DataDoe

DATA PROCESSING ADDENDUM

For customers acting as data controllers.

This Data Processing Addendum forms part of the Terms of Service between DataDoe, Inc. and you, our customer. It governs how DataDoe processes personal data on your behalf and incorporates the EU Standard Contractual Clauses and the UK International Data Transfer Addendum where applicable.

EFFECTIVE
29 June 2026

ISSUER
DataDoe, Inc.

CONTACT
contact@datadoe.com

JURISDICTION
Delaware, USA

V 2026.06.29

CONTENTS

Clauses & Annexes

ANNEXES

Annex D — Standard Contractual Clauses

01 — DEFINITIONS

Words that have a specific meaning here.

Capitalized terms not defined in this DPA have the meanings given to them in the Agreement (the Terms of Service between you and DataDoe). For purposes of this DPA:

- **"Applicable Data Protection Law"** means the EU General Data Protection Regulation 2016/679 (**"GDPR"**), the UK Data Protection Act 2018 and UK GDPR (**"UK GDPR"**), the Swiss Federal Act on Data Protection, the California Consumer Privacy Act as amended by the CPRA (**"CCPA"**), and any other applicable laws governing the processing of personal data.
- **"Personal Data"**, **"Process"**, **"Controller"**, **"Processor"**, **"Data Subject"**, **"Sub-processor"**, **"Personal Data Breach"**, and **"Supervisory Authority"** have the meanings given in the GDPR (or the equivalent terms under other Applicable Data Protection Law).
- **"Customer Personal Data"** means Personal Data Processed by DataDoe on behalf of Customer in connection with providing the Service.
- **"Standard Contractual Clauses"** or **"SCCs"** means the Module Two (Controller-to-Processor) standard contractual clauses adopted by European Commission Decision (EU) 2021/914 of 4 June 2021.
- **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office, version B1.0.

---

02 — SCOPE & ROLES

Who is the controller and who is the processor.

For Customer Personal Data processed under this DPA:

- **Customer is the Controller** (or where Customer is itself a processor acting on behalf of a third-party controller, Customer is a Processor and DataDoe is a Sub-processor).
- **DataDoe is the Processor** and processes Customer Personal Data only on Customer's documented instructions, as set out in the Agreement, this DPA, and any further written instructions accepted in writing by DataDoe.

This DPA applies to the extent DataDoe processes Personal Data in respect of which Applicable Data Protection Law applies and where Customer is the Controller (or upstream Processor).

---

03 — SUBJECT MATTER & DURATION

What is processed and for how long.

The **subject matter** of the processing is the provision of the Service described in the Agreement.

The **duration** of the processing is the term of the Agreement, plus the period after termination during which DataDoe retains Customer Personal Data in accordance with Section 11.

The **nature, purpose, types of Personal Data, and categories of Data Subjects** are described in Annex A.

04 — PROCESSOR OBLIGATIONS

What DataDoe commits to as Processor.

DataDoe shall:

- **Process Customer Personal Data only on documented instructions** from Customer, including with regard to transfers to a third country or international organization, unless required by law to which DataDoe is subject. Where required, DataDoe will inform Customer of such legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
- **Notify Customer** if, in DataDoe's opinion, an instruction infringes Applicable Data Protection Law.
- Ensure that **personnel authorized to process Customer Personal Data are bound by appropriate confidentiality obligations**, whether contractual or statutory.
- Implement and maintain **appropriate technical and organizational measures** as set out in Annex B, to ensure a level of security appropriate to the risk in accordance with Article 32 GDPR.
- **Engage Sub-processors** only in accordance with Section 6 and Annex C.
- **Assist Customer** by appropriate technical and organizational measures, insofar as possible, in fulfilling Customer's obligation to respond to requests from Data Subjects under Chapter III of the GDPR (or equivalent rights under other Applicable Data Protection Law).
- **Assist Customer** in ensuring compliance with the obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to DataDoe.
- At Customer's choice, **delete or return all Customer Personal Data** after the end of the provision of services relating to processing, in accordance with Section 11.
- **Make available** to Customer all information necessary to demonstrate compliance with Article 28 GDPR, and allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer, in accordance with Section 10.

