

Privacy and Data Flow Brief

AI Black Belt Agent | vendor review edition

Version 1.2 | 4 September 2026 | Effective when published

Purpose. This brief gives IT, security, procurement and privacy teams a concise view of the launch architecture and contractual position. It should be updated when configurations, subprocessors or markets change.

1. Executive summary

Question	Current answer
What is it?	Browser-based SaaS for Lean Six Sigma projects; no local agent or browser extension represented.
Launch markets	Australia, United Kingdom and United States; no EEA marketing or intentional offering at launch.
Where is production data?	Primary application, files and routine backups are in Sydney, Australia.
What leaves Australia?	Selected inference context to Anthropic in the US; billing data through Stripe Payments Australia Pty Ltd and relevant Stripe providers.
Training?	Almero does not use project data to train models; provider processing follows the accepted commercial API terms and DPA.
Deletion?	In-app deletion is prompt; closed-account active data within 30 days; then five-day file snapshots and approximately ten-day database recovery rotation.
Contact	privacy@almero.ai

2. Data categories and minimisation

- account and business contact data;
- subscription, invoice and payment-status data (card data handled by Stripe);
- prompts, conversation context, uploaded files, model responses and generated deliverables;
- IP address, timestamps, device/session and security events; and
- support communications and operational telemetry.

Almero applies data minimisation by separating billing information from project content and sending only selected conversation context required for model inference.

3. Data flow and subprocessors

1. The user's browser sends account information, prompts and files to Almero's application environment in Sydney.
2. The application selects conversation context and sends it over TLS to Anthropic's commercial API in the United States for inference.
3. Statistical and document tools execute in the managed application environment.
4. Files and generated deliverables are stored in the configured Sydney storage environment.

5.Stripe processes billing, fraud and payment information separately; project content is not intended to be sent to Stripe.

Provider	Function	Data	Location / caveat
Anthropic, PBC	model inference	selected prompts and context; output	United States; DPA accepted
Fly.io, Inc.	hosting, networking, storage and backups	application traffic and hosted data	Sydney production/backups; DPA accepted
Stripe Payments Australia Pty Ltd	billing/payments	billing, tax, fraud and transaction data	Australia and relevant Stripe provider locations; DPA accepted

4. Retention and deletion

Layer	Position
Active projects/files	retained while active; in-app deletion removes the active copy promptly
Closed account	deleted from active systems within 30 days, subject to lawful holds
File backups	daily Fly Volume snapshots retained five days
Database backups	approximately ten-day Managed Postgres recovery window
Billing/legal records	retained for applicable legal/accounting periods

5. Security controls

Almero uses TLS to protect data in transit and Fly.io's platform-managed encryption for production volumes at rest. Named administrator accounts, least-privilege permissions, access logging and account/project access controls are used to restrict access to authorised users and personnel. Passwords are protected using bcrypt hashing, and administrator access can be promptly revoked. If a personal data breach occurs, Almero will investigate and provide notifications within the timeframes required by applicable law and relevant contracts. No online service can guarantee absolute security.

6. Contract and compliance documents

- Privacy Policy, including cookie information, and voluntary US State Privacy Notice;
- Terms of Service with UK 14-day full-refund treatment;
- downloadable business-customer DPA with acceptance record;
- UK Addendum Execution Tables;
- EU SCC Schedule held for future use only; and
- founder-approved UK Data Protection Test retained internally.

7. Vendor review evidence available

Subject to confidentiality and availability: architecture/data-flow confirmation, subprocessor list, DPA, security control summary, incident process, retention schedule, provider assurance reports and completed questionnaires. Provider certifications are their certifications, not Almero's.