Data Processing Addendum (DPA)

Version	1.0
Effective Date	8 May 2026
Last Updated	8 May 2026
Maintained by	LegalInk AI · support@legalink.ai

Preamble

This Data Processing Addendum ("**DPA**") forms part of the agreement between LegalInk AI (**"LegalInk"**, **"we"**, **"us"**) and the customer entity that has accepted LegalInk's Terms of Service or executed a separate Master Services Agreement (the **"Customer"**, **"you"**) (together, the **"Agreement"**).

This DPA applies to all processing of Personal Data carried out by LegalInk on the Customer's behalf in the course of providing the LegalInk AI platform (the **"Service"**). It is referenced by, and incorporates, the LegalInk AI Subprocessor List (Exhibit A) and the LegalInk AI Document Retention Policy (Exhibit B). The Technical and Organisational Measures applicable to the Service are set out in Exhibit C.

This DPA is governed by the **Digital Personal Data Protection Act, 2023** ("**DPDP Act**") and other applicable Indian privacy law.

1. Definitions

The following terms, when capitalised, have the meanings set out below. Terms used but not defined here have the meanings given in the DPDP Act.

1.1 **"Customer Personal Data"** means Personal Data processed by LegalInk on behalf of the Customer in the course of providing the Service, including drafts, chat content, uploaded documents, account metadata, and voice recordings.

1.2 **"Data Fiduciary"** has the meaning given in §2(i) of the DPDP Act and corresponds to the role of "Data Controller" under analogous regimes. The Customer is the Data Fiduciary in respect of Customer Personal Data.

1.3 **"Data Processor"** means a person who processes Personal Data on behalf of a Data Fiduciary. LegalInk is the Data Processor in respect of Customer Personal Data.

1.4 **"Data Principal"** has the meaning given in §2(j) of the DPDP Act and refers to the natural person to whom Personal Data relates.

1.5 **"Personal Data"** has the meaning given in §2(t) of the DPDP Act.

1.6 **"Processing"** has the meaning given in §2(x) of the DPDP Act.

1.7 **"Subprocessor"** means any third party engaged by LegalInk to process Customer Personal Data on LegalInk's behalf, as listed in Exhibit A.

1.8 **"Personal Data Breach"** means a breach of security leading to accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, Customer Personal Data.

1.9 **"Applicable Privacy Law"** means the DPDP Act and any other privacy or data-protection law of competent jurisdiction that applies to the Processing of Customer Personal Data under this DPA.

2. Roles and scope

2.1 **Roles.** The Customer is the Data Fiduciary and LegalInk is the Data Processor in respect of Customer Personal Data.

2.2 **Scope.** This DPA applies to all Processing of Customer Personal Data carried out by LegalInk in the course of providing the Service. It does not apply to Personal Data processed by LegalInk for its own purposes (e.g., billing-contact data) — that processing is governed by LegalInk's Privacy Notice.

2.3 **Customer instructions.** LegalInk processes Customer Personal Data only on documented instructions from the Customer. The Customer's use of the Service in accordance with the Agreement and this DPA constitutes the Customer's documented instructions.

2.4 **Customer's obligations.** The Customer warrants that:

(a) it has obtained all necessary consents and lawful bases to enable LegalInk to process Customer Personal Data as contemplated by the Agreement;

(b) the Customer's instructions to LegalInk comply with Applicable Privacy Law;

(c) the Customer will not submit special-category data, sensitive personal data, or data of children under 18 without verified parental consent through the Service except where LegalInk has expressly agreed in writing to support such processing.

3. Subject matter, nature, and duration of processing

3.1 **Subject matter.** Provision of the LegalInk AI platform — an AI-assisted legal drafting and reasoning Service for the Indian legal market.

3.2 **Nature and purpose.** Storage; retrieval; AI-assisted analysis and generation; transmission; deletion. Performed for the purpose of providing the Service.

3.3 **Categories of Personal Data:**

- Account and identity data (name, email, profession, organisation);
- Authentication and access metadata (login timestamps, IP addresses, device fingerprints);
- Customer-generated content (drafts, chat conversations, uploaded documents, voice recordings and transcripts);
- Billing data (payment-method tokens, GSTIN where provided, transaction history);
- Audit-log data (records of actions taken in the Service).

3.4 **Categories of Data Principals.** The Customer's authorised users; persons named in or referred to in Customer-generated content.

3.5 **Duration.** For the duration of the Agreement and thereafter for the periods set out in Exhibit B.