05 — CONTROLLER OBLIGATIONS

What Customer commits to as Controller.

Customer shall:

- Ensure that it has, and will continue to have, the **legal basis** required by Applicable Data Protection Law for the processing of Customer Personal Data by DataDoe in accordance with the Agreement and this DPA, including providing any required notices to and obtaining any required consents from Data Subjects.
- Be responsible for the **accuracy, quality, and legality** of Customer Personal Data and the means by which Customer acquired Customer Personal Data.
- Ensure that **Customer's instructions** to DataDoe comply with Applicable Data Protection Law.
- Comply with all **laws applicable to Customer** as a Controller (or upstream Processor), including obligations relating to the rights of Data Subjects, transparency, and data security.

06 — SUB-PROCESSORS

How DataDoe uses other vendors.

Customer provides **general written authorization** for DataDoe to engage Sub-processors to assist in providing the Service. DataDoe's current Sub-processors are listed in Annex C.

Flow-down obligations

DataDoe shall enter into a written contract with each Sub-processor that imposes **data protection obligations equivalent to those set out in this DPA**, including those relating to the security of the processing and confidentiality.

Changes to Sub-processors

DataDoe may engage new Sub-processors or replace existing ones from time to time. The current authoritative list of Sub-processors is maintained at www.datadoe.com/legal/data-processing-agreement (Annex C). Customer is responsible for monitoring this page for updates.

Right to object

Customer may object to a new or replacement Sub-processor on **reasonable data protection grounds** by written notice to contact@datadoe.com within 30 days of the change appearing on the published list. If Customer's objection cannot be reasonably resolved, Customer may, as its sole and exclusive remedy, terminate the affected portion of the Service with a pro-rated refund of prepaid fees.

Liability

DataDoe remains **fully liable** to Customer for the performance of each Sub-processor's data protection obligations.

07 — INTERNATIONAL TRANSFERS

Cross-border processing safeguards.

DataDoe is established in the United States, and Customer Personal Data is processed primarily on AWS and GCP infrastructure located in the United States. Where Customer Personal Data is transferred from the European Economic Area, the United Kingdom, or Switzerland to a country that has not been the subject of an adequacy decision, the following safeguards apply.

EU transfers

The parties incorporate by reference the **Module Two (Controller-to-Processor) Standard Contractual Clauses**, with the following elections:

- **Clause 7 (Docking Clause)**: applicable.
- **Clause 9 (Use of sub-processors)**: option 2 (general written authorization), with notice period as set out in Section 6.
- **Clause 11 (Redress)**: optional independent dispute resolution body not selected.
- **Clause 17 (Governing law)**: the law of Ireland.
- **Clause 18 (Forum and jurisdiction)**: the courts of Ireland.
- **Annexes I, II, III** to the SCCs are completed by reference to Annex A, Annex B, and Annex C of this DPA respectively.

UK transfers

The **UK International Data Transfer Addendum** (version B1.0) is incorporated by reference and modifies the EU SCCs as necessary for UK transfers.

Swiss transfers

For transfers subject to the Swiss FADP, references to GDPR shall be read as references to the FADP, references to EU Member States shall include Switzerland, and the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.

08 — DATA SUBJECT REQUESTS

Helping you respond to Data Subjects.

DataDoe shall, taking into account the nature of the processing, assist Customer by appropriate technical and organizational measures, insofar as possible, to fulfill Customer's obligations to respond to requests by Data Subjects to exercise their rights under Applicable Data Protection Law.

Where DataDoe receives a request directly from a Data Subject in relation to Customer Personal Data, DataDoe will (unless legally prohibited) **forward the request to Customer without undue delay** and will not respond to the Data Subject except as instructed by Customer or required by law.

