

Data Processing Addendum

Version 2026-10-01 · Last updated October 1, 2026

Paperlink AI is a product of Intellidoc AI Private Limited.

This Data Processing Addendum ("DPA") forms part of the [Terms of Service](#) between Intellidoc AI Private Limited ("Processor") and the customer ("Controller"). It applies automatically when you accept the Terms. If you need a countersigned copy, email support@paperlinkai.com.

1. Definitions

"Data Protection Law" means all data protection laws that apply to the processing, including, where relevant, the EU GDPR, the UK GDPR, the US state privacy laws (such as the CCPA/CPRA) and India's Digital Personal Data Protection Act, 2023. "Customer Personal Data" means personal data in Customer Content that we process for the Controller. Other capitalized terms have the meaning given in the Terms or in Data Protection Law.

2. Roles and instructions

- The Controller determines the purposes and means of processing Customer Personal Data; we process it as Processor (or service provider) only on the Controller's documented instructions.
- The Terms, this DPA and the Controller's use and configuration of the Service are its complete instructions. We will tell the Controller if we believe an instruction breaks Data Protection Law.
- We will not sell or share Customer Personal Data, use it for our own purposes, combine it with other data except as needed to provide the Service, or use it to train AI models.
- The Controller is responsible for having a lawful basis and giving any notices (including to widget visitors) needed for the processing.

3. Confidentiality

Everyone we authorize to process Customer Personal Data is bound by confidentiality obligations and has access only as needed to run the Service.

4. Security

We implement and maintain the technical and organizational measures in Annex 2, and may update them as long as the overall level of protection does not decrease.

5. Personal data breaches

We notify the Controller without undue delay, and in any case within 72 hours, after becoming aware of a personal data breach affecting Customer Personal Data, with the information the Controller reasonably needs to meet its own obligations. We take reasonable steps to contain and remedy the breach.

6. Assistance

Taking into account the nature of the processing, we help the Controller respond to data subject requests (access, correction, deletion, export), and with data protection impact assessments and consultations with authorities. If a data subject contacts us directly, we forward the request to the Controller and do not respond ourselves unless instructed.

7. Subprocessors

- The Controller gives general authorization for us to use the subprocessors listed on our [Subprocessors](#) page.
- We impose data protection obligations on each subprocessor that are at least as protective as this DPA, and remain responsible for their performance.
- We give at least 30 days' notice of a new or replacement subprocessor. The Controller may object on reasonable data protection grounds within that period; if we cannot address the objection, the Controller may terminate the affected Service and receive a refund of prepaid fees for the unused period.

8. International transfers

Customer Personal Data is processed mainly in the United States. Where Data Protection Law requires a transfer mechanism, the EU Standard Contractual Clauses (Commission Decision 2021/914, Module 2 or 3 as applicable) and the UK International Data Transfer Addendum are incorporated by reference, with the details in Annex 1 and Annex 2 completing their appendices.

9. Return and deletion

The Controller can delete its documents in the dashboard at any time and can ask us for an export of its Customer Personal Data by email during the term. When the organization is deleted, we delete Customer Personal Data from active systems promptly, and backups expire within 30 days, unless the law requires us to keep it.

10. Audits

On written request, no more than once a year, we provide the information reasonably necessary to demonstrate compliance with this DPA, such as answers to security questionnaires and relevant documentation. Where that is not sufficient or a regulator requires it, the Controller may carry out an audit at its own cost, with 30 days' notice, during business hours, under confidentiality and without access to other customers' data.

11. Liability, order of precedence and law

Each party's liability under this DPA is subject to the limitations in the Terms, except where Data Protection Law does not allow it. If this DPA conflicts with the Terms, this DPA prevails for the processing of Customer Personal Data; the Standard Contractual Clauses prevail over both. This DPA is governed by the laws of India, with the courts at Kota, Rajasthan having exclusive jurisdiction, except where the Standard Contractual Clauses require otherwise.

Annex 1: Details of processing

Parties	Controller: the customer. Processor: Intellidoc AI Private Limited, Kota, Rajasthan, India, support@paperlinkai.com.
Subject matter and purpose	Providing Paperlink AI: storing and indexing the Controller's documents, answering questions about them in the dashboard and the embedded widget, sending conversation transcripts to the Controller on a visitor's request, support and security.
Nature of processing	Collection, storage, parsing, chunking, embedding, search, AI answer generation, transmission, deletion.
Data subjects	The Controller's authorized users; visitors who use the Controller's widget; individuals named in the Controller's documents.
Categories of personal data	Names and contact details of users; questions, answers and conversation metadata; email addresses and notes visitors choose to send; any personal data contained in uploaded documents; technical data such as IP addresses.
Special categories	None intended. The Controller should not upload special-category data unless agreed in writing.
Frequency and duration	Continuous, for the term of the Terms and until deletion under section 9.
Subprocessors	As listed on the Subprocessors page at the time of processing.

Annex 2: Technical and organizational measures

- Tenant isolation: each organization's documents, search index and conversations live in a dedicated store and vector namespace, reachable only with that organization's verified identity.
- Encryption of data in transit (TLS) and at rest.
- Access control: dashboard sign-in through Clerk with organization roles; hashed, revocable widget API keys; origin allow-lists and bot protection for the widget.
- Least-privilege access for staff, with secrets kept out of source code.
- Logging and analytics limited to metadata; no document, question or answer text in analytics.
- Rate limiting and abuse protection on public endpoints.
- Backups with limited retention (expiring within 30 days).
- Vendor review of subprocessors and written data protection terms with each.
- Incident response process with customer notification as described in section 5.

Questions about this document? Email support@paperlinkai.com.