

AUFTRAGSVERARBEITUNGSVERTRAG

(AI-Version – mit Einbeziehung von KI-Anbietern als Unterauftragsverarbeiter)

geschlossen gemäß Art. 28 Abs. 3 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (nachfolgend „**DSGVO**“) (nachfolgend der „**AVV**“)

zwischen:

Firma:	[●]
Sitz:	[●]
Reg.-Nr.:	[●]
Eingetragen:	im Handelsregister [●], Abteilung: [●], Nr. [●]
Vertreten durch:	[Name und Nachname], [Funktion]

(nachfolgend der „**Verantwortliche**“)

und

Firma:	Nethemba s. r. o.
Sitz:	Klemensova 2524/4, 811 09 Bratislava, Slowakische Republik
Reg.-Nr. (IČO):	36 777 234
Eingetragen:	im Handelsregister des Bezirksgerichts Bratislava I, Abteilung: Sro, Nr. 61232/B
Vertreten durch:	Ing. Pavol Lupták, Geschäftsführer
E-Mail:	info@nethemba.com

(nachfolgend der „**Auftragsverarbeiter**“)

(Verantwortlicher und Auftragsverarbeiter nachfolgend gemeinsam die „**Vertragsparteien**“)

1. Einleitende Bestimmungen

1.1 Die Vertragsparteien haben einen Vertrag über die Erbringung von Sicherheitsdienstleistungen geschlossen, auf dessen Grundlage der Auftragsverarbeiter dem Verantwortlichen Dienstleistungen im Bereich der IT-Sicherheit erbringt, insbesondere Penetrationstests und Sicherheitsaudits (nachfolgend der „**Hauptvertrag**“ und die „**Dienstleistungen**“).

1.2 Bei der Erbringung der Dienstleistungen kann es zur Verarbeitung personenbezogener Daten, die sich in den getesteten Systemen des Verantwortlichen oder in der Kommunikation mit ihnen befinden, durch den Auftragsverarbeiter im Auftrag des Verantwortlichen kommen.

Zweck dieses AVV ist die Regelung der gegenseitigen Rechte und Pflichten der Vertragsparteien bei einer solchen Verarbeitung gemäß Art. 28 DSGVO.

1.3 Die Begriffe „KI-Tools“ und „KI-Anbieter“ haben die Bedeutung gemäß dem Artikel des Hauptvertrags über die Nutzung von Werkzeugen künstlicher Intelligenz.

2. Gegenstand und Dauer der Verarbeitung

2.1 Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten im Auftrag des Verantwortlichen ausschließlich in dem Umfang und zu den Bedingungen zu verarbeiten, die in diesem AVV und im Hauptvertrag vereinbart sind. Eine detaillierte Beschreibung der Verarbeitung (Gegenstand, Art, Zweck, Kategorien betroffener Personen und Kategorien personenbezogener Daten) ist in Anlage Nr. 1 enthalten.

2.2 Dieser AVV wird für die Dauer des Hauptvertrags geschlossen. Pflichten der Vertragsparteien, die ihrer Natur nach auch nach Beendigung der Verarbeitung fortbestehen sollen (insbesondere Vertraulichkeit), bleiben auch nach Beendigung dieses AVV bestehen.

3. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich:

- (a) personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, auch in Bezug auf die Übermittlung in Drittländer, sofern nicht das Recht der EU oder eines Mitgliedstaats dies verlangt; als dokumentierte Weisung gilt auch der Hauptvertrag einschließlich seines Artikels über die Nutzung von KI-Tools;
- (b) zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- (c) unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO zu ergreifen; deren Grundbeschreibung ist in Anlage Nr. 3 enthalten;
- (d) die Bedingungen für die Einbeziehung von Unterauftragsverarbeitern gemäß Art. 4 dieses AVV einzuhalten;
- (e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen (Kapitel III DSGVO) nachzukommen;
- (f) den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zu unterstützen;

- (g) dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, nachdem er davon Kenntnis erlangt hat, spätestens jedoch innerhalb von 48 Stunden nach ihrer Feststellung, zu melden;
- (h) nach Abschluss der Erbringung der Dienstleistungen die personenbezogenen Daten zu löschen (gemäß den im Hauptvertrag vereinbarten Löschfristen, insbesondere Löschung des Abschlussberichts 60 Tage nach dessen Lieferung und Löschung der Logs und zugehörigen Daten gemäß der vereinbarten Archivierungsdauer) oder sie dem Verantwortlichen zurückzugeben und vorhandene Kopien zu löschen, sofern nicht das Recht der EU oder eines Mitgliedstaats deren Speicherung verlangt; die Vertragsparteien nehmen zur Kenntnis, dass sich die Löschung auf Seiten der KI-Anbieter nach deren Aufbewahrungsregeln gemäß Art. 4.4 dieses AVV richtet;
- (i) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen und Audits zu ermöglichen und dazu beizutragen, zu den Bedingungen gemäß Art. 6 dieses AVV.

