

# Cannon Caseworks

## Services Agreement

**Provider:** Cannon Creations LLC

**Effective date:** August 11, 2026

**Version:** 2026-08-11.1

**Contact:** support@cannoncaseworks.com

This review copy consolidates the online Services Agreement and its incorporated Data Processing Addendum. The Privacy Notice and Responsible AI Use notice remain available at [cannoncaseworks.com/legal](https://cannoncaseworks.com/legal).

### 1. Agreement, Acceptance, and Business Use

This Services Agreement (the "Agreement") is a binding agreement between Cannon Creations LLC ("Cannon," "we," "us," or "our") and the person accepting it and, when that person acts for a law firm, company, client, or other organization, that organization (the "Customer," "you," or "your"). This Agreement governs access to and use of Cannon Caseworks, including its litigation-support, document-review, case-intelligence, collaboration, and work-product features (the "Service"). References in an acceptance record or incorporated document to the "Terms" or "Terms of Service" mean this Agreement.

The Data Processing Addendum (the "DPA") is incorporated into these Terms when Cannon processes personal data for Customer. The Privacy Notice explains Cannon's own information practices, and the Responsible AI Use notice describes mandatory safeguards for AI-assisted features. By checking the acceptance box, creating an account, accepting an invitation, uploading Customer Content, or using the Service, you accept these Terms and the incorporated DPA and acknowledge those notices.

If you use the Service for an organization, you represent that you have authority to bind that organization. If you lack that authority or do not agree, you must not accept an invitation, upload content, or use the Service. Each Authorized User is also individually bound by the account-security, acceptable-use, confidentiality, intellectual-property, and dispute provisions applicable to that person's conduct.

The Service is offered only for business, professional, and authorized client-collaboration use. It is not offered for personal or household use, to minors, or as a self-help legal-representation service.

**Related materials:** Privacy Notice: </legal/privacy> | Responsible AI Use: </legal/ai-use> | Data Processing Addendum: </legal/dpa>

### 2. Defined Terms

"Authorized User" means a person whom Customer permits to access a workspace. "Customer Content" means documents, files, images, audio, video, extracted text, case details, personal information, prompts, instructions, annotations, attorney notes, and other material submitted to or generated from Customer's use of the Service. "AI Output" means a summary, label, category, classification, draft, recommendation, citation, extraction, or other output generated with an automated model.

"Operational Data" means account, authentication, role, device, audit, usage, performance, security, support, entitlement, and billing information used to operate and protect the Service. Operational Data does not include the substance of documents, extracted document text, case facts, prompts, attorney notes, or AI Output.

"Service Provider" means a vendor that processes information for Cannon solely to provide infrastructure, storage, authentication, OCR, email, billing, security, support, analytics, or AI-processing functions needed for the Service.

### 3. Accounts, Firm Administration, and Access

Customer is responsible for selecting Authorized Users, assigning appropriate roles, reviewing invitations, removing access promptly, and ensuring that each Authorized User complies with these Terms. Firm administrators may control workspace membership and access to Customer Content.

You are responsible for safeguarding passwords, authentication methods, invite links, devices, and billing credentials. You must promptly notify Cannon at the contact address below if you suspect unauthorized access, credential compromise, or an incorrect workspace role.

Customer is responsible for all activity performed through its accounts unless the activity results directly from Cannon's breach of these Terms or failure to follow Customer's documented access instructions.

### 4. Limited License and Service Restrictions

Subject to these Terms and payment of applicable fees, Cannon grants Customer a limited, non-exclusive, non-transferable, non-sublicensable right during the applicable service period to permit Authorized Users to access and use the Service for Customer's internal professional work and authorized client collaboration.

You may not use the Service to violate law, professional obligations, court orders, protective orders, client instructions, or third-party rights; access another customer's data; bypass access, security, usage, or billing controls; introduce malicious code; conduct security testing without written authorization; scrape the Service; or reverse engineer, copy, resell, or use the Service to develop a competing product or model except to the extent a restriction is prohibited by law.

You may not use the Service to make a solely automated decision that determines a person's eligibility for or access to employment, housing, education, credit, insurance, health care, legal services, government benefits, or another legally significant opportunity; to create or match a faceprint, voiceprint, or other biometric identifier; to conduct unlawful surveillance or interception; to discriminate unlawfully; or to generate unlawful sexual, exploitative, violent, fraudulent, or rights-infringing material.

