

LIGHTFIELD STANDARD ADDENDUM

Lightfield Data Processing and Privacy Addendum

Lightfield DPA Form v1.1 (2026-08-07)

Prepared	August 7, 2026
Status	Lightfield founder-approved standard form
Use	Subscription agreement attachment before personal-data processing or customer production-system connection.

This is Lightfield's founder-approved standard Data Processing and Privacy Addendum and forms part of the Agreement as stated below.

1. Parties and Scope

This Data Processing and Privacy Addendum ("Addendum") supplements the Lightfield Master Subscription Agreement and each applicable Order Form, or other Lightfield subscription agreement, between Lightfield, Inc. ("Lightfield") and the customer identified in that agreement ("Customer") (collectively, the "Agreement").

Capitalized terms used but not defined in this Addendum have the meanings given in the Agreement.

This Addendum applies when Lightfield processes Personal Data, Customer legal content, mailbox data, Slack or collaboration messages, attachments, prompts, outputs, or other Customer Data in connection with the Lightfield product.

For applicable privacy-law purposes, including US federal and state privacy laws, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and Alberta's Personal Information Protection Act (PIPA), Lightfield will process Customer Personal Data as a service provider, processor, or equivalent role under Customer's instructions and not for Lightfield's independent commercial purposes except as expressly permitted in the Agreement and this Addendum.

"Personal Data" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked with an identified or identifiable natural person, and includes equivalent terms under applicable privacy law.

"Customer Personal Data" means Personal Data contained in Customer Data that Lightfield processes on Customer's behalf.

"Security Incident" means a confirmed unauthorized acquisition of, access to, use of, disclosure of, alteration of, or destruction of Customer Personal Data or Customer legal content in systems controlled by Lightfield. Security Incident does not include unsuccessful attempts that do not compromise Customer Data, such as blocked scans, pings, denial-of-service attempts, or failed login attempts.

"De-identified Data" means data that cannot reasonably be used, alone or together with other information reasonably available to Lightfield, to identify Customer, an individual, Customer Data, or a Customer matter.

2. Processing Instructions

Lightfield may process Customer Data only to:

- provide, host, secure, maintain, support, troubleshoot, and improve the product for Customer;
- classify, summarize, route, prioritize, and manage Customer legal intake and workflow items;
- maintain audit logs, operational records, and security evidence;
- comply with law, enforce the agreement, prevent abuse, and respond to security incidents;

- create and use aggregated or de-identified operational data as described below.

Customer is responsible for the accuracy, legality, and authorization of Customer Data submitted to Lightfield.

3. AI and Model Use

Lightfield will not use Customer documents, messages, attachments, legal matter descriptions, prompts, outputs, or other Customer-identifiable legal content to train generalized, public, or third-party AI or machine-learning models.

Lightfield may use aggregated data and De-identified Data, including usage data, telemetry, logs, performance metrics, workflow data, classification outcomes, and other derived operational data, to operate, secure, test, evaluate, tune, and improve the product and Lightfield's internal classifiers, workflows, and features. Lightfield will maintain reasonable technical and organizational measures designed to prevent re-identification, will not attempt to re-identify De-identified Data, and will not disclose it externally in a form that identifies Customer, an individual, Customer Data, or a Customer matter.

Where supported by the model provider, Lightfield configures model calls that process Customer legal content — including intake detection, enrichment, summarization, routing, and prioritization calls — to avoid optional response/application-state storage (for OpenAI Agents SDK calls, `store=false`).

4. Security Measures

Lightfield will maintain a written information security program appropriate to the nature of the Customer Data and the service scope. The program will include commercially reasonable administrative, technical, and organizational safeguards, including:

- tenant-scoped access control and server-side tenant isolation;
- encryption in transit for application and API traffic;
- encryption at rest through hosting/database provider controls and application-level encryption for sensitive integration tokens or mailbox credentials;
- least-privilege administrative access;
- MFA for administrative and production access where supported;
- audit logging for security-relevant and customer-data actions;
- secure SDLC practices, dependency review, and security tests appropriate to the service;
- incident response procedures;
- vendor review based on access to sensitive data.

Human access to Customer Data will be limited to personnel or contractors with a need to know for support, security, abuse prevention, legal compliance, incident response, or product operation, and subject to confidentiality obligations.

5. Subprocessors

Lightfield may use subprocessors to provide the product. Lightfield will maintain a current subprocessor list identifying each material subprocessor, the processing purpose, and the relevant data categories.

Third-party services that Customer elects to connect (under MSA §5.7 or the equivalent provision of the Agreement) are not subprocessors requiring advance notice and are disclosed when the integration is enabled.

Lightfield will provide at least thirty (30) days' advance written notice before authorizing a new material subprocessor to process Customer Data. Customer may object during that notice period on reasonable security, privacy, or compliance grounds. The parties will work in good faith to resolve the objection. If Lightfield cannot reasonably resolve it, Lightfield may provide an alternative or disable the affected integration where doing so does not materially reduce the Product's core functionality; if neither is reasonably available, Customer may terminate the affected Order Form (or, where the Agreement has no Order Form, the Agreement) and receive a pro rata refund of prepaid unused Fees under it.

