Data Processing Agreement (DPA)

This Data Processing Agreement ("DPA") forms part of the Terms of Service (the "Agreement") between:

(1)Code Cube B.V. trading under the name Code-Cube.io, Grebbeberglaan 15, 3527 VX Utrecht, The Netherlands ("Processor"); and

(2) The Entity identified as the Customer in the Agreement ("Controller").

1. Definitions

- "Data Protection Laws" means the GDPR (EU 2016/679) and any national implementing laws.
- "Personal Data", "Processing", and "Data Subject" shall have the meanings given to them in the GDPR.
- "Services" means the Tag Monitoring and DataLayer Guard services provided by Processor.

2. Subject matter and duration

- Subject matter: The subject matter of the processing is the provision of the Services.
- Duration: The duration of the processing is the term of the Agreement plus the period until all data is deleted or returned.
- Nature/Purpose: Processing to monitor website tag health and ensure dataLayer (or any other JSON frontend object) integrity.
- Categories of data subjects: Customers of the controller (end-users of Controller's website).
- Types of personal data: IP addresses, unique identifiers (cookies), and any data points monitored within the dataLayer as configured by the Controller.

3. Processor's obligations

The Processor agrees to:

1. Instructions: Process personal data only on documented instructions from the Controller.
2. Confidentiality: Ensure that persons authorized to process the data have committed themselves to confidentiality.

3. Security: Implement appropriate technical and organizational measures (e.g., encryption, firewalls) as required by Article 32 GDPR.
4. Assistance: Assist the Controller in responding to data subjects' requests (Rights of Access, Erasure, etc.).
5. Audit: Make available to the Controller all information necessary to demonstrate compliance and allow for audits.

4. Sub-processors

The Controller grants general authorization to the Processor to engage sub-processors (e.g. Google Cloud Platform, SendGrid).

- A list of current sub-processors is maintained in the Processor's Privacy Policy.
- The Processor shall inform the Controller of any intended changes to sub-processors, giving the Controller the right to object.

5. International data transfers

Any transfer of data outside the European Economic Area (EEA) shall be governed by Standard Contractual Clauses (SCCs) or the EU-US Data Privacy Framework, ensuring an adequate level of protection.

6. Data deletion

Upon termination of the Services, the Processor shall, at the choice of the Controller, delete or return all personal data, unless local law requires storage of the data.

Annex 1: Technical and organizational measures (TOMs)

The Processor maintains the following security standards:

- Encryption: Data encrypted in transit via TLS 1.2+ and at rest via AES-256.
- Access: "Least Privilege" access model for all employees.
- Integrity: Regular backups and monitoring for unauthorized access.
- Anonymization: Where possible, IP addresses are anonymized before processing.