Cannon Caseworks

Data Processing Addendum

Provider: Cannon Creations LLC
Effective date: August 11, 2026
Version: 2026-08-11.1
Contact: support@cannoncaseworks.com

This Data Processing Addendum is incorporated into and forms part of the Cannon Caseworks Services Agreement. The governing agreement and related legal documents are available at cannoncaseworks.com/legal.

1. Scope and incorporation

This Data Processing Addendum (the "DPA") forms part of the Cannon Caseworks Terms of Service or other agreement that incorporates it (the "Agreement") between Cannon Creations LLC ("Cannon") and Customer. It applies when Cannon processes Personal Data contained in Customer Content on Customer's behalf. Capitalized terms not defined here have the meanings in the Agreement.

For that processing, Customer is the controller, business, or equivalent party that determines the purposes and means of processing, and Cannon is the processor, service provider, contractor, or equivalent party acting on Customer's documented instructions. Each party remains independently responsible for Personal Data it controls for its own account.

2. Processing details and instructions

The subject matter is Cannon's provision of the Service. Processing lasts for the applicable service period and the limited retention period described in the Agreement. Its nature and purpose are to receive, secure, host, organize, copy, transmit, extract, OCR, transcribe, index, search, retrieve, analyze, summarize, label, categorize, draft from, display, export, delete, and otherwise process Customer Content only to provide, secure, support, and administer the functions Customer requests.

The Agreement, Customer's use and configuration of the Service, and authorized support requests are Customer's documented instructions. Cannon will process Personal Data only on those instructions, including with respect to transfers, unless law requires otherwise. If law requires other processing, Cannon will notify Customer before processing unless legally prohibited. Cannon will promptly notify Customer if Cannon reasonably believes an instruction violates applicable data-protection law and may suspend only the affected processing while the parties address it.

- Data-subject categories may include Authorized Users; Customer personnel and clients; parties, witnesses, experts, custodians, employees, contractors, vendors, recipients, authors, and other people identified in litigation or investigation records; and people who contact Cannon.
- Personal Data may include identifiers and contact details; account and professional information; communications and connected-account content; device, network, audit, and usage data; billing details; documents, media, metadata, extracted text, annotations, prompts, notes, case facts, and AI Output; and sensitive or regulated information that Customer is lawfully authorized to submit.
- The frequency is continuous or as initiated by Customer and Authorized Users during use of the Service.

3. Customer obligations

Customer will comply with its obligations as controller, provide all required notices, establish a lawful basis for processing and transfer, respond to data-subject requests, obtain sensitive-data consent when required, limit instructions to authorized purposes, and submit only Personal Data that Customer has the legal and professional authority to process through the configured providers.

Customer is responsible for configuring access, minimizing data, applying legal holds and deletion restrictions, and determining whether a feature is appropriate for privilege, confidentiality, protective orders, sector-specific law, foreign transfer restrictions, or professional duties.

4. Confidentiality and personnel

Cannon will ensure that personnel authorized to process Personal Data are bound by confidentiality duties, receive access only as needed for their functions, and are informed of applicable security and data-handling obligations. Cannon will not disclose Customer Content to another customer.

5. Security measures

Cannon will maintain reasonable administrative, technical, and organizational measures appropriate to the nature of processing and risk. Current measures include authenticated and role-scoped access; logical firm, client, and matter segregation; deny-by-default browser access to Firestore and object storage; encrypted transport; provider-managed encryption at rest; short-lived signed file access; server-side authorization checks; encrypted OAuth credentials; logging and audit records; upload integrity checks and malware screening; protected secrets; recovery controls; and procedures for incident response and deletion.

Security measures may evolve as technology and risk change, provided Cannon does not materially reduce the overall protection of Customer Content during an active service period. No measure makes an internet or cloud system risk-free. Customer remains responsible for secure endpoints, credentials, role assignments, exports, and independent backups.

6. Security incidents

Cannon will notify Customer without undue delay after becoming aware of a breach of security that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data processed for Customer (a "Security Incident"). Notice will include information reasonably available to Cannon that Customer needs to meet applicable notification duties, and Cannon will take reasonable steps to contain, investigate, and remediate the Security Incident.

