

Data Processing Addendum

Last updated 7 October 2026 Version 2026-10-07

<https://www.ashdocs.com/dpa> · ASH Studios · Coimbatore, India · GSTIN 33DLEPA9895M2ZH

Applies automatically to accounts subject to the GDPR or UK GDPR; any other account can accept it from Settings → Legal or by emailing us. A signed PDF copy is available on request for customers whose procurement needs one.

1. Parties and scope

This Data Processing Addendum ("DPA") forms part of the Terms of Service between the account holder ("Customer") and ASH Studios, proprietorship of Ashwin Manikandan, Coimbatore, India, trading as ASHDOCS ("ASHDOCS"). It applies where ASHDOCS processes personal data on Customer's behalf in providing the Service. In that processing Customer is the controller (or a processor acting for its own controller) and ASHDOCS is the processor. "Data Protection Law" means the GDPR, the UK GDPR and Data Protection Act 2018, the Digital Personal Data Protection Act, 2023 (India), the CCPA/CPRA (California) and any other law that applies to the processing. Terms used here have the meaning Data Protection Law gives them.

2. Details of the processing

- **Subject matter:** creating, hosting, sending and tracking invoices and related documents; generating, extracting from and redacting documents; running Customer's automations.
- **Duration:** the term of Customer's account plus the retention periods in the Privacy Policy.
- **Nature and purpose:** storage, rendering, transmission by email and hosted link, status tracking, and the other operations needed to provide the Service as Customer configures it.
- **Categories of data subjects:** Customer's staff who use the dashboard; Customer's customers, suppliers and contacts who are named on invoices and documents; recipients of emails Customer sends through the Service.
- **Categories of personal data:** names, business names, email addresses, postal addresses, phone numbers, tax identifiers, invoice line items and amounts, payment references, IP addresses and view timestamps of hosted pages, and whatever else Customer chooses to put in a document.
- **Special categories:** none are intended. Customer agrees not to submit special-category data (health, biometric, political, religious and similar) or children's data unless it has a lawful basis and tells us in advance in writing.

3. Customer's obligations

Customer is responsible for the lawfulness of the personal data it submits and of its instructions, for having a lawful basis and giving any notices required to data subjects, for configuring the Service

appropriately (including who it gives dashboard access and API keys to), and for keeping its own copies of records it must retain.

4. ASHDOCS's obligations

ASHDOCS will:

1. process personal data only on Customer's documented instructions, which are the Terms of Service, this DPA, Customer's use of the dashboard and API, and any further written instructions Customer gives, unless Union, Member State, UK or Indian law requires otherwise, in which case ASHDOCS will tell Customer before processing unless the law prohibits it;
2. tell Customer promptly if it believes an instruction infringes Data Protection Law;
3. ensure that the only people with access to personal data are bound by confidentiality (at present, the proprietor; any future staff or contractors will sign confidentiality terms before access);
4. implement the technical and organisational measures in Annex 1 and not reduce their overall level of protection during the term;
5. help Customer, taking into account the nature of the processing, respond to data-subject requests (access, rectification, erasure, restriction, portability, objection), by forwarding any request ASHDOCS receives directly within 5 working days and by providing the export and deletion tools in the dashboard;
6. help Customer with security, breach notification, data-protection impact assessments and consultation with supervisory authorities, to the extent the information is in ASHDOCS's possession;
7. notify Customer without undue delay, and in any case within 48 hours of becoming aware, of a personal data breach affecting Customer's data, with the information Article 33(3) GDPR requires as it becomes available;
8. at Customer's choice, delete or return all personal data at the end of the Service, and delete remaining copies within the periods in the Privacy Policy, unless law requires storage;
9. make available the information needed to demonstrate compliance and allow and contribute to audits as set out in section 7.

5. Sub-processors

Customer gives general written authorisation for ASHDOCS to use the sub-processors listed at ashdocs.com/subprocessors. ASHDOCS will give at least 14 days' notice by email (to accounts that opt in to sub-processor notices) before adding or replacing a sub-processor. Customer may object on reasonable data-protection grounds within that period; if the parties cannot resolve the objection, Customer may terminate the affected Service and receive a pro-rata refund of prepaid fees for the unused period. ASHDOCS imposes data-protection obligations on each sub-processor equivalent to those in this DPA and remains liable to Customer for the sub-processor's performance.