You may not represent that Cannon provides legal advice, has verified AI Output, has approved a filing or disclosure, or has certified compliance with a court rule, discovery obligation, privilege determination, legal deadline, or professional standard.

### 5. Customer Content Ownership and Limited Processing License

As between Cannon and Customer, Customer retains all right, title, and interest it lawfully holds in Customer Content. Subject to third-party rights and applicable law, Cannon assigns to Customer any right, title, or interest Cannon may obtain in AI Output generated specifically for Customer through the Service.

Customer grants Cannon a limited, non-exclusive license to host, copy, transmit, format, extract, index, analyze, display, and otherwise process Customer Content only as necessary to provide, secure, support, and administer Customer's case workspace; perform the specific functions Customer requests; comply with Customer's documented instructions; prevent fraud or misuse; and comply with law. This license ends when the relevant processing is no longer reasonably necessary, subject to the retention provisions below.

Cannon does not acquire ownership of Customer Content. Similar or identical AI Output may be generated for other users because automated models can produce similar responses from similar instructions; this does not give another customer access to Customer Content.

## 6. Cannon's Restricted-Use Commitment

Cannon will use Customer Content only to operate and manage the Customer's case workspace and to deliver the workspace functions Customer requests, including document ingestion, OCR, search, summarization, labeling, categorization, relevance and priority review, case-context analysis, drafting, reporting, collaboration, support, and security.

Cannon will not sell, rent, broker, advertise against, or commercially exploit Customer Content; disclose it to other customers; use it to build profiles for advertising; or use it to train, fine-tune, evaluate, benchmark, or improve a Cannon-owned or generally available AI model or dataset. Cannon will not opt Customer Content into a third-party provider's voluntary data-sharing or model-training program.

Cannon may use Operational Data to authenticate users, administer accounts, meter usage, invoice, maintain audit trails, detect abuse, investigate incidents, troubleshoot, and improve the reliability and security of the Service. Cannon will not use the substance of Customer Content for generalized product analytics or product improvement unless Customer separately and expressly submits that material as feedback for that purpose.

## 7. Confidentiality, Privilege, and Compelled Disclosure

Cannon will treat Customer Content as Customer's confidential information and protect it using at least the same degree of care Cannon uses for its own confidential information of similar sensitivity, and no less than reasonable care. Cannon will use Customer Content only as permitted by this Agreement and limit access to personnel and Service Providers who need access to perform the Service and who are subject to confidentiality obligations. Cannon will not intentionally access the substance of Customer Content except to provide requested support, investigate a security or service issue, comply with Customer's instructions, or meet a legal obligation.

Customer will protect Cannon's nonpublic pricing, security materials, architecture, credentials, audit responses, product plans, and other information identified as confidential or that a reasonable person would understand to be confidential using at least reasonable care, and will use it only for evaluating, receiving, securing, and administering the Service. Confidential information does not include information the receiving party can document was lawfully known without restriction, independently developed without use of the information, rightfully received from another source without restriction, or made public through no breach of this Agreement.

The parties do not intend Cannon's processing to waive attorney-client privilege, work-product protection, confidentiality, or any other protection. Cannon does not determine whether a protection applies, and use of a third-party processor can affect a court's or authority's analysis. Customer remains responsible for privilege, confidentiality, ethical, protective-order, and client-authorization decisions.

If either party receives legal process seeking the other party's confidential information, it may disclose only the information it reasonably believes it is legally required to disclose. Unless prohibited by law or an emergency, the receiving party will use reasonable efforts to notify the other party before disclosure so that party may seek protection. Cannon may disclose information when reasonably necessary to address an imminent threat, prevent fraud or abuse, or protect the security and legal rights of Cannon, the Service, users, or others.

## 8. Service Providers and Necessary Disclosures

Customer understands that operating a cloud service requires limited disclosure of data to Service Providers. Cannon may provide Service Providers only the information reasonably necessary for their assigned function and may use them only to operate, secure, support, or deliver the Service—not for advertising, data brokerage, or an unrelated commercial purpose.

Depending on the requested feature and Cannon's configuration, Customer Content may be processed by Google Cloud and Firebase for backend compute, application hosting, authentication, database, object storage, application protection, task execution, malware scanning, OCR, document processing, and optional analytics; by Vercel for delivery and hosting of the web application; by OpenAI for generative AI processing; and by Brevo for transactional email. Email and billing providers ordinarily receive contact, delivery, or transaction information rather than case-document content, except when Customer directs content to be included in a communication.

