

SMLOUVA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

(AI verze – se zapojením AI poskytovatelů jako dalších zpracovatelů)

uzavřená podle čl. 28 odst. 3 Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „GDPR”) (dále jen „Smlouva o zpracování”)

mezi:

Obchodní firma:	[●]
Sídlo:	[●]
IČO:	[●]
Zapsaná:	v obchodním rejstříku vedeném [●], oddíl: [●], vložka č. [●]
Zastoupená:	[jméno a příjmení], [funkce]

(dále jen „Správce”)

a

Obchodní firma:	Nethemba s. r. o.
Sídlo:	Klemensova 2524/4, 811 09 Bratislava, Slovenská republika
IČO:	36 777 234
Zapsaná:	v Obchodním rejstříku Okresního soudu Bratislava I, oddíl: Sro, vložka č. 61232/B
Zastoupená:	Ing. Pavol Lupták, jednatel
Email:	info@nethemba.com

(dále jen „Zpracovatel”)

(Správce a Zpracovatel dále společně jen „Smluvní strany”)

1. Úvodní ustanovení

1.1 Smluvní strany uzavřely smlouvu o poskytování bezpečnostních služeb, na jejímž základě Zpracovatel poskytuje Správci služby v oblasti bezpečnosti informačních technologií, zejména penetrační testování a bezpečnostní audity (dále jen „Hlavní smlouva” a „Služby”).

1.2 Při poskytování Služeb může docházet ke zpracování osobních údajů, které se nacházejí v testovaných systémech Správce nebo v komunikaci s nimi, Zpracovatelem jménem Správce. Účelem této Smlouvy o zpracování je úprava vzájemných práv a povinností Smluvních stran při takovém zpracování v souladu s čl. 28 GDPR.

1.3 Pojmy „AI nástroje” a „AI poskytovatelé” mají význam podle článku Hlavní smlouvy upravujícího používání nástrojů umělé inteligence.

2. Předmět a doba zpracování

2.1 Zpracovatel se zavazuje zpracovávat osobní údaje jménem Správce výlučně v rozsahu a za podmínek sjednaných v této Smlouvě o zpracování a v Hlavní smlouvě. Podrobný popis zpracování (předmět, povaha, účel, kategorie subjektů údajů a kategorie osobních údajů) je uveden v Příloze č. 1.

2.2 Tato Smlouva o zpracování se uzavírá na dobu trvání Hlavní smlouvy. Povinnosti Smluvních stran, které mají z povahy věci trvat i po ukončení zpracování (zejména mlčenlivost), zůstávají zachovány i po zániku této Smlouvy o zpracování.

3. Povinnosti Zpracovatele

Zpracovatel se zavazuje:

- (a) zpracovávat osobní údaje pouze na základě doložených pokynů Správce, včetně předání do třetích zemí, s výjimkou případů, kdy to vyžaduje právo EU nebo právo členského státu; za doložený pokyn se považuje i Hlavní smlouva včetně jejího článku o používání AI nástrojů;
- (b) zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
- (c) přijmout s přihlédnutím ke stavu techniky, nákladům, povaze, rozsahu, kontextu a účelům zpracování přiměřená technická a organizační opatření podle čl. 32 GDPR; jejich základní popis je uveden v Příloze č. 3;
- (d) dodržovat podmínky zapojení dalších zpracovatelů podle čl. 4 této Smlouvy o zpracování;
- (e) po zohlednění povahy zpracování v co největší míře poskytnout Správci součinnost vhodnými technickými a organizačními opatřeními při plnění povinností Správce reagovat na žádosti o výkon práv subjektů údajů (kapitola III GDPR);
- (f) poskytnout Správci součinnost při zajišťování plnění povinností podle čl. 32 až 36 GDPR s přihlédnutím k povaze zpracování a informacím dostupným Zpracovateli;
- (g) oznámit Správci porušení zabezpečení osobních údajů bez zbytečného odkladu poté, co se o něm dozvěděl, nejpozději do 48 hodin od jeho zjištění;
- (h) po ukončení poskytování Služeb osobní údaje vymazat (v souladu s dobami výmazu sjednanými v Hlavní smlouvě, zejména výmaz závěrečné zprávy po 60 dnech od jejího dodání a výmaz Logů a souvisejících dat podle sjednané doby archivace) nebo je vrátit Správci, a vymazat existující kopie, pokud právo EU nebo členského státu nevyžaduje jejich uchovávání; Smluvní strany berou na vědomí, že výmaz na straně AI poskytovatelů se řídí jejich retenčními pravidly podle čl. 4.4 této Smlouvy o zpracování;

- (i) poskytnout Správci informace potřebné k prokázání splnění povinností podle čl. 28 GDPR a umožnit audity a přispět k nim za podmínek podle čl. 6 této Smlouvy o zpracování.

