

Data Processing Addendum

Business customers | controller-processor terms

Version 1.2 | 4 September 2026 | Effective 4 September 2026

This DPA forms part of the agreement between the customer identified in the Order or account (Customer) and Almero Pty Ltd (Almero). It applies only to personal data Almero processes on Customer's behalf in providing the Service. It does not apply to Almero's independent controller processing described in the Privacy Policy.

1. Definitions and precedence

Applicable Data Protection Law means laws governing the processing, privacy or security of Customer Personal Data, including the UK GDPR, UK Data Protection Act 2018, Australian Privacy Act 1988 and applicable US state privacy laws. EU GDPR provisions apply only if and when a Customer transfer or Almero activity is within their territorial scope. Customer Personal Data means personal data processed by Almero on Customer's behalf. Capitalised terms have their statutory meaning. This DPA prevails over the Agreement for data-protection conflict; an applicable transfer instrument prevails for restricted-transfer conflict.

2. Roles, scope and instructions

Customer is controller/business and Almero is processor/service provider. If Customer is a processor, Almero is its subprocessor. Customer instructs Almero to process Customer Personal Data to provide, secure and support the Service, comply with documented configurations and lawful written instructions, and make the transfers described here. Almero must notify Customer if an instruction infringes applicable law and may suspend that instruction. Customer is responsible for lawful collection, notices, instructions and rights to submit data.

3. Processor duties

- process only on documented instructions unless law requires otherwise, then notify Customer unless prohibited;
- ensure authorised personnel are bound by confidentiality;
- implement Article 32 / risk-appropriate technical and organisational measures;
- assist with data-subject requests, security, breach notification, DPIAs and regulator consultation, considering the processing and information available;
- maintain required processing records and make compliance information available;
- permit reasonable audits or independent assurance, subject to confidentiality, security, proportionality and cost allocation;
- not sell Customer Personal Data, share it for cross-context behavioural advertising, retain/use/disclose it outside the business purpose, or combine it except as permitted by US state law; and
- notify Customer if Almero can no longer meet an applicable US contractual restriction and allow reasonable remediation steps.

4. Security and breaches

Almero will maintain the measures in Schedule 2. Almero will notify Customer without undue delay after confirming a personal data breach affecting Customer Personal Data, provide information reasonably available for Customer's obligations, mitigate effects and cooperate. A fixed 24-hour

promise is not made unless an Order expressly adds it; Customer remains responsible for regulator and individual notices.

5. Subprocessors

Customer gives general written authorisation for Schedule 3 subprocessors. Almero will impose substantially equivalent data-protection obligations and remains responsible for their performance. Almero will give at least 30 days notice of a new subprocessor that will process Customer Personal Data. Customer may object within 14 days on reasonable documented data-protection grounds. The parties will seek a reasonable solution; if none exists, Customer may terminate the affected Service without penalty.

6. Return and deletion

During the term Customer may export available data and delete content using Service tools. In-app deletion removes data from active systems promptly. At termination, on Customer's choice communicated before termination, Almero will return or delete Customer Personal Data; if no choice is communicated, deletion is the default. Active-system deletion occurs within 30 days, subject to lawful holds. Deleted data then expires through routine Sydney backup rotation: Fly Volume snapshots are retained for five days and Fly Managed Postgres has an approximately ten-day recovery window. Lawfully retained data remains protected and is processed only for the retention purpose.

7. International transfers

For a restricted UK transfer, the UK International Data Transfer Addendum applies as completed by the UK Addendum Execution Tables, together with the Approved EU SCCs used as the underlying clauses. Almero has completed and approved a UK Data Protection Test for the restricted UK transfers described in this DPA. The EU SCC Execution Schedule is retained for future use only and does not become operative unless an EEA transfer is within EU GDPR scope and the parties validly incorporate it. For onward transfers Almero will use a lawful mechanism and required assessments.

Schedule 1 - Processing details

Item	Description
Subject matter and duration	Hosted AI Black Belt Agent services for the Agreement term plus deletion/backup period
Nature and purpose	hosting, storage, retrieval, model inference, analysis, output generation, support, security and deletion on Customer instructions
Data subjects	authorised users; employees, contractors, suppliers or other people whose data Customer includes
Personal data	identifiers, business contact data, credentials, device/security data, usage data, and user-submitted content
Sensitive data	not intended or required; Customer must not submit it without written agreement and appropriate safeguards
Frequency	continuous/on demand during Service use
Customer instructions	Agreement, DPA, account configuration, user actions and lawful written instructions

Item	Description
Return/deletion	section 6

Schedule 2 - Technical and organisational measures

Control	Measure
Access	named accounts; least privilege; account/project isolation; founder and developer production access from Australia; access promptly revocable
Authentication	bcrypt password hashing; MFA enabled for Fly.io, GitHub and Microsoft 365 administration; no end-user MFA at launch
Encryption	TLS for data in transit; Fly default provider-managed encryption for production volumes at rest; no representation of per-user encryption keys
Availability	Sydney-only routine backups: daily Fly Volume snapshots retained five days; Managed Postgres approximately ten-day recovery window
Security operations	application session metadata and Fly infrastructure logs; monitoring; written incident response; dependency and WordPress alerting with documented remediation targets
Personnel	confidentiality and limited support access
Deletion	user controls; active-system deletion within 30 days after closure; backup expiry after deletion
Supplier management	diligence, DPAs and subprocessor monitoring

Schedule 3 - Authorised subprocessors

Subprocessor	Service	Processing location / transfer
Anthropic, PBC	commercial API model inference	United States; DPA accepted; UK transfer mechanism as applicable
Fly.io, Inc.	hosting, networking, encrypted volumes and backups	Sydney region for production data/backups; DPA accepted; provider operations may be global
Stripe Payments Australia Pty Ltd and relevant Stripe affiliates/service providers	billing, payment, fraud and tax services	Australia and locations in Stripe documentation; DPA accepted

Execution

The downloadable DPA is incorporated for business customers through affirmative clickwrap, Order Form signature or other valid electronic acceptance. Almero records the user/account, timestamp, click event, and Terms, Privacy Policy and DPA versions. Customer legal name, address and contact are those in its account or Order. Almero: PO Box 123, Heidelberg, Victoria 3084, Australia; privacy@almero.ai. The parties intend electronic acceptance to sign this DPA and incorporated UK transfer terms.