Cannon remains responsible for its selection and configuration of Service Providers, but third-party services remain subject to their own technical limitations, legal obligations, security events, and contract terms. The provider-specific terms below control over an inconsistent general statement. Cannon may update subprocessors in accordance with the DPA and will not materially reduce the protection of Customer Content without notice when notice is legally or contractually required.

## 9. What Is Sent to OpenAI and Why

To perform a generative AI-assisted function, Cannon may transmit the minimum reasonably necessary portion of Customer Content to OpenAI. Depending on the function, this may include extracted document text, selected excerpts, filenames or limited metadata, case-specific review criteria, issue labels, prompts, user questions, bounded case context, images, audio, or draft work product.

OpenAI processes that material to return the requested summary, transcription, description, label, category, relevance or priority assessment, routing plan, answer, draft, or report. Cannon does not authorize OpenAI to use Customer Content for advertising or for another customer's workspace.

AI Output may be inaccurate, incomplete, outdated, biased, unsupported, or non-unique. It may omit material facts or misclassify privilege, responsiveness, relevance, chronology, parties, or legal significance. AI Output is an assistive draft and must be reviewed against source records by a qualified lawyer before reliance, filing, service, production, disclosure, or client communication.

## 10. OpenAI API Processing

Cannon may use OpenAI's business API services for reporting, case-context synthesis, answers, drafting, image description, and audio or video transcription. Cannon uses API access rather than placing Customer Content into a public consumer chat account.

OpenAI's published API data controls state that API data is not used to train or improve OpenAI models unless the API customer expressly opts in. Cannon does not opt Customer Content into model training or voluntary data sharing and configures requests not to store application state where the relevant endpoint supports that setting.

No-training is not the same as zero retention. Under OpenAI's standard API controls, prompts, responses, and derived metadata may be retained in abuse-monitoring logs for up to thirty days, unless longer retention is required by law or reasonably necessary to prevent harm. Zero Data Retention, modified monitoring, data residency, and a HIPAA business associate addendum apply only when Cannon confirms them in a separate written agreement; these Terms do not represent that those enhanced controls are enabled.

**Related materials:** OpenAI API data controls: <https://developers.openai.com/api/docs/guides/your-data>

## 11. Google Cloud and Document AI Processing

Cannon uses Google Cloud Run for its backend API, processing workers, and supporting compute services. Cannon uses Google Firebase and related Google Cloud services for authentication, application protection,

Firestore records, object storage, task execution, malware scanning, and related infrastructure. Vercel hosts and delivers the web application but does not replace Google Cloud as Cannon's backend compute and data infrastructure. When configured, Google Document AI receives PDFs, images, and related metadata to extract text and layout. Google Document AI is used for document processing and OCR, not as Cannon's generative model provider.

Google processing is governed by Cannon's applicable Google Cloud or API terms and configuration. Customer must not assume that a particular Google data-residency, HIPAA, customer-managed-key, or zero-retention control applies unless Cannon confirms it in a signed agreement. Firebase Analytics is not used for the substance of Customer Content and is subject to the tracking choice described in the Privacy Notice.

**Related materials:** Google Cloud data processing terms: <https://cloud.google.com/terms/data-processing-addendum> | Firebase privacy and security: <https://firebase.google.com/support/privacy> | Document AI security: <https://cloud.google.com/document-ai/docs/security>

## 12. Connected Accounts and One-Time Imports

At Customer's direction, the Service may connect to Gmail, Google Drive, Microsoft Outlook, or Microsoft OneDrive using provider OAuth authorization. The Service requests provider-specific read access, receives identifiers and access credentials, previews selected messages or files, and copies only Customer-selected or query-matched material and associated metadata into the designated case workspace.

Import grants are encrypted, limited to the authorizing user, case, provider, and import, and configured to expire after a short period. The Service deletes active grant records after completion, cancellation, failure, or expiry, subject to transient logs, provider records, backups, and legal preservation requirements. Revoking a grant prevents new provider access but does not delete material already copied into the workspace; that material follows the workspace retention and deletion rules.

