Data Processing Addendum

Effective Date: 2026-04-17 · **Last Updated:** 2026-04-17

This Data Processing Addendum ("DPA") is incorporated into and supplements the Cloud Services Agreement ("Agreement") between you ("Customer") and Schematic Inc. ("Provider") governing Customer's purchase and use of Provider's services.

1. PURPOSE AND SCOPE

In the course of providing the Services to Customer under the Agreement, Provider will Process Customer Data on Customer's behalf. Customer Data may include Personal Data. Exhibit A describes the subject matter and details of processing.

This DPA reflects the parties' agreement relating to the Processing of Customer Data in accordance with the requirements of Data Protection Laws and Regulations. This DPA accounts for the nature of the processing pursuant to the Agreement and describes the appropriate technical and organizational measures taken by Provider in processing Personal Data. This DPA will control in the event of any conflict with the Agreement.

2. DEFINITIONS

1. **"Customer Data"** means all Customer data that Provider Processes on Customer's behalf while providing the Services. Customer Data does not include Service Data.

2. **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* as amended by the California Privacy Rights Act of 2020, and applicable implementing regulations, all as amended from time to time.

3. **"Data Controller"** means the entity that determines the purposes and means of Processing of Personal Data.

4. **"Data Processor"** means the entity that Processes Personal Data on behalf of the Data Controller, including as applicable any "service provider" as that term is defined in the CCPA.

5. **"Data Protection Laws and Regulations"** means any data protection laws and regulations applicable to the Processing of Personal Data under the Agreement, including the applicable laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states.

6. **"Data Subject"** means the individual to whom Personal Data relates.

7. **"Personal Data"** means any information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, to an identified or identifiable individual.

8. **"Processing"**, **"Processes"** or **"Process"** means any operation or set of operations performed upon Personal Data whether or not by automated means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, erasure, or destruction.

9. **"Services"** means the services that Provider provides to Customer under the Agreement.

10. **"Standard Contractual Clauses"** means the controller to processor standard contractual clauses for transfers of personal data to third countries which do not show an adequate level of data protection as approved by the European Commission decision 2021/914, dated June 4, 2021, and incorporated herein by reference.

11. **"Subprocessor"** means Provider's Affiliates or other third-party service providers that Process Customer Data for Provider in connection with the Services.

12. **"Service Data"** means data generated by or collected in connection with Customer's and its authorized users' use of the Services, including account identifiers, configuration settings, product telemetry, feature usage events, API call metadata, and diagnostic and performance data. Service Data may include Personal Data relating to Customer's administrative users.

3. PROCESSING OF CUSTOMER DATA

3.1 Data Processing Roles

As between Provider and Customer, Customer is the Data Controller of Customer Data and Provider is the Data Processor. Customer controls the categories of Data Subjects and Personal Data Processed under the Agreement and provides such Personal Data to Provider for business purposes only. Customer is solely responsible for the accuracy, quality, and legality of the Customer Data and the means by which it acquired the Customer Data.

3.2 Data Processing Instructions

This DPA and the Agreement are Customer's complete and final instructions to Provider for the Processing of Customer Data and the transfer of Customer Data to any country or territory reasonably necessary to provide the Services. Provider and Customer must agree on any additional or alternate instructions. Provider will inform Customer if, in Provider's opinion, Customer's instructions violate Data Protection Laws and Regulations. Provider will process Customer Data in accordance with the Agreement (including all documents incorporated in the Agreement), and to comply with other reasonable instructions Customer provides to Provider (including by email) where its instructions are consistent with the Agreement.

3.3 Service Data

This DPA does not apply to Service Data. With respect to Service Data that constitutes Personal Data, Provider acts as an independent Data Controller and Processes such data for its own legitimate business purposes, including operating, improving, securing, and supporting the Services. Provider's collection and use of Service Data is governed by Provider's Privacy Policy, available at `https://schematichq.com/privacy`. Provider will handle Service Data in compliance with applicable Data Protection Laws and Regulations in its capacity as an independent Controller.

3.4 CCPA Restrictions

Provider processes Customer Data as a "service provider" under the CCPA. Provider does not sell or share (as those terms are defined in the CCPA) Customer Data with third parties. Provider will not collect, retain, use, or disclose Customer Data, or combine Customer Data with other Personal Data (A) for any purpose other than for

the specific business purpose set forth in the Agreement, or (B) outside the direct business relationship between Provider and Customer. Provider will disclose Customer Data if required to do so by applicable law, in which case Provider will inform Customer in advance unless Provider is prohibited from doing so. Provider certifies that it understands and will comply with the restrictions in this Section 3.

