

ZMLUVA O SPRACÚVANÍ OSOBNÝCH ÚDAJOV

(AI verzia – so zapojením AI poskytovateľov ako ďalších sprostredkovateľov)

uzatvorená podľa čl. 28 ods. 3 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „GDPR“) (ďalej len „Zmluva o spracúvaní“)

medzi:

Obchodné meno:	[●]
Sídlo:	[●]
IČO:	[●]
Zapísaná:	v Obchodnom registri Okresného súdu [●], oddiel: [●], vložka č. [●]
Zastúpená:	[meno a priezvisko], [funkcia]

(ďalej len „Prevádzkovateľ“)

a

Obchodné meno:	Nethemba s. r. o.
Sídlo:	Klemensova 2524/4, 811 09 Bratislava, Slovenská republika
IČO:	36 777 234
Zapísaná:	v Obchodnom registri Okresného súdu Bratislava I, oddiel: Sro, vložka č. 61232/B
Zastúpená:	Ing. Pavol Lupták, konateľ
Email:	info@nethemba.com

(ďalej len „Sprostredkovateľ“)

(Prevádzkovateľ a Sprostredkovateľ ďalej spoločne len „Zmluvné strany“)

1. Úvodné ustanovenia

1.1 Zmluvné strany uzavreli zmluvu o poskytovaní služieb bezpečnosti, na základe ktorej Sprostredkovateľ poskytuje Prevádzkovateľovi služby v oblasti bezpečnosti informačných technológií, najmä penetračné testovanie a bezpečnostné audity (ďalej len „Hlavná zmluva“ a „Služby“).

1.2 Pri poskytovaní Služieb môže dochádzať k spracúvaniu osobných údajov, ktoré sa nachádzajú v testovaných systémoch Prevádzkovateľa alebo v komunikácii s nimi, Sprostredkovateľom v mene Prevádzkovateľa. Účelom tejto Zmluvy o spracúvaní je úprava vzájomných práv a povinností Zmluvných strán pri takomto spracúvaní v súlade s čl. 28 GDPR.

1.3 Pojmy „AI nástroje” a „AI poskytovatelia” majú význam podľa článku Hlavnej zmluvy upravujúceho používanie nástrojov umelej inteligencie.

2. Predmet a doba spracúvania

2.1 Sprostredkovateľ sa zaväzuje spracúvať osobné údaje v mene Prevádzkovateľa výlučne v rozsahu a za podmienok dohodnutých v tejto Zmluve o spracúvaní a v Hlavnej zmluve.

Podrobný popis spracúvania (predmet, povaha, účel, kategórie dotknutých osôb a kategórie osobných údajov) je uvedený v Prílohe č. 1.

2.2 Táto Zmluva o spracúvaní sa uzatvára na dobu trvania Hlavnej zmluvy. Povinnosti Zmluvných strán, ktoré majú z povahy veci trvať aj po ukončení spracúvania (najmä mlčanlivosť), zostávajú zachované aj po zániku tejto Zmluvy o spracúvaní.

3. Povinnosti Sprostredkovateľa

Sprostredkovateľ sa zaväzuje:

- (a) spracúvať osobné údaje len na základe zdokumentovaných pokynov Prevádzkovateľa, vrátane prenosu do tretích krajín, s výnimkou prípadov, keď si to vyžaduje právo EÚ alebo právo členského štátu; za zdokumentovaný pokyn sa považuje aj Hlavná zmluva vrátane jej článku o používaní AI nástrojov;
- (b) zabezpečiť, aby sa osoby oprávnené spracúvať osobné údaje zaviazali k mlčanlivosti alebo aby sa na ne vzťahovala zákonná povinnosť mlčanlivosti;
- (c) prijať so zohľadnením stavu techniky, nákladov, povahy, rozsahu, kontextu a účelov spracúvania primerané technické a organizačné opatrenia podľa čl. 32 GDPR; ich základný popis je uvedený v Prílohe č. 3;
- (d) dodržiavať podmienky zapojenia ďalších sprostredkovateľov podľa čl. 4 tejto Zmluvy o spracúvaní;
- (e) po zohľadnení povahy spracúvania v čo najväčšej miere poskytnúť Prevádzkovateľovi súčinnosť vhodnými technickými a organizačnými opatreniami pri plnení povinností Prevádzkovateľa reagovať na žiadosti o výkon práv dotknutých osôb (kapitola III GDPR);
- (f) poskytnúť Prevádzkovateľovi súčinnosť pri zabezpečení plnenia povinností podľa čl. 32 až 36 GDPR s prihliadnutím na povahu spracúvania a informácie dostupné Sprostredkovateľovi;
- (g) oznámiť Prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvedel, najneskôr do 48 hodín od jeho zistenia;
- (h) po ukončení poskytovania Služieb osobné údaje vymazať (v súlade s dobami výmazu dohodnutými v Hlavnej zmluve, najmä výmaz záverečnej správy po 60 dňoch od jej dodania a výmaz Logov a súvisiacich dát podľa dohodnutej doby archivácie) alebo ich vrátiť Prevádzkovateľovi, a vymazať existujúce kópie, pokiaľ právo EÚ alebo členského štátu nepožaduje ich uchovávanie; Zmluvné strany berú na vedomie, že výmaz na strane

AI poskytovateľov sa spravuje ich retenčnými pravidlami podľa čl. 4.4 tejto Zmluvy o spracúvaní;

- (i) poskytnúť Prevádzkovateľovi informácie potrebné na preukázanie splnenia povinností podľa čl. 28 GDPR a umožniť audity a príspeť k nim za podmienok podľa čl. 6 tejto Zmluvy o spracúvaní.

4. Ďalší sprostredkovatelia (sub-processori)

4.1 Prevádzkovateľ udeľuje Sprostredkovateľovi všeobecné písomné povolenie v zmysle čl. 28 ods. 2 GDPR na zapojenie ďalších sprostredkovateľov. Zoznam ďalších sprostredkovateľov zapojených ku dňu uzavretia tejto Zmluvy o spracúvaní, vrátane AI poskytovateľov, tvorí Prílohu č. 2.

4.2 Sprostredkovateľ informuje Prevádzkovateľa o akýchkoľvek zamýšľaných zmenách v zapojení ďalších sprostredkovateľov (pridanie alebo nahradenie) vopred, a to najmenej 14 dní pred zapojením, čím sa Prevádzkovateľovi dáva možnosť namietať voči týmto zmenám. Ak Prevádzkovateľ námietku nevznesie do začatia zapojenia, zmena sa považuje za odsúhlasenú. Informovanie je možné vykonať e-mailom alebo aktualizáciou verejného zoznamu na webovom sídle Sprostredkovateľa spojenou s e-mailovým upozornením.

4.3 Ak Prevádzkovateľ vznesie odôvodnenú námietku voči zapojeniu ďalšieho sprostredkovateľa, ktorý je AI poskytovateľom podľa Hlavnej zmluvy, Zmluvné strany prerokujú náhradné riešenie; ak sa nedohodnú, môže ktorákoľvek Zmluvná strana ukončiť Hlavnú zmluvu v časti, ktorej sa námietka týka, pričom Prevádzkovateľ uhradí cenu za Služby poskytnuté do ukončenia.

4.4 Sprostredkovateľ uloží každému ďalšiemu sprostredkovateľovi prostredníctvom zmluvy rovnaké povinnosti ochrany osobných údajov, aké sú stanovené v tejto Zmluve o spracúvaní. V prípade AI poskytovateľov sa tieto povinnosti spravujú ich štandardnými zmluvami o spracúvaní údajov (Data Processing Agreement / Addendum) uzatvorenými medzi Sprostredkovateľom a príslušným AI poskytovateľom; Prevádzkovateľ berie na vedomie, že podmienky spracúvania (vrátane retenčných dôb) na strane AI poskytovateľov nemôže Sprostredkovateľ individuálne meniť. Ak ďalší sprostredkovateľ nesplní svoje povinnosti ochrany údajov, Sprostredkovateľ zostáva voči Prevádzkovateľovi plne zodpovedný za plnenie povinností tohto ďalšieho sprostredkovateľa, s obmedzeniami zodpovednosti dohodnutými v Hlavnej zmluve.

