Aegis Shield — Vendor Data Processing Agreement

Template for execution between the Customer (Controller) and Aegis Shield (Processor).

1. Subject Matter

Aegis Shield processes AI prompt and response traffic solely to detect and redact personal data, protected health information and other regulated content before forwarding to the Customer's chosen model provider.

2. Zero-Retention Processing

All payloads are processed in memory at the edge. Aegis Shield does not persistently store prompt or completion content. Audit logs contain metadata only (timestamps, rule identifiers, redaction counts).

3. Data Residency

Processing occurs in the operating region selected by the Customer (United States, European Union or India). Data is not transferred outside that region except as instructed by the Customer.

4. Regulatory Frameworks

Processing supports Customer obligations under GDPR, the EU AI Act, India's Digital Personal Data Protection Act and HIPAA, as configured in the Customer's policy matrix.

5. Security Measures

TLS 1.3 in transit, isolated processing environments, least-privilege access, continuous monitoring and annual third-party assessment.

6. Sub-processors

Aegis Shield maintains a current list of sub-processors and gives 30 days' notice of changes, with the right to object.

7. Breach Notification

Aegis Shield will notify the Customer without undue delay and within 72 hours of becoming aware of a personal data breach.

8. Service Level

Aegis Shield targets 99.99% monthly uptime for the production gateway.

9. Term and Deletion

This agreement remains in force for the duration of the subscription. Upon termination, any Customer configuration data is deleted within 30 days.

Customer (Controller)	Aegis Shield (Processor)
Signature: _____	Signature: _____
Name: _____	Name: _____
Date: _____	Date: _____