Zásady ochrany osobních údajů (Privacy Policy)

Provozovatel / Správce: 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
Účinnost: 1. května 2025
Kontakt: support@lexaitechnologies.com

1. Úvod a základní zásady

LexAI Technologies, s.r.o. (dále jen „LexAI" nebo „my") provozuje platformu LexAI — AI-asistovaný právní nástroj (dále jen „Platforma"). Při zpracování osobních údajů dbáme na ochranu soukromí našich uživatelů a dodržujeme veškeré platné právní předpisy, zejména:

- **Nařízení (EU) 2016/679 (GDPR)** — obecné nařízení o ochraně osobních údajů;
- **Zákon č. 110/2019 Sb.** — o zpracování osobních údajů;
- příslušné sektorové právní předpisy.

Naše klíčové zásady

- **Privacy-first architektura:** Platforma je postavena na principu zero-knowledge — obsah vašich konverzací je šifrován přímo na vašem zařízení; my jako Provozovatel k nim nemáme technický přístup.
- **Žádné trénování AI:** Vaše data nikdy nepoužíváme k trénování AI modelů. Využíváme výhradně komerční API Anthropic Claude.
- **Minimalizace dat:** Sbíráme pouze data nezbytná pro poskytování Služby.
- **Transparentnost:** Přesně vám sdělujeme, co sbíráme, proč a jak dlouho.

2. Kdo jsme (správce osobních údajů)

Správcem osobních údajů ve smyslu čl. 4 odst. 7 GDPR je:

LexAI Technologies, s.r.o.
IČO: 23589825
Sídlo: Školská 660/3, Praha 1 - Nové Město 110 00 Praha 1
Email: support@lexaitechnologies.com
Web: www.lexaitechnologies.com

LexAI neurčila pověřence pro ochranu osobních údajů (DPO), neboť to není povinné vzhledem k povaze a rozsahu zpracování. V případě dotazů týkajících se ochrany osobních údajů kontaktujte: support@lexaitechnologies.com.

3. Jaké osobní údaje zpracováváme a proč

3.1 Přehled kategorií zpracovávaných dat

Kategorie	Konkrétní data	Účel zpracování	Právní základ
Účet	Email (ověřený), jméno, hashované heslo	Registrace, autentizace, správa účtu	Plnění smlouvy (čl. 6 odst. 1 písm. b) GDPR)
Konverzace	Chat historie, dotazy a odpovědi AI	Poskytování AI asistence, správa projektů	Plnění smlouvy
Dokumenty	Nahrané soubory (PDF, DOCX), extrahovaný text	Analýza a zpracování dokumentů	Plnění smlouvy
Platby	Stripe customer ID, subscription ID, faktury	Fakturace, správa předplatného	Plnění smlouvy; Právní povinnost (daňové účely)
Bezpečnost	IP adresy, informace o zařízení, 2FA tokeny, WebAuthn credentials	Bezpečnostní monitoring, prevence podvodů	Oprávněný zájem (čl. 6 odst. 1 písm. f) GDPR)
Používání	Počet tokenů, webových vyhledávání a dotazů za měsíc	Správa limitů, fakturace, optimalizace Služby	Plnění smlouvy; Oprávněný zájem
Gamifikace	XP body, achievements	Funkce platformy	Plnění smlouvy
Komunikace	Obsah emailů zaslaných Uživateli (logy SendGrid)	Podpora, notifikace, ověření emailu	Plnění smlouvy; Oprávněný zájem

3.2 Zvláštní kategorie osobních údajů

LexAI záměrně **nezpracovává** zvláštní kategorie osobních údajů ve smyslu čl. 9 GDPR (zdravotní údaje, biometrické údaje, údaje o rasovém původu apod.) jako součást registrace nebo nastavení profilu.

Upozorňujeme však, že Uživatelé mohou do Platformy nahrávat právní dokumenty, které zvláštní kategorie osobních údajů obsahují (např. smlouvy, soudní podání, lékařské posudky v rámci soudních sporů). V takovém případě:

- LexAI zpracovává tyto dokumenty výhradně jako technický zprostředkovatel na pokyn Uživatele;
- odpovědnost za zákonnost zpracování takových dat v dokumentech leží na Uživateli;
- tyto dokumenty jsou šifrovány na zařízení Uživatele (zero-knowledge architektura) a LexAI k nim nemá nešifrovaný přístup.

4. Zero-knowledge architektura a šifrování

Tato sekce je klíčová pro pochopení toho, jak LexAI nakládá s vašimi konverzacemi a dokumenty.

4.1 Co to znamená v praxi

LexAI provozuje **zero-knowledge architekturu** inspirovanou ProtonMailem. To konkrétně znamená:

- **Vaše heslo nikdy neopustí váš prohlížeč.** Veškerá kryptografická derivace klíčů probíhá výhradně na vašem zařízení (client-side). Na naše servery se heslo v žádné formě neposílá.
- **Obsah vašich konverzací je šifrován třemi nezávislými vrstvami** (AES-256-GCM) přímo ve vašem prohlížeči ještě před odesláním na naše servery.
- **Na naše servery ukládáme pouze zašifrovaná data.** Nemáme technickou možnost číst obsah vašich konverzací ani obnovit vaše heslo.

4.2 Technické parametry šifrování

Komponenta	Algoritmus	Parametry
Šifrování dat	AES-256-GCM	12-byte IV, 128-bit auth tag
Derivace klíčů	PBKDF2-SHA256	600 000 iterací
Hashování hesel	PBKDF2	600 000 iterací, constant-time porovnání
Device binding	PBKDF2	100 000 iterací

4.3 Co server ukládá a nevidí

Co server **nikdy nevidí** v nešifrované podobě:

- Master Key uživatele
- Recovery Phrase (ukládáme pouze PBKDF2 hash)
- Obsah konverzací
- Šifrovací klíče konverzací
- Heslo uživatele

Co server ukládá (vše zašifrované):

- Zašifrovaný Master Key (zašifrovaný device nebo recovery key)
- PBKDF2 hash Recovery Phrase + salt
- Zašifrované klíče konverzací (content key, transport key, storage key — vše šifrováno Master Key)

4.4 Recovery Phrase

12slovná obnovovací fráze je **jediným způsobem obnovení přístupu** k datům při ztrátě hesla. Server ukládá pouze její hash (PBKDF2). LexAI nemůže přístup k datům obnovit jiným způsobem. Bezpečné uschování Recovery Phrase je výhradní odpovědností Uživatele.

4.5 Automatické čištění klíčů

Trigger	Akce
Zavření záložky	Vymazání klíčů z paměti
2 hodiny neaktivity	Vymazání session klíčů
Odhlášení	Vymazání všech klíčů
Expirace session	24 hodin maximální životnost

5. Zpracování dat při AI asistenci (Anthropic)

5.1 Jak funguje zpracování AI dotazů

Když zadáváte dotaz do AI chatu nebo nahráváte dokument k analýze:

1. Data jsou **dešifrována výhradně na vašem zařízení** (v paměti prohlížeče).
2. Dešifrovaný obsah je odeslán přes zabezpečené HTTPS spojení na servery LexAI (serverless Vercel edge functions).
3. Serverless funkce předá obsah do **Anthropic API** ke zpracování AI modelem.
4. Odpověď AI je vrácena, **zašifrována na vašem zařízení** a uložena na serverech LexAI v zašifrované podobě.

5.2 Anthropic jako zpracovatel

Anthropic (Anthropic, PBC, USA) zpracovává obsah vašich dotazů a dokumentů jako náš **zpracovatel (procesor) dat** v souladu s jejich podmínkami API a Data Processing Agreement. Klíčové body:

- Anthropic **nepoužívá data zaslaná přes API k trénování svých modelů** (dle jejich aktuálních podmínek API).
- Na zpracování dat Anthropic se vztahuje **Anthropic Privacy Policy** (dostupná na anthropic.com).
- Servery Anthropic jsou primárně umístěny v USA; zpracování probíhá na základě standardních smluvních doložek (SCC) dle čl. 46 GDPR.

6. Subprocesory a třetí strany

LexAI využívá ke zpracování dat následující subprocesory. Tím, že souhlasíte s těmito Zásadami, souhlasíte s předáváním dat těmto subprocesorům v rozsahu popsaném níže.

Subprocesor	Sídlo	Účel	Zpracovávaná data
Anthropic	USA	Zpracování AI dotazů	Obsah chat zpráv, dokumenty k analýze
Supabase	EU (Frankfurt)	Databáze a autentizace	Veškerá uživatelská data (v zašifrované podobě)
Vercel	USA / EU	Serverless hosting	Request logy, API volání
Hetzner	EU (Frankfurt)	Vlastní servery (vektorová DB pro legislativu, bezpečnostní logy, zpracování dokumentů)	Security logy, zpracování dokumentů pro export/import
Qdrant	EU (Frankfurt, self-hosted na Hetzner)	Vektorová databáze pro veřejnou legislativu	Embeddings veřejných právních zdrojů (zákonů, judikatury, legislativy EU) — žádná uživatelská data
Stripe	USA (EU compliance)	Platební brána	Platební údaje, faktury, subscription ID
SendGrid (Twilio)	USA	Emailová komunikace	Emailové adresy, obsah notifikačních emailů
SerpAPI	USA	Webové vyhledávání	Vyhledávací dotazy (bez identifikátorů uživatele)
Brave Search	USA	Alternativní	Vyhledávací dotazy

		webové vyhledávání	(bez identifikátorů uživatele)
IPInfo	USA	Geolokace IP adres	IP adresy uživatelů

Předávání dat do třetích zemí

Někteří subprocesori (Anthropic, Vercel, Stripe, SendGrid, SerpAPI, Brave Search, IPInfo) sídlí v USA. Předávání dat do USA probíhá na základě standardních smluvních doložek (Standard Contractual Clauses, SCC) dle čl. 46 odst. 2 písm. c) GDPR nebo v souladu s rozhodnutím o přiměřenosti EU-U.S. Data Privacy Framework, pokud je to relevantní.

7. Cookies a sledování

LexAI **nepoužívá cookies ani obdobné sledovací technologie** pro marketingové nebo analytické účely. Z tohoto důvodu **nevyžadujeme souhlas s cookies** a neimplementujeme cookie banner.

Platforma může technicky využívat session storage a IndexedDB výhradně pro bezpečné ukládání šifrovacích klíčů na zařízení Uživatele (viz sekce 4). Toto ukládání je nezbytné pro fungování zero-knowledge architektury a není využíváno ke sledování Uživatele.

8. Uchovávání dat (Data Retention)

Kategorie dat	Doba uchovávání
Konverzace — placené tiery (Plus, Premium, Business, Enterprise)	Dle preference uživatele v nastavení (platí pro nearchivované chaty); archivované konverzace uchovávány bez časového omezení
Konverzace — Free tier	Hard limit 60 dní; uživatelská preference omezena na max. 14 dní; archivované konverzace nejsou z limitu vyjmuty
Top-up tokeny (záznamy)	3 měsíce od nákupu
Faktury a platební záznamy	Neomezeně (povinnost dle zákona o účetnictví a daňových předpisů)
Bezpečnostní logy	90 dní
Emaily a email logy	180 dní
Data Účtu — placené tiery	Do smazání Účtu Uživatelem; nebo hard limit 2 roky od posledního přihlášení (po uplynutí bez aktivity zašleme upozornění a Účet smažeme)
Data Účtu — Free tier	Do smazání Účtu Uživatelem; nebo hard limit 6 měsíců od posledního přihlášení
Nahrané dokumenty	Dle nastavení Uživatele; automaticky mazány při smazání konverzace nebo Účtu

Po uplynutí doby uchovávání jsou data bezpečně vymazána nebo anonymizována.

9. Vaše práva (práva subjektů údajů)

Jako subjekt údajů máte dle GDPR následující práva:

9.1 Právo na přístup (čl. 15 GDPR)

Máte právo získat potvrzení o tom, zda zpracováváme vaše osobní údaje, a pokud ano, získat jejich kopii a informace o zpracování.

9.2 Právo na opravu (čl. 16 GDPR)

Máte právo požadovat opravu nepřesných nebo doplnění neúplných osobních údajů.

9.3 Právo na výmaz — „právo být zapomenut" (čl. 17 GDPR)

Máte právo požadovat výmaz svých osobních údajů, pokud:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny;
- odvoláte souhlas, na němž bylo zpracování založeno;
- vznesete námitku proti zpracování a neexistují žádné převažující oprávněné důvody.

Výmaz lze provést přímo v nastavení Platformy (smazání Účtu) nebo kontaktováním support@lexaitechnologies.com. Výmaz se nevztahuje na data, která jsme povinni uchovávat ze zákona (zejm. faktury a účetní záznamy).

9.4 Právo na omezení zpracování (čl. 18 GDPR)

Máte právo požadovat omezení zpracování vašich osobních údajů v případech stanovených GDPR (např. při zpochybnění přesnosti údajů nebo vznesení námitky).

9.5 Právo na přenositelnost údajů (čl. 20 GDPR)

Máte právo obdržet své osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu a právo předat je jinému správci. Platforma poskytuje funkci exportu dat (data export endpoint).

9.6 Právo vznést námitku (čl. 21 GDPR)

Máte právo vznést námitku proti zpracování osobních údajů prováděnému na základě oprávněného zájmu (čl. 6 odst. 1 písm. f) GDPR). V takovém případě osobní údaje dále nezpracováváme, pokud neprokážeme závažné oprávněné důvody.

9.7 Právo odvolat souhlas

Zpracování na základě souhlasu (je-li relevantní) lze kdykoli odvolat bez negativních důsledků pro dosavadní zpracování.

9.8 Jak uplatnit svá práva

Žádosti o uplatnění práv zasílejte na: **support@lexaitechnologies.com**

Na vaši žádost odpovíme bez zbytečného odkladu, nejpozději do **30 dnů** od jejího přijetí. V případě složitých nebo rozsáhlých žádostí lze tuto lhůtu prodloužit o dalších 60 dnů, o čemž vás budeme informovat.

9.9 Právo podat stížnost dozorovému úřadu

Máte právo podat stížnost u dozorového úřadu pro ochranu osobních údajů:

Úřad pro ochranu osobních údajů (ÚOOÚ)
Pplk. Sochora 27, 170 00 Praha 7
Web: www.uoou.cz
Email: posta@uoou.gov.cz

10. Bezpečnostní opatření

LexAI implementuje rozsáhlá technická a organizační bezpečnostní opatření:

Technická opatření

- **HTTPS:** Veškerá komunikace je šifrována protokolem TLS.
- **Zero-knowledge šifrování:** AES-256-GCM s trojvrstvým šifrováním konverzací (viz sekce 4).
- **Rate limiting:** Omezení počtu požadavků na úrovni IP adresy i Uživatele; speciální limity pro kryptografické operace (decrypt: 15/s, encrypt: 20/s, key derivace: 2/s).
- **WebAuthn / TOTP 2FA:** Podpora přihlášení bez hesla a dvoufaktorového ověření.
- **Row Level Security (RLS):** Databázová izolace dat jednotlivých uživatelů na úrovni Supabase.
- **Input sanitization:** Ochrana proti XSS útokům (DOMPurify).
- **CORS restriction:** Omezení přístupu k API.
- **Session binding:** Záložkový XOR token zabraňující zneužití ukradených session dat.
- **Non-extractable keys:** Šifrovací klíče vytvořeny s příznakem extractable: false; prohlížeč zabraňuje jejich exportu.
- **Device binding a password re-verification:** Ověření každých 14 dní.
- **Anonymaly detection:** 5 bezpečnostních incidentů → 5minutový lockout.

Organizační opatření

- Přístup k systémům LexAI je omezen na oprávněné zaměstnance na principu nejnižších privilegií.
- Bezpečnostní logy jsou uchovávány 90 dní.
- Pravidelné interní bezpečnostní přezkoumání (code review, kontrola konfigurace, testování zabezpečení).

Hlášení bezpečnostních incidentů

V případě porušení zabezpečení osobních údajů, které může mít za následek riziko pro práva a svobody fyzických osob, budeme dozorovému úřadu (ÚOOÚ) incident hlásit do 72 hodin od jeho zjištění. Pokud incident představuje vysoké riziko pro vaše práva a svobody, budeme vás informovat bez zbytečného odkladu.

11. Zpracování dat dětí

Platforma není určena osobám mladším 18 let. LexAI vědomě neshromažďuje osobní údaje dětí. Pokud zjistíme, že jsme od dítěte mladšího 18 let získali osobní údaje bez ověřeného souhlasu zákonného zástupce, tyto údaje bezodkladně vymažeme.

Pokud máte důvod se domnívat, že osoba mladší 18 let nám poskytla osobní údaje, kontaktujte nás na support@lexaitechnologies.com.

12. Právní základ zpracování — shrnutí

Právní základ (čl. 6 GDPR)	Příklady zpracování
Plnění smlouvy (písm. b)	Registrace, autentizace, AI asistence, ukládání konverzací, fakturace
Plnění právní povinnosti (písm. c)	Uchovávání faktur a účetních dokladů
Oprávněný zájem (písm. f)	Bezpečnostní monitoring, prevence podvodů, rate limiting, optimalizace Služby
Souhlas (písm. a)	V případě zpracování, které není pokryto výše uvedenými základy (bude-li relevantní)

Zpracování na základě **oprávněného zájmu:** Provádíme tzv. balancing test, kde zvažujeme oprávněné zájmy LexAI (bezpečnost Platformy, prevence podvodů, zlepšování Služby) vůči právům a svobodám Uživatelů. Jste oprávněni kdykoliv vznést námitku (viz sekce 9.6).

13. Změny těchto Zásad

LexAI si vyhrazuje právo tyto Zásady ochrany osobních údajů kdykoli změnit. O podstatných změnách budeme Uživatele informovat emailem nebo oznámením v rámci Platformy nejméně **14 dní** před nabytím jejich účinnosti. Datum poslední aktualizace je vždy uvedeno v záhlaví tohoto dokumentu.

Pokračování v užívání Platformy po nabytí účinnosti změn se považuje za souhlas s aktualizovanými Zásadami.

14. Kontakt a dotazy

Máte-li jakékoli dotazy týkající se zpracování vašich osobních údajů, uplatnění práv nebo těchto Zásad, kontaktujte nás:

LexAI Technologies, s.r.o.
Školská 660/3, Praha 1 - Nové Město 110 00 Praha 1
Email: support@lexaitechnologies.com
Web: www.lexaitechnologies.com

Odpovíme nejpozději do 30 dní od přijetí vaší žádosti.

Verze 1.0 — účinná od 1. května 2025