

Data Processing Addendum

Effective date: October 26, 2026

This Data Processing Addendum (the “**DPA**”) is part of the agreement between Caldera PBC (“**Caldera**”) and the customer named in it (“**Customer**”) for Customer’s use of the Service, whether that agreement is Caldera’s Customer Terms of Service or a separately negotiated agreement (the “**Agreement**”). It sets out, in one document, the commitments the Agreement makes about personal information in Customer Content, with a description of the processing (Schedule 1) and a summary of Caldera’s security measures (Schedule 2). Where the Agreement is the Customer Terms of Service, this DPA restates their data protection section and doesn’t expand or reduce either party’s obligations under it.

1. DEFINITIONS AND ROLES

1.1 Definitions. Capitalized terms not defined in this DPA have the meanings given in the Agreement, or, where the Agreement doesn’t define them, in Caldera’s Customer Terms of Service. “**Applicable Privacy Law**” means the United States federal and state laws on privacy and data protection that apply to the processing of Personal Information under the Agreement, including the California Consumer Privacy Act. “**Personal Information**” means information in Customer Content that Applicable Privacy Law protects as personal information or personal data.

1.2 Roles. Customer is the business or controller of Personal Information, and Caldera is its service provider, contractor, or processor, as Applicable Privacy Law uses those terms.

2. PROCESSING

2.1 Instructions. Caldera will process Personal Information only on Customer’s behalf, in accordance with Customer’s instructions. The Agreement and this DPA, together with Customer’s configuration and use of the Service, constitute those instructions; Customer may give additional written instructions consistent with the Agreement. Caldera will notify Customer if it believes an instruction violates Applicable Privacy Law.

2.2 Purposes. Caldera will process Personal Information only for the purposes described in Schedule 1: providing, securing, supporting, and maintaining the Service and Professional Services, and as Customer otherwise directs in writing.

2.3 Use Restrictions. Caldera will not: (A) sell or share Personal Information; (B) retain, use, or disclose Personal Information for any purpose other than those stated in Section 2.2 (Purposes), including any commercial purpose, or outside the direct business relationship between Customer and Caldera, except as Applicable Privacy Law permits a service provider or processor to; or (C) combine Personal Information with personal information Caldera receives from or on behalf of others, or collects from its own interactions with individuals, except as Applicable Privacy Law permits.

2.4 Compliance. Caldera will comply with the obligations Applicable Privacy Law imposes on it as Customer’s service provider, contractor, or processor, and will provide the level of privacy protection that law requires. Caldera will notify Customer if it determines that it can no longer meet these obligations, in which case Customer may take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information.

2.5 Customer Responsibilities. Customer determines the Personal Information it puts in the Service, and is responsible for providing any notices and obtaining any consents Applicable Privacy Law requires for Caldera to process it, and for ensuring its instructions comply with Applicable Privacy Law.

2.6 No Training. Caldera will not use Customer Content, including Personal Information, to train or fine-tune artificial intelligence models, and Caldera's agreements with the providers of the AI models used in the Service prohibit those providers from doing so.

3. PERSONNEL, SECURITY, AND LOCATION

3.1 Personnel. Caldera will limit access to Personal Information to personnel who need it to perform the Agreement, and will ensure that each person who processes Personal Information is bound by a duty of confidentiality, whether contractual or statutory.

3.2 Security Measures. Caldera will implement and maintain reasonable and appropriate administrative, physical, and technical safeguards designed to protect Personal Information against accidental or unlawful loss, access, use, alteration, or disclosure, including the measures summarized in Schedule 2. Caldera may update its security measures but will not materially reduce the overall security of the Service during a Subscription Term.

3.3 Data Location. Caldera will store Customer Content in the United States.

4. SUB-PROCESSORS

4.1 Authorization. Customer authorizes Caldera to engage Sub-processors to process Personal Information. Caldera lists its current Sub-processors in its trust center at trust.calderapbc.com, and updates the list before a new Sub-processor begins processing Personal Information.

4.2 Sub-processor Obligations. Caldera will enter into a written agreement with each Sub-processor that requires it to protect Personal Information in a manner at least as protective as this DPA, to the extent applicable to the services it provides, and remains responsible for the acts and omissions of its Sub-processors.

5. SECURITY INCIDENTS

5.1 Notice. Caldera will notify Customer of a Security Incident without undue delay, and in any event within 72 hours after Caldera confirms it.

5.2 Response. Caldera will provide information about the Security Incident as it becomes known or as Customer reasonably requests, and will promptly take reasonable steps to contain, investigate, and remediate it. Caldera's notice of or response to a Security Incident is not an acknowledgment of fault or liability.

