

Data Processing Addendum

Adopted August 2, 2026

This Data Processing Addendum (“DPA”) supplements and forms part of the Maverick Terms of Service (the “Terms”) between Mike Sheridan Digital LLC, a West Virginia limited liability company (“MSD,” “we,” “us”), and the customer agreeing to the Terms (“Customer,” “you”). It explains how we handle personal data you submit, who processes it on our behalf, and what we commit to. Capitalized terms not defined here have the meanings given in the Terms and in our Privacy Practices. This DPA is automatically incorporated into the Terms; no separate signature is required.

1. Definitions

“Customer Content” has the meaning given in the Terms: the queries, documents, and other materials you submit, and the research results and conversations generated in the Workbench.

“Personal Data” means information relating to an identified or identifiable natural person contained in Customer Content or in Customer’s account data.

“Processing,” “Controller,” “Processor,” and “Data Subject” have the meanings given under applicable data protection law. “Subprocessor” means a third party engaged by MSD to Process Personal Data on Customer’s behalf.

“Security Incident” means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by MSD. Unsuccessful attempts, routine scans, and pings that do not compromise Personal Data are not Security Incidents.

2. Roles and scope

As between the parties, Customer is the Controller and MSD is the Processor with respect to Personal Data in Customer Content. Where Customer acts as a processor for its own clients, MSD acts as a subprocessor, and Customer’s instructions are deemed to reflect its own clients’ instructions.

Customer is responsible for the lawfulness of Personal Data it submits, including obtaining any client consent required under applicable rules of professional conduct before submitting particular materials.

This DPA applies only to Processing performed by MSD. It does not apply to processing performed by an AI provider Customer designates under Section 7.3, which is governed by Customer’s own agreement with that provider.

Health information. The service is not a HIPAA-compliant service. MSD is not a business associate of Customer within the meaning of 45 C.F.R. Parts 160 and 164, does not execute Business Associate Agreements, and assumes none of a business associate’s obligations. MSD recognizes that legal matters —

personal-injury and medical-malpractice matters in particular — routinely involve medical records, and that a lawyer researching such a matter may need to describe medical facts. Customer may submit health information incidental to a legal matter it is handling, on the same confidentiality terms as all other Customer Content. Customer must not use the service to process protected health information on behalf of, or as a service provider to, a HIPAA covered entity or business associate, and must not submit health information in bulk or for any purpose other than researching a legal matter. Customer remains solely responsible for determining what material to submit, for minimizing identifiable health information where practicable, and for its own obligations under HIPAA and applicable professional-responsibility rules. MSD has no liability arising from Customer's submission of health information in breach of this Section.

3. Processing instructions

MSD will Process Personal Data only to provide, secure, and support the service; as otherwise documented in the Terms, the Privacy Practices, and this DPA; and per Customer's other lawful written instructions.

MSD does not sell Personal Data, does not use Customer Content to target advertising, and does not use Customer Content to train its own models.

If MSD believes an instruction violates applicable law, it will inform Customer and may suspend that Processing.

4. Confidentiality

MSD treats Customer Content as confidential, consistent with Section 8 of the Terms and Section 7 of the Privacy Practices. MSD limits access to personnel who need it to operate and support the service, and binds them to confidentiality obligations.

MSD acknowledges Customer Content may reflect privileged or confidential client matters. Access is limited to what is necessary to operate and support the service.

5. Security

MSD maintains administrative, technical, and organizational safeguards designed to protect Personal Data, including encryption in transit, access controls, and scoped credentials, as described in Section 8 of the Privacy Practices.

MSD will not materially degrade the overall security of the service during the term.

6. Subprocessors

Customer generally authorizes MSD to engage Subprocessors. The current list appears in Schedule A below.

MSD imposes data protection obligations on each Subprocessor no less protective than those in this DPA, and remains liable for its Subprocessors' performance.

Notice and objection. MSD will notify Customer before adding a new Subprocessor that Processes Customer Content, by email to the account's registered address or by updating Schedule A with notice. Customer may object on reasonable data protection grounds within fifteen (15) days. If the parties cannot resolve the objection, Customer may terminate the affected subscription and receive a pro-rata refund of prepaid, unused fees.

7. Artificial-intelligence processing

Which parties enter the processing chain depends on the plan you choose. This Section states that plainly.

Retrieval (all plans). Delivering research requires converting queries into vector embeddings to search the corpus. Query text is transmitted to our embeddings provider (Schedule A) on every plan, including bring-your-own-AI. Retrieval is not avoidable by plan selection.

Hosted AI (MSD-designated provider). Where Customer uses the hosted Workbench, MSD transmits queries and retrieved source text to the AI provider identified in Schedule A as MSD's Subprocessor, under MSD's agreement with that provider.