4. Další zpracovatelé (sub-processoři)

4.1 Správce uděluje Zpracovateli obecné písemné povolení ve smyslu čl. 28 odst. 2 GDPR k zapojení dalších zpracovatelů. Seznam dalších zpracovatelů zapojených ke dni uzavření této Smlouvy o zpracování, včetně AI poskytovatelů, tvoří Přílohu č. 2.

4.2 Zpracovatel informuje Správce o jakýchkoli zamýšlených změnách v zapojení dalších zpracovatelů (přidání nebo nahrazení) předem, a to nejméně 14 dní před zapojením, čímž se Správci dává možnost vznést vůči těmto změnám námitky. Pokud Správce námitku nevznese do zahájení zapojení, změna se považuje za odsouhlasenou. Informování je možné provést e-mailem nebo aktualizací veřejného seznamu na webových stránkách Zpracovatele spojenou s e-mailovým upozorněním.

4.3 Pokud Správce vznese odůvodněnou námitku vůči zapojení dalšího zpracovatele, který je AI poskytovatelem podle Hlavní smlouvy, Smluvní strany projednají náhradní řešení; pokud se nedohodnou, může kterákoli Smluvní strana ukončit Hlavní smlouvu v části, které se námitka týká, přičemž Správce uhradí cenu za Služby poskytnuté do ukončení.

4.4 Zpracovatel uloží každému dalšímu zpracovateli prostřednictvím smlouvy stejné povinnosti ochrany osobních údajů, jaké jsou stanoveny v této Smlouvě o zpracování. V případě AI poskytovatelů se tyto povinnosti řídí jejich standardními smlouvami o zpracování údajů (Data Processing Agreement / Addendum) uzavřenými mezi Zpracovatelem a příslušným AI poskytovatelem; Správce bere na vědomí, že podmínky zpracování (včetně retenčních dob) na straně AI poskytovatelů nemůže Zpracovatel individuálně měnit. Pokud další zpracovatel nesplní své povinnosti ochrany údajů, Zpracovatel zůstává vůči Správci plně odpovědný za plnění povinností tohoto dalšího zpracovatele, s omezeními odpovědnosti sjednanými v Hlavní smlouvě.

5. Předání do třetích zemí

5.1 Smluvní strany berou na vědomí, že další zpracovatelé uvedení v Příloze č. 2 mohou zpracovávat osobní údaje na serverech mimo EU/EHP, zejména v USA. Každé takové předání se uskuteční pouze při zajištění vhodných záruk podle kapitoly V GDPR, zejména na základě rozhodnutí o odpovídající ochraně (EU-U.S. Data Privacy Framework, pokud je příslušný subjekt certifikován) nebo standardních smluvních doložek přijatých Evropskou komisí.

6. Audit

6.1 Správce je oprávněn provést audit dodržování této Smlouvy o zpracování u Zpracovatele nejvýše jednou za 12 měsíců, na vlastní náklady, po písemném oznámení doručeném nejméně 30 dní předem, v běžné pracovní době a způsobem, který nepřiměřeně nenarušuje provoz Zpracovatele. Osoby provádějící audit musí být vázány mlčenlivostí.

6.2 Ve vztahu k dalším zpracovatelům (včetně AI poskytovatelů) se audit provádí prostřednictvím certifikací, zpráv z auditů a další dokumentace, kterou tito zpracovatelé

zpřístupňují (např. certifikace ISO 27001, zprávy SOC 2). Správce bere na vědomí, že Zpracovatel nemá právo provést fyzický audit u AI poskytovatelů.

7. Odpovědnost

7.1 Odpovědnost Smluvních stran podle této Smlouvy o zpracování se řídí ustanoveními o odpovědnosti a limitaci náhrady škody sjednanými v Hlavní smlouvě, včetně vyloučení odpovědnosti Zpracovatele za jednání nebo opomenutí AI poskytovatelů v rozsahu sjednaném v Hlavní smlouvě. Tím nejsou dotčena práva subjektů údajů a odpovědnost podle čl. 82 GDPR.

8. Závěrečná ustanovení

8.1 Tato Smlouva o zpracování nabývá platnosti a účinnosti dnem jejího podpisu oběma Smluvními stranami. V případě rozporu mezi touto Smlouvou o zpracování a Hlavní smlouvou má ve věcech ochrany osobních údajů přednost tato Smlouva o zpracování.