4. LegalInk's obligations as Data Processor

4.1 **Compliance with instructions.** LegalInk processes Customer Personal Data only as set out in this DPA, the Agreement, or as otherwise instructed in writing by the Customer, and in accordance with Applicable Privacy Law. LegalInk will inform the Customer if, in its opinion, an instruction violates Applicable Privacy Law.

4.2 **Confidentiality.** LegalInk ensures that personnel authorised to process Customer Personal Data are bound by confidentiality obligations that survive termination of their engagement.

4.3 **Security.** LegalInk implements and maintains the Technical and Organisational Measures set out in Exhibit C, designed to ensure a level of security appropriate to the risk of the Processing.

4.4 **Personnel limitation.** Production access to Customer Personal Data is limited to authorised personnel who require such access to perform their duties. All such access is logged.

4.5 **No training on Customer Personal Data.** LegalInk does not use Customer Personal Data to train, fine-tune, or otherwise improve any artificial-intelligence model. LegalInk uses enterprise API tiers from its AI Subprocessors that contractually exclude training on customer data.

4.6 **Assistance with Data Principal requests.** Where the Customer receives a Data Principal request (e.g., access, correction, erasure under §11 of the DPDP Act) requiring LegalInk's assistance, LegalInk will provide reasonable technical and organisational assistance to enable the Customer to respond within statutory timelines. If a Data Principal sends such a request directly to LegalInk, LegalInk will promptly forward it to the Customer.

4.7 **Assistance with Data Fiduciary obligations.** LegalInk will provide reasonable assistance to the Customer in meeting other obligations under Applicable Privacy Law, including data-protection impact assessments and prior consultations with the Data Protection Board of India where required.

5. Subprocessors

5.1 **General authorisation.** The Customer provides general authorisation for LegalInk to engage Subprocessors, subject to this Section 5.

5.2 **List of Subprocessors.** A current list is maintained at **legalink.co.in/trust/subprocessors** and at Exhibit A.

5.3 **Notice of changes.** Where LegalInk intends to add, replace, or materially change a Subprocessor, LegalInk will give at least **30 days' written notice** to the Customer's billing contact and update Exhibit A.

5.4 **Right to object.** The Customer may object in writing within the 30-day notice period. Where the objection is reasonable and based on data-protection grounds, the parties will work in good faith to identify a commercially reasonable alternative. If no alternative is feasible, the Customer may terminate the affected portion of the Service for that cause without penalty, with a pro-rata refund of pre-paid fees for the unused term.

5.5 **Subprocessor obligations.** LegalInk will impose on each Subprocessor data-protection obligations no less protective than those in this DPA. LegalInk remains liable to the Customer for the performance of Subprocessors as if it performed the Processing itself.

6. Cross-border transfer

6.1 **Hosting region.** As of the Effective Date, the primary infrastructure for storing Customer Personal Data is hosted on Supabase's enterprise infrastructure in the **Tokyo (ap-northeast-1) region**. Some Subprocessors process Customer Personal Data in the United States, the European Union, or globally distributed networks (see Exhibit A).

6.2 **DPDP §16 compliance.** Cross-border transfer is permitted under §16 of the DPDP Act, subject to such restrictions as the Central Government may notify. Where a country or class of transfers is restricted, LegalInk will not transfer Customer Personal Data to that destination without a lawful basis or alternative safeguard.

6.3 **Safeguards.** LegalInk implements:

(a) encryption in transit (TLS 1.2 or higher) and at rest (AES-256);

(b) contractual data-protection terms with each Subprocessor at least as protective as this DPA;

(c) hosting on infrastructure that is, at minimum, ISO 27001-certified.

6.4 **India (Mumbai) data residency.** Migration to the India (Mumbai, ap-south-1) region is on LegalInk's published roadmap for **Q4 2026**. Customers requiring India residency before that date may contact LegalInk to discuss commercially reasonable accommodations.

7. Personal Data Breach notification

7.1 **Notification to Customer.** LegalInk will notify the Customer in writing **without undue delay, and in any event within 72 hours** of becoming aware of a Personal Data Breach.

7.2 **Content.** To the extent known, the notification will include:

(a) a description of the nature of the Breach, including (where possible) the categories and approximate number of Data Principals and records affected;

(b) the likely consequences;

(c) the measures taken or proposed to address the Breach and mitigate its effects;

(d) the contact point at LegalInk for further information.

7.3 **Updates.** Information not available at initial notification will be provided in subsequent updates without undue delay.

7.4 **Customer's notifications.** The Customer is responsible for any notifications it must make to the Data Protection Board of India, other competent authorities, or affected Data Principals. LegalInk will provide reasonable assistance.

