

Data Processing Addendum

Version 3.2

Processor terms for Customer Personal Data processed through the Meikai Services, including Annex I (processing details), Annex II (security measures), and Annex III (subprocessors).

Version: 3.2

Prepared for: meikai.ai customer agreements

Status: Simple form of Data Processing Addendum

This Data Processing Addendum (the "**DPA**") is entered into by and between:

- **MEIKAI LTD**, a private limited company incorporated under the laws of England and Wales, with company number **16607357** and registered office at **51h Wickham Road, London, England, SE4 1LT** ("**Meikai**"); and
- the customer identified in the applicable Master Services Agreement, Order Form, subscription agreement, or other written agreement governing the Services ("**Customer**").

This DPA forms part of, and is incorporated into, the agreement between the parties governing Customer's use of the Services (the "**Agreement**"). If there is any conflict between this DPA and the Agreement with respect to the Processing of Customer Personal Data, this DPA controls to that extent. If the SCCs, the UK Addendum, the IDTA, or other mandatory transfer terms apply to a Restricted Transfer, those terms control to the extent of any conflict solely for that transfer.

1. Definitions

For purposes of this DPA:

- "**Applicable Data Protection Law**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, where applicable, the GDPR, UK GDPR, the Swiss Federal Act on Data Protection, and applicable U.S. state privacy laws.
- "**Controller**" means the entity that determines the purposes and means of Processing Personal Data, including any equivalent concept such as "**Business**" where relevant.
- "**Customer Personal Data**" means Personal Data Processed by Meikai on behalf of Customer in connection with the Services.
- "**Data Subject Request**" means a request from a data subject to exercise a right under Applicable Data Protection Law.
- "**Personal Data**", "**Processing**", "**Processor**", "**Subprocessor**", and "**Personal Data Breach**" have the meanings given in Applicable Data Protection Law, including equivalent concepts such as "**Service Provider**" where relevant.
- "**Restricted Transfer**" means a transfer of Customer Personal Data to a country or recipient that requires an approved transfer mechanism under Applicable Data Protection Law.
- "**Services**" means the Meikai platform and related services provided under the Agreement, including brand visibility analytics, site and traffic analysis, prompt and response analysis, reporting, support, and related services described in the Agreement.
- "**SCCs**" means the standard contractual clauses approved by the European Commission under Implementing Decision (EU) 2021/914, as may be amended, replaced, or supplemented from time to time.
- "**UK Addendum**" means the United Kingdom International Data Transfer Addendum to the SCCs, as may be amended, replaced, or supplemented from time to time.

- **"IDTA"** means the United Kingdom International Data Transfer Agreement, as may be amended, replaced, or supplemented from time to time.

2. Scope and Roles

2.1 Appointment

Customer appoints Meikai to Process Customer Personal Data on Customer's behalf for the limited purposes described in the Agreement, this DPA, and Customer's documented instructions.

2.2 Roles

As between the parties:

- Customer acts as Controller of Customer Personal Data, except to the extent Applicable Data Protection Law provides otherwise.
- Meikai acts as Processor, or Service Provider where relevant, of Customer Personal Data.

2.3 Scope

This DPA applies only to Customer Personal Data that Meikai Processes on behalf of Customer in connection with the Services. Each party remains independently responsible for Personal Data it Processes as an independent Controller outside that scope, including ordinary business contact information used for account management, billing, contract administration, and legal compliance.

2.4 U.S. State Privacy Terms

To the extent required by applicable U.S. state privacy laws, Meikai will:

- Process Customer Personal Data only for the business purposes described in the Agreement and this DPA;
- not sell or share Customer Personal Data;
- not retain, use, or disclose Customer Personal Data except as permitted by the Agreement, this DPA, or applicable law; and
- provide reasonable assistance to Customer as required by Applicable Data Protection Law and reasonably appropriate to the Services.

2.5 Processing Details

The subject matter, duration, nature, and purpose of the Processing, and the categories of Customer Personal Data and data subjects, are described in **Annex I**.

3. Customer Obligations

Customer represents and warrants that:

- it has all rights, notices, consents, and other lawful bases required for Meikai to Process Customer Personal Data in connection with the Services;
- its instructions to Meikai comply with Applicable Data Protection Law; and

- it will not provide Meikai with special categories of Personal Data or Personal Data relating to children unless the parties expressly agree in writing that such Processing is required and appropriate safeguards are in place.

