



DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") forms part of and is incorporated into the Vellor Terms of Service (the "Agreement") between Ellis Tech LLC ("Vellor," "we," "us") and the customer that accepts the Agreement ("Customer," "you"). It governs Vellor's Processing of Customer Personal Data and takes effect when you accept the Agreement or execute this DPA (the "Effective Date").

1. Definitions

- **Applicable Privacy Laws** means the U.S. state privacy laws applicable to the Processing, including the California Consumer Privacy Act as amended by the CPRA ("CCPA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and comparable state laws as they take effect.
- **Customer Personal Data** means Personal Information within Customer Data that Vellor Processes on Customer's behalf under the Agreement.
- **Controller, Business, Processor, Service Provider, Process/Processing, Sell, Share, Consumer, and Data Subject** have the meanings given in Applicable Privacy Laws.
- **Sub-processor** means a third party engaged by Vellor to Process Customer Personal Data.
- **Security Incident** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to Customer Personal Data.

2. Roles and scope of Processing

For Customer Personal Data, Customer is the Controller and Business, and Vellor is the Processor and Service Provider. Where Customer acts as a processor on behalf of another controller, Vellor acts as a sub-processor. Vellor will Process Customer Personal Data only to provide the Service, as described in Exhibit A, and on Customer's documented instructions (which include the Agreement and Customer's use of the Service). Vellor will inform Customer if, in its opinion, an instruction violates Applicable Privacy Laws.

3. Customer obligations

Customer is responsible for the accuracy and lawfulness of Customer Personal Data and for having all rights, consents, and authorizations necessary to provide it to Vellor, consistent with Customer's professional and ethical obligations, including the duty of confidentiality (for example, ABA Model Rule 1.6 and the equivalent rule in Customer's jurisdiction). Customer's instructions to Vellor will comply with Applicable Privacy Laws.

4. Vellor's Processing obligations

- Process Customer Personal Data only on Customer's documented instructions and only as needed to provide the Service;
- not Process Customer Personal Data for any other purpose;
- ensure that personnel authorized to Process Customer Personal Data are bound by confidentiality;
- implement and maintain the security measures described in Section 7 and Exhibit B; and
- assist Customer as described in Sections 10 through 12.

5. Service Provider and Processor restrictions

Vellor will not:

- Sell or Share Customer Personal Data, as those terms are defined under the CCPA and similar laws;
- retain, use, or disclose Customer Personal Data for any purpose other than performing the Service, or outside the direct business relationship with Customer, except as permitted by Applicable Privacy Laws; or
- combine Customer Personal Data with personal information from other sources, except as permitted by Applicable Privacy Laws to perform the Service.

Vellor certifies that it understands the restrictions in this Section and the Agreement and will comply with them. Vellor provides the Service for the limited and specified purposes described in Exhibit A.

6. Confidentiality

Vellor treats Customer Personal Data as confidential and limits access to personnel who need it to provide and support the Service, under obligations of confidentiality.

7. Security measures

Vellor maintains reasonable and appropriate technical and organizational measures designed to protect Customer Personal Data against a Security Incident, as described in Exhibit B, including encryption in transit and at rest, access controls, and monitoring.

8. AI Processing and no model training

When Customer uses AI features, the inputs Customer provides are sent to Vellor's AI Sub-processor (currently Anthropic) to generate output, which is returned to Customer. Vellor does not use Customer Personal Data to train its own or any third party's general-purpose AI models, and, under its commercial terms, Vellor's AI Sub-processor does not use Customer inputs or outputs to train its models.

9. Sub-processors

Customer authorizes Vellor to engage the Sub-processors listed in Exhibit C to Process Customer Personal Data. Vellor will impose data-protection obligations on each Sub-processor that are no less protective than this DPA and remains responsible for its Sub-processors' performance. Vellor will give notice of any new Sub-processor (for example, by updating Exhibit C or the Data Security and Confidentiality statement), and Customer may object on reasonable data-protection grounds. If the parties cannot resolve the objection, Customer may terminate the affected portion of the Service.

10. Security Incident notification

Vellor will notify Customer without undue delay after becoming aware of a Security Incident affecting Customer Personal Data, provide the information then available, and reasonably cooperate with Customer to help Customer meet its own notification obligations.

11. Data Subject and Consumer requests

Taking into account the nature of the Processing, Vellor will provide reasonable assistance, including appropriate technical and organizational measures, to help Customer respond to verified Consumer or Data Subject requests (such as access, deletion, correction, portability, and opt-out). If Vellor receives such a request directly, it will direct the individual to Customer unless legally required to respond.

12. Audits and verification

Vellor will make available information reasonably necessary to demonstrate compliance with this DPA and will allow for and contribute to audits on reasonable prior written notice, no more than once per year (absent a Security Incident or legal requirement), subject to confidentiality, during business hours, and without unreasonable disruption. Vellor may satisfy these obligations by providing summaries, attestations, or third-party reports where available.

13. Return and deletion of data

On termination or expiration of the Agreement, Vellor will, at Customer's option, make Customer Personal Data available for export for 30 days and will then delete Customer Personal Data within 90 days, except where retention is required by law. Backups are purged on a rolling basis, generally within 90 days.

14. International transfers

The Service is provided in and operated from the United States and is not offered to users in the European Union or United Kingdom. Customer will not provide Vellor with personal data subject to the EU GDPR or UK GDPR without a separate written addendum. Customer Personal Data is Processed in the United States.

15. Liability

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

16. Term

This DPA is effective on the Effective Date and continues for the term of the Agreement and for as long as Vellor Processes Customer Personal Data.

17. Governing law; order of precedence; miscellaneous

This DPA is governed by the laws of the State of Maryland and the dispute-resolution terms of the Agreement. If there is a conflict between this DPA and the rest of the Agreement regarding the Processing of Customer Personal Data, this DPA controls. All other terms of the Agreement remain in full force and effect.

Exhibit A — Details of Processing

Item	Description
Subject matter	Provision of the Vellor Service to Customer under the Agreement.
Duration	The term of the Agreement plus the retention and deletion period in Section 13.
Nature and purpose	Hosting, storing, and Processing Customer Data to provide AI-assisted tools for legal practice, including intake, document drafting preparation, client communication, and matter follow-through.
Types of Personal Information	As determined and submitted by Customer; may include names, contact details, and other information about Customer's clients and matters, which may include sensitive information.
Categories of Data Subjects	Customer's clients, prospective clients, and contacts, and Customer's personnel.

Exhibit B — Technical and Organizational Security Measures

- Encryption of Customer Personal Data in transit (TLS) and at rest;
- Access controls, authentication, and least-privilege access;
- Logging and monitoring;
- Secure, reputable cloud infrastructure (Vercel) and database hosting (Supabase);
- Regular backups; and
- Confidentiality obligations for personnel.

These measures are further described in Vellor's Data Security and Confidentiality statement, which is incorporated by reference.

Exhibit C — Approved Sub-processors

Sub-processor	Purpose	Location
Stripe	Payment processing	United States
Vercel	Application hosting and infrastructure	United States
Supabase	Database and storage	United States
Resend	Transactional and account email	United States
Anthropic	AI processing of inputs to generate output (no model training on Customer data)	United States

Confirm each Sub-processor's actual Processing region and configure US data residency where offered.

Contact: Ellis Tech LLC, 1125 West St., Ste. 581, Annapolis, MD 21401 — support@ellisaitech.com