7.5 **CERT-In.** LegalInk will independently meet any direct CERT-In notification obligations once that framework is operational. As of the Effective Date, the formal CERT-In process is on LegalInk's published roadmap for Q3 2026.

8. Audits and inspections

8.1 **Right to audit.** Subject to the conditions in this Section 8, the Customer (or an independent third-party auditor mandated by the Customer and bound by confidentiality) may audit LegalInk's compliance with this DPA.

8.2 **Conditions:**

(a) **Frequency.** No more than once per calendar year, except in case of a regulator-led audit or a Personal Data Breach reasonably attributable to LegalInk.

(b) **Notice.** The Customer provides at least 30 days' written notice.

(c) **Scope.** Reasonably scoped to verify compliance with this DPA, conducted during normal business hours.

(d) **Confidentiality.** The auditor is bound by written confidentiality obligations.

(e) **Cost.** Borne by the Customer, except where the audit reveals a material breach by LegalInk, in which case LegalInk reimburses reasonable third-party audit costs.

8.3 **Alternative.** As an alternative or in conjunction with on-site audit, LegalInk will respond in writing to the Customer's reasonable compliance questionnaires and provide existing third-party certifications under confidentiality.

8.4 **Subprocessor audits.** Where the Customer requires audit information about a Subprocessor, LegalInk will use reasonable efforts to obtain and share such information (e.g., a SOC 2 report) on the same confidentiality terms.

9. Return or deletion of Customer Personal Data

9.1 **At the Customer's option.** Upon expiry or termination of the Agreement, the Customer may, by written request within **30 days** of termination, request that LegalInk return or delete all Customer Personal Data.

9.2 **Default — deletion.** If the Customer makes no election within 30 days of termination, LegalInk will delete Customer Personal Data in accordance with Exhibit B.

9.3 **Statutory retention.** Notwithstanding 9.1 and 9.2, LegalInk may retain Customer Personal Data to the extent and for the period required by Applicable Privacy Law, Indian tax law (Income Tax Act §44AA, CGST Act §35), Indian company law (Companies Act §128), or a binding legal hold. Retained data is segregated and not used for any other purpose.

9.4 **Backups.** Live-system deletion is immediate. Residual copies in encrypted backups expire on a 30-day rolling cycle and are not used for any purpose other than disaster recovery.

9.5 **Certification on request.** Upon written request, LegalInk will provide written confirmation that deletion has been completed, identifying any data retained on legal grounds.

10. Liability

10.1 **Liability cap.** The aggregate liability of each party arising out of or related to this DPA is subject to the liability cap and exclusions in the Agreement, except where Applicable Privacy Law provides for direct claims by Data Principals or competent authorities, which are not capped by contract.

10.2 **No indirect liability.** Neither party is liable to the other for indirect, consequential, special, exemplary, or punitive damages arising out of this DPA, except where prohibited by Applicable Privacy Law.

10.3 **Order of precedence.** In the event of a conflict between the Agreement and this DPA in respect of Processing, this DPA prevails.

11. Term and termination

11.1 **Term.** This DPA becomes effective on the Effective Date and remains in effect for the duration of the Agreement.

11.2 **Survival.** Sections 4.5 (no training), 7 (breach notification, as to Breaches occurring during the term), 9 (return or deletion), and 10 (liability) survive termination.

12. Governing law and jurisdiction

12.1 **Governing law.** This DPA is governed by the laws of the Republic of India.

12.2 **Jurisdiction.** Disputes arising out of or related to this DPA are subject to the exclusive jurisdiction of the courts at Mumbai, Maharashtra, India.

12.3 **Severability.** If any provision is held invalid or unenforceable, it will be modified to the minimum extent necessary to render it valid; the remaining provisions remain in full force.

13. Notices

All notices under this DPA must be in writing and sent to:

To LegalInk: support@legalink.ai

Subject line conventions:

- "DPA notification — [Customer Name]"
- "Personal Data Breach inquiry — [Customer Name]"
- "Subprocessor objection — [Customer Name]"
- "Audit request — [Customer Name]"

To the Customer: the email address designated as the Customer's billing or compliance contact in the Customer's account, or as otherwise notified to LegalInk in writing.

14. Update history

Date	Version	Change	Reason
8 May 2026	1.0	Initial publication	Trust & Compliance program launch

EXHIBIT A — Subprocessor List

The current Subprocessor List forms part of this DPA and is available at **legalink.co.in/trust/subprocessors**. The version in effect on the Effective Date is incorporated by reference. Subsequent updates are governed by Section 5 of this DPA.

