V1.0

Status	Effective April 28, 2026
Effective	April 28, 2026
Canonical source	https://secapi.ai/trust

Data Processing Agreement

Version 1.0 — Effective April 28, 2026. This DPA is incorporated by reference into the underlying agreement between Provider and Customer and is binding on the Parties as of the effective date. Provider may update this DPA from time to time; the version in effect is the version posted at `secapi.ai/trust#dpa`. A downloadable PDF is provided for procurement and legal review at `/trust/dpa.pdf`.

This Data Processing Agreement ("**DPA**") is incorporated into and forms part of the agreement between secapi.ai ("**Provider**") and the customer that has accepted Provider's Terms of Service or executed a written order form ("**Customer**") (each a "**Party**" and together the "**Parties**"). This DPA reflects the Parties' agreement regarding the Processing of Customer Personal Data in connection with the Services.

In the event of a conflict between this DPA and the underlying agreement, this DPA controls with respect to the subject matter of Data Protection Laws.

1. Definitions

Capitalized terms used but not defined in this DPA have the meanings given to them in the underlying agreement or in Applicable Data Protection Laws.

- **"Applicable Data Protection Laws"** means all data protection and privacy laws applicable to the Processing of Personal Data under the underlying agreement, including (a) the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"); (b) the GDPR as incorporated into United Kingdom law by the Data Protection Act 2018 ("**UK GDPR**"); (c) the Swiss Federal Act on Data Protection ("**FADP**"); (d) the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act ("**CCPA**"); and (e) any other equivalent legislation in other jurisdictions where the Customer or its Authorized Affiliates are established or to which the Processing is subject.
- **"Authorized Affiliate"** means any entity that controls, is controlled by, or is under common control with Customer, where "control" means ownership of more than 50% of the voting interests of the entity.
- **"Customer Personal Data"** means any Personal Data that Provider Processes on behalf of Customer in the course of providing the Services, as further described in Annex I.
- **"Data Protection Officer"** has the meaning given in Article 37 of the GDPR.
- **"Data Subject"** means an identified or identifiable natural person to whom Personal Data relates.
- **"EEA"** means the European Economic Area.
- **"Personal Data"** means any information relating to an identified or identifiable natural person processed under this DPA, as defined under Applicable Data Protection Laws.
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored, or otherwise Processed by Provider or its Sub-processors.
- **"Process," "Processing,"** and **"Processed"** have the meanings given to them under Applicable Data Protection Laws.
- **"Restricted Transfer"** means a transfer (including onward transfer) of Personal Data subject to Applicable Data Protection Laws to a country outside the EEA, the United Kingdom, or Switzerland that is not subject to an adequacy decision.
- **"Services"** means the API, dashboard, MCP tools, SDKs, hosted documentation, and related software and services provided by Provider under the underlying agreement.

- **"Standard Contractual Clauses"** or **"SCCs"** means (a) the standard contractual clauses approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "**EU SCCs**"); (b) the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office (the "**UK Addendum**"); and (c) where applicable, the Swiss adaptations to the EU SCCs.
- **"Sub-processor"** means any third party engaged by Provider to Process Customer Personal Data in connection with the Services. The current list of Sub-processors is published at `secapi.ai/trust#sub-processors`.

---

2. Scope and roles of the Parties

2.1 **Roles.** With respect to Customer Personal Data, Customer acts as the Controller (or, where Customer is itself a Processor on behalf of a third-party Controller, as a Processor) and Provider acts as the Processor (or Sub-processor).

2.2 **Authorized Affiliates.** Customer enters into this DPA on behalf of itself and its Authorized Affiliates. Each Authorized Affiliate is bound by the obligations of "Customer" under this DPA in respect of Personal Data of which it is the Controller.

2.3 **Customer instructions.** Provider Processes Customer Personal Data only on documented instructions from Customer, including with regard to Restricted Transfers, unless required to do so by Union or Member State law to which Provider is subject. The underlying agreement (including Customer's configuration of the Services) constitutes the documented instructions of Customer to Provider for the Processing of Customer Personal Data. Provider will inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Laws.

2.4 **Customer responsibilities.** Customer is solely responsible for: (a) the accuracy, quality, and legality of Customer Personal Data and the means by which it acquired Personal Data; (b) complying with all Applicable Data Protection Laws applicable to its collection and use of Personal Data, including providing appropriate notices to and obtaining all necessary consents from Data Subjects; and (c) Customer's instructions to Provider regarding the Processing of Customer Personal Data.