5. Prenos do tretích krajín

5.1 Zmluvné strany berú na vedomie, že ďalší sprostredkovatelia uvedení v Prílohe č. 2 môžu spracúvať osobné údaje na serveroch mimo EÚ/EHP, najmä v USA. Každý takýto prenos sa uskutoční len pri zabezpečení primeraných záruk podľa kapitoly V GDPR, najmä na základe rozhodnutia o primeranosti (EU-U.S. Data Privacy Framework, ak je príslušný subjekt certifikovaný) alebo štandardných zmluvných doložiek prijatých Európskou komisiou.

6. Audit

6.1 Prevádzkovateľ je oprávnený vykonať audit dodržiavania tejto Zmluvy o spracúvaní u Sprostredkovateľa najviac raz za 12 mesiacov, na vlastné náklady, po písomnom oznámení doručenom najmenej 30 dní vopred, v bežnom pracovnom čase a spôsobom, ktorý neprímerane nenarušuje prevádzku Sprostredkovateľa. Osoby vykonávajúce audit musia byť zaviazané mlčanlivosťou.

6.2 Vo vzťahu k ďalším sprostredkovateľom (vrátane AI poskytovateľov) sa audit vykonáva prostredníctvom certifikácií, správ z auditov a ďalšej dokumentácie, ktorú títo sprostredkovatelia sprístupňujú (napr. certifikácie ISO 27001, správy SOC 2). Prevádzkovateľ berie na vedomie, že Sprostredkovateľ nemá právo vykonať fyzický audit u AI poskytovateľov.

7. Zodpovednosť

7.1 Zodpovednosť Zmluvných strán podľa tejto Zmluvy o spracúvaní sa spravuje ustanoveniami o zodpovednosti a limitácii náhrady škody dohodnutými v Hlavnej zmluve, vrátane vylúčenia zodpovednosti Sprostredkovateľa za konanie alebo opomenutie AI poskytovateľov v rozsahu dohodnutom v Hlavnej zmluve. Tým nie sú dotknuté práva dotknutých osôb a zodpovednosť podľa čl. 82 GDPR.

8. Záverečné ustanovenia

8.1 Táto Zmluva o spracúvaní nadobúda platnosť a účinnosť dňom jej podpisu oboma Zmluvnými stranami. V prípade rozporu medzi touto Zmluvou o spracúvaní a Hlavnou zmluvou má vo veciach ochrany osobných údajov prednosť táto Zmluva o spracúvaní.

8.2 Táto Zmluva o spracúvaní sa spravuje právnym poriadkom Slovenskej republiky a GDPR. Zmeny je možné vykonať len písomným dodatkom.

8.3 Neoddeliteľnou súčasťou tejto Zmluvy o spracúvaní sú: Príloha č. 1 (Popis spracúvania), Príloha č. 2 (Zoznam ďalších sprostredkovateľov) a Príloha č. 3 (Technické a organizačné opatrenia).

V [●], dňa [●]

Prevádzkovateľ

Za: [●]

Meno: [●]

Funkcia: [●]

V Bratislave, dňa

Sprostredkovateľ

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

Meno: Ing. Pavol Lupták

Funkcia: konateľ

Príloha č. 1 – Popis spracúvania

Predmet spracúvania

Osobné údaje nachádzajúce sa v testovaných systémoch Prevádzkovateľa, v komunikácii s nimi alebo v podkladoch dodaných Prevádzkovateľom pre poskytnutie Služieb

