Vaipm Data Processing Agreement (DPA)

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

1. Definitions and Scope

(1) This Data Processing Agreement (the “DPA”) sets forth the terms under which Vaigate, Inc. (“Vaigate” or “we”) processes the Customer’s personal data in connection with the Vaipm service.

(2) This DPA forms part of the Vaipm Terms of Service (the “Terms”). In the event of conflict, this DPA prevails for data protection matters.

(3) “Customer Personal Data” means personal data that the Customer inputs into the Service or that Vaigate processes in connection with Service delivery.

(4) Terms such as “processing,” “controller,” “processor,” and “personal data” have the meanings given under applicable data protection law (APPI, GDPR, etc.).

2. Roles of the Parties

(1) Where Vaigate processes Customer Personal Data on the Customer’s instructions, Vaigate acts as a commissioned processor under APPI or a Processor under GDPR.

(2) For account management, billing, security, fraud prevention, and service operations, Vaigate may act as an independent controller.

3. Processing Activities

(1) Vaigate performs the following processing as necessary for Service delivery:

• Retrieval, text extraction, and indexing of public information from the Customer’s official website (HTML and PDF)

• Sending queries to AI platforms and collecting AI responses

• Analysis, summarization, judgment, and classification of AI responses

• Report generation, translation, and export

(2) Vaigate sends queries, analysis target names, competitor names, custom questions, AI responses, official site text, analysis results, translation text, and other necessary information to external AI APIs. Such information may include personal data.

(3) 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.

4. Customer Obligations

(1) The Customer is responsible for ensuring that it has the necessary legal basis, authority, and notices for personal data processed by Vaigate.

(2) The Customer shall not, without Vaigate’s prior consent, input sensitive personal information, government-issued IDs, financial account numbers, or other high-risk information unnecessary for the Service.

5. Security Measures

Vaigate implements, or is in the process of implementing based on business scale, data nature, and risk, technical and organizational security measures including encryption, access controls, log

monitoring, vulnerability management, and incident response. Details are available in the Security Overview.

6. Subprocessors

(1) The Customer authorizes Vaigate to engage subprocessors necessary for Service delivery.

(2) Vaigate will notify the Customer at least 30 days before adding a new subprocessor. The Customer may object in writing within 30 days of receiving notification.

(3) In cases of security, availability, legal compliance, or other urgent and reasonable grounds, Vaigate may temporarily engage an alternative subprocessor without 30-day prior notice and will notify the Customer as promptly as practicable.

(4) The current subprocessor list is available in the Subprocessor List.

7. Data Subject Rights

Where the Customer receives a data subject rights request relating to Customer Personal Data processed by Vaigate as Processor, Vaigate will provide reasonable assistance. Data subject requests should be directed through the Customer.

8. Data Retention and Deletion

(1) Vaigate retains Customer Personal Data for the period necessary for Service delivery.

(2) The Customer should export data before contract termination.

(3) After termination, Vaigate will delete or render inaccessible target data in active production environments within 30 days and provide reasonable confirmation of deletion. Target data includes account settings, Track settings, analysis results, reports, and other production data controlled by Vaigate.

(4) Logs, backups, billing records, and legally required records are retained per this DPA, the Privacy Policy, and applicable subprocessor terms.

9. Data Breach Notification

(1) Vaigate will notify the Customer 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.

(2) Where an APPI-reportable incident occurs, Vaigate will cooperate with the Customer and provide information reasonably necessary for preliminary reports and final reports.

10. Audit

Vaigate will respond to audit requests by providing security questionnaires, relevant policies, third-party audit reports (if available), and other reasonable information. On-site audits are limited to cases required by law or where a material data breach is reasonably suspected, and are conducted under separately agreed scope and terms.

11. International Data Transfers

Where Customer Personal Data is transferred outside Japan, Vaigate implements appropriate measures under APPI Article 28 and/or GDPR safeguards such as Standard Contractual Clauses (SCCs). Key destination countries are listed in the Subprocessor List.

12. Amendments

Vaigate may amend this DPA for changes in applicable law, service scope, or other reasonable grounds. Material changes will be communicated with reasonable notice by email, website posting, or other reasonable means. Changes that materially adversely affect Customer rights require separate consent.

13. Contact

Inquiries regarding this DPA: compliance@vaigate.com

Web: https://vaipm.ai