4. RIGHTS OF DATA SUBJECTS

4.1 Correction, Blocking and Deletion

If Customer does not have the ability to amend, block, or delete Customer Data as required by Data Protection Laws and Regulations, Customer can provide written instructions to Provider to act on its behalf. Provider will follow Customer's instructions to the extent they are technically feasible and legally permissible. Provider will action such instructions within thirty (30) days of receipt.

4.2 Data Subject Requests

If permitted, Provider will promptly notify Customer of any request from a Data Subject for access to, correction, amendment or deletion of that Data Subject's Personal Data. Provider will not respond to any Data Subject request without Customer's prior written consent, except to confirm that the request relates to Customer.

4.3 Cooperation and Assistance

Provider will assist Customer to address any request, complaint, notice, or communication Customer receives relating to Provider's processing of Customer Data received from (A) a Data Subject whose Personal Data is contained within the Customer Data, or (B) any applicable data protection authority. Provider will also assist Customer with its reasonable requests for information to confirm compliance with this DPA or to conduct a privacy impact assessment.

5. PROVIDER PERSONNEL

5.1 Confidentiality

Provider will inform its personnel engaged in the Processing of Customer Data about the confidential nature of such Customer Data. These personnel receive appropriate training on their responsibilities and are subject to written agreements with confidentiality obligations that survive the termination of their relationship with Provider.

5.2 Limitation of Access

Provider ensures that access to Customer Data is limited to those personnel who require access to Process Customer Data under the Agreement.

6. SUBPROCESSORS

6.1 Authorization

Customer expressly authorizes Provider to use Subprocessors to perform specific services on Provider's behalf to enable Provider to perform Provider's obligations under the Agreement. Provider's current Subprocessors are

listed in Exhibit D and are also published at `https://schematichq.com/subprocessors`. Provider has written agreements with its Subprocessors that contain obligations substantially similar to Provider's obligations under this DPA. Provider is liable for any breach of this DPA caused by an act or omission of its Subprocessors.

6.2 Notice and Objection

Provider will give notice of any new Subprocessor at least thirty (30) days before that Subprocessor begins processing Customer Data. Notice will be given by (A) publishing the new Subprocessor at `https://schematichq.com/subprocessors`, (B) sending an email to all subscribers of the notification list maintained at that page, and (C) where Customer has designated a notice contact in its account settings, sending an email to that contact.

For the avoidance of doubt, the following do not constitute the engagement of a new Subprocessor and do not trigger the notice requirements in this Section 6.2: (i) changes to the internal vendors, infrastructure, or sub-subprocessors used by an existing Subprocessor; (ii) changes to an existing Subprocessor's corporate structure, affiliates, or legal entity that do not change the nature or location of processing; and (iii) the addition of an existing Subprocessor's capability in a region or facility that is not used to process Customer Data.

Notwithstanding the notice period above, Provider may engage a new Subprocessor without prior notice where necessary to respond to an urgent security incident, service continuity event, or legal compliance requirement. Provider will notify Customer of any such emergency engagement as soon as reasonably practicable.

Customer has a right to reasonably object to Provider's use of a new Subprocessor by notifying Provider in writing within thirty (30) days after Provider gives notice. If Customer does so, Provider will use reasonable efforts to change the affected Service, or recommend a commercially reasonable change to Customer's configuration or use of the affected Service, to avoid Processing of Customer Data by the new Subprocessor. If Provider is unable to make or recommend such a change within a reasonable period of time, not to exceed sixty (60) days, Customer may terminate the subscription term for the Service that Provider cannot provide without using the new Subprocessor. Customer must provide written notice of termination to Provider in accordance with the Agreement. Provider will promptly refund Customer the fees applicable to the unused portion of the subscription term for the terminated Service.

7. SECURITY AND AUDIT

7.1 Controls for the Protection of Customer Data

Provider maintains appropriate administrative, technical and organizational safeguards designed to protect Customer Data from unauthorized or unlawful Processing, from accidental loss, destruction, or damage (collectively, a "**breach**"). These safeguards are summarized in Exhibit B.

7.2 Third-Party Certifications

Provider maintains SOC 2 Type II compliance. Provider will provide Customer with a copy of its current SOC 2 Type II report and any other relevant certifications or independent auditor reports upon request, subject to reasonable confidentiality obligations.

