

ASHDOCS Data Processing Agreement

Template — to be reviewed by counsel before execution.

This addendum forms part of the agreement between ASHDOCS ("Processor") and the customer identified in the applicable order form or account ("Controller"), and applies to Processor's processing of personal data on Controller's behalf. Drafted to track GDPR Article 28(3)'s required contract terms; nothing in this document is legal advice, and it is not effective until both parties execute a countersigned copy.

1. Subject matter and duration of processing

The subject matter is document processing performed by the ASHDOCS API and dashboard (conversion, editing, OCR, structured data extraction, redaction, and related tools) at Controller's instruction. Processing continues for the duration of the underlying service agreement and ceases, per document, on completion of the job or on deletion per Section 6, whichever is earlier.

2. Nature and purpose of processing

Automated transformation and extraction of data contained in documents Controller submits via API or dashboard. Processor does not use document contents for any purpose other than fulfilling the specific tool call Controller invoked — never for model training, analytics, or any other secondary use.

3. Types of personal data and categories of data subjects

Types and categories are determined entirely by what Controller includes in the documents it submits — potentially names, contact details, financial account numbers, or other personal data appearing in invoices, statements, contracts, or scanned records. Data subjects are typically Controller's own customers, employees, or counterparties. Processor has no visibility into document contents beyond what a given tool call requires to complete.

4. Processor obligations (GDPR Art. 28(3))

Processor shall: a. Process personal data only on Controller's documented instructions (including regarding international transfers), unless required otherwise by law binding on Processor, in which case Processor will inform Controller before processing unless that law prohibits such notice. b. Ensure persons authorized to process the personal data are subject to confidentiality obligations. c. Implement appropriate technical and organizational measures per Article 32 — see Section 5. d. Not engage another processor (sub-processor) without Controller's prior general or specific written authorization — see Section 7. e. Taking into account the nature of the processing, assist Controller by appropriate technical and organizational measures for fulfilling Controller's obligation to respond to data subject rights requests. f. Assist Controller in ensuring compliance with Articles 32–36 (security, breach notification, impact assessments), taking into account the nature of processing and the information available to Processor. g. At Controller's choice, delete or return all personal data after the end of the provision of services, and delete existing copies unless retention is required by law. h. Make available to Controller all information necessary to demonstrate compliance with this Article and allow for and contribute to audits, including inspections, conducted by Controller or an auditor mandated by Controller.

5. Security measures

TLS 1.2+ in transit; AES-256 at rest for stored objects (Cloudflare R2); Fernet-encrypted third-party credentials (OAuth tokens, delivery-destination keys) before they reach the database; every uploaded file scanned before processing; SSRF guards on every URL-fetching endpoint; HMAC-SHA256-signed webhook deliveries. Per-request or account-wide zero-retention mode is available — see Section 6. Full detail: [/security](#).

Processor holds no SOC 2, ISO 27001, HIPAA, or PDF/UA certification as of the date of this template. These technical controls are offered as concrete, verifiable measures in their place — not as a substitute for a certification Controller may separately require by contract.

6. Retention and deletion

Default retention is 24 hours from job completion, after which source files and outputs are purged by an automated sweep. Controller may set `options.retention="zero"` per request, or enable zero-retention account-wide, in which case source files and results are never persisted beyond the request itself (purged within minutes of job completion). This applies uniformly regardless of data subject location.

7. Sub-processors

Controller provides general authorization for Processor to engage the following sub-processors, each engaged under terms providing an equivalent level of data protection:

Sub-processor	Function	Touches document contents?
DigitalOcean	API compute hosting	Transiently, during processing
MongoDB Atlas	Primary database	Metadata only — document bytes are not stored in Mongo
Cloudflare (R2)	Object storage for source/output files	Yes
Vercel	Marketing site and dashboard hosting	No
Resend	Transactional email	No
Razorpay	Billing	No — account/payment data only
Anthropic	AI-driven structured data extraction (pdf-to-data and related tools)	Yes, only when an extraction tool is invoked
Google	OAuth sign-in; optional Google Drive delivery	Only when Controller configures a Drive destination
PostHog	Product analytics	No — usage metadata only

Processor will give Controller notice before adding or replacing a sub-processor that touches document contents, and Controller may object on reasonable data-protection grounds.

8. International transfers

Processing runs on infrastructure operated by the sub-processors listed in Section 7, which may process data outside Controller's jurisdiction. Where a transfer of personal data originating in the EEA, UK, or Switzerland occurs, Processor relies on the relevant sub-processor's Standard Contractual Clauses or equivalent adequacy mechanism. Region-pinned storage is not offered as of the date of this template.

9. Data subject requests

Where a data subject request reaches Processor concerning data Controller controls, Processor forwards it to Controller without undue delay and provides reasonable assistance with access, rectification, or erasure — most directly by enabling zero-retention mode, after which Processor typically holds no document data responsive to such a request.

10. Breach notification

Processor notifies Controller without undue delay after becoming aware of a personal data breach affecting Controller's data, providing the information reasonably available at the time and supplementing it as the investigation progresses.

This template was generated from ASHDOCS's own infrastructure survey (reports/block-1.md, Block 1) rather than copied from a generic boilerplate — every sub-processor and retention figure above is drawn from what the codebase actually does, not assumed. It still requires counsel review before either party relies on it.