smlouva o zpracovávání osobních údajů (DPA)

podle čl. 28 nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR)

Zpracovatel: LexAI Technologies, s.r.o., IČO: 23589825, se sídlem Školská 660/3, Praha 1 - Nové Město 110 00 Praha 1, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze

Správce: [NÁZEV SPOLEČNOSTI / JMÉNO], IČO/ID: [DOPLNIT], se sídlem [DOPLNIT]

Datum uzavření: [DOPLNIT]

Kontakt Zpracovatele: support@lexaitechnologies.com

Preambule

Tato Smlouva o zpracování osobních údajů (dále jen „DPA" nebo „Smlouva") je uzavřena mezi výše uvedeným Zpracovatelem a Správcem (dohromady „Smluvní strany") v souladu s čl. 28 Nařízení Evropského parlamentu a Rady (EU) 2016/679 (dále jen „GDPR").

Správce využívá platformu LexAI (dále jen „Platforma" nebo „Služba") poskytovanou Zpracovatelem na základě Podmínek užívání dostupných na www.lexaitechnologies.app (dále jen „Hlavní smlouva"). V rámci poskytování Služby může docházet ke zpracování osobních údajů fyzických osob, vůči nimž je Správce v postavení správce ve smyslu čl. 4 odst. 7 GDPR. Tato DPA upravuje podmínky, za nichž Zpracovatel zpracovává taková data jménem Správce.

V případě rozporu mezi touto DPA a Hlavní smlouvou má v otázkách ochrany osobních údajů přednost tato DPA.

Článek 1 — Definice

Pro účely této Smlouvy mají níže uvedené pojmy následující význam:

- **„GDPR"** — Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů.
- **„Osobní údaje Správce"** — osobní údaje, které Správce předává Zpracovateli ke zpracování v rámci využívání Služby, nebo které Zpracovatel zpracovává jménem Správce v důsledku poskytování Služby.
- **„Subjekt údajů"** — fyzická osoba, jejíž osobní údaje jsou zpracovávány; zejména klienti, zaměstnanci nebo jiné fyzické osoby, jejichž data Správce prostřednictvím Platformy zpracovává.
- **„Zpracování"** — jakákoli operace nebo soubor operací s osobními údaji ve smyslu čl. 4 odst. 2 GDPR.
- **„Porušení zabezpečení"** — porušení zabezpečení vedoucí k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému zpřístupnění osobních údajů.
- **„Sub-zpracovatel"** — třetí strana zapojená Zpracovatelem ke zpracování osobních údajů jménem Správce.
- **„Standardní smluvní doložky" / „SCC"** — standardní smluvní doložky pro předávání osobních údajů do třetích zemí přijaté Evropskou komisí.
- **„EHP"** — Evropský hospodářský prostor.

Ostatní pojmy mají tentýž význam jako v GDPR nebo v Hlavní smlouvě.

Článek 2 — Předmět a povaha zpracování

2.1 Předmět zpracování

Zpracovatel zpracovává Osobní údaje Správce výhradně za účelem poskytování Služby dle Hlavní smlouvy, konkrétně:

- zpracování právních dokumentů, smluv a jiných textů prostřednictvím AI modelů;
- provádění právního výzkumu na základě dotazů obsahujících osobní údaje;
- ukládání a správa konverzací a projektů v rámci Platformy;
- technická podpora a provoz Platformy.

2.2 Povaha zpracování

Zpracování probíhá automatizovaně prostřednictvím AI modelů (Claude, Anthropic) a zahrnuje zejména: čtení, analýzu, sumarizaci, klasifikaci a ukládání osobních údajů obsažených v dokumentech a dotazech předaných Správcem.

2.3 Kategorie subjektů údajů

Zpracování se může týkat následujících kategorií subjektů údajů:

- klienti Správce (fyzické osoby);
- zaměstnanci nebo spolupracovníci Správce;
- protistrany v právních věcech;
- jiné fyzické osoby uvedené v dokumentech předaných Správcem ke zpracování.