7.3 Incident Management and Breach Notification

Provider will notify Customer without undue delay, and in any event no later than seventy-two (72) hours after becoming aware of a breach of Customer Data. To the extent known, the notice will include (A) a description of the nature of the Personal Data breach, including the categories and approximate number of Data Subjects concerned and the categories and approximate number of records concerned; (B) the name and contact details of a Provider contact point for more information; (C) the measures Provider is taking to address the breach, including measures to mitigate its possible adverse effects.

7.4 Audit Rights

If the information provided in Section 7.2 (Third-Party Certifications) is insufficient to reasonably demonstrate Provider's compliance with its obligations under this DPA, Provider will provide Customer with additional information, and will allow and contribute to audits, including inspections, reasonably necessary to demonstrate compliance. Customer will not exercise this right more than once per year, except as required by a data protection authority or following a confirmed breach of Customer Data.

7.5 Impact Assessments and Consultations

Provider will reasonably cooperate with Customer in connection with any data protection impact assessment or consultation with regulatory authorities that may be required by Data Protection Laws and Regulations.

8. RETURN AND DELETION OF CUSTOMER DATA

Upon termination or expiration of Customer's subscription term, or at any time upon Customer's request, Provider will return or destroy all Customer Data in accordance with the Agreement. If the Services allow Customer to retrieve Customer Data at any time prior to the end of a subscription term, then providing this functionality through the Services during the subscription term satisfies Provider's obligation to return Customer Data under this section. Provider will delete Customer Data within thirty (30) days of termination or expiration of the Agreement, except where retention is required by applicable law.

9. CROSS-BORDER DATA TRANSFERS

To the extent Provider's processing of Customer Data requires the transfer of Customer Data from the European Economic Area, the United Kingdom or Switzerland, to countries that do not ensure an adequate level of protection under Data Protection Laws and Regulations, such transfers will be subject to the Standard Contractual Clauses attached hereto as Exhibit C and the additional terms in Exhibits A and B.

10. CONTACT

Questions or notices related to this DPA should be sent to `privacy@schematichq.com`.

Provider's EU Representative under Article 27 GDPR:

Osano International Compliance Services Limited
ATTN: GKRD
25 North Wall Quay
Dublin 1
D01 H104

Provider's UK Representative under Article 27 UK GDPR:

Osano UK Compliance LTD
ATTN: GKRD
42-46 Fountain Street
Belfast
Antrim
BT1 - 5EF

EXHIBIT A — SUBJECT MATTER AND DETAILS OF PROCESSING

1. NATURE AND PURPOSE OF PROCESSING

Provider will process Personal Data as a Processor in accordance with Customer's instructions in Section 3 (Processing of Customer Data) of the DPA. Provider does not sell or share (as those terms are defined in the CCPA) Customer Data and does not share Customer Data with third parties other than Subprocessors engaged in providing the Services.

2. PROCESSING ACTIVITIES

Customer Data is processed to provide the Services as described in the Agreement, including but not limited to feature entitlement management, usage-based billing, pricing table rendering, customer portal operation, and related analytics.

3. DURATION OF PROCESSING

Provider will process Customer Data for the duration of the Agreement. Following termination of the Agreement, Provider will permanently delete all Customer Data within thirty (30) days, except where retention is required by applicable law.

4. CATEGORIES OF DATA SUBJECTS

The Data Subjects may include Customer's customers (end users of Customer's applications and services) and Customer's employees and contractors who access Provider's administrative interfaces.

5. CATEGORIES OF PERSONAL DATA

Customer controls what Personal Data it submits to Provider. Categories of Personal Data reasonably include:

- Name
- Email address
-

Billing address (when submitted via Stripe integration)

Customer shall not submit to Provider any Personal Data beyond these categories without Provider's prior written agreement.

6. SENSITIVE DATA OR SPECIAL CATEGORIES OF DATA

The Services are not intended to process sensitive data or special categories of personal data as defined under GDPR Article 9 or analogous provisions of other Data Protection Laws and Regulations. Customer shall not submit any such data to Provider without Provider's prior written agreement.

7. HOSTING AND DATA LOCATION

Customer Data is hosted on Amazon Web Services infrastructure in the `us-east-1` region (Northern Virginia, United States). Backups may be replicated to additional AWS regions within the United States for resilience.

EXHIBIT B — TECHNICAL AND ORGANISATIONAL MEASURES

1. MEASURES OF PSEUDONYMIZATION AND ENCRYPTION OF PERSONAL DATA

Pseudonymization is not provided by the Provider, but any Personal Data sent to the Provider can be pre-processed by Customer to ensure pseudonymization if needed. All data, both at rest and in transit, is encrypted using industry-standard encryption algorithms and protocols.

