FlowAI

KYC/AML Compliance Automation

Security & Compliance Pack

Version 1.0 · 2026-06-13 · Confidential — For Prospect Use

This document covers FlowAI's security posture, compliance roadmap, sub-processors, data handling practices, AI model handling, sanctions data sources, and incident response procedures. It is intended for security reviewers and procurement teams.

AT A GLANCE

SOC 2 Type I	**Q3 2026**
SOC 2 Type II	**Q3 2027**
GDPR / CCPA	**Live**
Encryption at rest	**AES-256**
Encryption in transit	**TLS 1.3**
AI data retention	**Zero (OpenAI ZDR tier)**
Sanctions lists	**OFAC, EU, UN — daily refresh**
Incident SLA	**24h customer notification**

Compliance Posture

FlowAI is building toward SOC 2 Type I (Q3 2026) and SOC 2 Type II (Q3 2027). ISO 27001 is queued for enterprise accounts. GDPR and CCPA alignment is live today with configurable data retention and a Data Processing Agreement (DPA) available on request.

Compliance Milestones

Framework	Status	Notes
GDPR / CCPA	Live	Configurable retention (30/90/365 days). Deletion within 7 days on request. DPA available.
SOC 2 Type I	Q3 2026	Audit scheduled. Report available under NDA on request.
SOC 2 Type II	Q3 2027	12-month observation period begins after Type I closes.
ISO 27001	Roadmap	Queued for enterprise accounts. Contact us to discuss timeline.

Data Handling

- Encryption at rest: AES-256 via Neon PostgreSQL block-storage encryption.
- Encryption in transit: TLS 1.3. All older cipher suites disabled. No plaintext channels.
- Configurable retention: 30, 90, or 365 days. Default 90 days. Auto-purge after window.
- Deletion on request: cryptographic shredding within 7 days. Send case_id to security@flowai.polsia.app.
- No model training: customer data is never used to train, fine-tune, or evaluate any model.
- Audit log retention: triage events retained per customer retention window, then purged.

Sub-Processors

The following third-party services may process customer data. This list is intentionally short. Customers on Growth and Scale plans can request 30-day advance notice of material changes.

Complete Sub-Processor List

Vendor	Purpose	Data Handled	Region	DPA
Render	Compute / hosting	All application traffic	US (Oregon)	Available
Neon	PostgreSQL database	Audit logs, triage records, KYC metadata	US (AWS us-east-1)	Available
OpenAI	Document extraction & risk scoring	Document URLs + extracted identity metadata. Zero-retention API endpoint — no data retained beyond the request.	US	Zero-retention
Stripe	Billing only	Payment method data. No PII from triage flows passes through Stripe.	US	Available
Postmark	Transactional email	Work email address (for result delivery and notifications only).	US	Available

OpenAI Zero-Retention Policy

FlowAI uses OpenAI's enterprise zero-data-retention (ZDR) API endpoints where available. Under ZDR: request/response data is not persisted to OpenAI storage, not used for model training or evaluation, and not accessible to OpenAI staff except for safety monitoring. This is a contractual obligation on OpenAI's side — not a preference on ours.

FLOWAI SECURITY & COMPLIANCE PACK

Access Controls & Incident Response

Identity & Access Management

- Least-privilege IAM: service accounts scoped to minimum required permissions.
- MFA required for all production system access. No exceptions.
- Database credentials not shared between services. Each service has its own scoped credentials.
- All secrets injected at runtime via environment variables. Never hardcoded or committed to source control.
- Access reviewed and rotated quarterly, or immediately on personnel change.
- Audit logging: all production access events logged with actor, action, and timestamp.

Incident Response

Severity	Definition	SLA
P0 — Data Breach	Unauthorized access to customer PII or triage records	24h customer notification. Immediate containment.
P1 — Service Outage	Full API unavailability	Public status update within 1h. Post-mortem within 5 business days.
P2 — Degraded Performance	Elevated error rates or latency	Status update within 4h.
P3 — Minor Issues	Non-customer-facing bugs or performance blips	Tracked and resolved in normal release cycle.

Incident notifications are sent to the customer's registered email and posted to status.flowai.polsia.app. P0 and P1 post-mortems are shared with affected customers. Security incident reports: security@flowai.polsia.app

FLOWAI SECURITY & COMPLIANCE PACK

AI Model Handling & Sanctions Data

AI Models Used

- Primary model: OpenAI GPT-4o for document extraction and structured risk scoring.
- Invoked exclusively via OpenAI's zero-retention enterprise API tier.
- No customer data is retained by OpenAI beyond the duration of the API call.
- No fine-tuning or model customization on customer data — ever.
- Model outputs are deterministic risk scores (0–100) plus a structured decision rationale.
- Human-in-the-loop: ESCALATE cases route to a human reviewer. No fully automated adverse action on REJECT without the option to appeal.

Risk Scoring Architecture

The FlowAI risk score is a composite of three signals: (1) identity extraction confidence from the submitted documents, (2) sanctions screening result against OFAC, EU, and UN consolidated lists, and (3) document consistency checks. Each signal contributes a weighted sub-score. The final score (0–100) maps to: 0–30 APPROVE, 31–69 ESCALATE, 70–100 REJECT. Thresholds are configurable on Growth and Scale plans.

Sanctions Data Sources

List	Source	Refresh Cadence	Coverage
OFAC SDN	US Treasury Office of Foreign Assets Control	Daily	Specially Designated Nationals — individuals and entities
EU Consolidated	European Union External Action Service	Daily	EU consolidated list of persons, groups, and entities subject to EU financial sanctions
UN Consolidated	United Nations Security Council	Daily	UN consolidated list — all UNSC sanctions regimes

Contact & Legal

Security Contacts

Contact	Email	Use For
Security Team	security@flowai.polsia.app	Vulnerability reports, deletion requests, incident inquiries, DPA requests
Sales / Procurement	hello@flowai.polsia.app	MSA redlines, enterprise procurement questions, pricing, Scale plan
General	hello@flowai.polsia.app	Product questions, demos, onboarding

Legal Documents Available

- Data Processing Agreement (DPA): available to all paying customers. Request via security@flowai.polsia.app.
- Master Services Agreement (MSA): standard commercial agreement. Redlines considered on Growth and Scale plans.
- Privacy Policy: https://flowai-4-n41s.polsia.app/trust
- Security & Trust page (live): https://flowai-4-n41s.polsia.app/trust

Vulnerability Disclosure

FlowAI accepts responsible disclosure of security vulnerabilities. Contact security@flowai.polsia.app with a description of the vulnerability, steps to reproduce, and your preferred contact method. We will acknowledge within 24 hours and keep you updated as we investigate and remediate. We do not currently operate a paid bug bounty program, but we recognize coordinated disclosures publicly with the reporter's permission.

FlowAI Security & Compliance Pack — v1.0 — 2026-06-13