Customer represents that it has authority to access and collect the connected account, messages, files, attachments, participants, metadata, and custodial material and is responsible for preservation, employee notice, consent, communications-privacy, discovery, and cross-border requirements.

## 13. Data Processing Addendum

When Cannon processes personal data in Customer Content on Customer's behalf, Customer is the controller or business and Cannon is the processor or service provider, as those terms or their equivalents are used by applicable privacy law. The incorporated DPA states the processing instructions, subject matter, duration, purposes, data and data-subject categories, confidentiality, security, assistance, incident, deletion or return, assessment, and subprocessor obligations.

Customer is responsible for its independent controller obligations, including lawful collection, notices, legal bases, rights handling, data minimization, sensitive-data consent where required, and instructions to Cannon. Cannon will notify Customer if it reasonably believes a documented instruction violates applicable privacy law and may suspend the affected processing while the parties address it.

**Related materials:** Data Processing Addendum: </legal/dpa>

## 14. Restricted and Regulated Data

Unless Cannon agrees otherwise in a signed agreement, the Service is not represented as compliant with HIPAA, data-residency mandates, government-classification requirements, export-controlled-data requirements, criminal-justice information requirements, biometric-data laws, or any customer-specific

security framework. A general confidentiality obligation is not a substitute for a required data-processing agreement, business associate agreement, protective-order undertaking, or security addendum.

Customer must not upload classified information, payment-card authentication data, account passwords, private encryption keys, unlawful surveillance material, or content whose processing by the configured providers is prohibited. Customer must minimize Social Security numbers, financial-account credentials, medical details, children's data, biometric identifiers, and similarly sensitive information unless necessary, authorized, and covered by appropriate written terms.

If Customer requires provider restrictions, zero retention, regional processing, a business associate agreement, a data-processing agreement, a security review, a subprocessor commitment, or custom deletion terms, those requirements must be agreed in writing before the affected content is submitted.

## 15. Security, Incidents, and Customer Safeguards

Cannon uses administrative, technical, and organizational safeguards designed to protect Customer Content against unauthorized access, use, alteration, and disclosure. No cloud, AI, authentication, storage, or communication system can be guaranteed perfectly secure, uninterrupted, or error-free.

After Cannon becomes aware of a security incident involving unauthorized access to, acquisition of, or legally reportable loss of Customer Content, Cannon will notify the affected Customer without undue delay and within any period applicable to Cannon as a processor or data custodian, consistent with legitimate containment, investigation, remediation, and law-enforcement restrictions. Notice is not an admission of fault or liability. Cannon may provide notice through the workspace administrator's account email unless a signed agreement specifies another method.

Customer must use appropriate access roles, multifactor authentication where available, secure devices and networks, independent backups, privilege and production-review procedures, and its own legal-hold and deadline systems. The Service must not be used as the only copy of an important record or as the sole system for legal holds, deadline control, privilege review, or production authorization.

## 16. Retention, Export, and Deletion

Cannon may retain Customer Content while the applicable workspace remains active and for the period reasonably necessary to provide requested features, maintain authorized backups and audit records, complete deletion processes, resolve disputes, investigate abuse or security events, and comply with law. Cannon will not retain Customer Content merely to train models, build generalized datasets, advertise, or sell data.

Subject to workspace authority, technical feasibility, legal holds, legal requirements, and third-party rights, Customer may request deletion of an account or workspace by contacting Cannon. Deletion from active systems may not immediately remove encrypted backups, security logs, billing records, acceptance records, or information that Cannon must preserve by law; retained copies remain subject to applicable confidentiality and use restrictions until deleted or rendered inaccessible through ordinary operations.

Third-party providers may maintain their own copies under their applicable retention rules. In particular, standard OpenAI monitoring retention may continue after Cannon deletes its active copy. Cannon will reasonably assist with a verified provider-related rights request when the provider offers an applicable mechanism and the request is legally available.

## 17. Customer Authority and Professional Responsibilities

Customer represents that it has all ownership rights, licenses, client permissions, data-processing authority, protective-order permissions, confidentiality permissions, and other approvals needed to submit Customer Content, permit Service Provider processing, and instruct Cannon as described in these Terms.

Customer is solely responsible for attorney supervision, competence, confidentiality and privilege decisions, client disclosures and informed consent, conflicts, court and professional rules, legal research and citation checks, discovery and preservation obligations, redaction, admissibility, deadlines, filings, service, productions, and every decision to rely on, edit, send, file, produce, or disclose Customer Content or AI Output.