2. MEASURES FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

All data, both at rest and in transit, is encrypted using industry-standard algorithms and protocols. Access to API systems is provided using API keys that are scoped by account (i.e., customer) and environment within that account. All infrastructure is kept up to date with the latest versions and security patches. Provider maintains SOC 2 Type II compliance with continuous monitoring across 80+ controls.

3. MEASURES FOR ENSURING THE ABILITY TO RESTORE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT

All data is backed up periodically. Provider maintains business continuity and disaster recovery procedures that are tested at least annually via tabletop exercises.

4. PROCESS FOR REGULAR TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES IN ORDER TO ENSURE THE SECURITY OF PROCESSING

Provider is SOC 2 Type II certified with continuous control monitoring. Provider also publishes its security practices at `https://docs.schematichq.com/security` and commissions periodic third-party penetration testing.

5. MEASURES FOR USER IDENTIFICATION AND AUTHORIZATION

Provider uses Clerk (a third-party authentication service) for user authentication. Customers may use username/password or authenticate via OAuth. All administrative access to production systems requires multi-factor authentication.

6. MEASURES FOR THE PROTECTION OF DATA DURING TRANSMISSION

All data is encrypted in transit using TLS 1.2 or higher with industry-standard cipher suites.

7. MEASURES FOR THE PROTECTION OF DATA DURING STORAGE

All data is encrypted at rest using AES-256 or equivalent industry-standard encryption.

8. MEASURES FOR ENSURING PHYSICAL SECURITY OF LOCATIONS AT WHICH PERSONAL DATA ARE PROCESSED

Customer Data is hosted on AWS infrastructure, which maintains SOC 2, ISO 27001, and other physical security certifications. Provider maintains a remote work policy that mandates secure work environments for all team members, including encrypted disks and machine locking.

9. MEASURES FOR ENSURING EVENTS LOGGING

Access, event, and server logging is implemented for all services. Logs are aggregated in Datadog and retained per Provider's log retention policy.

10. MEASURES FOR ENSURING SYSTEM CONFIGURATION, INCLUDING DEFAULT CONFIGURATION

System configuration is managed as code via Pulumi and via environment variables that are deployed per environment. Default configurations are defined in code and version controlled.

11. MEASURES FOR INTERNAL IT AND IT SECURITY GOVERNANCE AND MANAGEMENT

Access to IT assets is granted on a least-privilege basis. Production access is limited to a named set of personnel and is reviewed periodically. Provider uses Twingate for zero-trust network access to internal systems.

12. MEASURES FOR CERTIFICATIONS / ASSURANCE OF PROCESSES AND PRODUCTS

Provider maintains SOC 2 Type II certification. Additional details are available at `https://docs.schematichq.com/security`.

13. MEASURES FOR ENSURING DATA MINIMIZATION

Data is only pulled in from integration sources as needed to satisfy product requirements. Customers are encouraged to provide minimal integration credentials and to send only the necessary data from application integrations.

14. MEASURES FOR ENSURING DATA QUALITY

All APIs have validation constraints for their inputs. Data brought in via direct integrations is validated via client-side validation and database schemas.

15. MEASURES FOR ENSURING LIMITED DATA RETENTION

Customer Data is retained for the duration of the Agreement and deleted within thirty (30) days following termination, except where retention is required by applicable law. In-service deletion requests submitted to `support@schematichq.com` are actioned within thirty (30) days.

16. MEASURES FOR ENSURING ACCOUNTABILITY

Every member of Provider's organization has a clearly defined role with responsibilities outlined, ensuring that everyone understands their duties concerning data processing and protection. Access to systems and data is only provided to roles for which it is needed. Access reviews are performed on a periodic basis.

17. MEASURES FOR ALLOWING DATA PORTABILITY AND ENSURING ERASURE

Data deletion requests can be submitted to `support@schematichq.com` or `privacy@schematichq.com`. Internal operations to complete these requests are tracked in an internal ticketing system. Customer can achieve data portability for most resources via Provider's API.

18. FOR TRANSFERS TO SUB-PROCESSORS, SPECIFIC TECHNICAL AND ORGANISATIONAL MEASURES

Provider only transfers Personal Data to Subprocessors listed in Exhibit D. Each Subprocessor is contractually required to maintain security measures substantially equivalent to those described in this Exhibit B and is bound to process Personal Data only on Provider's documented instructions.

