DATA PROCESSING AGREEMENT

(AI version – with the engagement of AI Providers as sub-processors)

concluded pursuant to Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "**GDPR**") (hereinafter the "**DPA**")

between:

Company name:	**[●]**
Registered seat:	**[●]**
Company ID No.:	**[●]**
Registered:	in the Commercial Register of the District Court **[●]**, Section: **[●]**, File No. **[●]**
Represented by:	[name and surname], [position]

(hereinafter the "**Controller**")

and

Company name:	**Nethemba s. r. o.**
Registered seat:	Klemensova 2524/4, 811 09 Bratislava, Slovakia
Company ID No.:	36 777 234
Registered:	in the Commercial Register maintained by the District Court in Bratislava I, section Sro, insert No. 61232/B
Represented by:	Ing. Pavol Lupták, managing director
Email:	info@nethemba.com

(hereinafter the "**Processor**")

(Controller and Processor hereinafter jointly the "**Parties**")

1. Introductory provisions

1.1 The Parties have concluded a contract on the provision of security services, under which the Processor provides to the Controller services in the area of IT security, in particular penetration testing and security audits (hereinafter the "**Main Contract**" and the "**Services**").

1.2 In the course of the provision of the Services, personal data contained in the Controller's tested systems or in communication with them may be processed by the Processor on behalf of

the Controller. The purpose of this DPA is to regulate the mutual rights and obligations of the Parties in relation to such processing in accordance with Article 28 GDPR.

1.3 The terms “AI Tools” and “AI Providers” have the meaning given in the article of the Main Contract regulating the use of artificial intelligence tools.

2. Subject matter and duration of the processing

2.1 The Processor undertakes to process personal data on behalf of the Controller solely within the scope and under the conditions agreed in this DPA and in the Main Contract. A detailed description of the processing (subject matter, nature, purpose, categories of data subjects and categories of personal data) is set out in Annex No. 1.

2.2 This DPA is concluded for the duration of the Main Contract. Obligations of the Parties which by their nature are intended to survive the end of the processing (in particular confidentiality) shall survive the termination of this DPA.

3. Obligations of the Processor

The Processor undertakes to:

(a) process personal data only on documented instructions from the Controller, including with regard to transfers to third countries, unless required to do so by EU or Member State law; the Main Contract, including its article on the use of AI Tools, is also deemed a documented instruction;

(b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, implement appropriate technical and organisational measures pursuant to Article 32 GDPR; their basic description is set out in Annex No. 3;

(d) respect the conditions for engaging sub-processors set out in Article 4 of this DPA;

(e) taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Controller’s obligation to respond to requests for exercising the data subjects’ rights (Chapter III GDPR);

(f) assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to the Processor;

(g) notify the Controller of a personal data breach without undue delay after becoming aware of it, and in any event within 48 hours of its detection;

(h) after the end of the provision of the Services, delete the personal data (in accordance with the deletion periods agreed in the Main Contract, in particular deletion of the final

report 60 days after its delivery and deletion of Logs and related data in accordance with the agreed archiving period) or return them to the Controller, and delete existing copies unless EU or Member State law requires their storage; the Parties acknowledge that deletion on the side of the AI Providers is governed by their retention rules pursuant to Article 4.4 of this DPA;

(i) make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and allow for and contribute to audits under the conditions set out in Article 6 of this DPA.

4. Sub-processors

4.1 The Controller grants the Processor a general written authorisation within the meaning of Article 28(2) GDPR for the engagement of sub-processors. The list of sub-processors engaged as of the date of conclusion of this DPA, including the AI Providers, forms Annex No. 2.

4.2 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors in advance, at least 14 days before the engagement, thereby giving the Controller the opportunity to object to such changes. If the Controller does not raise an objection before the commencement of the engagement, the change shall be deemed approved. The information may be provided by e-mail or by updating the public list on the Processor's website combined with an e-mail notice.

4.3 If the Controller raises a justified objection to the engagement of a sub-processor which is an AI Provider under the Main Contract, the Parties shall discuss an alternative solution; if no agreement is reached, either Party may terminate the Main Contract in the part affected by the objection, and the Controller shall pay the price for the Services provided until the termination.

4.4 The Processor shall impose on each sub-processor, by way of a contract, the same data protection obligations as set out in this DPA. In the case of the AI Providers, these obligations are governed by their standard data processing agreements/addenda concluded between the Processor and the respective AI Provider; the Controller acknowledges that the Processor cannot individually modify the processing terms (including retention periods) on the side of the AI Providers. Where a sub-processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that sub-processor's obligations, subject to the limitations of liability agreed in the Main Contract.

5. Transfers to third countries

5.1 The Parties acknowledge that the sub-processors listed in Annex No. 2 may process personal data on servers outside the EU/EEA, in particular in the USA. Any such transfer shall take place only subject to appropriate safeguards pursuant to Chapter V GDPR, in particular on the basis of an adequacy decision (the EU-U.S. Data Privacy Framework, where the respective entity is certified) or standard contractual clauses adopted by the European Commission.