6. ASSISTANCE

6.1 Individual Requests. Customer is responsible for responding to requests from individuals to exercise their rights under Applicable Privacy Law with respect to Personal Information. Where Customer cannot fulfill a request using the functionality of the Service, Caldera will provide reasonable assistance. If Caldera receives such a request directly, it will refer the individual to Customer and will not otherwise respond to it unless Customer authorizes it or Applicable Privacy Law requires it.

6.2 Assessments. Caldera will provide reasonable assistance with any data protection assessment Applicable Privacy Law requires of Customer, to the extent the information needed is available to Caldera and not otherwise to Customer.

7. COMPLIANCE INFORMATION

7.1 Reports. Caldera will maintain an annual SOC 2 Type II examination, or a comparable successor, and will provide its most recent report to Customer on request, subject to the confidentiality terms of the Agreement.

7.2 Questions. On written request no more than once a year, Caldera will answer Customer's reasonable written questions about Caldera's processing of Personal Information and its security practices, and will provide other information reasonably necessary to demonstrate Caldera's compliance with this DPA.

8. EXPORT AND DELETION

8.1 Export. Customer may export Customer Content at any time during the Subscription Term, using the functionality of the Service. For 30 days after the Subscription Term ends, Caldera will, on request, make Customer Content available to Customer for export.

8.2 Deletion. After that period, Caldera will delete Customer Content, including Personal Information, from the Service within 60 days, and will delete it from backups on Caldera's normal backup schedule, except to the extent applicable law requires Caldera to retain it. On request, Caldera will certify the deletion in writing.

9. GENERAL

9.1 Term. This DPA remains in effect for as long as Caldera processes Personal Information under the Agreement.

9.2 Liability. Each party's liability arising out of or relating to this DPA is subject to the limitations and exclusions of liability in the Agreement.

9.3 Precedence. If this DPA conflicts with the Agreement with respect to the processing of Personal Information, this DPA controls.

SCHEDULE 1: DESCRIPTION OF PROCESSING

Item	Description
Subject matter	Caldera's provision of the Service and any Professional Services to Customer under the Agreement.
Duration	The Subscription Term, and any period afterward in which Caldera holds Customer Content under Section 8 (Export and Deletion).
Nature and purpose	Hosting, storing, retrieving, analyzing, generating, transmitting, and displaying Customer Content, including with the AI features of the Service, as needed to provide, secure, support, and maintain the Service and Professional Services, and as Customer otherwise directs in writing.
Categories of individuals	Determined by Customer. Typically Customer's Authorized Users, and individuals whose information appears in the records, documents, and data Customer puts in the Service or connects to it, such as members of the public, applicants, property owners, and Customer's employees and contractors.
Categories of Personal Information	Determined by Customer. Typically names, contact information, identifiers, and other information contained in Customer's records and data.
Sensitive or regulated information	Determined by Customer, subject to the Agreement's terms on Regulated Data.

SCHEDULE 2: SECURITY MEASURES

A summary of the measures Caldera maintains under Section 3.2 (Security Measures). More detail is available at calderapbc.com/security and in Caldera's trust center at trust.calderapbc.com.

- **Independent assurance.** Annual SOC 2 Type II examination by an independent CPA firm. Administrative, physical, and technical safeguards required by the HIPAA Security Rule, monitored continuously alongside SOC 2 controls.
- **Hosting and location.** The Service runs on Google Cloud in the United States. Sub-processors that store Customer Content are pinned to United States regions, and requests to AI models are routed only to United States infrastructure.
- **Encryption.** Data is encrypted in transit with TLS 1.2 or higher and at rest with AES-256, including backups. Encryption keys are managed in Google Cloud Key Management Service.
- **Backups and recovery.** The primary database is backed up automatically with point-in-time recovery. The disaster recovery plan is tested at least once a year.
- **Customer access controls.** Single sign-on through Customer's identity provider (SAML or OIDC), so Customer's multi-factor authentication and session policies apply. Administrators control access to documents and folders by user or group, and can review activity in an audit log.
- **Caldera personnel access.** Access to Customer Content is limited to personnel whose role requires it, and is reviewed regularly. All personnel pass a background check before joining and complete security training every year.
- **Monitoring and incident response.** Production is monitored continuously, with alerts to an on-call engineer. A documented incident response plan is tested at least once a year.
- **Secure development.** Every code change is peer reviewed and passes static analysis, dependency scanning, and secret scanning before it is deployed.
- **AI model providers.** AI models are used through the providers' enterprise APIs, under agreements that prohibit training on Customer Content.