Vaipm Security Overview

Version 3.0 | Effective: June 6, 2026 | Classification: Public

1. Company Overview

Company	Vaigate, Inc.
Founded	May 29, 2026
Address	Nagareyama, Chiba, Japan
Service	Vaipm — AI Perception Monitoring Service
Security Contact	compliance@vaigate.com

2. Architecture Overview

Vaipm retrieves public information from the Customer's official website (HTML and PDF), sends queries to AI platforms to collect responses, performs analysis and judgment, and generates reports with translation.

2.1 Infrastructure

Component	Overview
Data Storage	AWS ap-northeast-1 (Tokyo). Encryption at rest using cloud provider encryption features
Portal	Vercel + Next.js. Encryption in transit (TLS 1.2+)
Authentication	Clerk (email/password)
Payment	Stripe. Card numbers are not stored by Vaigate
Local Inference	Some analysis runs within Vaigate-managed infrastructure. No external transmission
External AI APIs	OpenAI, Google Gemini, Anthropic Claude, Perplexity Sonar

3. Security Controls

Vaigate implements, or is in the process of implementing based on business scale, data nature, and risk, the following technical and organizational security measures.

3.1 Encryption

At rest: Cloud provider encryption features

In transit: TLS 1.2+ for primary external communications and production public endpoints

3.2 Access Control

Role-based access control (RBAC). Customer data logically separated by organization ID.

MFA (multi-factor authentication) applied to administrative accounts.

3.3 Logging and Monitoring

API and administrative operation logs collected. Review and alerting configured as appropriate. Log retention periods follow log type and service configuration.

3.4 Vulnerability Management

Regular dependency updates. Timely application of security patches.

3.5 Incident Response

Documented Incident Response Plan (IRP). We notify customers without undue delay, and within 72 hours where possible, upon becoming aware of a confirmed security incident affecting Customer Personal Data or a significant suspicion reasonably requiring notification. Details in the DPA and IRP.

4. External AI API Security

We use commercial AI API services under terms intended to prevent submitted data from being used for foundation model training. Retention, logging, and training policies are governed by each provider's API terms.

Structured prompts, input validation, and output validation are used to mitigate prompt injection risks.

Customer data is logically separated by organization ID and Track ID to reduce the risk of cross-customer data mixing or leakage.

5. Data Retention and Deletion

Customer data is retained for the period necessary for service delivery. After termination, target data in active production environments is deleted or rendered inaccessible within 30 days. Details in the DPA.

6. Compliance

Law / Standard	Status
APPI	Privacy Policy published. DPA available
GDPR	DPA and SCCs available. Controls in progress
SOC 2	Controls being developed with reference to SOC 2 criteria. Third-party audit timing considered based on business scale, customer requirements, and operational maturity

7. Subprocessors

A list of subprocessors used by Vaigate is available in the Subprocessor List.

8. Contact

Security inquiries: compliance@vaigate.com

Web: https://vaipm.ai