Customer remains responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which it was collected.

4. Meikai Obligations

Meikai will:

- Process Customer Personal Data only on Customer's documented instructions, as set out in the Agreement and this DPA, or as required by applicable law;
- promptly inform Customer if, in Meikai's opinion, an instruction infringes Applicable Data Protection Law;
- ensure that persons authorized to Process Customer Personal Data are subject to confidentiality obligations;
- implement appropriate technical and organizational measures designed to protect Customer Personal Data, as described in **Annex II**;
- provide reasonable assistance to Customer with Data Subject Requests and other obligations that apply to Processors under Applicable Data Protection Law, taking into account the nature of the Processing and the information available to Meikai;
- notify Customer without undue delay and, where feasible, within seventy-two (72) hours after becoming aware of a Personal Data Breach affecting Customer Personal Data; and
- upon termination of the Agreement, delete or return Customer Personal Data within thirty (30) days of Customer's request, unless retention is required by applicable law.

Meikai may retain archived backup copies until deleted or overwritten in the ordinary course of business, provided they remain protected and are only restored where necessary for disaster recovery or legal compliance.

5. Subprocessors

Customer grants Meikai a general authorization to engage Subprocessors in connection with the Services, provided that Meikai:

- enters into a written agreement with each Subprocessor imposing data protection obligations appropriate to the services performed by that Subprocessor; and
- remains responsible for the Subprocessor's Processing of Customer Personal Data to the extent required by Applicable Data Protection Law.

Meikai will maintain and make available a current list of Subprocessors, whether in **Annex III** or through a separate notice or webpage made available to Customer.

If Meikai adds or replaces a Subprocessor in a manner that materially affects the Processing of Customer Personal Data, Meikai will give notice and Customer may object on reasonable data protection

grounds. If the parties cannot resolve the objection in good faith, Customer may terminate the affected portion of the Services.

6. International Transfers

Where Meikai makes a Restricted Transfer, Meikai will ensure that an appropriate transfer mechanism is in place under Applicable Data Protection Law.

Where required, the parties agree that:

- the SCCs apply to transfers subject to the GDPR;
- the UK Addendum or IDTA applies to transfers subject to the UK GDPR; and
- the SCCs, with any required Swiss adaptations, apply to transfers subject to Swiss data protection law.

Customer is the data exporter and Meikai is the data importer where that allocation is required for the relevant transfer mechanism.

7. Data Subject Requests and Audit

If Meikai receives a Data Subject Request relating to Customer Personal Data, Meikai will promptly notify Customer unless legally prohibited from doing so and will not respond except on Customer's instructions or as required by law.

Upon reasonable written request, Meikai will make available information reasonably necessary to demonstrate compliance with this DPA, including through provision of third-party audit reports where available. If that information is not sufficient, Customer may request a reasonable audit no more than once per year, subject to appropriate confidentiality obligations and reasonable limits designed to protect security, confidentiality, and other customers' information.

8. Liability, Term, and Miscellaneous

The liability of each party arising out of or relating to this DPA is subject to the exclusions and limitations of liability set out in the Agreement, except to the extent such limitations are not permitted under Applicable Data Protection Law.

This DPA takes effect on the effective date of the Agreement or the date it is executed, whichever is earlier, and remains in effect for as long as Meikai Processes Customer Personal Data under the Agreement.

Except as expressly modified by this DPA, the Agreement remains in full force and effect. This DPA may be executed electronically and in counterparts.

Privacy notices and communications under this DPA will be sent to:

- **Meikai:** legal@meikai.ai, with a copy to support@meikai.ai
- **Customer:** the contact set out in the Agreement, unless Customer designates another privacy contact in writing.

This DPA is governed by the governing law and dispute resolution provisions set out in the Agreement, except to the extent Applicable Data Protection Law requires otherwise.

Signature Block

MEIKAI LTD

By: _____

Name: _____

Title: _____

Date: _____

CUSTOMER

By: _____

Name: _____

Title: _____

Date: _____

Annex I - Details of Processing

A. Subject Matter and Duration

Meikai Processes Customer Personal Data for the duration of the Agreement and for any limited post-termination period reasonably required to complete deletion, return, backup rotation, or legal retention obligations.

