Data Processing Agreement (DPA)

pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR)

Processor: 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
Controller: [COMPANY NAME / INDIVIDUAL NAME], Company ID / Registration No.: [TO BE COMPLETED], registered office / address: [TO BE COMPLETED]
Date of execution: [TO BE COMPLETED]
Processor contact: support@lexaitechnologies.com

Preamble

This Data Processing Agreement (hereinafter "DPA" or "Agreement") is entered into between the Processor and the Controller identified above (together, the "Parties") in accordance with Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter "GDPR").

The Controller uses the LexAI platform (hereinafter "Platform" or "Service") provided by the Processor under the Terms of Use available at www.lexaitechnologies.app (hereinafter "Main Agreement"). In the course of providing the Service, the Processor may process personal data of natural persons in respect of whom the Controller acts as controller within the meaning of Article 4(7) GDPR. This DPA governs the terms on which the Processor processes such data on behalf of the Controller.

In the event of any conflict between this DPA and the Main Agreement, this DPA shall prevail with respect to matters of personal data protection.

Article 1 — Definitions

For the purposes of this Agreement, the following definitions apply:

- **"GDPR"** — Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.
- **"Controller Personal Data"** — personal data that the Controller transfers to the Processor for processing in the course of using the Service, or that the Processor processes on behalf of the Controller as a result of providing the Service.
- **"Data Subject"** — a natural person whose personal data is being processed; in particular clients, employees, or other natural persons whose data the Controller processes through the Platform.
- **"Processing"** — any operation or set of operations performed on personal data within the meaning of Article 4(2) GDPR.
- **"Security Breach"** — a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal data.
- **"Sub-processor"** — a third party engaged by the Processor to process personal data on behalf of the Controller.

- **"Standard Contractual Clauses" / "SCC"** — standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission.
- **"EEA"** — the European Economic Area.

All other terms shall have the same meaning as in the GDPR or the Main Agreement.

Article 2 — Subject Matter and Nature of Processing

2.1 Subject Matter

The Processor processes Controller Personal Data solely for the purpose of providing the Service under the Main Agreement, including:

- processing legal documents, contracts, and other texts through AI models;
- conducting legal research based on queries containing personal data;
- storing and managing conversations and projects within the Platform;
- technical support and operation of the Platform.

2.2 Nature of Processing

Processing is carried out in an automated manner through AI models (Claude, Anthropic) and includes in particular: reading, analysing, summarising, classifying, and storing personal data contained in documents and queries submitted by the Controller.

2.3 Categories of Data Subjects

Processing may concern the following categories of data subjects:

- the Controller's clients (natural persons);
- the Controller's employees or associates;
- counterparties in legal matters;
- other natural persons identified in documents submitted by the Controller for processing.

2.4 Categories of Personal Data

Personal data processed may include in particular:

- identification data (name, surname, date of birth, national identification number);
- contact data (address, email, telephone);
- data relating to legal matters and disputes;
- financial and asset data;
- special categories of personal data under Article 9 GDPR (health data, data relating to criminal proceedings, etc.), where contained in submitted documents.

2.5 Duration of Processing

Processing shall continue for the duration of the Main Agreement, unless otherwise specified in this DPA.

Article 3 — Obligations of the Processor

3.1 Processing Only on Controller's Instructions

The Processor shall process Controller Personal Data solely on the basis of documented instructions from the Controller, which shall consist of: the Main Agreement, this DPA, and instructions given by the Controller through the Platform. The Processor shall not process Controller Personal Data for its own purposes or transfer it to third parties, except as provided in this DPA.

If the Processor is required to process personal data pursuant to EU or member state law applicable to it, it shall inform the Controller of that legal requirement before processing, unless such law prohibits notification on grounds of public interest.

3.2 Confidentiality

The Processor shall ensure that persons authorised to process Controller Personal Data are subject to a duty of confidentiality, whether contractual or statutory.

3.3 Technical and Organisational Security Measures

The Processor shall implement and maintain technical and organisational measures appropriate to the risk of processing, in accordance with Article 32 GDPR. These measures include in particular:

Technical measures:

- Zero-knowledge architecture: conversation content is encrypted with three independent layers of AES-256-GCM encryption directly on the Controller's device; the Processor has no technical access to unencrypted content.
- Encryption of data at rest and in transit (AES-256-GCM, TLS).
- Cryptographic key derivation using PBKDF2-SHA256 (600,000 iterations).
- Multi-factor authentication (WebAuthn, TOTP 2FA).
- Database-level isolation of individual customers' data (Row Level Security).
- Rate limiting and anomaly detection.
- Automatic deletion of session keys after 2 hours of inactivity.

Organisational measures:

- Access to systems on a least-privilege basis.
- Regular internal security reviews.
- Security logs retained for 90 days.