8.2 Tato Smlouva o zpracování se řídí právním řádem Slovenské republiky a GDPR. Změny lze provést pouze písemným dodatkem.

8.3 Nedílnou součástí této Smlouvy o zpracování jsou: Příloha č. 1 (Popis zpracování), Příloha č. 2 (Seznam dalších zpracovatelů) a Příloha č. 3 (Technická a organizační opatření).

V [●], dne [●]

Správce

Za: [●]

Jméno: [●]

Funkce: [●]

V Bratislavě, dne

Zpracovatel

Za: **Nethemba s. r. o.**

Jméno: Ing. Pavol Lupták

Funkce: jednatel

Příloha č. 1 – Popis zpracování

Předmět zpracování

Osobní údaje nacházející se v testovaných systémech Správce, v komunikaci s nimi nebo v podkladech dodaných Správcem pro poskytnutí Služeb

Doba zpracování

Po dobu poskytování Služeb; výmaz podle dob sjednaných v Hlavní smlouvě (závěrečná zpráva – 60 dní od dodání; Logy a související data – podle sjednané doby archivace, max. 24 měsíců)

Povaha zpracování

Získávání, prohlížení, analýza, dočasné uchovávání a výmaz údajů při penetračním testování a bezpečnostních auditech, včetně zpracování prostřednictvím AI nástrojů podle Hlavní smlouvy

Účel zpracování

Posouzení bezpečnosti testovaných systémů,

Kategorie subjektů údajů

identifikace zranitelností a vypracování závěrečné zprávy

Kategorie osobních údajů

Zaměstnanci, zákazníci, dodavatelé a uživatelé systémů Správce; jiné osoby, jejichž údaje se nacházejí v testovaných systémech

Identifikační a kontaktní údaje, přihlašovací a síťové identifikátory (e-mail, IP adresa, cookies), obsah komunikace a jakékoli další běžné osobní údaje nacházející se v testovaných systémech; zvláštní kategorie údajů pouze v rozsahu, v jakém se v testovaných systémech nacházejí, přičemž nejsou cílem zpracování

Příloha č. 2 – Seznam dalších zpracovatelů

AI poskytovatelé (podle článku Hlavní smlouvy o používání AI nástrojů):

Subjekt	Sídlo	Služba	Záruky pro předání
Anthropic, PBC (vč. Anthropic Ireland, Limited)	USA / Irsko	Claude, Claude Code	EU-U.S. DPF / SCC
OpenAI, Inc. / OpenAI, L.L.C. (vč. OpenAI Ireland Ltd)	USA / Irsko	ChatGPT, Codex, GPT API	EU-U.S. DPF / SCC
Google LLC / Google Ireland Limited	USA / Irsko	Gemini, Vertex AI	EU-U.S. DPF / SCC
Microsoft Corporation / Microsoft Ireland Operations Limited	USA / Irsko	Azure OpenAI, GitHub Copilot	EU-U.S. DPF / SCC
xAI Corp.	USA	Grok	SCC
Mistral AI SAS	Francie	Le Chat, La Plateforme	– (EU)
Amazon Web Services, Inc.	USA	cloudová infrastruktura	EU-U.S. DPF / SCC

Jiní další zpracovatelé: [●] (např. subdodavatelé – specialisté podle Hlavní smlouvy; doplnit nebo vyškrtnout)

Příloha č. 3 – Technická a organizační opatření

- Přístup k osobním údajům mají pouze oprávněné osoby vázané mlčenlivostí, v rozsahu nezbytném pro poskytnutí Služeb (need-to-know).
- Šifrování údajů při přenosu (TLS, SSH, VPN); šifrovaná a digitálně podepsaná e-mailová komunikace (PGP nebo S/MIME), pokud ji Správce umožní.
- Šifrování datových nosičů pracovních stanic (full-disk encryption); vícefaktorová autentizace při přístupu k systémům Zpracovatele.
- Minimalizace: údaje se zpracovávají pouze v rozsahu potřebném pro posouzení bezpečnosti; přístupové údaje (hesla, API klíče, tokeny) se AI nástrojům nepřístupňují v použitelné podobě (best effort podle Hlavní smlouvy).
- U AI nástrojů se používají placené/firemní/API verze se smluvním zákazem trénování na vstupech a výstupech a, pokud jsou dostupné, režimy zero data retention.
- Výmaz: závěrečná zpráva do 60 dnů od dodání; Logy a související data podle sjednané doby archivace; bezpečné vymazání nosičů.
- Řízení incidentů: interní postup pro detekci, eskalaci a oznamování porušení zabezpečení osobních údajů (oznámení Správci do 48 hodin od zjištění).