2.4 Kategorie osobních údajů

Zpracovávané osobní údaje mohou zahrnovat zejména:

- identifikační údaje (jméno, příjmení, datum narození, rodné číslo);
- kontaktní údaje (adresa, email, telefon);
- údaje o právních věcech a sporech;
- finanční a majetkové údaje;
- zvláštní kategorie osobních údajů dle čl. 9 GDPR (zdravotní údaje, údaje o trestních řízeních apod.), pokud jsou obsaženy v předaných dokumentech.

2.5 Trvání zpracování

Zpracování trvá po dobu platnosti Hlavní smlouvy, není-li v této DPA stanoveno jinak.

Článek 3 — Povinnosti Zpracovatele

3.1 Zpracování výhradně dle pokynů Správce

Zpracovatel zpracovává Osobní údaje Správce výhradně na základě doložených pokynů Správce, jimiž jsou zejména: Hlavní smlouva, tato DPA a pokyny udělené Správcem prostřednictvím Platformy. Zpracovatel

nezpracovává Osobní údaje Správce pro vlastní účely ani je nepředává třetím stranám, s výjimkou případů stanovených touto DPA.

Pokud je Zpracovatel povinen zpracovávat osobní údaje z důvodu právního předpisu EU nebo členského státu, který se na něj vztahuje, informuje o tom Správce před zahájením zpracování, ledaže by takový právní předpis toto oznámení zakazoval z důvodů veřejného zájmu.

3.2 Důvěrnost

Zpracovatel zajistí, aby osoby oprávněné zpracovávat Osobní údaje Správce byly vázány povinností mlčenlivosti, a to buď smluvní, nebo zákonnou.

3.3 Technická a organizační bezpečnostní opatření

Zpracovatel implementuje a udržuje technická a organizační opatření přiměřená riziku zpracování v souladu s čl. 32 GDPR. Tato opatření zahrnují zejména:

Technická opatření:

- Zero-knowledge architektura: obsah konverzací je šifrován třemi nezávislými vrstvami AES-256-GCM přímo na zařízení Správce; Zpracovatel nemá technický přístup k nešifrovanému obsahu.
- Šifrování dat v klidu a při přenosu (AES-256-GCM, TLS).
- Derivace šifrovacích klíčů pomocí PBKDF2-SHA256 (600 000 iterací).
- Vícefaktorová autentizace (WebAuthn, TOTP 2FA).
- Databázová izolace dat jednotlivých zákazníků (Row Level Security).
- Rate limiting a anomaly detection.
- Automatické mazání session klíčů po 2 hodinách neaktivity.

Organizační opatření:

- Přístup k systémům na principu nejnižších privilegií.
- Pravidelné interní bezpečnostní přezkoumání.
- Bezpečnostní logy uchovávány 90 dní.

Zpracovatel může tato opatření průběžně aktualizovat za předpokladu, že jejich úroveň ochrany neklesne pod standard stanovený touto DPA.

3.4 Zapojení Sub-zpracovatelů

Správce uděluje Zpracovateli obecné předchozí povolení k zapojení Sub-zpracovatelů. Aktuální seznam Sub-zpracovatelů tvoří **Přílohu č. 1** této DPA.

Zpracovatel:

- před zapojením nového nebo změnou stávajícího Sub-zpracovatele informuje Správce s předstihem nejméně **30 dní**, a to prostřednictvím emailového oznámení nebo aktualizace Zásad ochrany osobních údajů dostupných na Platformě;
- Správce má právo vznést odůvodněné námitky proti novému Sub-zpracovateli ve lhůtě 14 dní od oznámení; pokud námitka není vyřešena, může Správce ukončit Hlavní smlouvu;

- zajistí, aby Sub-zpracovatelé byli vázáni povinnostmi ochrany osobních údajů přinejmenším rovnocennými těm, které jsou stanoveny touto DPA;
- odpovídá Správci za plnění povinností Sub-zpracovatelů.

