enterprise Platform" means the Licensed Software facilities enabling End Users to access the Licensor's services as described in the TOA.

1.9 "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.10 "Licensed Software" means the software provided by the Licensor under the Software License Agreement, including the Graph.Swiss platform, AI Chat features, API access, and Enterprise Dashboard.

1.11 "Personal Data" or "Personal Information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with a particular Data Subject or household, which is included in Customer Data Processed by the Licensor on behalf of Customer under the Agreement.

1.12 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by the Licensor on behalf of Customer under the Agreement.

1.13 "Personnel" means persons authorized by the Licensor to Process Customer's Personal Data.

1.14 "Process" or "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.15 "Processor" means the entity that processes Personal Data on behalf of the Controller.

1.16 "Proprietary Data Lake" means the Licensor's data repository containing public/open data, licensed data of third-party providers, and proprietary AI extracted output, including curated selection of private and public companies, decision makers, and other data.

1.17 "Zero-Data Retention" or "ZDR" means the principle whereby data inputs and outputs are processed temporarily and deleted immediately after delivery to the End User.

2 PARTIES AND ROLES

Details on the identities of the parties can be found in the SLA. In this context and for the purposes of relevant Data Protection Laws, the Licensee is the Data Controller, and the Licensor is the Data Processor (for non-self-hosted implementations).

3 DATA PROCESSING

3.1 This DPA applies when Personal Data is Processed by the Licensor strictly on behalf of the Customer, as part of the Licensor's provision of the Service.

3.2 Subject Matter

The Licensor Processes Customer's Personal Data as part of providing Customer with the Service, pursuant to the specifications under the Agreement.

3.3 Processing by Subprocessors

The Licensor may engage third-party service providers to Process Personal Data on behalf of the Customer ("Sub-Processors"). The Sub-Processors are listed in Appendix A.

3.4 Technical and organizational measures are listed in Appendix B.

3.5 Insofar as a data processing operation falls within the scope of the GDPR, the competent authority in the EEA/EU is the authority according to art. 77 GDPR. A list of competent national data protection authorities in the EEA/EU can be found at https://edpb.europa.eu/about-edpb/about-edpb/members_en.

3.6 Insofar as persons in Switzerland are affected or the data is processed in or from Switzerland, the competent authority is the Federal Data Protection and Information Commissioner (FDPIC). The contact details of the FDPIC can be found at https://www.edoeb.admin.ch.

3.7 Insofar as a data processing operation falls within the scope of the UK GDPR, the competent supervisory authority is the Information Commissioner's Office (ICO) in the United Kingdom.

3.8 Insofar as a data processing operation falls within the scope of applicable US federal or state privacy laws, the competent authority varies by jurisdiction and may include the Federal Trade Commission (FTC) at the federal level, state attorneys general, or other designated regulatory bodies as specified under the relevant state privacy legislation.

3.9 Insofar as a data processing operation falls within the scope of the Personal Data Protection Act (PDPA) in Singapore, the competent authority is the Personal Data Protection Commission (PDPC). The contact details of the PDPC can be found at https://www.pdpc.gov.sg.

3.10 Categories of data subjects whose personal data is processed

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following Categories of Data Subjects:

a) Prospects, customers, business partners, and vendors of Customers (who are natural persons)

b) Employees or contact persons of Customer's prospects, customers, business partners, and vendors

c) Employees, agents, advisors, and freelancers of Customers (who are natural persons)

d) Customer's End Users authorized by Customer to use the Services

3.11 Categories of personal data processed

The Licensor collects information that alone or in combination with other information could be used to identify ("Personal Information"). Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following Categories of Personal Data:

a) First and last name

b) Title

c) Position

d) Employer

e) Contact information (company, email, phone, physical business address)

f) ID data

g) Professional life data

h) Personal life data

i) Localization data

The processor may collect further categories of Personal Data depending on how End Users use the Licensor's Services:

j) Account Information: When a Controller's End User creates an account with the Licensor, the Licensor may collect information associated with an End User account, including the End User's name and email address (collectively, "Account Information").

k) User Content: When the Controller uses the Licensor's Services, the Licensor may collect Personal Information that is included in the input, file uploads, output, or feedback that the Controller provides to the Licensor's Services ("Content").

l) Communication Information: If the Controller's End Users communicate with the Licensor via a support channel, the Licensor may collect the Controller's End User name, contact information, and the contents of any messages they send ("Communication Information").