The Processor may update these measures on an ongoing basis, provided that the level of protection does not fall below the standard set out in this DPA.

3.4 Engagement of Sub-processors

The Controller grants the Processor general prior authorisation to engage Sub-processors. The current list of Sub-processors is set out in **Schedule 1** to this DPA.

The Processor shall:

- notify the Controller at least **30 days** in advance of engaging any new Sub-processor or making material changes to an existing Sub-processor, by email or by updating the Privacy Policy available on the Platform;
- give the Controller the right to raise reasonable objections to a new Sub-processor within 14 days of notification; if the objection cannot be resolved, the Controller may terminate the Main Agreement;
- ensure that Sub-processors are bound by data protection obligations at least equivalent to those set out in this DPA;
- remain liable to the Controller for the performance of Sub-processors' obligations.

3.5 Assistance to the Controller

The Processor shall assist the Controller — taking into account the nature of processing and the information available — in fulfilling its obligations under the GDPR, including in particular:

- responding to requests from data subjects exercising their rights (access, rectification, erasure, portability, restriction, objection);
- compliance with obligations under Articles 32–36 GDPR (security, breach notification, data protection impact assessments);
- providing information necessary to demonstrate compliance with this DPA.

Assistance provided by the Processor beyond its standard obligations may be charged at applicable rates or as otherwise agreed.

3.6 Security Breach Notification

The Processor shall notify the Controller without undue delay, and in any event within **48 hours** of becoming aware, of any Security Breach affecting Controller Personal Data. The notification shall include at minimum:

- a description of the nature of the Security Breach, including the categories and approximate number of data subjects and records affected;
- contact details for obtaining further information;
- a description of the likely consequences of the Security Breach;
- a description of the measures taken or proposed to address the Security Breach.

The Processor is not required to notify Security Breaches that are unlikely to result in a risk to the rights and freedoms of natural persons.

3.7 Data Protection Impact Assessments (DPIA)

Where the Controller intends to carry out processing that requires a Data Protection Impact Assessment (DPIA) under Article 35 GDPR, the Processor shall, upon request, provide the Controller with available information necessary for the performance of such assessment.

3.8 Deletion or Return of Data Upon Termination

Upon termination of the Main Agreement, the Processor shall, at the Controller's choice:

- delete all Controller Personal Data and any existing copies thereof; or
- return all Controller Personal Data to the Controller in a machine-readable format.

Deletion or return shall be completed within **30 days** of termination of the Main Agreement, unless retention is required by EU or member state law. The Processor shall, upon request, provide the Controller with written confirmation of deletion.

Article 4 — Obligations of the Controller

The Controller represents and warrants that:

- it has a lawful legal basis for the processing of Personal Data it transfers to the Processor;
- it has provided data subjects with all information required by the GDPR, including information about processing through the LexAI Platform;
- the instructions given to the Processor are compliant with the GDPR and other applicable legislation;
- before transferring special categories of personal data under Article 9 GDPR for processing through the Platform, it has assessed the lawfulness of such processing and is satisfied it is compliant with the GDPR;
- it will promptly notify the Processor of any change that may affect the Processor's obligations under this DPA.

Article 5 — International Transfers of Personal Data

5.1 Processing Within the EEA

The Processor primarily processes Controller Personal Data within the EEA (Supabase EU Frankfurt, Hetzner EU Frankfurt, Qdrant EU Frankfurt).

5.2 Transfers Outside the EEA

Certain Sub-processors of the Processor are located outside the EEA, in particular in the USA (Anthropic, Vercel, Stripe, SendGrid, SerpAPI, Brave Search, IPInfo). Transfers to these countries are carried out on the basis of:

- **Standard Contractual Clauses (SCC)** adopted by the European Commission pursuant to Article 46(2)(c) GDPR; and/or
- **adequacy decisions** (EU–U.S. Data Privacy Framework), where applicable.

Copies of the relevant SCCs are available to the Controller upon request.

5.3 Special Conditions for Transfers to Anthropic

The Controller acknowledges that the content of conversations and documents is transferred to Anthropic (USA) for processing by AI models. Anthropic does not use data submitted via API to train its models. This transfer is safeguarded by SCCs concluded between the Processor and Anthropic.

Article 6 — Audit Rights

6.1 Right to Information and Audit

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 GDPR and shall allow audits or inspections conducted by the Controller or

an auditor mandated by the Controller.

6.2 Conditions for Audit

Any audit must be:

- notified to the Processor in writing at least **30 days** in advance;
- conducted during the Processor's normal business hours;
- conducted so as to minimise disruption to the Processor's operations;
- limited to information necessary to verify compliance with this DPA.

The Processor may deny access to information concerning other customers or information protected by trade secret, provided that it offers sufficient alternative assurances.