3.5 Pomoc Správci při plnění povinností

Zpracovatel pomáhá Správci — s ohledem na povahu zpracování a dostupné informace — při plnění jeho povinností dle GDPR, zejména:

- při vyřizování žádostí subjektů údajů o výkon jejich práv (přístup, oprava, výmaz, přenositelnost, omezení, námitka);
- při zajišťování souladu s povinnostmi dle čl. 32–36 GDPR (bezpečnost, hlášení porušení, posouzení vlivu na ochranu osobních údajů);
- při předávání informací potřebných k doložení souladu s touto DPA.

Pomoc Zpracovatele nad rámec jeho standardních povinností může být zpoplatněna dle platného ceníku nebo na základě dohody.

3.6 Hlášení porušení zabezpečení

Zpracovatel bez zbytečného odkladu, nejpozději do **48 hodin** od zjištění, informuje Správce o jakémkoli Porušení zabezpečení týkajícím se Osobních údajů Správce. Oznámení obsahuje alespoň:

- popis povahy Porušení zabezpečení včetně kategorií a přibližného počtu dotčených subjektů údajů a záznamů;
- kontaktní údaje pro získání dalších informací;
- popis pravděpodobných důsledků Porušení zabezpečení;
- popis opatření přijatých nebo navrhovaných k nápravě.

Zpracovatel není povinen oznamovat Porušení zabezpečení, pokud je nepravděpodobné, že by mělo za následek riziko pro práva a svobody fyzických osob.

3.7 Posouzení vlivu na ochranu osobních údajů (DPIA)

Pokud Správce hodlá provádět zpracování, které si vyžaduje posouzení vlivu na ochranu osobních údajů (DPIA) dle čl. 35 GDPR, poskytne Zpracovatel Správci na jeho žádost dostupné informace potřebné k provedení takového posouzení.

3.8 Výmaz nebo vrácení dat po ukončení smlouvy

Po ukončení Hlavní smlouvy Zpracovatel dle volby Správce:

- vymaže veškeré Osobní údaje Správce a jejich existující kopie; nebo
- vrátí Správci veškeré Osobní údaje ve strojově čitelném formátu.

Výmaz nebo vrácení proběhne do **30 dní** od ukončení Hlavní smlouvy, není-li uchovávání vyžadováno právními předpisy EU nebo členského státu. O provedení výmazu vystaví Zpracovatel na žádost Správce písemné potvrzení.

Článek 4 — Povinnosti Správce

Správce prohlašuje a zaručuje, že:

- má zákonný právní základ pro zpracování Osobních údajů, které předává Zpracovateli ke zpracování;
- poskytl subjektům údajů veškeré informace požadované GDPR, včetně informace o zpracování prostřednictvím Platformy LexAI;
- pokyny udělené Zpracovateli jsou v souladu s GDPR a dalšími aplikovatelnými právními předpisy;
- před předáním zvláštních kategorií osobních údajů dle čl. 9 GDPR ke zpracování prostřednictvím Platformy posoudil zákonnost takového zpracování a je přesvědčen o jeho souladu s GDPR;
- neprodleně informuje Zpracovatele o jakékoli změně, která by mohla mít vliv na povinnosti Zpracovatele dle této DPA.

Článek 5 — Předávání osobních údajů do třetích zemí

5.1 Předávání v rámci EHP

Zpracovatel primárně zpracovává Osobní údaje Správce v rámci EHP (Supabase EU Frankfurt, Hetzner EU Frankfurt, Qdrant EU Frankfurt).

5.2 Předávání mimo EHP

Někteří Sub-zpracovatelé Zpracovatele sídlí mimo EHP, zejména v USA (Anthropic, Vercel, Stripe, SendGrid, SerpAPI, Brave Search, IPInfo). Předávání do těchto zemí probíhá na základě:

- **Standardních smluvních doložek (SCC)** přijatých Evropskou komisí dle čl. 46 odst. 2 písm. c) GDPR; a/nebo
- **rozhodnutí o přiměřenosti** (EU–U.S. Data Privacy Framework), kde je to aplikovatelné.