3.12 Sensitive categories of data processed

Customer may submit Special Categories of Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.13 Nature of processing

The nature of data processing is the collection and processing of the information for provision of the Licensed Software.

3.14 Purposes for Processing Personal Data on behalf of the Controller

Enterprise Platform / AI Chat use case:

The Processor will store and process:

a) Internal documents and document texts that have been uploaded or connected to the Service by the Controller via API, data feed, cloud, CRMs, or direct upload

b) Account information provided by the Controller's End Users

c) Prompts and answers of the Controller's End Users

d) Data from the Licensor's Proprietary Data Lake as delivered through API or interface access

Further, the Processor uses the Customer's personal data and metadata for the following purposes:

e) To facilitate, operate, enhance, and provide the Services

f) To provide the Customers and users with assistance and support

g) To gain a better understanding of how individuals use and interact with our Sites and Services, and how we could improve their and others' user experience, and continue improving our products, offerings and the overall performance of our Services

h) To contact the Customers with general service-related messages

i) To support and enhance the Processor's data security measures, including for the purposes of preventing and mitigating the risks of fraud, error, or any illegal or prohibited activity

j) To comply, and maintain compliance, with applicable laws, regulations, and standards

3.15 Duration of processing

The Licensor will retain the Customer's personal data for as long as is reasonably necessary to maintain and provide its services, to comply with its legal and contractual obligations, or to protect the Licensor from any potential disputes (i.e., as required by law for log-keeping, record keeping, and accounting purposes, and to have evidence and proof of its relationship with the Customer in the event that any legal issues arise after the Customer ceases to use the Services), all in accordance with the Licensor's Data Retention Policy.

Please note that except as required by applicable law or the specific agreements between the Provider and the Customer, the Licensor will not be obligated to retain personal data for any particular period (except, audit logs will be kept for 10 years), and is free to securely delete it or restrict access to it for any reason and at any time, with or without notice to the client.

In accordance with the TOA, Enterprise Platform data inputs and outputs are processed (via API) temporarily and deleted immediately after delivery to the End User - implementing Zero-Data Retention (ZDR) principle on all stages.

4 DATA PROTECTION

4.1 The Provider must, at all times, take all necessary security and protective measures against, in particular, destruction, loss, access by unauthorized third parties or alteration of or to data provided or administered by the Client or its subcontractors to which the Provider has access for the purposes of fulfilling its obligations under the Agreement.

4.2 The Provider undertakes to and shall ensure to report to Client any incident impacting the confidentiality, integrity, and availability of Client's or its subcontractors' data, promptly and without undue delay, but in no event later than 24 hours after becoming aware of any incident, by sending an email to the Licensor's Enterprise address and by calling the contact person designated (from time to time) by the Client. The email must detail the known details of the incident, the implications, and the Provider's actions undertaken in response to such an event.

4.3 All data in transit including internal data connectors/uploads, AI queries and Licensor Data Lake requests are protected using TLS encryption.

5 DATA PROPERTY

All Confidential Information is and shall remain the Client's exclusive property, and shall be treated as the Client's Confidential Information. Likewise, the information generated by the systems, such as application logs, tables, reports, accounts, and printed material of any and all types (account statements, etc.), is the Client's exclusive property. The Provider shall acquire no rights over this information or data and only use the Confidential Information to the extent necessary for the performance of the Services. Unless written approval from the Client is given in advance, Confidential Information must not be, notably:

a) used by the Provider and/or its employees, agents, or representatives other than for the strict fulfillment of those obligations stipulated in the Agreement, which implies the data shall be rigorously physically and/or logically segregated from data of the Provider's other users;

b) disclosed, sold, given, handed over, or made accessible in any other way by the Provider and/or by its employees, agents, or representatives to third parties.

6 DATA OWNERSHIP AND PRIVACY

6.1 In accordance with the TOA, the Licensee at all times retains full ownership of all data submitted and any output generated or API requests made and respective data received.

6.2 Data/Inputs could be submitted by The Licensee via API and enterprise dashboard interface, as well as via direct ingestions from Licensee sources.