6. Audit

6.1 The Controller is entitled to audit the Processor's compliance with this DPA at most once every 12 months, at its own cost, upon written notice delivered at least 30 days in advance,

during normal business hours and in a manner which does not unreasonably interfere with the Processor's operations. Persons performing the audit must be bound by confidentiality.

6.2 With respect to sub-processors (including the AI Providers), the audit shall be performed by means of certifications, audit reports and other documentation made available by such sub-processors (e.g. ISO 27001 certifications, SOC 2 reports). The Controller acknowledges that the Processor has no right to perform a physical audit at the AI Providers.

7. Liability

7.1 The liability of the Parties under this DPA is governed by the liability and limitation of damages provisions agreed in the Main Contract, including the exclusion of the Processor's liability for acts or omissions of the AI Providers to the extent agreed in the Main Contract. This is without prejudice to the rights of data subjects and liability under Article 82 GDPR.

8. Final provisions

8.1 This DPA becomes valid and effective on the date of its signature by both Parties. In the event of a conflict between this DPA and the Main Contract, this DPA shall prevail in matters of personal data protection.

8.2 This DPA is governed by the laws of the Slovak Republic and the GDPR. Amendments may only be made by a written amendment.

8.3 The following Annexes form an integral part of this DPA: Annex No. 1 (Description of the processing), Annex No. 2 (List of sub-processors) and Annex No. 3 (Technical and organisational measures).

In [●], on [●]	**In Bratislava, on ……..**
Controller	**Processor**
For: **[●]**	For: **Nethemba s. r. o.**
Name: **[●]**	Name: Ing. Pavol Lupták
Position: **[●]**	Position: managing director
_____	_____

Annex No. 1 – Description of the processing

Subject matter of the processing	Personal data contained in the Controller's tested systems, in communication with them or in materials supplied by the Controller for the provision of the Services
Duration of the processing	For the duration of the provision of the Services; deletion in accordance with the periods agreed in the Main Contract (final report – 60 days after delivery; Logs and related data – in accordance with the agreed

	archiving period, max. 24 months)
Nature of the processing	Collection, viewing, analysis, temporary storage and deletion of data in the course of penetration testing and security audits, including processing by means of AI Tools pursuant to the Main Contract
Purpose of the processing	Assessment of the security of the tested systems, identification of vulnerabilities and preparation of the final report
Categories of data subjects	Employees, customers, suppliers and users of the Controller's systems; other persons whose data are contained in the tested systems
Categories of personal data	Identification and contact data, login and network identifiers (e-mail, IP address, cookies), content of communication and any other ordinary personal data contained in the tested systems; special categories of data only to the extent they are contained in the tested systems, while they are not the target of the processing

Annex No. 2 – List of sub-processors

AI Providers (pursuant to the article of the Main Contract on the use of AI tools):

Entity	Seat	Service	Transfer safeguards
Anthropic, PBC (incl. Anthropic Ireland, Limited)	USA / Ireland	Claude, Claude Code	EU-U.S. DPF / SCC
OpenAI, Inc. / OpenAI, L.L.C. (incl. OpenAI Ireland Ltd)	USA / Ireland	ChatGPT, Codex, GPT API	EU-U.S. DPF / SCC
Google LLC / Google Ireland Limited	USA / Ireland	Gemini, Vertex AI	EU-U.S. DPF / SCC
Microsoft Corporation / Microsoft Ireland Operations Limited	USA / Ireland	Azure OpenAI, GitHub Copilot	EU-U.S. DPF / SCC
xAI Corp.	USA	Grok	SCC
Mistral AI SAS	France	Le Chat, La Plateforme	– (EU)

Entity	Seat	Service	Transfer safeguards
Amazon Web Services, Inc.	USA	cloud infrastructure	EU-U.S. DPF / SCC

Other sub-processors: [●] *(e.g. subcontractors – specialists under the Main Contract; complete or strike out)*

Annex No. 3 – Technical and organisational measures

- Access to personal data is limited to authorised persons bound by confidentiality, to the extent necessary for the provision of the Services (need-to-know).
- Encryption of data in transit (TLS, SSH, VPN); encrypted and digitally signed e-mail communication (PGP or S/MIME), where enabled by the Controller.
- Full-disk encryption of workstations; multi-factor authentication for access to the Processor's systems.
- Minimisation: data are processed only to the extent necessary for the security assessment; credentials (passwords, API keys, tokens) are not disclosed to AI Tools in usable form (best effort pursuant to the Main Contract).
- AI Tools are used in paid/business/API versions with a contractual prohibition of training on inputs and outputs and, where available, zero data retention modes.
- Deletion: final report within 60 days of delivery; Logs and related data in accordance with the agreed archiving period; secure erasure of media.
- Incident management: internal procedure for detection, escalation and notification of personal data breaches (notification to the Controller within 48 hours of detection).