09 — PERSONAL DATA BREACH

What happens if data is exposed.

DataDoe shall **notify Customer without undue delay, and in any event within 48 hours of confirmed awareness**, of any Personal Data Breach affecting Customer Personal Data. The notification shall include, to the extent then known:

- The nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and records concerned;
- The name and contact details of DataDoe's point of contact;
- The likely consequences of the Personal Data Breach;
- The measures taken or proposed to address the Personal Data Breach and to mitigate its possible adverse effects.

DataDoe will **cooperate with Customer** and provide reasonable assistance in the investigation, mitigation, and remediation of the breach. DataDoe does not undertake to make notifications to Supervisory Authorities or Data Subjects on Customer's behalf — those notifications remain Customer's responsibility as Controller.

10 — AUDITS & INSPECTIONS

How Customer can verify compliance.

Customer may, once per calendar year and on **at least 30 days' prior written notice**, audit DataDoe's compliance with this DPA. Audits shall be:

- Conducted during normal business hours and in a manner that minimizes disruption to DataDoe's operations;
- Subject to reasonable confidentiality obligations;
- Limited in scope to the processing of Customer Personal Data and DataDoe's obligations under this DPA.

Customer may rely on **third-party audit reports** (such as SOC 2 or ISO 27001 reports, once available) in lieu of an on-site audit where these adequately address the scope of the audit. Customer bears the costs of the audit, except where the audit reveals material non-compliance, in which case DataDoe bears the reasonable costs.

If a Supervisory Authority requires an audit or inspection in connection with Customer Personal Data, DataDoe will cooperate as required by Applicable Data Protection Law.

11 — RETURN & DELETION

What happens to data when the contract ends.

Upon termination or expiry of the Agreement, DataDoe shall, at Customer's choice exercised in writing within 30 days of termination, either:

- **Return** Customer Personal Data to Customer in a structured, commonly used, machine-readable format; or
- **Delete** Customer Personal Data from DataDoe's active systems.

In either case, DataDoe shall delete Customer Personal Data within **30 days of termination**, except where retention is required by applicable law. Backups containing residual data are overwritten in accordance with DataDoe's standard backup rotation. Security and audit logs may be retained in accordance with Section 8 of the Agreement.

For **buyer PII received from Amazon**, deletion occurs no later than 30 days after order delivery, in accordance with Amazon's SP-API Data Protection Policy.

12 — CCPA-SPECIFIC TERMS

For Customers subject to the CCPA.

For Personal Data subject to the CCPA, DataDoe acts as a **"Service Provider"** as that term is defined in the CCPA. DataDoe shall not:

- **Sell** or **share** Personal Data as those terms are defined under the CCPA;
- Retain, use, or disclose Personal Data for any purpose other than the specific purpose of providing the Service set out in the Agreement, including retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Service;
- Retain, use, or disclose Personal Data outside the direct business relationship between DataDoe and Customer;
- Combine Personal Data received from or on behalf of Customer with Personal Data received from or on behalf of any other person, or collected from DataDoe's own interaction with consumers, except as permitted by the CCPA.

DataDoe certifies that it understands the restrictions in this Section 12 and shall comply with them.

13 — LIABILITY

How liability is allocated.

Each party's liability arising out of or in connection with this DPA, whether in contract, tort, or under any other theory of liability, is subject to the **limitations and exclusions of liability set out in the Agreement**, and any reference to a party's liability means aggregate liability of that party under the Agreement and this DPA combined.

```
Nothing in this DPA limits or excludes liability that cannot be limited or excluded under Applicable Data Protection Law, including liability under Article 82 GDPR for damage suffered by Data Subjects, or as required by the SCCs.
```

14 — TERM & TERMINATION

How long this DPA is in force.

This DPA takes effect on the date Customer accepts the Agreement (or executes this DPA, whichever is later) and remains in effect for the duration of the Agreement. Provisions of this DPA that by their nature are intended to **survive termination** — including but not limited to Sections 11 (Return & Deletion), 10 (Audits), 13 (Liability), and 15 (Order of Precedence) — shall survive termination of the Agreement.