Kopii příslušných SCC lze na žádost poskytnout Správci.

5.3 Zvláštní podmínky pro předávání dat Anthropic

Správce bere na vědomí, že obsah konverzací a dokumentů je předáván ke zpracování AI modely Anthropic (USA). Anthropic nezpracovává data zaslaná přes API za účelem trénování svých modelů. Toto předávání je zajištěno SCC uzavřenými mezi Zpracovatelem a Anthropic.

Článek 6 — Práva na audit

6.1 Právo na informace a audit

Zpracovatel zpřístupní Správci veškeré informace nezbytné k doložení souladu s povinnostmi stanovenými v čl. 28 GDPR a umožní audity nebo inspekce prováděné Správcem nebo auditorem pověřeným Správcem.

6.2 Podmínky auditu

Audit musí být:

- oznámen Zpracovateli písemně nejméně **30 dní** předem;

- prováděn v běžné pracovní době Zpracovatele;
- prováděn tak, aby minimálně narušoval provoz Zpracovatele;
- omezen na informace nezbytné pro ověření souladu s touto DPA.

Zpracovatel může odmítnout přístup k informacím, které se týkají jiných zákazníků nebo jsou chráněny obchodním tajemstvím, za předpokladu, že poskytne dostatečná alternativní ujištění.

6.3 Náklady auditu

Náklady na audit nese Správce, pokud audit neodhalí podstatné porušení povinností Zpracovatele dle této DPA.

Článek 7 — Odpovědnost

7.1 Odpovědnost za škodu

Každá Smluvní strana odpovídá druhé Smluvní straně za škody způsobené porušením povinností dle této DPA nebo GDPR, a to v rozsahu stanoveném aplikovatelným právem.

7.2 Omezení odpovědnosti Zpracovatele

Odpovědnost Zpracovatele vůči Správci vyplývající z této DPA nebo v souvislosti s ní nepřesáhne celkovou výši plateb skutečně uhrazených Správcem Zpracovateli za Službu v posledních **12 měsících** před vznikem škodní události, s výjimkou škod způsobených hrubou nedbalostí nebo úmyslným jednáním Zpracovatele.

7.3 Pokuty uložené dozorovým úřadem

Pokud dozorový úřad uloží Správci pokutu v důsledku porušení GDPR způsobeného výhradně prokazatelným porušením povinností Zpracovatele dle této DPA, uhradí Zpracovatel Správci přiměřenou část takové pokuty odpovídající míře zavinění Zpracovatele.

Článek 8 — Trvání a ukončení

8.1 Trvání

Tato DPA je účinná po celou dobu platnosti Hlavní smlouvy mezi Smluvními stranami.

8.2 Ukončení

Tato DPA zaniká automaticky s ukončením Hlavní smlouvy. Ustanovení, která mají ze své povahy přetrvat ukončení (zejm. čl. 3.8, čl. 7), zůstávají v platnosti.

Článek 9 — Závěrečná ustanovení

9.1 Rozhodné právo

Tato DPA se řídí právem České republiky, zejména zákonem č. 89/2012 Sb., občanský zákoník, a GDPR.

9.2 Řešení sporů

Veškeré spory vzniklé z této DPA nebo v souvislosti s ní budou řešeny věcně příslušnými soudy České republiky.

9.3 Změny DPA

Zpracovatel může tuto DPA jednostranně měnit v rozsahu nezbytném pro zajištění souladu s GDPR nebo v důsledku změn v poskytování Služby. O podstatných změnách bude Správce informován emailem nejméně 30 dní předem.

9.4 Oddělitelnost

Pokud se jakékoli ustanovení této DPA ukáže jako neplatné nebo nevymahatelné, zůstávají ostatní ustanovení v plné platnosti.

9.5 Celá dohoda

Tato DPA spolu s Hlavní smlouvou a Zásadami ochrany osobních údajů tvoří úplnou dohodu Smluvních stran ohledně zpracování osobních údajů a nahrazuje veškerá předchozí ujednání v této věci.

Příloha č. 1 — Seznam Sub-zpracovatelů

Sub-zpracovatel	Sídlo	Účel	Předávaná data
Anthropic, PBC	USA	Zpracování AI dotazů (Claude API)	Obsah konverzací, dokumenty k analýze
Supabase, Inc.	EU (Frankfurt)	Databáze a autentizace	Veškerá uživatelská data (v zašifrované podobě)
Vercel, Inc.	USA / EU	Serverless hosting	Request logy, API volání
Hetzner Online GmbH	EU (Frankfurt)	Vlastní servery (vektorová DB, bezpečnostní logy, zpracování dokumentů)	Security logy, zpracování dokumentů
Qdrant	EU (Frankfurt, self-hosted na Hetzner)	Vektorová databáze pro veřejnou legislativu	Embeddings veřejných právních zdrojů — žádná uživatelská data
Stripe, Inc.	USA (EU compliance)	Platební brána	Platební údaje, fakturační data
Twilio SendGrid	USA	Emailová komunikace	Emailové adresy, notifikační emaily
SerpAPI	USA	Webové vyhledávání	Vyhledávací dotazy
Brave Search	USA	Alternativní webové vyhledávání	Vyhledávací dotazy
IPInfo	USA	Geolokace IP adres	IP adresy uživatelů

Zpracovatel si vyhrazuje právo tento seznam aktualizovat dle čl. 3.4 této DPA.

Příloha č. 2 — Technická a organizační bezpečnostní opatření

Tato příloha popisuje bezpečnostní opatření implementovaná Zpracovatelem ve smyslu čl. 32 GDPR a čl. 3.3 této DPA.

Šifrování a kryptografie

Komponenta	Standard	Parametry
Šifrování konverzací	AES-256-GCM (3 vrstvy)	12-byte IV, 128-bit auth tag, unikátní klíče per konverzace
Derivace klíčů	PBKDF2-SHA256	600 000 iterací
Hashování hesel	PBKDF2	600 000 iterací, constant-time porovnání
Device binding	PBKDF2	100 000 iterací
Přenos dat	TLS 1.2+	HTTPS enforced

Přístupová kontrola

- Vícefaktorová autentizace: WebAuthn (FIDO2) a TOTP
- Row Level Security (RLS) na úrovni databáze Supabase
- Přístup zaměstnanců na principu nejnižších privilegií
- Opětovné ověření hesla každých 14 dní
- Session timeout: 2 hodiny neaktivity, max. 24 hodin

Odolnost a dostupnost

- Serverless architektura (Vercel edge functions) pro horizontální škálování
- Primární data v EU (Frankfurt)
- Rate limiting na úrovni IP adresy i uživatele

Monitoring a auditování

- Bezpečnostní logy uchovávány 90 dní
- Anomaly detection: 5 incidentů → 5minutový lockout
- Kryptografické operace logovány (success/failure)

Zero-Knowledge architektura

- Heslo uživatele nikdy neopustí jeho zařízení
- Derivace klíčů probíhá výhradně client-side
- Zpracovatel nemá technický přístup k obsahu konverzací

Podpisy

Tato DPA je uzavřena dnem uvedeným v záhlaví tohoto dokumentu.

Za Zpracovatele — LexAI Technologies, s.r.o.:

Jméno: _____
Funkce: _____
Datum: _____
Podpis: _____

Za Správce — [NÁZEV SPOLEČNOSTI]:

Jméno: _____
Funkce: _____
Datum: _____
Podpis: _____

Verze 1.0 — template, upravit před podpisem dle konkrétního zákazníka