---

3. Provider obligations

3.1 **Compliance.** Provider will comply with all Applicable Data Protection Laws in its Processing of Customer Personal Data.

3.2 **Confidentiality.** Provider ensures that personnel authorized to Process Customer Personal Data are subject to a duty of confidentiality (whether contractual or statutory) and have received appropriate data protection training.

3.3 **Security measures.** Provider implements appropriate technical and organizational measures to protect Customer Personal Data as further described in Annex II.

3.4 **Cooperation.** Taking into account the nature of the Processing, Provider assists Customer (insofar as this is possible) in fulfilling Customer's obligations to respond to Data Subject requests under Applicable Data Protection Laws. Provider notifies Customer without undue delay if it receives a request from a Data Subject relating to Customer Personal Data and does not respond to the Data Subject directly except as instructed by Customer or required by law.

3.5 **Data Protection Impact Assessments.** Provider provides Customer with reasonable cooperation and assistance, taking into account the nature of Processing and the information available to Provider, to enable Customer to conduct any data protection impact assessments (DPIAs) and prior consultations with supervisory authorities as required under Articles 35 and 36 of the GDPR.

3.6 **Records.** Provider maintains records of its Processing activities in accordance with Article 30(2) of the GDPR.

---

4. Sub-processors

4.1 **General authorization.** Customer grants Provider general authorization to engage Sub-processors to Process Customer Personal Data, subject to the requirements of this Section 4. The current list of Sub-processors is available at `secapi.ai/trust#sub-processors`.

(the "**Sub-processor List**").

4.2 **Sub-processor obligations.** Provider enters into a written agreement with each Sub-processor that imposes on the Sub-processor data protection obligations no less protective than those imposed on Provider under this DPA. Provider remains liable to Customer for the performance of each Sub-processor's obligations.

4.3 **Notice of changes.** Provider will provide Customer with at least thirty (30) days' prior written notice (which may be by email or by updating the Sub-processor List on Provider's website) before authorizing any new Sub-processor to Process Customer Personal Data.

4.4 **Right to object.** Customer may object to Provider's use of a new Sub-processor on reasonable grounds relating to data protection by notifying Provider in writing within fifteen (15) days of receipt of Provider's notice. The Parties will work in good faith to resolve the objection. If the Parties cannot resolve the objection within thirty (30) days, Customer may terminate the underlying agreement (or the affected portion thereof) without penalty by providing written notice to Provider.

5. International data transfers

5.1 **Restricted Transfers.** To the extent the provision of the Services involves a Restricted Transfer of Customer Personal Data, the EU SCCs (Module Two: Controller to Processor, or Module Three: Processor to Processor, as applicable) apply to such transfers and are incorporated by reference into this DPA, with the following selections:

- **Clause 7 (Docking clause):** Optional clause does not apply.
- **Clause 9 (Use of sub-processors):** Option 2 (general written authorization), with the notice period set out in Section 4.3 above.
- **Clause 11 (Redress):** The optional language does not apply.
- **Clause 17 (Governing law):** The law of Ireland.
- **Clause 18 (Choice of forum and jurisdiction):** The courts of Ireland.
- **Annex I.A (List of Parties):** Customer is the data exporter; Provider is the data importer. Contact details are those provided in the underlying agreement.
- **Annex I.B (Description of transfer):** As set out in Annex I to this DPA.
- **Annex I.C (Competent supervisory authority):** The supervisory authority of the EU Member State in which the data exporter is established.
- **Annex II (Technical and organizational measures):** As set out in Annex II to this DPA.
- **Annex III (Sub-processors):** As set out in the Sub-processor List.

5.2 **UK Restricted Transfers.** The UK Addendum applies to transfers of Personal Data subject to the UK GDPR. Tables 1, 2, and 3 of the UK Addendum are completed by reference to Annex I and Annex II of this DPA. Table 4 ("Ending the Addendum"): the data importer may end the UK Addendum.

5.3 **Swiss Restricted Transfers.** For transfers subject to the FADP, the EU SCCs apply with the modifications described in Section 5.1 and the following adaptations: references to the GDPR are deemed to refer to the FADP; references to the EU and Member States are deemed to refer to Switzerland; and the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

5.4 **Conflict.** In the event of a conflict between this DPA and the SCCs, the SCCs prevail with respect to the subject matter of Restricted Transfers.