6.3 Costs of Audit

The costs of any audit shall be borne by the Controller, unless the audit reveals a material breach of the Processor's obligations under this DPA.

Article 7 — Liability

7.1 Liability for Damages

Each Party shall be liable to the other for damages caused by a breach of its obligations under this DPA or the GDPR, to the extent provided by applicable law.

7.2 Limitation of Processor's Liability

The Processor's total liability to the Controller arising out of or in connection with this DPA shall not exceed the total amount of payments actually made by the Controller to the Processor for the Service in the **12 months** immediately preceding the event giving rise to the claim, except for damages caused by the Processor's gross negligence or wilful misconduct.

7.3 Regulatory Fines

If a supervisory authority imposes a fine on the Controller as a result of a GDPR infringement caused solely by a demonstrable breach of the Processor's obligations under this DPA, the Processor shall reimburse the Controller for a proportionate share of such fine corresponding to the degree of the Processor's fault.

Article 8 — Term and Termination

8.1 Term

This DPA is effective for the entire duration of the Main Agreement between the Parties.

8.2 Termination

This DPA terminates automatically upon termination of the Main Agreement. Provisions that by their nature survive termination (in particular Articles 3.8 and 7) shall remain in force.

Article 9 — General Provisions

9.1 Governing Law

This DPA is governed by the laws of the Czech Republic, in particular Act No. 89/2012 Coll. (the Civil Code) and the GDPR.

9.2 Dispute Resolution

All disputes arising out of or in connection with this DPA shall be resolved by the courts of the Czech Republic with subject-matter jurisdiction.

9.3 Amendments

The Processor may unilaterally amend this DPA to the extent necessary to ensure compliance with the GDPR or as a result of changes to the Service. The Controller will be notified of material changes by email at least 30 days in advance.

9.4 Severability

If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

9.5 Entire Agreement

This DPA, together with the Main Agreement and the Privacy Policy, constitutes the entire agreement of the Parties with respect to the processing of personal data and supersedes all prior arrangements or understandings in this regard.

Schedule 1 — List of Sub-processors

Sub-processor	Location	Purpose	Data Transferred
Anthropic, PBC	USA	AI query processing (Claude API)	Conversation content, documents for analysis
Supabase, Inc.	EU (Frankfurt)	Database and authentication	All user data (in encrypted form)
Vercel, Inc.	USA / EU	Serverless hosting	Request logs, API calls
Hetzner Online GmbH	EU (Frankfurt)	Proprietary servers (vector DB, security logs, document processing)	Security logs, document processing
Qdrant	EU (Frankfurt, self-hosted on Hetzner)	Vector database for public legislation	Embeddings of public legal sources — no user data
Stripe, Inc.	USA (EU compliance)	Payment gateway	Payment data, billing records
Twilio SendGrid	USA	Email communications	Email addresses, notification emails
SerpAPI	USA	Web search	Search queries
Brave Search	USA	Alternative web search	Search queries
IPInfo	USA	IP address geolocation	User IP addresses

The Processor reserves the right to update this list in accordance with Article 3.4 of this DPA.

Schedule 2 — Technical and Organisational Security Measures

This Schedule describes the security measures implemented by the Processor pursuant to Article 32 GDPR and Article 3.3 of this DPA.

Encryption and Cryptography

Component	Standard	Parameters
Conversation encryption	AES-256-GCM (3 layers)	12-byte IV, 128-bit auth tag, unique keys per conversation
Key derivation	PBKDF2-SHA256	600,000 iterations
Password hashing	PBKDF2	600,000 iterations, constant-time comparison
Device binding	PBKDF2	100,000 iterations
Data in transit	TLS 1.2+	HTTPS enforced

Access Control

- Multi-factor authentication: WebAuthn (FIDO2) and TOTP
- Row Level Security (RLS) at Supabase database level
- Employee access on a least-privilege basis
- Password re-verification every 14 days
- Session timeout: 2 hours of inactivity, 24-hour maximum lifetime

Resilience and Availability

- Serverless architecture (Vercel edge functions) for horizontal scaling
- Primary data stored in the EU (Frankfurt)
- Rate limiting at IP address and user level

Monitoring and Auditing

- Security logs retained for 90 days
- Anomaly detection: 5 incidents → 5-minute lockout
- Cryptographic operations logged (success/failure)

Zero-Knowledge Architecture

- User password never leaves the user's device
- Key derivation performed exclusively client-side
- Processor has no technical access to conversation content

Signatures

This DPA is entered into on the date stated in the header of this document.

On behalf of the Processor — LexAI Technologies, s.r.o.:

Name: _____
Title: _____
Date: _____
Signature: _____

On behalf of the Controller — [COMPANY NAME]:

Name: _____
Title: _____
Date: _____
Signature: _____

Version 1.0 — template, to be reviewed and customised before execution