EXHIBIT C — ADDITIONAL TERMS FOR DATA TRANSFERS

1. TRANSFERS FROM THE EUROPEAN ECONOMIC AREA

For data transfers from the European Economic Area that are subject to the Standard Contractual Clauses, the Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

1.1 Modules

Module Two (Controller to Processor) will apply where Customer is the Data Controller of Customer Data and Provider is a Processor of Customer Data. Module Three (Processor to Processor) will apply where Customer is a Processor of Customer Data and Provider is a Subprocessor of Customer Data.

1.2 Options

For each Module, where applicable:

(a) In Clause 7, the optional docking clause will not apply.

(b) In Clause 9, Option 2 (general written authorization) will apply, and the time period for prior notice of sub-processors is set forth in Section 6 (Subprocessors) of the DPA.

(c) In Clause 11, the optional clause will not apply.

(d) In Clause 17 (Option 1), the law of Ireland will apply.

(e) In Clause 18(b), disputes will be resolved in the courts of Ireland.

1.3 Annex I, Part A — List of Parties

Data Exporter:

- Name: Customer and its authorized Affiliates.
- Contact Details: Customer's account address and the privacy/legal contact provided by Customer in its account settings.
- Data Exporter Role: Customer's role is described in Section 3.1 (Data Processing Roles) of the DPA.
- Signature & Date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses, including their Annexes, as of the Effective Date.

Data Importer:

- Name: Schematic Inc.
- Contact Details: `privacy@schematichq.com`; Schematic Inc., 1012 Hawthorn Ave, Boulder, CO 80304, United States.
-

Data Importer Role: Provider's role is described in Section 3.1 (Data Processing Roles) of the DPA.

- Signature & Date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses, including their Annexes, as of the Effective Date.

1.4 Annex I, Part B — Description of Transfer

(a) The categories of Data Subjects are described in Exhibit A, Section 4.

(b) The categories of Personal Data are described in Exhibit A, Section 5.

(c) Sensitive data is addressed in Exhibit A, Section 6.

(d) The frequency of the transfer is on a continuous basis for the duration of the Agreement.

(e) The nature of the processing is described in Exhibit A, Section 1.

(f) The purpose of the processing is described in Exhibit A, Section 1.

(g) The period for which the Personal Data will be retained is described in Exhibit A, Section 3.

1.5 Annex I, Part C — Competent Supervisory Authority

The Irish Data Protection Commission will be the competent supervisory authority.

1.6 Annex II — Technical and Organisational Measures

Exhibit B of this DPA serves as Annex II of the Standard Contractual Clauses.

2. TRANSFERS FROM THE UNITED KINGDOM

For data transfers from the United Kingdom, the Standard Contractual Clauses apply as modified in Section 1 (Transfers from the European Economic Area) of this Exhibit C, subject to the following:

(a) The International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, in force 21 March 2022) ("**UK Addendum**") applies and is hereby incorporated by reference.

(b) The information provided in Sections 1.1 (Modules), 1.2 (Options), 1.3 (Annex I, Part A), 1.4 (Annex I, Part B), and 1.6 (Annex II) of this Exhibit C provides the information required for completing the UK Addendum.

(c) The Parties select the "neither Party" option of Table 4 (Ending this Addendum when the Approved Addendum Changes) of the UK Addendum.

3. TRANSFERS FROM SWITZERLAND

For data transfers from Switzerland, the Standard Contractual Clauses apply as modified in Section 1 (Transfers from the European Economic Area) of this Exhibit C, subject to the following:

(a) In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner if the transfer is governed by the Swiss Federal Act on Data Protection (FADP).

(b) References to "Member State" refer to Switzerland and Data Subjects located in Switzerland may exercise and enforce their rights under the Standard Contractual Clauses in Switzerland.

(c) References to the General Data Protection Regulation (GDPR) refer to the FADP, as amended or replaced.

4. PRECEDENCE

To the extent there is any conflict between the Standard Contractual Clauses (including as amended by this Exhibit C) and the DPA, the provisions of the Standard Contractual Clauses (including as amended by this Exhibit C) will apply.

EXHIBIT D — LIST OF SUBPROCESSORS

The following Subprocessors process Customer Personal Data in support of the Services. The current list is also published at https://schematichq.com/subprocessors.

Subprocessor	Purpose	Location	Categories of Personal Data Processed
Amazon Web Services, Inc.	Cloud infrastructure and hosting	United States (`us-east-1`)	All Customer Data
ClickHouse, Inc.	Event and analytics data storage	United States (AWS `us-east-1`)	Customer event and usage data, which may include end-user identifiers
Datadog, Inc.	Application observability, logging, and monitoring	United States	Log data, which may include Customer Data