6. Personal Data Breach

6.1 **Notification.** Provider notifies Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. Notification will be sent to the security contact designated by Customer in the dashboard or, if not designated, to the Customer's primary account email.

6.2 **Information provided.** To the extent reasonably available to Provider, the notification will describe: (a) the nature of the Personal Data Breach including the categories and approximate number of Data Subjects and records concerned; (b) the likely consequences of the Personal Data Breach; (c) the measures taken or proposed by Provider to address the Personal Data Breach, including measures to mitigate its possible adverse effects; and (d) the name and contact details of Provider's security contact.

6.3 **Cooperation.** Provider provides Customer with reasonable cooperation and assistance to enable Customer to comply with its own breach-notification obligations under Applicable Data Protection Laws.

6.4 **Provider security operations.** Provider's incident response procedures, including escalation paths and post-incident review, are summarized at `secapi.ai/trust#security`. Notifications and breach reports may be directed to `security@secapi.ai`.

7. Audits and inspections

7.1 **Audit rights.** Provider makes available to Customer all information reasonably necessary to demonstrate compliance with this DPA. Provider allows for and contributes to audits, including inspections, conducted by Customer or another auditor mandated by Customer (subject to Section 7.2).

7.2 **Audit procedure.** Audits will be conducted no more than once in any twelve (12) month period (except where required by a supervisory authority or following a Personal Data Breach), on at least sixty (60) days' prior written notice, during normal business hours, in a manner that does not unreasonably interfere with Provider's business operations, and subject to the auditor entering into a confidentiality agreement reasonably acceptable to Provider. Customer bears its own costs and Provider's reasonable costs of any audit.

7.3 **Third-party reports.** To the extent applicable and requested by Customer, Provider will satisfy its obligations under Sections 7.1 and 7.2 by providing Customer with: (a) Provider's then-current SOC 2 Type 1 or Type 2 report (when available — see `secapi.ai/trust#soc2` for current status); (b) Provider's penetration testing summary; and (c) responses to Provider's then-current Due Diligence Questionnaire (DDQ) at `secapi.ai/trust#ddq`.

8. Return and deletion of Customer Personal Data

8.1 **End of provision.** On termination or expiration of the underlying agreement, Provider deletes or returns all Customer Personal Data to Customer at Customer's election, and deletes existing copies, except to the extent (a) Union or Member State law requires retention of the Personal Data, or (b) such Personal Data is held in routine system backups, in which case Provider continues to apply this DPA's protections until the backup is overwritten in the normal course.

8.2 **Customer self-service deletion.** During the term of the underlying agreement, Customer may delete or request deletion of Customer Personal Data through the dashboard or by contacting `support@secapi.ai`.

9. Liability

The Parties' aggregate liability arising out of or in connection with this DPA is subject to the limitations and exclusions of liability set forth in the underlying agreement. Nothing in this DPA limits or excludes either Party's liability where such limitation or exclusion is prohibited by Applicable Data Protection Laws.

10. General

10.1 **Term.** This DPA takes effect on the effective date of the underlying agreement and remains in force for so long as Provider Processes Customer Personal Data on behalf of Customer.

10.2 **Order of precedence.** In the event of a conflict between this DPA and the underlying agreement, this DPA controls with respect to the subject matter of Data Protection Laws. In the event of a conflict between this DPA and the SCCs, the SCCs control.

10.3 **Severability.** If any provision of this DPA is held invalid, illegal, or unenforceable, the remaining provisions remain in full force and effect.

10.4 **Updates.** Provider may update this DPA from time to time to reflect changes in Applicable Data Protection Laws or Provider's Processing activities, provided that no update will materially diminish the protections afforded to Customer Personal Data without Customer's consent. Updated versions will be published at `secapi.ai/trust#dpa` with a new version number and effective date.

Annex I — Description of Processing

A. List of Parties

- **Data exporter:** Customer (as identified in the underlying agreement).
- **Data importer:** secapi.ai (the "Provider").

B. Subject matter, nature, and purpose of Processing

Provider Processes Customer Personal Data to provide the Services to Customer, including: (a) authenticating and authorizing API requests; (b) operating the dashboard, MCP tools, and SDKs; (c) delivering hosted documentation; (d) operating support and billing workflows; (e) generating product analytics and operational telemetry; and (f) complying with Provider's legal obligations.

C. Categories of Data Subjects

- Customer's authorized users of the Services (e.g., engineers, product managers, finance personnel, designated administrators).
- Customer's end users to the extent Customer routes Personal Data through the Services.