Unsuccessful attempts, pings, scans, denial-of-service attempts, blocked malware, and other events that do not compromise Personal Data are not Security Incidents. Notice and cooperation do not constitute an admission of fault or liability.

7. Assistance and data-subject requests

Taking into account the nature of processing and information available to Cannon, Cannon will reasonably assist Customer with verified data-subject requests, security obligations, breach notifications, and required data-protection assessments. If Cannon receives a request concerning Customer Content directly from a data subject, Cannon will ordinarily direct the requester to Customer and will not act contrary to Customer's instructions unless required by law.

Customer is responsible for determining whether a request is valid and for communicating with the requester or regulator. Assistance beyond standard Service functionality or arising from Customer's noncompliance may be subject to reasonable fees agreed in advance.

8. Subprocessors

Customer generally authorizes Cannon to use subprocessors to provide hosting, authentication, storage, database, OCR, document processing, AI processing, email, security, support, and related Service functions. Current material categories and providers are identified in the Privacy Notice and provider-specific Terms sections.

Cannon will bind each subprocessor that processes Personal Data on Cannon's behalf by written data-protection obligations appropriate to its role and will remain responsible for Cannon's own obligations under this DPA. When applicable law requires notice of a new material subprocessor, Cannon will provide reasonable notice through the Service, email, or an updated provider list. Customer may object on reasonable, documented data-protection grounds; the parties will work in good faith on a commercially reasonable alternative, and Cannon may suspend the affected feature or permit termination of it if no reasonable alternative is available.

9. Return, deletion, and preservation

During the service period, Customer may use available export and deletion functions. At Customer's verified direction or after termination, Cannon will delete or return Personal Data processed on Customer's behalf, unless law, a legal hold, security need, dispute-preservation duty, or the Agreement permits or requires retention. Deletion from active systems does not immediately remove encrypted backups, provider abuse-monitoring records, acceptance records, billing records, or security logs; retained data remains protected and is deleted or rendered inaccessible through ordinary retention cycles.

A case-file purge removes case-scoped active records and stored objects while retaining a minimized case shell and deletion audit receipt. A simple archive or case-list deletion is not a case-file purge. Customer must use or request the appropriate deletion operation.

10. Demonstrating compliance and assessments

On reasonable written request, Cannon will provide information in its possession necessary to demonstrate compliance with this DPA. Where required by applicable law and subject to confidentiality, security, scope, frequency, and noninterference safeguards, Cannon will cooperate with a reasonable assessment by Customer or a qualified independent assessor. The parties will first use current certifications, summaries, questionnaires, and third-party reports when they reasonably satisfy the request.

Customer may not use an assessment to access another customer's data, privileged material, source code, vulnerability details that would create security risk, or information Cannon is prohibited from disclosing. Assessments are ordinarily limited to once per year unless a Security Incident or regulator legally requires more.

11. Restricted data and international transfers

This DPA is not a HIPAA business associate agreement, payment-card agreement, biometric-data consent, criminal-justice agreement, export-control authorization, or government-classified-data authorization. Customer must not submit data requiring those terms until Cannon signs the required addendum and confirms the applicable configuration.

The standard Service is operated for United States business use. Customer must not cause a transfer of Personal Data from the EEA, United Kingdom, Switzerland, or another jurisdiction requiring a transfer mechanism unless Customer has established a lawful mechanism and Cannon has signed any required transfer addendum.

12. Sale, advertising, and model training restrictions

Cannon will not sell Customer Content, share it for cross-context behavioral advertising, use it for targeted advertising, or use it to train a Cannon-owned or generally available AI model. Cannon will not voluntarily opt Customer Content into a third-party model-training program. Any signed Customer-specific data instruction controls over this standard provision for its subject matter.

13. Conflict, liability, and contact

If this DPA conflicts with the Agreement about processing Personal Data, this DPA controls for that subject. A signed customer-specific data agreement controls over this standard DPA for its subject matter. The liability exclusions, caps, dispute terms, governing law, and termination rights in the Agreement apply to this DPA to the maximum extent permitted by law.

Data-protection notices and requests under this DPA may be sent to support@cannoncaseworks.com with "Data Processing" in the subject line.