A summary as of the Effective Date:

Category	Subprocessor	Region
AI reasoning	Anthropic, PBC	United States, European Union
AI drafting / OCR	Google LLC (Gemini API via Lovable AI Gateway)	Multi-region (US, EU, Asia-Pacific)
Voice transcription	Groq, Inc.	United States
Database / storage	Supabase, Inc. (managed by Lovable)	**Tokyo, Japan**
Application hosting	Lovable Tech, Inc.	Multi-region (US, EU)
Payments	Razorpay Software Pvt. Ltd.	India
Transactional email	Resend, Inc.	United States
Legal research	IndianKanoon	India
Analytics	Google LLC (GA4 / Google Ads)	Multi-region

Full details, purposes, data categories, and privacy-policy links are at the public URL above.

EXHIBIT B — Document Retention Schedule

The current Document Retention Policy forms part of this DPA and is available at **legalink.co.in/trust/retention**. The version in effect on the Effective Date is incorporated by reference.

Key retention periods as of the Effective Date:

Category	Retention
Drafts, chat history, uploaded files	Until user deletes; otherwise account closure + 90 days
Voice audio recordings	Not retained beyond transcription
Voice transcripts	30 days
Account profile	While active; 30 days post-deletion request
Audit logs	24 months
Application error logs	90 days
Edge function logs	30 days
Search queries to legal databases	90 days
Payment records	**7 years** (Indian tax law mandate)
GSTIN / tax identifiers	7 years
DPA, MSA, signed contracts	7 years from contract end
Encrypted database backups	30-day rolling window

Full details and the operational basis for each are at the public URL above.

EXHIBIT C — Technical and Organisational Measures

LegalInk maintains the following Technical and Organisational Measures ("**TOMs**"), designed to ensure a level of security appropriate to the risk of the Processing.

C.1 — Access controls

- **Authentication.** Email-and-password authentication with strength requirements (length minimum 10 characters; HIBP breach-database screening). Google OAuth 2.0 for federated sign-in.
- **Role-based access control.** Row-level security at the database layer enforced for all customer accounts including Enterprise team workspaces.
- **Administrative access.** Production access by LegalInk personnel is limited to authorised personnel and logged in an internal access log.

C.2 — Encryption

- **In transit.** TLS 1.2 or higher for all customer-facing endpoints. HSTS enabled.
- **At rest.** AES-256 encryption for the primary database, file storage, and encrypted backups.

C.3 — Network security

- All public endpoints terminate at a hardened edge layer (TLS termination, basic DDoS-resilience, request-rate limiting).
- Database is not directly internet-exposed; all access is mediated through application and edge-function layers.

C.4 — Application security

- Customer drafts, chat content, and uploaded files are stored in tenant-isolated rows protected by row-level security policies.
- Files are processed in-memory for AI generation. Upstream AI Subprocessors operate under enterprise API tiers that contractually exclude training on Customer data.
- Audit logs are captured at the application layer for security-relevant events.

C.5 — Operational security

- **Backup integrity.** Encrypted backups on a 30-day rolling window. Backups are not used for any purpose other than verified disaster recovery.
- **Error monitoring.** Application errors are captured server-side with PII redacted before storage.
- **Edge function logs.** Retained for 30 days for incident review.

C.6 — Incident management

- **Triage.** Security incidents are triaged within 24 hours of discovery.
- **Customer notification.** Affected customers are notified directly within 72 hours of confirmed impact.
- **Post-mortem.** A written post-mortem is published within 7 days for any incident affecting Customer Personal Data.

C.7 — Personnel

Authorised personnel are bound by confidentiality obligations. Production access is limited and logged. Access is revoked promptly on personnel changes.

C.8 — Subprocessor management

Subprocessors are engaged under written terms imposing data-protection obligations no less protective than this DPA. Subprocessor selections and material changes are notified to Customers per Section 5.

C.9 — Roadmap measures

The following measures are on LegalInk's published compliance roadmap and not yet implemented as of the Effective Date:

Measure	Target
DPDP §11 export & deletion automation	Q2 2026
SOC 2 Type 1 audit	Q3 2026
CERT-In notification framework	Q3 2026
ISO 27001 readiness	Q4 2026
India (Mumbai) data residency	Q4 2026
SOC 2 Type 2 attestation	2027

LegalInk will update this Exhibit C and Section 6.4 of the DPA as each roadmap item is completed.

Acceptance

By accepting LegalInk's Terms of Service or executing a separate Master Services Agreement, the Customer accepts this DPA as part of the Agreement.

For Enterprise customers requiring counter-signature, a counter-signed copy is available on written request to support@legalink.ai.

This document forms part of LegalInk AI's Trust & Compliance package. The current version of this DPA is available at legalink.co.in/trust/dpa.