6.3 The Licensor does not claim rights, resell or share with third parties, or train any AI model on Licensee data.

6.4 Enterprise platform data inputs and outputs are processed (via API) temporarily and deleted immediately after delivery to the End User - implementing Zero-Data Retention (ZDR) principle on all stages.

6.5 The Licensee acknowledges and understands that data inputs that are used for AI features are shared with LLM API providers which have their own respective policies on data retention including ZDR. The Licensor is operating Openrouter and Amazon Bedrock to connect multiple LLM providers in a secure manner. Details on data processing and protection for each option can be found on Openrouter | Data Processing and AWS Bedrock | Data Protection.

6.6 The Licensee can submit a preferred data processing and storage region for both the external LLM requests and Enterprise Platform operations and the Licensor will apply the region restriction subject to availability of preferred region in each third-party service in question.

7 DATA STORAGE, RETURN, AND DESTRUCTION

7.1 The Provider will accurately and completely collect and maintain information regarding the storage location, media, and method of storage of all Confidential Information on an ongoing basis. The storage shall remain in Switzerland or in a location specified by the Customer subject to availability. At the Client's request and by the termination of the Agreement at the latest, the Provider undertakes, at its own costs:

a) to return to the Client, within a reasonable time and in its existing format, data which the Provider has knowledge of, and

b) to delete or destroy all or part of any such data that might remain in the Provider's possession or of which the Provider might have retained a copy (especially in archived or backed-up files) which is subject to the applicable legal provisions, particularly record keeping.

7.2 Except in those cases where the Provider is using the Client's material, the Provider shall guarantee a backup policy on its material to enable recovery of the data related to the Services in the event of data loss. Any associated costs shall be borne by the Provider.

7.3 In accordance with the TOA, upon termination of the business relationship between Licensor and Licensee, for any reason, the Licensee must cease all use of the Frontend and Software, Source Code and Data and delete all copies, derivatives, and records of the Software, Source Code and Data within their possession or control. Licensee may keep the output built on their proprietary inputs.

7.4 The Licensee agrees to provide written confirmation to the Licensor within thirty (30) business days of the termination date that all actions required under this clause have been completed.

8 AI MODEL AND LLM PROCESSING

8.1 AI-generated responses are generated using Openrouter LLM provider API routing engine and Amazon Bedrock instance to be combined with the Licensor's Proprietary Data Lake in a Graph-based Retrieval Augmented Generation (GraphRAG) output.

8.2 The Licensor never accesses the internal data and AI input/output of Licensee.

8.3 The Licensor does not use Customer data to train, improve, or develop any AI models or algorithms.

8.4 Customer acknowledges that the use of third-party LLM providers is subject to such providers' own data processing terms, and the Licensor has implemented measures to ensure compliance with data protection requirements including Zero-Data Retention where available.

9 GOVERNING LAW AND EXCLUSIVE COURTS

Unless the GDPR is mandatory or otherwise specified in the Software License Agreement, this Agreement shall be governed exclusively by Swiss substantive law, without regard to its choice of law or conflicts of law principles, Customer and the Licensor consent to the exclusive jurisdiction and venue in the courts in Zug, Switzerland.

APPENDIX A – LIST OF THE SUB-PROCESSORS OF THE DPA

Disclosure of sub-processors activities:

Name	Purpose	Location of Data	More Information
Amazon Web Services (AWS)	Enterprise Platform Infrastructure, Amazon Bedrock LLM services	EU/CH or chosen location by the client	Cloud computing, networking and storage provider. Processing of AI queries through Amazon Bedrock for Graph RAG output. AWS Bedrock | Data Protection
Openrouter	LLM API Routing	EU or chosen location by the client	LLM provider API routing engine for connecting multiple LLM providers securely. Openrouter | Data Processing
Neo4j	GraphRAG infrastructure	EU/CH or chosen location by the client	Knowledge graph storage database and GraphRAG pipeline infrastructure. Neo4j Trust Center
Hetzner	Public Platform Infrastructure, Hosting	EU	European cloud hosting and data center services. Hetzner Data Privacy Policy
Cloudflare Inc.	Edge & CDN	USA/Global	Cloudflare and GDPR compliance | Cloudflare
Vercel Inc.	Public Platform Hosting (frontend)	USA/Global	Vercel Privacy Policy

APPENDIX B - TECHNICAL AND ORGANIZATIONAL MEASURES (“TOM”)

TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define the Licensor's current security measures. The Licensor may change these at any time without notice so long as they maintain a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

Physical Access Control

Unauthorized persons are prevented from gaining physical access to premises, buildings, or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

• The Licensor protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.