15 — ORDER OF PRECEDENCE

Which terms win if they conflict.

In the event of any conflict or inconsistency between the documents governing the processing of Personal Data, the following order of precedence applies (highest first):

- The **Standard Contractual Clauses** (where applicable to a given transfer);
- The **UK International Data Transfer Addendum** (where applicable);
- This **Data Processing Addendum**;
- The **Agreement** (including the Terms of Service and Privacy Policy).

This precedence applies only with respect to matters of personal data processing. For all other matters, the order set out in the Agreement controls.

16 — MISCELLANEOUS

Closing terms.

Governing law. Except where the SCCs require otherwise, this DPA is governed by the laws of the State of Delaware, without regard to its conflict of laws rules. The choice-of-law and jurisdiction provisions of the SCCs and UK Addendum apply to their own subject matter.

Severability. If any provision of this DPA is held to be invalid, illegal, or unenforceable, that provision shall be severed and the remaining provisions shall continue in full force and effect.

No modification. This DPA may only be modified by a written instrument signed by both parties, or by an updated version published by DataDoe with at least 30 days' prior written notice to Customer.

Notices. Notices under this DPA shall be sent to contact@datadoe.com in the case of DataDoe, and to the email address on Customer's account in the case of Customer.

Entire agreement. This DPA, together with the Agreement, constitutes the entire agreement between the parties with respect to the processing of Customer Personal Data and supersedes any prior arrangements, whether oral or written.

ANNEX A — DETAILS OF PROCESSING

Categories, purposes, and durations.

Categories of Data Subjects

- Customer's authorized users (employees, contractors, agency staff) who access the Service
- Buyers of products sold through Customer's Amazon accounts, where Customer has enabled the optional Amazon PII access add-on

Categories of Personal Data

- **Authorized user data** — name, email address, authentication credentials, role, activity logs
- **Buyer PII from Amazon orders** (only where PII access add-on enabled) — name, shipping address, order metadata
- **Order, advertising, inventory, listings, and brand analytics data** from Amazon Seller Central, Vendor Central, and Amazon Ads
- **Usage data** — MCP queries, REST API requests, AI prompts, exports, and platform activity
- **Technical data** — device information, browser type, IP address

Special Categories of Personal Data

None. The Service is not designed to process special categories of personal data within the meaning of Article 9 GDPR.

Nature of Processing

Collection, recording, organization, structuring, storage, retrieval, consultation, use, disclosure by transmission (e.g., to authorized AI clients via MCP, to BigQuery datasets you operate), alignment, restriction, erasure, and destruction.

Purpose of Processing

Providing the Service to Customer in accordance with the Agreement, including delivery of pre-built reports, REST API, MCP server, BigQuery dataset sharing, and (where authorized) write operations on Customer's Amazon accounts.

Frequency of Transfer

Continuous, for the duration of the Agreement.

Duration of Processing

- **General Customer Personal Data** — for the term of the Agreement plus 30 days after termination, except where longer retention is required by law.
- **Buyer PII received from Amazon** — no longer than 30 days after order delivery, except where longer retention is required by law.
- **Security and audit logs** — minimum 12 months, scrubbed of PII where not legally required.

ANNEX B — TECHNICAL AND ORGANIZATIONAL MEASURES

How DataDoe secures the processing.

DataDoe implements and maintains the technical and organizational measures set out below, which are designed to ensure a level of security appropriate to the risk in accordance with Article 32 GDPR. DataDoe takes reference from **ISO/IEC 27001**, **ISO/IEC 27002**, and the **NIST Cybersecurity Framework**.