4. Unterauftragsverarbeiter

4.1 Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine schriftliche Genehmigung im Sinne von Art. 28 Abs. 2 DSGVO zur Einbeziehung von Unterauftragsverarbeitern. Die Liste der zum Zeitpunkt des Abschlusses dieses AVV einbezogenen Unterauftragsverarbeiter, einschließlich der KI-Anbieter, bildet Anlage Nr. 2.

4.2 Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern im Voraus, mindestens 14 Tage vor der Einbeziehung, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Erhebt der Verantwortliche bis zum Beginn der Einbeziehung keinen Einspruch, gilt die Änderung als genehmigt. Die Information kann per E-Mail oder durch Aktualisierung der öffentlichen Liste auf der Website des Auftragsverarbeiters in Verbindung mit einer E-Mail-Benachrichtigung erfolgen.

4.3 Erhebt der Verantwortliche einen begründeten Einspruch gegen die Einbeziehung eines Unterauftragsverarbeiters, der ein KI-Anbieter gemäß dem Hauptvertrag ist, erörtern die Vertragsparteien eine Alternativlösung; kommt keine Einigung zustande, kann jede Vertragspartei den Hauptvertrag in dem vom Einspruch betroffenen Teil beenden, wobei der Verantwortliche den Preis für die bis zur Beendigung erbrachten Dienstleistungen zahlt.

4.4 Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auf, wie sie in diesem AVV festgelegt sind. Im Falle der KI-Anbieter richten sich diese Pflichten nach deren Standard-Datenverarbeitungsvereinbarungen (Data Processing Agreement/Addendum), die zwischen dem Auftragsverarbeiter und dem jeweiligen KI-Anbieter geschlossen wurden; der Verantwortliche nimmt zur Kenntnis, dass der Auftragsverarbeiter die Verarbeitungsbedingungen (einschließlich Aufbewahrungsfristen) auf Seiten der KI-Anbieter nicht individuell ändern kann. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, bleibt der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Erfüllung der Pflichten dieses Unterauftragsverarbeiters

vollumfänglich haftbar, vorbehaltlich der im Hauptvertrag vereinbarten Haftungsbeschränkungen.

5. Übermittlung in Drittländer

5.1 Die Vertragsparteien nehmen zur Kenntnis, dass die in Anlage Nr. 2 genannten Unterauftragsverarbeiter personenbezogene Daten auf Servern außerhalb der EU/des EWR, insbesondere in den USA, verarbeiten können. Jede derartige Übermittlung erfolgt nur bei Gewährleistung geeigneter Garantien gemäß Kapitel V DSGVO, insbesondere auf der Grundlage eines Angemessenheitsbeschlusses (EU-U.S. Data Privacy Framework, sofern die jeweilige Stelle zertifiziert ist) oder der von der Europäischen Kommission erlassenen Standardvertragsklauseln.

6. Audit

6.1 Der Verantwortliche ist berechtigt, die Einhaltung dieses AVV beim Auftragsverarbeiter höchstens einmal in 12 Monaten, auf eigene Kosten, nach schriftlicher Ankündigung mit einer Frist von mindestens 30 Tagen, während der üblichen Geschäftszeiten und in einer Weise zu prüfen, die den Betrieb des Auftragsverarbeiters nicht unangemessen beeinträchtigt. Die das Audit durchführenden Personen müssen zur Vertraulichkeit verpflichtet sein.

6.2 In Bezug auf Unterauftragsverarbeiter (einschließlich der KI-Anbieter) erfolgt das Audit mittels Zertifizierungen, Auditberichten und sonstiger Dokumentation, die diese Unterauftragsverarbeiter zur Verfügung stellen (z. B. ISO-27001-Zertifizierungen, SOC-2-Berichte). Der Verantwortliche nimmt zur Kenntnis, dass der Auftragsverarbeiter nicht berechtigt ist, ein physisches Audit bei den KI-Anbietern durchzuführen.

7. Haftung

7.1 Die Haftung der Vertragsparteien aus diesem AVV richtet sich nach den im Hauptvertrag vereinbarten Haftungs- und Haftungsbeschränkungsbestimmungen, einschließlich des Ausschlusses der Haftung des Auftragsverarbeiters für Handlungen oder Unterlassungen der KI-Anbieter in dem im Hauptvertrag vereinbarten Umfang. Die Rechte der betroffenen Personen und die Haftung nach Art. 82 DSGVO bleiben unberührt.

8. Schlussbestimmungen

8.1 Dieser AVV wird mit seiner Unterzeichnung durch beide Vertragsparteien gültig und wirksam. Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag hat in Angelegenheiten des Schutzes personenbezogener Daten dieser AVV Vorrang.

8.2 Dieser AVV unterliegt dem Recht der Slowakischen Republik und der DSGVO. Änderungen können nur durch einen schriftlichen Nachtrag vorgenommen werden.

8.3 Integrale Bestandteile dieses AVV sind: Anlage Nr. 1 (Beschreibung der Verarbeitung), Anlage Nr. 2 (Liste der Unterauftragsverarbeiter) und Anlage Nr. 3 (Technische und organisatorische Maßnahmen).