Bring your own AI (Customer-designated provider). Where Customer designates its own AI provider, that provider processes Customer Content under Customer's own account and that provider's terms. That provider is not MSD's Subprocessor, MSD does not control its retention or training practices, and Section 2.3 applies.

Retention at the AI provider. MSD's designated AI provider is Anthropic, PBC, operating under Anthropic's Commercial Terms of Service and the Data Processing Addendum automatically incorporated therein. Under Anthropic's standard API terms, inputs and outputs are deleted within thirty (30) days of receipt or generation, except where longer retention is required to enforce Anthropic's usage policy or comply with law. MSD does not currently have a zero-data-retention arrangement with Anthropic. Customer should account for this in its own confidentiality assessment. This paragraph does not apply where Customer designates its own AI provider.

Output. AI output is probabilistic and may be inaccurate or incomplete, as stated in Sections 1, 2, and 11 of the Terms. Nothing in this DPA alters those disclaimers.

8. Data subject requests

Taking into account the nature of the Processing, MSD will provide reasonable assistance to enable Customer to respond to Data Subject requests.

If MSD receives such a request directly, it will not respond substantively except to direct the Data Subject to Customer, unless legally required otherwise.

9. Security incident notification

MSD will notify Customer without undue delay, and in any event within seventy-two (72) hours, of becoming aware of a Security Incident affecting Customer's Personal Data.

The notice will describe, to the extent known: the nature of the incident, the categories and approximate volume of affected data, likely consequences, and measures taken or proposed.

Notice is not an acknowledgment of fault or liability.

10. Retention, return, and deletion

Workbench conversations are ephemeral. They purge automatically after 24 hours by default; Customer may select a longer period (up to 90 days) in account settings. Retention is Customer-configurable and Customer-selected.

Account and billing information is retained while the account is active and thereafter as needed for legitimate business and legal purposes.

On termination, MSD will delete or de-identify Personal Data within a reasonable period, except where retention is required by law or where data has been aggregated or de-identified such that it no longer identifies any person.

Customer may export or delete its data through the service before termination.

11. Audits and information

MSD will make available information reasonably necessary to demonstrate compliance with this DPA, including responses to reasonable security questionnaires, no more than once per twelve (12) months absent a Security Incident or legal requirement.

Given the size and nature of the service, on-site audits are not offered. Requests are satisfied through written information and documentation.

12. Location of processing

MSD Processes Personal Data in the United States. Production hosting — the application, database, legal corpus, and search serving — is located in New Jersey, USA. The API gateway, encrypted database backups, and secrets management are located in the eastern United States.

MSD does not currently transfer Personal Data outside the United States in the ordinary course of providing the service. Where any such transfer becomes necessary, MSD will implement an appropriate transfer mechanism where required by applicable law.

13. General

Order of precedence. In case of conflict regarding Processing of Personal Data, this DPA controls over the Terms. In all other respects the Terms control.

Liability. Each party's liability under this DPA is subject to the limitations and exclusions in Section 12 of the Terms.

Incorporation and term. This DPA is automatically incorporated into and forms part of the Terms; no separate signature is required. By accepting the Terms, Customer accepts this DPA. It continues while MSD Processes Personal Data on Customer's behalf.

Governing law. These provisions are governed by the laws of the State of West Virginia, with exclusive venue in the state or federal courts located in Greenbrier County, West Virginia, per Section 16 of the Terms.

Beta. The service is offered on a beta basis per Section 1 of the Terms. This DPA does not alter that status.

Contact. Questions about this DPA: support@mavericklegalresearch.com — Mike Sheridan Digital LLC, Post Office Box 204, Maxwelton, West Virginia 24957.

Schedule A — Subprocessors

The following process Customer Content — research queries and material you submit:

Vultr Holdings LLC — primary production hosting: application, database, legal corpus, and search serving. Processes all Customer Content at rest and in transit. Located in New Jersey, USA.

Microsoft Azure — API gateway, encrypted database backups, and secrets management. Processes API traffic in transit and backups containing Customer Content.

Voyage AI — query embeddings for corpus retrieval, on all plans including bring-your-own-AI. Processes query text.

Anthropic, PBC — hosted AI model provider, used only on the hosted “Use Our AI” path. Processes queries and retrieved source text.

The following process account, billing, and support data, and do not receive research content unless a user submits it in a message or support request:

Stripe, Inc. — payment processing (billing details, card metadata).

Postmark (ActiveCampaign) — transactional email (name, email, message content).

Zoho Corporation — support ticketing (Desk) and accounting (Books): contact details and any content a user includes in a ticket.

GitHub, Inc. — in-app bug and feature reports: the report text a user submits.

Sentry (Functional Software, Inc.) — error monitoring and diagnostics, configured with personal-information collection disabled.

An AI provider that Customer designates under Section 7.3 is not an MSD Subprocessor and is not listed here.