• In general, buildings are secured through access control systems.

• As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.

• Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures.

Additional measures for Data Centers:

• All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised.

• Only authorized representatives have access to systems and infrastructure within the Data Center facilities.

• The Licensor and all third-party Data Center providers log the names and times of persons entering the Licensor's private areas within the Data Centers.

System Access Control

Data processing systems used to provide the Licensor's Services must be prevented from being used without authorization.

Measures:

• Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data.

• All users access the Licensor's systems with a unique identifier (user ID).

• Two-factor authentication is enforced in data center operations and for critical systems.

• The Licensor has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines.

• The Licensor has established a password policy that prohibits the sharing of passwords and requires complex passwords.

• The company network is protected from the public network by firewalls.

• Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.

• Full remote access to the Licensor's corporate network and critical infrastructure is protected by strong authentication.

Data Access Control

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified, or removed without authorization in the course of processing, use, and storage.

Measures:

• As part of the Licensor's Security Policy, Personal Data requires at least the same protection level as "confidential" information.

• Access to personal, confidential, or sensitive information is granted on a need-to-know basis.

• All production servers are operated in the Data Centers or in secure server rooms.

• The Licensor conducts internal and external security checks and penetration tests on its IT systems.

• The Licensor does not allow the installation of personal software or other software that has not been approved.

• A security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

Data Transmission Control

Except as necessary for the provision of the Services in accordance with the relevant service agreement, Personal Data must not be read, copied, modified, or removed without authorization during transfer.

Measures:

• Personal Data transfer over the Licensor's internal networks is protected in the same manner as any other confidential data.

• When data is transferred between the Licensor and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant Agreement.

• All data in transit is protected using TLS encryption.

Data Input Control

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from the Licensor's data processing systems.

Measures:

• The Licensor only allows authorized persons to access Personal Data as required in the course of their work.

• The Licensor has implemented a logging system for input, modification and deletion, or blocking of Personal Data.

Job Control

Personal Data being processed on commission is processed solely in accordance with the relevant agreement and related instructions of the customer.

Measures:

• The Licensor uses controls and processes to ensure compliance with contracts between the Licensor and its customers, subprocessors, or other service providers.

• All the Licensor's employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information.

Availability Control

Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

• The Licensor employs backup processes and other measures that ensure rapid restoration of business-critical systems as and when necessary.

• The Licensor uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.

• The Licensor has defined contingency plans as well as business and disaster recovery strategies for the provided Services.

• Emergency processes and systems are regularly tested.

Data Separation Control

Personal Data collected for different purposes can be processed separately.

Measures:

• The Licensor uses logical separation to achieve data separation among Personal Data originating from multiple customers, and physical separation to achieve data separation among Personal Data originating from multiple enterprise customers.

• The Licensor uses strictly separated production and testing environments.

• Customers (including their Affiliates) have access only to their own data and/or proprietary licensed data of the Licensor.

Data Integrity Control

Personal Data will remain intact, complete, and current during processing activities. The Licensor has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

Measures:

• Firewalls

• Security Monitoring Center

• Backup and recovery

• External and internal penetration testing

• Regular external audits to prove security measures

• Risk management

• Privileged access management

APPENDIX C - LIST OF PARTIES

Controller(s):

Name: *as specified in the Software License Agreement*

Address: *as specified in the Software License Agreement*

Contact person's name, position, and contact details: *as specified in the Software License Agreement*

Signature and accession date: *as specified in the Software License Agreement*

Processor(s):

Name: *Nerturbo AG*

Address: *Bahnhofstrasse 7, 6300 Zug, Switzerland*

Contact person's name, position, and contact details: *as specified in the Software License Agreement*

Registration: *CHE-373.011.053*

Signature and accession date: *as specified in the Software License Agreement*