Customer must independently verify material statements and citations against the source record and controlling authority. A label or workflow status does not establish that a document is privileged, non-privileged, responsive, non-responsive, admissible, authentic, complete, accurate, or safe to disclose.

## 18. No Legal Services or Professional Relationship

Cannon Creations LLC is not a law firm and does not provide legal advice, representation, legal opinions, malpractice coverage, or professional judgment. No attorney-client, fiduciary, expert-witness, co-counsel, or similar professional relationship is created between Cannon and Customer, an Authorized User, a client, or any person identified in Customer Content.

The Service is a software work aid. Outputs are not court findings, certified legal research, final discovery coding, or a substitute for review by a lawyer competent in the relevant matter and jurisdiction.

## 19. Fees, Plans, Taxes, and Service Changes

Fees, seats, usage allowances, service periods, renewal terms, onboarding, taxes, payment timing, and refunds may be stated in an order form, invoice, statement of work, or separate agreement. Except where law or a signed agreement requires otherwise, fees are non-refundable and Customer is responsible for applicable taxes other than taxes on Cannon's net income.

Cannon may correct billing, entitlement, metering, or tax errors and may change, suspend, or retire features, providers, models, plans, limits, or workflows. Cannon will use reasonable efforts to give notice before a change that materially reduces a paid core function or materially changes the disclosed handling of Customer Content, when practicable.

Provider outages, policy changes, rate limits, safety restrictions, model changes, and infrastructure failures may delay or prevent processing. Cannon may substitute a provider only in a manner consistent with these Terms or after providing an updated material data-use notice.

## 20. Suspension and Termination

Cannon may suspend or restrict access when reasonably necessary to address a Terms violation, nonpayment, legal requirement, security threat, provider restriction, abuse, unauthorized use, or operational risk. When practicable, Cannon will limit a suspension to the affected account, workspace, content, or feature and provide notice and a reasonable opportunity to cure.

Customer may stop using the Service at any time and may request account or workspace closure. Termination does not eliminate accrued payment obligations or provisions that should survive by their nature, including ownership, confidentiality, restricted use, retention, disclaimers, liability limits, indemnity, disputes, and record-preservation rights.

## 21. Disclaimers

TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE SERVICE AND ALL AI OUTPUT ARE PROVIDED "AS IS" AND "AS AVAILABLE." CANNON DISCLAIMS ALL EXPRESS, IMPLIED, STATUTORY, AND OTHER WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, AVAILABILITY, SECURITY, AND UNINTERRUPTED OR ERROR-FREE OPERATION.

Cannon does not warrant that the Service or AI Output will satisfy professional duties, client instructions, outside-counsel guidelines, court rules, discovery obligations, evidentiary standards, privilege or confidentiality requirements, deadlines, regulatory obligations, or any legal, financial, business, or operational outcome.

## 22. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY LAW, CANNON AND ITS AFFILIATES, OWNERS, OFFICERS, EMPLOYEES, CONTRACTORS, LICENSORS, AND SERVICE PROVIDERS WILL NOT BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY, PUNITIVE, OR ENHANCED DAMAGES; LOSS OF PROFITS, REVENUE, GOODWILL, DATA, OPPORTUNITIES, OR BUSINESS; PROFESSIONAL NEGLIGENCE BY USERS; MISSED DEADLINES; FILING, DISCOVERY, PRIVILEGE, PRODUCTION, OR REDACTION ERRORS; COURT SANCTIONS; CLIENT DISPUTES; OR RELIANCE ON AI OUTPUT, EVEN IF ADVISED THAT SUCH DAMAGES WERE POSSIBLE.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE TOTAL AGGREGATE LIABILITY OF CANNON AND THE OTHER CANNON PARTIES FOR ALL CLAIMS ARISING OUT OF OR RELATING TO THE SERVICE OR THESE TERMS WILL NOT EXCEED THE GREATER OF THE AMOUNTS PAID TO CANNON FOR THE AFFECTED WORKSPACE DURING THE TWELVE MONTHS BEFORE THE EVENT GIVING RISE TO LIABILITY OR ONE HUNDRED U.S. DOLLARS.

The exclusions and cap apply collectively under all theories of liability and even if a remedy fails of its essential purpose. They do not exclude liability that applicable law does not permit the parties to exclude or limit.