Before a subprocessor processes Customer Data, Lightfield will bind it by a written agreement requiring privacy, confidentiality, security, use restrictions, and return or deletion obligations that are no less protective than the applicable obligations in this Addendum, taking into account the nature of the services. Lightfield will require each subprocessor to return or delete Customer Data as needed for Lightfield to meet Section 7.

Lightfield remains responsible for subprocessors' processing of Customer Data as required by applicable law and the Agreement.

6. Security Incidents

Lightfield will notify Customer without undue delay, and in any event no later than 72 hours after confirming a Security Incident affecting Customer Personal Data or Customer legal content, unless a shorter period is required by applicable law or law enforcement requests delayed notice.

Notice will include, to the extent known and legally permitted:

- the nature of the incident;
- Customer Data reasonably believed to be affected;
- likely consequences;
- steps taken or planned to contain, investigate, and remediate the incident;
- recommended Customer actions, if any.

Lightfield will provide reasonable updates as the investigation progresses and will cooperate with Customer's legally required notices or regulatory responses.

7. Return, Export, and Deletion

During the subscription term and for a reasonable post-termination period, Lightfield will provide Customer a commercially reasonable way to retrieve or export Customer Data in a commonly usable format, unless termination resulted from Customer's uncured breach or unlawful use.

After the post-termination export period, or earlier upon Customer's written request, Lightfield will delete Customer Data from live production systems within 30 days, except for records retained as legally required or under legal hold.

Backup and disaster-recovery copies will be deleted or overwritten according to Lightfield's ordinary retention cycle, not to exceed 90 days. Copies retained under legal hold, as legally required, or in immutable security or audit logs may remain for the applicable retention period only if they are inaccessible to routine Product use, are not restored to production except for disaster recovery or legal compliance, remain subject to confidentiality, security, and no-use restrictions, and are deleted when the applicable exception ends.

Upon request, Lightfield will provide written confirmation of deletion based on available system records and the deletion process completed, and will identify any copies still retained under the exceptions above.

8. Data Minimization for Non-Legal Mail

For ignored or non-legal messages reviewed by the intake classifier, Lightfield will not intentionally retain the full source message body locally solely for false-negative review. Lightfield may retain minimal operational metadata, such as provider message ID, thread ID, mailbox UID or provider timestamp, classification reason, source type, and review/correction status.

If Customer or an authorized manager later promotes an ignored message for legal review, Lightfield may create a manual-review matter using the retained metadata and may require the authorized user to reopen or resubmit source content from the original mailbox or collaboration system.

9. Assistance

Taking into account the nature of the processing and information available to Lightfield, Lightfield will provide reasonable assistance for:

- Customer data subject requests, where applicable;
- security incident investigation and notices;
- privacy or security assessments reasonably required for the service;
- deletion, export, and subprocessor inquiries.

Lightfield may decline requests that would compromise security, disclose another customer's data, reveal confidential security details, or exceed the reasonable support scope under the Agreement unless separately agreed.

10. No Sale; No Cross-Context Behavioral Advertising

Lightfield will not sell Customer Personal Data or share it for cross-context behavioral advertising as those terms are defined under applicable US state privacy laws.

11. Conflict

For this Addendum's subject matter — processing of Personal Data and other Customer Data within its scope — this Addendum controls over conflicting terms of the Agreement. Lightfield's expressly permitted use of aggregated and de-identified operational data remains permitted only to the extent consistent with this Addendum.

Schedule 1: Processing Details

Purpose: AI-assisted legal intake and workflow management for Customer's internal legal team.

Activities: ingesting selected customer communications or manual requests; classifying legal relevance; summarizing legal intake items; routing and prioritizing matters; tracking status, comments, attachments, and audit events; supporting export, deletion, security, and customer support.

Data subjects: Customer employees, contractors, business contacts, counterparties, vendors, applicants, customers, and other individuals whose information appears in Customer-submitted legal intake materials.

Data categories: names, email addresses, business contact details, employment or role information, legal intake requests, legal matter descriptions, messages, attachments, prompts, outputs, status metadata, comments, audit events, integration metadata, and operational telemetry.

Sensitive data: Customer may submit privileged legal material, confidential business information, employment information, regulated or sensitive personal information, or other sensitive content depending on the connected systems and Customer use. Customer must not submit protected health information, payment-card data, or export-controlled technical data unless a separate written agreement permits the applicable data class.

Duration: each applicable Order Term or subscription term, plus the deletion/export and backup-retention periods described above.

Signatures

Signed by electronic signature. For an initial execution, MSA §11.10 (envelope atomicity) applies.

LIGHTFIELD, INC.

By: _____

Name:

Title:

Date:

CUSTOMER

By: _____

Name:

Title:

Date: