Privacy Policy

Controller / Operator: LexAI Technologies, s.r.o., Company ID (IČO): 23589825, registered office: Školská 660/3, Praha 1 - Nové Město 110 00 Praha 1, entered in the Commercial Register maintained by the Municipal Court in Prague
Effective date: 1 May 2025
Contact: support@lexaitechnologies.com

1. Introduction and Core Principles

LexAI Technologies, s.r.o. (hereinafter "LexAI" or "we") operates the LexAI platform — an AI-assisted legal tool (hereinafter "Platform"). When processing personal data, we are committed to protecting the privacy of our users and comply with all applicable legislation, in particular:

- **Regulation (EU) 2016/679 (GDPR)** — the General Data Protection Regulation;
- **Act No. 110/2019 Coll.** — on personal data processing (Czech implementing legislation);
- applicable sector-specific legal requirements.

Our Core Principles

- **Privacy-first architecture:** The Platform is built on a zero-knowledge principle — the content of your conversations is encrypted directly on your device; we, as Operator, have no technical access to it.
- **No AI training:** We never use your data to train AI models. We use exclusively the commercial Anthropic Claude API.
- **Data minimisation:** We collect only the data necessary to provide the Service.
- **Transparency:** We tell you precisely what we collect, why, and for how long.

2. Who We Are (Data Controller)

The data controller within the meaning of Article 4(7) GDPR is:

LexAI Technologies, s.r.o.
Company ID (IČO): 23589825
Registered office: Školská 660/3, Praha 1 - Nové Město 110 00 Praha 1
Email: support@lexaitechnologies.com
Website: www.lexaitechnologies.com

LexAI has not designated a Data Protection Officer (DPO), as this is not obligatory given the nature and scope of the processing carried out. For any data protection queries, please contact: support@lexaitechnologies.com.

3. What Personal Data We Process and Why

3.1 Categories of Data Processed

Category	Specific Data	Purpose	Legal Basis
Account	Email (verified), name, hashed password	Registration, authentication, account management	Performance of contract (Art. 6(1)(b) GDPR)
Conversations	Chat history, AI queries and responses	Providing AI assistance, project management	Performance of contract
Documents	Uploaded files (PDF, DOCX), extracted text	Document analysis and processing	Performance of contract
Payments	Stripe customer ID, subscription ID, invoices	Billing, subscription management	Performance of contract; Legal obligation (tax purposes)
Security	IP addresses, device information, 2FA tokens, WebAuthn credentials	Security monitoring, fraud prevention	Legitimate interest (Art. 6(1)(f) GDPR)
Usage	Token count, web searches, and query count per month	Limit management, billing, service optimisation	Performance of contract; Legitimate interest
Gamification	XP points, achievements	Platform features	Performance of contract
Communications	Content of emails sent to the User (SendGrid logs)	Support, notifications, email verification	Performance of contract; Legitimate interest

3.2 Special Categories of Personal Data

LexAI intentionally **does not process** special categories of personal data within the meaning of Article 9 GDPR (health data, biometric data, racial or ethnic origin, etc.) as part of registration or profile settings.

We note, however, that Users may upload legal documents that contain special categories of personal data (e.g. contracts, court submissions, medical reports in the context of litigation). In such cases:

- LexAI processes those documents solely as a technical intermediary acting on the User's instructions;
- responsibility for the lawfulness of processing such data in uploaded documents lies with the User;
- such documents are encrypted on the User's device (zero-knowledge architecture) and LexAI has no access to them in unencrypted form.

4. Zero-Knowledge Architecture and Encryption

This section is key to understanding how LexAI handles your conversations and documents.

4.1 What This Means in Practice

LexAI operates a **zero-knowledge architecture** inspired by ProtonMail. This specifically means:

- **Your password never leaves your browser.** All cryptographic key derivation takes place exclusively on your device (client-side). Your password is never transmitted to our servers in any form.
- **The content of your conversations is encrypted with three independent layers** (AES-256-GCM) directly in your browser before being sent to our servers.
- **We store only encrypted data on our servers.** We have no technical ability to read the content of your conversations or to recover your password.

4.2 Technical Encryption Parameters

Component	Algorithm	Parameters
Data encryption	AES-256-GCM	12-byte IV, 128-bit auth tag
Key derivation	PBKDF2-SHA256	600,000 iterations
Password hashing	PBKDF2	600,000 iterations, constant-time comparison
Device binding	PBKDF2	100,000 iterations

4.3 What the Server Stores and Never Sees

What the server **never sees** in unencrypted form:

- User Master Key
- Recovery Phrase (we store only its PBKDF2 hash)
- Conversation content
- Conversation encryption keys
- User password

What the server stores (all encrypted):

- Encrypted Master Key (encrypted by device or recovery key)
- PBKDF2 hash of the Recovery Phrase + salt
- Encrypted conversation keys (content key, transport key, storage key — all encrypted by the Master Key)

4.4 Recovery Phrase

The 12-word Recovery Phrase is the **only means of recovering access** to data if the password is lost. The server stores only its hash (PBKDF2). LexAI cannot restore access to data by any other method. The User is solely responsible for keeping their Recovery Phrase safe.