6. International transfers

ASHDOCS is in India and its sub-processors are in India, the United States and the EU. Where personal data protected by the GDPR or UK GDPR is transferred to a country without an adequacy decision, the transfer is made under the European Commission's Standard Contractual Clauses (Decision 2021/914), Module Two (controller to processor) or Module Three (processor to processor) as applicable, and for UK data the UK International Data Transfer Addendum to those clauses, which are incorporated into this DPA by reference with the following selections: Clause 7 (docking) included; Clause 9 Option 2 (general authorisation) with the 14-day notice period above; Clause 11 optional language not included; Clause 13 and Annex I.C: the supervisory authority of the EU Member State in which Customer is established, or, where Customer is not in the EU, Ireland; Clause 17: Irish law; Clause 18: courts of Ireland. Annex I is completed by section 2 of this DPA and the parties' account details; Annex II by Annex 1 below; Annex III by the sub-processor page. If a future adequacy decision or other valid mechanism covers the transfer, it may be used instead.

7. Audits

Once in any 12-month period, or after a personal data breach, Customer may ask ASHDOCS for written responses to a reasonable security questionnaire and for copies of the most recent third-party reports available from ASHDOCS's sub-processors (for example DigitalOcean, MongoDB Atlas and Cloudflare publish SOC 2 reports). If those do not reasonably satisfy a requirement of Data Protection Law or a supervisory authority, Customer may conduct an audit on 30 days' notice, during business hours, at its own cost, by an independent auditor bound by confidentiality, limited to what is needed to verify compliance with this DPA.

8. California

Where the CCPA/CPRA applies, ASHDOCS is a service provider. It will not sell or share personal information, retain, use or disclose it outside the direct business relationship with Customer or for any purpose other than the business purpose in section 2, or combine it with personal information from other sources except as the CCPA permits for service providers. ASHDOCS certifies it understands these restrictions and will tell Customer if it can no longer meet them.

9. India

Where the Digital Personal Data Protection Act, 2023 applies, Customer is the Data Fiduciary and ASHDOCS the Data Processor under a valid contract, which this DPA constitutes. ASHDOCS will delete personal data when the purpose is served or Customer withdraws its instruction, subject to the retention periods the law allows, and will support Customer's obligations toward Data Principals and the Data Protection Board.

10. Liability and precedence

Each party's liability under this DPA is subject to the limitation of liability in the Terms of Service, except where Data Protection Law does not allow it to be limited. If this DPA conflicts with the Terms of Service, this DPA prevails for the processing of personal data; the Standard Contractual Clauses prevail over both where they apply.

Annex 1 — Technical and organisational measures

- **Encryption:** TLS 1.2 or higher on every connection; encryption at rest provided by MongoDB Atlas, Cloudflare R2 and DigitalOcean volumes; passwords stored as salted hashes; API keys stored hashed and shown once.
- **Access control:** infrastructure access restricted to the proprietor with multi-factor authentication on every provider console; per-account isolation in the database; dashboard roles where offered; API keys scoped to one account and one mode (test or live).
- **Logging and monitoring:** request logs kept 30 days; audit records for billing, key and account events; error tracking; uptime monitoring with alerts.
- **Resilience:** daily automated database backups kept up to 35 days; object storage with provider-side redundancy; documented restore procedure tested at least twice a year.
- **Secure development:** changes deployed from version control; dependencies updated regularly; secrets kept in environment configuration, never in code; automated tests run before deployment.
- **Abuse and rate limiting:** signup abuse detection, per-key rate limits, signed webhooks with per-account secrets.
- **Data minimisation and deletion:** one-off conversion files deleted within 24 hours; deleted invoices removed from storage within 30 days; account deletion available to the Customer without contacting support.
- **Incident response:** written procedure covering detection, containment, assessment, notification within 48 hours to affected customers, and post-incident review.
- **Organisational:** ASHDOCS is currently operated by its proprietor alone. Before any employee or contractor is given access to customer data they will be bound by confidentiality and this Annex, and the measures above will be reviewed.