Encryption

- Data in transit: **HTTPS with TLS 1.3** on internal and external networks
- Data at rest: **AES-256-GCM** on AWS and GCP storage

Access & credential management

- Multi-factor authentication required for all administrative and cloud access
- Least-privilege role-based access via AWS IAM and GCP IAM; no shared admin accounts
- Secrets, API keys, and database credentials stored in **AWS Secrets Manager** — never hardcoded in source
- Quarterly access reviews; access revoked within 24 hours of personnel termination
- Password policy: minimum 12 characters, no reuse of the last 10, annual rotation

Network & application security

- Public S3 buckets blocked; bucket-level encryption enforced; Secure Transport condition required
- Segregated test and production environments; changes pass through code review and CI/CD gating
- Dark-web monitoring for company domains and employee email accounts

Logging & monitoring

- Access, event, and security logs retained for a minimum of 12 months
- Logs are scrubbed of PII where not legally required
- Logs are protected against unauthorized access and tampering

Pseudonymization & data minimization

- Buyer PII from Amazon is only retrieved where Customer has explicitly enabled the optional add-on
- Personal data is tagged at the source and logically isolated by tenant
- Logs avoid storing PII where not strictly necessary

Resilience, backup, and recovery

- Automated backups of production data with defined retention windows
- Annual testing of backup restoration procedures
- Multi-AZ deployment for critical production components

Personnel

- Mandatory security awareness training at onboarding and annually, covering PII handling, phishing/social engineering, and incident reporting
- Confidentiality obligations included in every employment and contractor agreement

Incident response

- Documented Incident Management Plan covering detection, classification, containment, eradication, recovery, and post-incident review
- Plan reviewed at least every six months and after any material infrastructure or system change
- Defined point of contact for security incidents: contact@datadoe.com

ANNEX C — APPROVED SUB-PROCESSORS

Vendors authorized to process Customer Personal Data.

Customer authorizes DataDoe to engage the following Sub-processors. Each is contractually bound by confidentiality and data-protection obligations consistent with this DPA.

SUB-PROCESSOR	PURPOSE	REGION
Amazon Web Services, Inc.	Hosting, compute, storage (S3, RDS, DynamoDB), secrets management	United States
Google LLC (Google Cloud Platform)	BigQuery dataset sharing, Cloud Storage	United States
Stripe, Inc.	Payment processing & subscription billing	United States
AWS Real User Monitoring	Application performance & error observability	United States
Anthropic, OpenAI, Google	AI model inference for in-product features (no training on customer data)	United States

The current authoritative list is maintained at datadoe.com/legal/data-processing-agreement. Customer is responsible for monitoring it for changes. The right to object to a new or replacement Sub-processor is set out in Section 6.

ANNEX D — STANDARD CONTRACTUAL CLAUSES

Cross-border transfer mechanism.

The **Module Two (Controller-to-Processor) Standard Contractual Clauses** adopted by European Commission Decision (EU) 2021/914 of 4 June 2021 are incorporated into this DPA by reference and form an integral part of it, subject to the elections set out in Section 7.

The **UK International Data Transfer Addendum** (version B1.0) issued by the UK Information Commissioner's Office is also incorporated by reference and modifies the EU SCCs as necessary for UK transfers.

For the purposes of the SCCs:

- **Data exporter**: Customer
- **Data importer**: DataDoe, Inc.
- **Annex I.A (List of parties)**: as identified in the Agreement and in this DPA
- **Annex I.B (Description of transfer)**: as set out in Annex A
- **Annex I.C (Competent supervisory authority)**: the supervisory authority of the EU Member State in which the data exporter is established, or — where the data exporter is not established in an EU Member State — the Irish Data Protection Commission
- **Annex II (Technical and organizational measures)**: as set out in Annex B
- **Annex III (List of sub-processors)**: as set out in Annex C

A counter-signed copy of the SCCs is available on written request to contact@datadoe.com.

> By accepting this DPA, both parties agree to the SCCs and UK Addendum as if they had been signed on the Effective Date of this DPA. In the event of any conflict between this DPA and the SCCs/UK Addendum, the SCCs/UK Addendum prevail in respect of cross-border transfers.