4.5 Automatic Key Clearing

Trigger	Action
Tab close	Keys cleared from memory
2 hours of inactivity	Session keys cleared
Logout	All keys cleared
Session expiry	24-hour maximum lifetime

5. Data Processing for AI Assistance (Anthropic)

5.1 How AI Query Processing Works

When you submit a query to the AI chat or upload a document for analysis:

1. Data is **decrypted exclusively on your device** (in browser memory).
2. The decrypted content is sent over a secure HTTPS connection to LexAI's servers (serverless Vercel edge functions).
3. The serverless function passes the content to the **Anthropic API** for processing by the AI model.
4. The AI response is returned, **encrypted on your device**, and stored on LexAI's servers in encrypted form.

5.2 Anthropic as Data Processor

Anthropic (Anthropic, PBC, USA) processes the content of your queries and documents as our **data processor** in accordance with their API terms and Data Processing Agreement. Key points:

- Anthropic **does not use data submitted via API to train its models** (pursuant to their current API terms).
- Data processed by Anthropic is subject to the **Anthropic Privacy Policy** (available at anthropic.com).
- Anthropic's servers are primarily located in the USA; data transfers take place on the basis of Standard Contractual Clauses (SCC) pursuant to Article 46 GDPR.

6. Sub-processors and Third Parties

LexAI uses the following sub-processors for data processing. By accepting this Privacy Policy, you consent to the transfer of data to these sub-processors to the extent described below.

Sub-processor	Location	Purpose	Data Processed
Anthropic	USA	AI query processing	Chat message content, documents for analysis
Supabase	EU (Frankfurt)	Database and authentication	All user data (in encrypted form)
Vercel	USA / EU	Serverless hosting	Request logs, API calls
Hetzner	EU (Frankfurt)	Proprietary servers (legislation vector DB, security logs, document processing)	Security logs, document processing for export/import
Qdrant	EU (Frankfurt, self-hosted on Hetzner)	Vector database for public legislation	Embeddings of public legal sources (statutes, case law, EU legislation) — no user data
Stripe	USA (EU compliance)	Payment gateway	Payment data, invoices, subscription IDs
SendGrid (Twilio)	USA	Email communications	Email addresses, content of notification emails
SerpAPI	USA	Web search	Search queries (without user identifiers)
Brave Search	USA	Alternative web search	Search queries (without user identifiers)

IPInfo	USA	IP address geolocation	User IP addresses

Transfers to Third Countries

Several sub-processors (Anthropic, Vercel, Stripe, SendGrid, SerpAPI, Brave Search, IPInfo) are based in the USA. Transfers of data to the USA are carried out on the basis of Standard Contractual Clauses (SCC) pursuant to Article 46(2)(c) GDPR, or in accordance with the EU–U.S. Data Privacy Framework adequacy decision where applicable.

7. Cookies and Tracking

LexAI **does not use cookies or similar tracking technologies** for marketing or analytical purposes. For this reason, **we do not require cookie consent** and we do not implement a cookie banner.

The Platform may technically use session storage and IndexedDB exclusively for the secure storage of encryption keys on the User's device (see Section 4). This storage is necessary for the functioning of the zero-knowledge architecture and is not used to track the User.

8. Data Retention

Data Category	Retention Period
Conversations — paid tiers (Plus, Premium, Business, Enterprise)	As per the user's preference in settings (applies to non-archived chats); archived conversations retained indefinitely
Conversations — Free tier	Hard limit of 60 days; user preference capped at 14 days; archived conversations are not exempt from the hard limit
Top-up token records	3 months from purchase
Invoices and payment records	Indefinitely (statutory obligation under accounting and tax law)
Security logs	90 days
Emails and email logs	180 days
Account data - paid tier	Until Account deletion by the User; or a hard limit of 2 years from last login (after this period of inactivity, we will send a notification and delete the Account)
Account data — Free tier	Until Account deletion by the User; or a hard limit of 6 months from last login
Uploaded documents	As per the User's settings; automatically deleted upon deletion of the conversation or Account

After the applicable retention period, data is securely deleted or anonymised.

9. Your Rights (Data Subject Rights)

As a data subject under the GDPR, you have the following rights:

9.1 Right of Access (Article 15 GDPR)

You have the right to obtain confirmation as to whether we process your personal data and, if so, to receive a copy of it along with information about the processing.

9.2 Right to Rectification (Article 16 GDPR)

You have the right to request correction of inaccurate or completion of incomplete personal data.

9.3 Right to Erasure — "Right to be Forgotten" (Article 17 GDPR)

You have the right to request erasure of your personal data where:

- the personal data is no longer necessary for the purposes for which it was collected;
- you withdraw the consent on which the processing was based;
- you object to the processing and there are no overriding legitimate grounds.