D. Categories of Personal Data

- Account data: name, email address, organization affiliation, role, hashed credentials, API key identifiers (not the keys themselves), session tokens, multi-factor authentication state.
- Usage data: API request metadata (endpoint, timestamp, response status, byte counts), MCP tool invocations, dashboard navigation events, error reports.
- Billing data: billing contact name, address, tax identifier, payment method tokens (held by Stripe, not Provider), invoice history.
- Support data: messages and attachments submitted to `support@secapi.ai` or the dashboard support widget.
- Telemetry data: IP address, user-agent, device and browser characteristics, performance metrics.

E. Sensitive data

The Services are not designed for the Processing of special categories of Personal Data (Article 9 GDPR) or criminal-conviction data (Article 10 GDPR). Customer is responsible for ensuring that Customer Personal Data submitted to the Services does not include such categories without prior arrangement.

F. Frequency of transfer

Continuous, on a request-by-request basis as Customer uses the Services.

G. Duration of Processing

For the term of the underlying agreement and thereafter only as required to comply with legal obligations or until deletion in accordance with Section 8.

H. Sub-processors

See `secapi.ai/trust#sub-processors`.

Annex II — Technical and organizational measures

Authentication and access control

- API authentication via long-lived API keys (stored as SHA-256 hashes; raw keys are never persisted) and short-lived WorkOS bearer tokens.
- Multi-factor authentication required for administrator accounts.
- Tenant-isolated data access enforced at the application layer; rate limiting enforced per organization.
- All administrative actions are written to an audit log with actor, timestamp, and resource references.

Encryption

- All Customer Personal Data is encrypted in transit using TLS 1.2 or higher.
- Mutual TLS is used for connections from application tier to PostgreSQL.
- All Customer Personal Data at rest is encrypted using industry-standard symmetric encryption (AES-256 or equivalent).
- Secrets and credentials are stored in a centralized secrets manager (Infisical) with scoped access policies.

Network and infrastructure

- All ingress traffic terminates at a Cloudflare-managed edge with WAF and DDoS protection.
- API and application services are hosted in a managed cloud environment with isolated tenant networking.
- Public-facing endpoints subject to Provider's published auth model are exempt from credential checks (`/v1/healthz` , `/v1/status/summary` , etc.) and serve no Personal Data.

Logging, monitoring, and incident response

- Centralized error tracking via Sentry; Provider's on-call engineer receives alerts for critical incidents.
- Uptime monitoring via BetterStack with public status page at `secapi.ai/status` .
- Documented incident response runbook with severity classification, communication plan, and post-incident review requirements. See `secapi.ai/trust#security` .

Vulnerability management

- Static application security testing (SAST) on every change via CodeQL, Semgrep, gitleaks, and trufflehog.
- Comprehensive auth-boundary audit and threat model maintained internally; published summary at `secapi.ai/trust#security` .
- Dependencies scanned for known vulnerabilities; security patches applied per documented severity SLAs.

Personnel and physical security

- Personnel with access to Customer Personal Data are subject to background checks (where permitted by law) and confidentiality obligations.
- All personnel complete security and privacy training upon onboarding and annually thereafter.
- Production access is limited to a documented set of operations personnel using hardware-backed keys and ephemeral credentials.

Business continuity

- Daily encrypted backups of primary databases with documented restore procedures.
- Regional redundancy for critical infrastructure tiers.
- Documented disaster-recovery plan tested at least annually.

Annex III — Sub-processors

The current Sub-processor List is published at `secapi.ai/trust#sub-processors` and is incorporated by reference into this DPA. As of the effective date, the Sub-processor List includes (categories and primary purpose):

- **Cloudflare** — edge CDN, WAF, DDoS protection (US, global)
- **Stripe** — billing and payment processing (US)
- **Anthropic** — large language model API (US)
- **OpenAI** — large language model API (US, optional per Customer configuration)
- **Infisical** — secrets management (US)
- **BetterStack** — uptime monitoring and public status page (EU/US)
- **Sentry** — error tracking (US/EU)
- **PostHog** — product analytics (US/EU, optional)
- **Resend** — transactional email (US)
- **Railway** — application hosting (US, multiple regions)
- **WorkOS** — authentication, directory, session management (US)

The list is current as of the effective date of this DPA and may be updated in accordance with Section 4.

End of Data Processing Agreement v1.0.