

# Data Processing Agreement

Effective date: 30 May 2026

Last updated: 29 February 2026

This Data Processing Agreement (the "DPA") is entered into between LaunchDocs Ltd. (the "Processor") and the customer identified in the LaunchDocs subscription record (the "Controller"). It forms part of, and is subject to, the LaunchDocs Terms of Service available at [launchdocs.ai/terms](https://launchdocs.ai/terms). Capitalised terms not defined here have the meaning given to them in the Terms of Service or, where applicable, in the GDPR.

## 1. Scope of processing

LaunchDocs processes personal data on behalf of the Controller solely to provide the LaunchDocs documentation, compliance, and procurement service. Personal data processed under this DPA includes account data of the Controller's authorised users, the contents of files uploaded into the workspace, and operational telemetry necessary to operate the service. To the extent of any conflict between this DPA and the Terms of Service, this DPA prevails for matters relating to data protection.

## 2. Purpose and instructions

LaunchDocs only processes personal data on the documented instructions of the Controller. The Terms of Service, the in-product configuration, and any subsequent written instructions issued by the Controller constitute those documented instructions. LaunchDocs will inform the Controller without undue delay if, in its opinion, an instruction infringes the GDPR or other applicable data-protection law.

## 3. Duration

This DPA is in force for the term of the Controller's subscription. On termination, LaunchDocs will delete or return personal data in accordance with Section 7 below, unless retention is required by applicable law.

## 4. Sub-processors

The Controller authorises LaunchDocs to engage the sub-processors listed at the end of this DPA. Each sub-processor is bound by data-protection obligations no less protective than those in this DPA. LaunchDocs will notify the Controller of any intended addition or replacement of sub-processors at least 30 days in advance, by email and via the in-product changelog, giving the Controller the opportunity to object on reasonable data-protection grounds.

## 5. Security measures

LaunchDocs implements technical and organisational measures appropriate to the risk presented by the processing, including encryption of personal data in transit (TLS 1.2 or above) and at rest, role-based access control with strict tenant isolation, mandatory Two-Factor Authentication for administrative accounts, audit logging of authentication, data-access and admin events (retained for 2 years), dependency vulnerability scanning on every release, and a documented incident-response plan with GDPR-compliant breach-notification procedures.

## **6. Assistance with data-subject rights**

LaunchDocs provides self-service tools in Settings → Account that let the Controller's users exercise their rights of access, portability, and erasure without LaunchDocs intervention. For any request that cannot be fulfilled through those tools, LaunchDocs will assist the Controller within 5 working days of a written request to [privacy@launchdocs.ai](mailto:privacy@launchdocs.ai).

## **7. Return and deletion on termination**

On termination of the subscription the Controller may export all data via Settings → Account → Download my data within 30 days. Thirty days after termination LaunchDocs will permanently delete the Controller's personal data from production systems. Encrypted backups containing the data will be rotated out within the standard 35-day backup window and will then be irreversibly destroyed. Audit-log entries are retained for 2 years in accordance with our security and regulatory obligations.

## **8. International data transfers**

Where personal data is transferred from the EEA, the UK or Switzerland to a country that has not received an adequacy decision, LaunchDocs and the relevant sub-processor rely on the European Commission's Standard Contractual Clauses (Decision 2021/914) and, where applicable, the UK Addendum issued by the UK Information Commissioner.

## **9. Audits and inspections**

LaunchDocs makes available to the Controller all information reasonably necessary to demonstrate compliance with this DPA, including the security overview at [launchdocs.ai/security](https://launchdocs.ai/security) and any third-party attestations published from time to time. Where the Controller requires further assurance, LaunchDocs will, on reasonable written notice and during normal business hours, cooperate with a Controller audit at the Controller's cost.

## **10. Personal-data breach notification**

LaunchDocs will notify the Controller without undue delay, and in any event within 72 hours of becoming aware, of any personal-data breach affecting the Controller's data. The notification will describe the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, and the measures taken or proposed to address the breach.

# Annex 1 — Sub-processors

Provider	Purpose	Country	Transfer safeguard
Anthropic	AI generation (Claude)	USA	Standard Contractual Clauses
Stripe	Payment processing	USA / IE	Standard Contractual Clauses
Resend	Transactional email	USA	Standard Contractual Clauses
MongoDB Atlas	Primary database (encrypted at rest)	EU / USA configurable	Standard Contractual Clauses
Cloud hosting provider	Application hosting	EU	EEA hosting

For questions about this DPA, email [privacy@launchdocs.ai](mailto:privacy@launchdocs.ai).