In [●], am [●]

In Bratislava, am

Verantwortlicher

Für: [●]

Name: [●]

Funktion: [●]

AuftragsverarbeiterFür: **Nethemba s. r. o.**

Name: Ing. Pavol Lupták

Funktion: Geschäftsführer

Anlage Nr. 1 – Beschreibung der Verarbeitung**Gegenstand der Verarbeitung**

Personenbezogene Daten, die sich in den getesteten Systemen des Verantwortlichen, in der Kommunikation mit ihnen oder in vom Verantwortlichen für die Erbringung der Dienstleistungen bereitgestellten Unterlagen befinden

Dauer der Verarbeitung

Für die Dauer der Erbringung der Dienstleistungen; Löschung gemäß den im Hauptvertrag vereinbarten Fristen (Abschlussbericht – 60 Tage nach Lieferung; Logs und zugehörige Daten – gemäß der vereinbarten Archivierungsdauer, max. 24 Monate)

Art der Verarbeitung

Erhebung, Einsichtnahme, Analyse, vorübergehende Speicherung und Löschung von Daten im Rahmen von Penetrationstests und Sicherheitsaudits, einschließlich der Verarbeitung mittels KI-Tools gemäß dem Hauptvertrag

Zweck der Verarbeitung

Bewertung der Sicherheit der getesteten Systeme, Identifizierung von Schwachstellen und Erstellung des Abschlussberichts

Kategorien betroffener Personen

Mitarbeiter, Kunden, Lieferanten und Nutzer der Systeme des Verantwortlichen; andere Personen, deren Daten sich in den getesteten Systemen befinden

Kategorien personenbezogener Daten

Identifikations- und Kontaktdaten, Anmelde- und Netzwerkkennungen (E-Mail, IP-Adresse, Cookies), Kommunikationsinhalte und alle sonstigen gewöhnlichen personenbezogenen Daten, die sich in den getesteten Systemen befinden; besondere Kategorien von Daten nur in dem Umfang, in dem sie sich in den getesteten Systemen befinden, wobei sie nicht Ziel der

Verarbeitung sind

Anlage Nr. 2 – Liste der Unterauftragsverarbeiter

KI-Anbieter (gemäß dem Artikel des Hauptvertrags über die Nutzung von KI-Tools):

Unternehmen	Sitz	Dienst	Übermittlungsgarantien
Anthropic, PBC (einschl. Anthropic Ireland, Limited)	USA / Irland	Claude, Claude Code	EU-U.S. DPF / SCC
OpenAI, Inc. / OpenAI, L.L.C. (einschl. OpenAI Ireland Ltd)	USA / Irland	ChatGPT, Codex, GPT API	EU-U.S. DPF / SCC
Google LLC / Google Ireland Limited	USA / Irland	Gemini, Vertex AI	EU-U.S. DPF / SCC
Microsoft Corporation / Microsoft Ireland Operations Limited	USA / Irland	Azure OpenAI, GitHub Copilot	EU-U.S. DPF / SCC
xAI Corp.	USA	Grok	SCC
Mistral AI SAS	Frankreich	Le Chat, La Plateforme	– (EU)
Amazon Web Services, Inc.	USA	Cloud-Infrastruktur	EU-U.S. DPF / SCC

Sonstige Unterauftragsverarbeiter: [●] (z. B. Subunternehmer – Spezialisten gemäß dem Hauptvertrag; ergänzen oder streichen)

Anlage Nr. 3 – Technische und organisatorische Maßnahmen

- Zugriff auf personenbezogene Daten haben nur befugte, zur Vertraulichkeit verpflichtete Personen, im für die Erbringung der Dienstleistungen erforderlichen Umfang (Need-to-know).
- Verschlüsselung der Daten bei der Übertragung (TLS, SSH, VPN); verschlüsselte und digital signierte E-Mail-Kommunikation (PGP oder S/MIME), sofern vom Verantwortlichen ermöglicht.
- Festplattenverschlüsselung der Arbeitsplatzrechner (Full-Disk Encryption); Multi-Faktor-Authentifizierung beim Zugriff auf die Systeme des Auftragsverarbeiters.
- Minimierung: Daten werden nur in dem für die Sicherheitsbewertung erforderlichen Umfang verarbeitet; Zugangsdaten (Passwörter, API-Schlüssel, Tokens) werden KI-

Tools nicht in verwendbarer Form zugänglich gemacht (Best Effort gemäß dem Hauptvertrag).

- Bei KI-Tools werden bezahlte/Business-/API-Versionen mit vertraglichem Trainingsverbot für Ein- und Ausgaben und, sofern verfügbar, Zero-Data-Retention-Modi verwendet.
- Löschung: Abschlussbericht innerhalb von 60 Tagen nach Lieferung; Logs und zugehörige Daten gemäß der vereinbarten Archivierungsdauer; sichere Löschung von Datenträgern.
- Incident-Management: internes Verfahren zur Erkennung, Eskalation und Meldung von Verletzungen des Schutzes personenbezogener Daten (Meldung an den Verantwortlichen innerhalb von 48 Stunden nach Feststellung).