Erasure can be carried out directly in the Platform settings (Account deletion) or by contacting support@lexaitechnologies.com. Erasure does not apply to data we are legally obliged to retain (in particular invoices and accounting records).

9.4 Right to Restriction of Processing (Article 18 GDPR)

You have the right to request restriction of the processing of your personal data in the cases provided for by the GDPR (e.g. where the accuracy of data is contested or an objection has been lodged).

9.5 Right to Data Portability (Article 20 GDPR)

You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller. The Platform provides a data export function (data export endpoint).

9.6 Right to Object (Article 21 GDPR)

You have the right to object to the processing of personal data carried out on the basis of legitimate interest (Article 6(1)(f) GDPR). In that case, we will cease processing unless we demonstrate compelling legitimate grounds that override your rights and interests.

9.7 Right to Withdraw Consent

Where processing is based on consent (where applicable), consent may be withdrawn at any time without any negative consequence for processing already carried out.

9.8 How to Exercise Your Rights

Submit requests to exercise your rights to: **support@lexaitechnologies.com**

We will respond without undue delay and in any event within **30 days** of receiving your request. In the case of complex or extensive requests, this period may be extended by a further 60 days, of which we will inform you.

9.9 Right to Lodge a Complaint with a Supervisory Authority

You have the right to lodge a complaint with a data protection supervisory authority. The lead supervisory authority for LexAI is:

Office for Personal Data Protection (Úřad pro ochranu osobních údajů — ÚOOÚ)
Pplk. Sochora 27, 170 00 Prague 7, Czech Republic
Website: www.uoou.cz
Email: posta@uoou.gov.cz

You may also contact the supervisory authority in the EU member state of your habitual residence, place of work, or place of the alleged infringement.

10. Security Measures

LexAI implements comprehensive technical and organisational security measures:

Technical Measures

- **HTTPS:** All communications are encrypted using TLS.
- **Zero-knowledge encryption:** AES-256-GCM with three-layer conversation encryption (see Section 4).
- **Rate limiting:** Request throttling at IP address and User level; specific limits for cryptographic operations (decrypt: 15/s, encrypt: 20/s, key derivation: 2/s).
- **WebAuthn / TOTP 2FA:** Support for passwordless login and two-factor authentication.
- **Row Level Security (RLS):** Database-level isolation of individual users' data within Supabase.
- **Input sanitisation:** Protection against XSS attacks (DOMPurify).
- **CORS restrictions:** Restriction of API access.
- **Session binding:** Tab-specific XOR token preventing misuse of stolen session data.
- **Non-extractable keys:** Encryption keys created with the extractable: false flag; the browser prevents their export.
- **Device binding and password re-verification:** Re-verification required every 14 days.
- **Anomaly detection:** 5 security incidents → 5-minute lockout.

Organisational Measures

- Access to LexAI's systems is restricted to authorised personnel on a least-privilege basis.
- Security logs are retained for 90 days.
- Regular internal security reviews (code review, configuration checks, security testing).

Security Incident Notification

In the event of a personal data breach likely to result in a risk to the rights and freedoms of natural persons, we will notify the supervisory authority (ÚOOÚ) within 72 hours of becoming aware of the breach. Where the breach is likely to result in a high risk to your rights and freedoms, we will notify you without undue delay.

11. Processing of Children's Data

The Platform is not intended for persons under the age of 18. LexAI does not knowingly collect personal data from children. If we become aware that we have collected personal data from a person under 18 without verified parental or guardian consent, we will delete such data without delay.

If you have reason to believe that a person under 18 has provided us with personal data, please contact us at support@lexaitechnologies.com.

12. Legal Bases for Processing — Summary

Legal Basis (Article 6 GDPR)	Examples of Processing
Performance of contract (Art. 6(1)(b))	Registration, authentication, AI assistance, conversation storage, billing
Legal obligation (Art. 6(1)(c))	Retention of invoices and accounting records
Legitimate interest (Art. 6(1)(f))	Security monitoring, fraud prevention, rate limiting, service optimisation
Consent (Art. 6(1)(a))	Any processing not covered by the above bases (where applicable)

Where processing is based on **legitimate interest**, we carry out a balancing test weighing LexAI's legitimate interests (Platform security, fraud prevention, service improvement) against the rights and freedoms of Users. You are entitled to object at any time (see Section 9.6).

13. Changes to this Privacy Policy

LexAI reserves the right to amend this Privacy Policy at any time. Users will be notified of material changes by email or by notice within the Platform at least **14 days** before the

changes take effect. The date of the most recent update is always stated in the header of this document.

Continued use of the Platform after the effective date of any changes constitutes acceptance of the updated Privacy Policy.

14. Contact and Queries

For any questions regarding the processing of your personal data, the exercise of your rights, or this Privacy Policy, please contact us:

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

We will respond within 30 days of receiving your request.

Version 1.0 — effective from 1 May 2025