## 23. Indemnity

Customer will defend, indemnify, and hold harmless Cannon and its affiliates, owners, officers, employees, contractors, licensors, and Service Providers from third-party claims, liabilities, damages, judgments, settlements, penalties, losses, and reasonable legal fees arising from Customer Content; Customer's or an Authorized User's use of the Service; breach of these Terms; violation of law, court order, professional duty, client instruction, or third-party right; or a dispute between Customer and its client, user, employee, opposing party, or another third party.

Cannon will promptly notify Customer of an indemnified claim, permit Customer to control the defense with qualified counsel, and provide reasonable cooperation at Customer's expense. Customer may not settle a claim in a manner that admits fault by, imposes an obligation on, or fails to fully release a Cannon indemnified party without Cannon's written consent, which will not be unreasonably withheld. Cannon may participate with counsel at its own expense.

## 24. Disputes, Arbitration, Governing Law, and Claim Period

Before filing a claim, a party must send written notice describing the dispute and requested relief and allow at least thirty days for good-faith informal resolution, unless urgent injunctive or equitable relief is reasonably necessary.

To the maximum extent permitted by law, disputes arising out of or relating to the Service or these Terms will be resolved by binding individual arbitration under the Federal Arbitration Act and the American Arbitration Association Commercial Arbitration Rules then in effect, before one arbitrator. Arbitration may be conducted remotely unless the arbitrator requires otherwise. The arbitration will be conducted in English, and the legal seat will be Texas. Judgment on the award may be entered in any court with jurisdiction.

YOU AND CANNON WAIVE TRIAL BY JURY AND PARTICIPATION IN CLASS, COLLECTIVE, CONSOLIDATED, PRIVATE-ATTORNEY-GENERAL, OR REPRESENTATIVE PROCEEDINGS TO THE EXTENT ENFORCEABLE. Either party may bring an eligible individual claim in small-claims court or seek temporary or preliminary injunctive relief in court to preserve the status quo, protect confidentiality or intellectual property, or prevent unauthorized access or an imminent security threat without waiving arbitration of the merits.

You may opt out of arbitration and the class-action waiver by emailing Cannon within thirty days after first accepting these Terms and clearly stating your name, account email, organization, and decision to opt out. Opting out does not affect the other Terms.

These Terms are governed by Texas law, without regard to conflict-of-law rules. When arbitration does not apply, the parties consent to exclusive jurisdiction and venue in the state or federal courts having jurisdiction over Cannon's principal office in Texas. To the maximum extent permitted by law, a claim arising from the Service or these Terms must be brought within one year after the claim accrued.

## 25. Updates, Order of Precedence, and General Terms

Cannon may update these Terms prospectively. Cannon will identify the effective date and provide reasonable notice of a material change through the Service, by email, or another reasonable method. Cannon may require affirmative reacceptance. Continued use after the effective date constitutes acceptance when permitted by law, but a material change does not retroactively alter a claim that accrued before the change.

A signed order form, statement of work, data-processing agreement, business associate agreement, security addendum, or enterprise agreement may supplement these Terms. For a direct conflict, the signed document controls only for its subject matter, followed by these Terms and then incorporated policies, unless the signed document states a different order.

Cannon may assign these Terms in connection with a merger, acquisition, financing, reorganization, asset sale, corporate transaction, or transfer of the Service. Customer may not assign these Terms without Cannon's prior written consent. The parties are independent contractors; these Terms create no partnership, joint venture, franchise, employment, or agency relationship.

If a provision is unenforceable, it will be enforced to the greatest lawful extent and the remaining provisions will remain effective. Failure to enforce a provision is not a waiver. Headings are for convenience. These Terms and the documents identified above are the complete agreement about the Service and supersede prior or contemporaneous discussions on that subject.

## 26. Contact and Legal Notices

Questions, legal notices, arbitration opt-outs, security notices, privacy requests, and data-use questions may be sent to Cannon Creations LLC at the contact email below. Notice to Customer may be sent to the workspace

owner's or administrator's account email and is effective when sent, unless a signed agreement provides otherwise.

## Exhibit A

### Data Processing Addendum

This Data Processing Addendum is incorporated into and forms part of the Cannon Caseworks Services Agreement above.

#### 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](mailto:support@cannoncaseworks.com) with "Data Processing" in the subject line.