B. Nature and Purpose of the Processing

Meikai may Process Customer Personal Data to:

- provide the Services to Customer;
- collect and analyze website visit and referral events, including traffic from AI platforms;
- collect and analyze crawler and CDN log data relating to Customer's websites;
- generate dashboards, reports, and analytics for Customer;
- provide onboarding, implementation, support, troubleshooting, and maintenance; and
- secure, monitor, and maintain the Services.

For clarity, the Services are designed to measure website visits, referrals, and crawler activity, not to identify individual end users or build consumer profiles. However, some data processed through the Services may still constitute Personal Data under Applicable Data Protection Law.

C. Categories of Data Subjects

Depending on Customer's use of the Services, data subjects may include:

- Customer personnel, users, administrators, employees, contractors, and agents;
- visitors to Customer's websites or digital properties;
- individuals whose Personal Data appears in content, URLs, logs, prompts, or other materials submitted to or analyzed through the Services.

D. Categories of Customer Personal Data

Depending on Customer's use of the Services, Customer Personal Data may include:

- account and contact data such as name, business email address, role, and organization;
- support and implementation communications;
- technical and event data such as user agent, timestamps, referrer, page URL, and other request metadata;
- CDN log data such as IP address, user agent, referrer, requested URL, and similar request-level fields; and

- optional identifiers sent by Customer, such as internal user or event identifiers, where Customer chooses to include them.

E. Sensitive Data

The Services are not intended for the Processing of special categories of Personal Data or Personal Data relating to children.

F. Processing Location

Customer Personal Data processed through the Services is primarily hosted in the European Union, in Google Cloud region **europa-west1** (Belgium). This includes Cloud Run, Cloud Storage (raw CDN logs), BigQuery (analytics), and related Google Cloud services used to operate the Services. Transfers outside the European Union may occur only where required for support or resilience and are subject to appropriate safeguards under Section 6.

G. Retention

- **Raw CDN log files.** Raw CDN log files received from Customer's CDN provider are stored in Cloud Storage and automatically deleted thirty (30) days after receipt.
- **Crawler analytics.** Only requests whose user agent matches a known AI or search crawler are retained in Meikai's analytics tables. All other requests, including requests from human visitors, are discarded and are not retained beyond the raw log files described above.
- **Client IP addresses.** IP addresses contained in CDN log data are used only to verify that a request identified as a crawler originates from that crawler's published IP ranges. Customer may exclude the client IP field from the CDN log data it sends to Meikai, in which case this verification is not performed.
- **Tracking pixel.** The tracking pixel does not record the visitor's IP address and does not set cookies.
- **Account and support data.** Account, contact, and support data is retained for the term of the Agreement and the thirty (30) day deletion or return period set out in Section 4.

Archived backup copies of any of the above remain subject to Section 4.

Annex II - Technical and Organizational Security Measures

Meikai will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data, including, where appropriate to the Services and the risks presented by the Processing:

- multi-factor authentication for administrative access to production systems;
- role-based access controls with periodic access review;
- encryption in transit using TLS 1.2 or higher and encryption at rest where appropriate;
- access logging and monitoring for production systems where appropriate;
- incident response procedures with defined escalation paths;
- logical access controls and least-privilege access;
- confidentiality obligations for authorized personnel;
- vulnerability management and patching processes;
- backup and recovery measures; and
- procedures for detecting, responding to, and remediating security incidents.

Meikai may update these measures from time to time, provided that the overall level of protection is not materially reduced.

Annex III - Subprocessors

Meikai uses Google Cloud Platform to host and operate the Services. Meikai may update this Annex III from time to time and will make any updated Subprocessor information available to Customer.

Subprocessor	Service Description	Categories of Personal Data	Processing Location(s)	Transfer Mechanism
Google Cloud	Cloud hosting and infrastructure services provided by Google, including Cloud Run, Cloud Storage, BigQuery, Pub/Sub, Cloud Logging, and related Google Cloud services used to operate the Services	Account data, support data, tracking event data, CDN log data, and related request-level technical metadata processed through the Services	European Union (Google Cloud region europe-west1 , Belgium), including Cloud Storage and BigQuery. Transfers outside the EU only where required for support or resilience, with appropriate safeguards.	As applicable, adequacy decision, SCCs, UK Addendum, IDTA, or other valid transfer mechanism under Applicable Data Protection Law