Doba spracúvania	Po dobu poskytovania Služieb; výmaz podľa dôb dohodnutých v Hlavnej zmluve (záverečná správa – 60 dní od dodania; Logy a súvisiace dáta – podľa dohodnutej doby archivácie, max. 24 mesiacov)
Povaha spracúvania	Získavanie, prehliadanie, analýza, dočasné uchovávanie a výmaz údajov pri penetračnom testovaní a bezpečnostných auditoch, vrátane spracúvania prostredníctvom AI nástrojov podľa Hlavnej zmluvy
Účel spracúvania	Posúdenie bezpečnosti testovaných systémov, identifikácia zraniteľností a vypracovanie záverečnej správy
Kategórie dotknutých osôb	Zamestnanci, zákazníci, dodávatelia a používatelia systémov Prevádzkovateľa; iné osoby, ktorých údaje sa nachádzajú v testovaných systémoch
Kategórie osobných údajov	Identifikačné a kontaktné údaje, prihlasovacie a sieťové identifikátory (e-mail, IP adresa, cookies), obsah komunikácie a akékoľvek ďalšie bežné osobné údaje nachádzajúce sa v testovaných systémoch; osobitné kategórie údajov len v rozsahu, v akom sa v testovaných systémoch nachádzajú, pričom nie sú cieľom spracúvania

Príloha č. 2 – Zoznam ďalších sprostredkovateľov

AI poskytovatelia (podľa článku Hlavnej zmluvy o používaní AI nástrojov):

Subjekt	Sídlo	Služba	Záruky pre prenos
Anthropic, PBC (vrát. Anthropic Ireland, Limited)	USA / Írsko	Claude, Claude Code	EU-U.S. DPF / SCC
OpenAI, Inc. / OpenAI, L.L.C. (vrát. OpenAI Ireland Ltd)	USA / Írsko	ChatGPT, Codex, GPT API	EU-U.S. DPF / SCC
Google LLC / Google Ireland Limited	USA / Írsko	Gemini, Vertex AI	EU-U.S. DPF / SCC
Microsoft Corporation /	USA / Írsko	Azure OpenAI, GitHub Copilot	EU-U.S. DPF / SCC

Subjekt	Sídlo	Služba	Záruky pre prenos
Microsoft Ireland Operations Limited			
xAI Corp.	USA	Grok	SCC
Mistral AI SAS	Francúzsko	Le Chat, La Plateforme	– (EÚ)
Amazon Web Services, Inc.	USA	cloudová infraštruktúra	EU-U.S. DPF / SCC

Iní ďalší sprostredkovatelia: [●] (napr. subdodávatelia – špecialisti podľa Hlavnej zmluvy; doplniť alebo vyčiarknuť)

Príloha č. 3 – Technické a organizačné opatrenia

- Prístup k osobným údajom majú len oprávnené osoby viazané mlčanlivosťou, v rozsahu nevyhnutnom na poskytnutie Služieb (need-to-know).
- Šifrovanie údajov pri prenose (TLS, SSH, VPN); šifrovaná a digitálne podpísaná e-mailová komunikácia (PGP alebo S/MIME), ak ju Prevádzkovateľ umožní.
- Šifrovanie dátových nosičov pracovných staníc (full-disk encryption); viacfaktorová autentifikácia pri prístupe k systémom Sprostredkovateľa.
- Minimalizácia: údaje sa spracúvajú len v rozsahu potrebnom na posúdenie bezpečnosti; prístupové údaje (heslá, API kľúče, tokeny) sa AI nástrojom nesprístupňujú v použiteľnej podobe (best effort podľa Hlavnej zmluvy).
- Pri AI nástrojoch sa používajú platené/firemné/API verzie so zmluvným zákazom trénovania na vstupoch a výstupoch a, ak sú dostupné, režimy zero data retention.
- Výmaz: záverečná správa do 60 dní od dodania; Logy a súvisiace dáta podľa dohodnutej doby archivácie; bezpečné vymazanie nosičov.
- Riadenie incidentov: interný postup pre detekciu, eskaláciu a oznamovanie porušení ochrany osobných údajov (oznámenie Prevádzkovateľovi do 48 hodín od zistenia).