

Cookie and Tracking Technology Policy

Operator: LexAI Technologies, s.r.o., Company ID: 23589825, registered office at Školská 660/3, Praha 1 – Nové Město, 110 00 Praha 1, Czech Republic, registered in the Commercial Register maintained by the Municipal Court in Prague

Effective date: 1 June 2025

Contact: support@lexaitechnologies.com

1. Introduction

This Cookie and Tracking Technology Policy (the "Policy") explains how LexAI Technologies, s.r.o. (hereinafter "LexAI" or "we") approaches tracking technologies, cookies, and browser storage on the LexAI platform available at www.lexaitechnologies.app and on the website www.lexaitechnologies.com (collectively, the "Platform").

This Policy is issued in accordance with:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR);
- Directive 2002/58/EC of the European Parliament and of the Council (ePrivacy Directive) as amended by Directive 2009/136/EC;
- Czech Act No. 127/2005 Coll. on Electronic Communications.

2. Privacy-First Architecture — No Cookies

LexAI does not use cookies.

The LexAI Platform is built on a privacy-by-design principle. We have made a deliberate architectural decision not to implement cookies or any equivalent tracking technologies. In practice, this means:

- No analytics or marketing cookies. Google Analytics, Hotjar, Mixpanel, Facebook Pixel, and similar tracking tools are entirely absent from the Platform.
- No third-party cookies for behavioral tracking or user profiling.
- No cookie consent banner is displayed on the Platform, as there is no legal basis requiring one — cookie consent is only required where cookies are

actually used.

The Stripe payment integration is implemented server-side via an npm package and does not set any client-side cookies. Email communication via SendGrid is handled exclusively on the server side with no browser impact.

3. Browser Storage Technologies We Use

Although the Platform does not use cookies, it uses other standard browser technologies strictly necessary for functionality and security. These technologies **are not used to track users** and do not require consent under the ePrivacy Directive, as they constitute technically necessary operations.

3.1 sessionStorage (Temporary — Cleared on Tab Close)

sessionStorage holds data only for the duration of the browser session and is automatically cleared when the tab or browser is closed. We use it for:

Key	Purpose	Tracking?
lexai_session_token	JWT access token (Supabase authentication)	No
lexai_refresh_token	Session refresh credential	No
lexai_session_expires	Session expiry timestamp	No
lexai_authenticated	Authentication state flag	No
Session encryption keys	Temporary cryptographic keys for zero-knowledge operations	No
Temporary form data	Intermediate state of form fields	No

3.2 localStorage (Persistent — Until Cleared by the User)

localStorage stores user preferences and settings that persist across sessions. It allows the Platform to remember user configuration without transmitting it to the server. We use it for:

Key	Purpose	Tracking?
theme	Light/dark mode preference	No
fontSize, chatFontFamily	Font size and typeface settings	No
timezone, dateFormat, currency	Localization preferences	No
sidebarCollapsed, lexiChatWidth	UI layout state	No
DEVICE_ID_KEY	Device identifier for security purposes (see Section 3.4)	Security — not marketing

3.3 IndexedDB

IndexedDB is used exclusively for secure client-side storage of cryptographic keys as part of the zero-knowledge architecture. Keys are stored with the extractable: false flag, which instructs the browser to prevent their export — this is a technical measure preventing key theft. IndexedDB is not used for tracking or profiling.

3.4 Device Identifier (DEVICE_ID_KEY)

The Platform stores a device identifier (DEVICE_ID_KEY) in localStorage. This identifier serves as a security mechanism for binding encryption keys to a specific user device (device binding). This identifier:

- is not shared with any third party for tracking purposes;
- is used solely as a fallback element of the cryptographic protection of user data;
- does not create a marketing profile of the user.

4. Third Parties and Their Cookies

The LexAI Platform does not include any third-party scripts that could set cookies in your browser. For transparency, we list all integrated third parties and their relationship to tracking technologies:

Third Party	Integration	Cookies in User's Browser?
Stripe	Server-side npm package	No
SendGrid (Twilio)	Server-side email communication	No
Supabase	Server-side database, token-based authentication	No
Anthropic	Server-side API call	No
Vercel	Serverless hosting	No
Hetzner	Server infrastructure	No
SerpAPI / Brave Search	Server-side search API	No
IPInfo	Server-side geolocation	No

5. Legal Basis for Browser-Side Data Processing

All browser storage technologies described in Section 3 are technically necessary for providing the Service that the user has requested. The legal basis is:

- **Performance of a contract** under Art. 6(1)(b) GDPR — authentication tokens, encryption keys, and user preferences are necessary for the Platform to function.
- **Legitimate interest** under Art. 6(1)(f) GDPR — the device identifier (DEVICE_ID_KEY) is necessary for the security integrity of the zero-knowledge architecture.

None of the described technologies require consent under the ePrivacy Directive, as they are not cookies used for tracking, profiling, or marketing.

6. Managing Browser-Stored Data

Although the Platform does not use cookies, you retain full control over data stored in your browser:

Clearing browser data: All data stored in sessionStorage, localStorage, and IndexedDB can be cleared at any time through your browser settings (Developer Tools → Application/Storage → Clear site data). Please note that clearing this data will result in being logged out of the Service and may require you to reconfigure your preferences.

Account deletion: Deleting your account via the Platform settings or by submitting a request to support@lexaitechnologies.com will permanently erase your server-side data in accordance with the terms described in the Privacy Policy.

Data export: You can export your data at any time using the GDPR export function available in Platform settings.

7. Changes to This Policy

LexAI reserves the right to update this Policy at any time, in particular in the event of technical changes to the Platform or amendments to applicable legislation. We will notify users of material changes by email or in-Platform notification at least 14 days before they take effect. The current version is always available at www.lexaitechnologies.com/en/cookie-policy.

8. Contact

If you have any questions regarding this Policy or browser-side data processing, please contact us:

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

Version 1.0 — effective 1 June 2025