DATA PROCESSING ADDENDUM

1. APPLICATION

1.1 This Data Processing Addendum and its Schedules ("**DPA**") is incorporated into and forms part of the Services Agreement ("**Agreement**") between [COMPANY NAME] ("**Company**") and Navu, Inc. ("**Service Provider**") pursuant to which Service Provider provides the Services to Company, each a "**Party**" and together the "**Parties**."

1.2 The provisions of this DPA shall apply to the extent required by Data Protection Laws with respect to Service Provider's Processing of Personal Data on behalf of the Company in providing the Services.

1.3 In the event and to the extent of a conflict between this DPA and the Agreement, this DPA shall prevail.

2. DEFINITIONS

2.1 Unless otherwise defined in the Agreement:

"**Controller**" means a party that determines the purposes and means of Processing Personal Data.

"**Services**" means as defined in the Agreement.

"**Data Exporter**" means Company when it transfers Personal Data directly or via onward transfer to Service Provider, and Company is located in a jurisdiction that triggers additional requirements for the protection of Personal Data being transferred in accordance with applicable Data Protection Laws.

"**Data Importer**" means Service Provider where it is located in a country that triggers additional requirements for the protection of Personal Data being transferred in accordance with applicable Data Protection Laws.

"**Data Protection Law(s)**" means applicable laws and regulations on privacy, data protection, or data security.

"**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

"**Processing**" (including its cognate, "**Process**") means any operation or set of operations that is performed upon data, whether or not by automatic means, including, but not limited to, collection, recording, organization, storage, retention, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction.

"**Processor**" means a party that Processes Personal Data on behalf of a Controller.

"**Restricted Transfer**" means a transfer of Personal Data from a Data Exporter located in one jurisdiction to a Data Importer in another jurisdiction where Data Protection Laws require additional safeguards for the protection of the transferred Personal Data.

"**Supervisory Authority**" means any regulatory, supervisory, governmental, or other competent authority with jurisdiction, oversight, or enforcement power in relation to compliance with Data Protection Laws.

2.2 The Parties acknowledge that Data Protection Laws may set forth analogous terms. Where necessary to ensure compliance with such Data Protection Law, the definitions above should be conformed to such analogous terms set forth in the relevant Data Protection Laws.

2.3 Other capitalized terms used in this DPA shall have the meaning ascribed to them in the Agreement (including any other exhibits or schedules incorporated therein).

2.4 A reference to a law, regulation or other document is a reference to such law, regulation or document as amended, superseded or repealed from time to time.

3. ROLES OF THE PARTIES

3.1 Service Provider and Company acknowledge that, to the extent such concepts are recognized under Data Protection Laws, Company is the Controller of Personal Data and Service Provider is the Processor where Service Provider is providing the Services to Company under the Agreement.

4. DETAILS OF PERSONAL DATA PROCESSING

4.1 The Processing description is set out at **Schedule 1** of this DPA.

5. COMPLIANCE WITH LAWS AND COMPANY'S PROCESSING INSTRUCTIONS

5.1 The Parties shall comply with Data Protection Laws. Without limitation, Company shall ensure that its Processing of Personal Data and instructions to Service Provider comply with Data Protection Laws, including by verifying that any Personal Data it shares or provides access to has been obtained in accordance with Data Protection Laws, including with respect to any notices provided to, or consents (if any) obtained from, Data Subjects.

5.2 Service Provider shall Process Personal Data on behalf of Company in accordance with Company's documented instructions, unless required otherwise by applicable law, in which case Service Provider shall inform Company of the legal requirement where legally permitted to do so before commencing such Processing. Service Provider shall inform Company if, in its opinion, an instruction from Company constitutes or would cause a violation of Data Protection Laws.

5.3 For the avoidance of doubt, and to the extent required under Data Protection Laws, Service Provider shall not retain, use, disclose, combine, sell, share, or otherwise Process Personal Data except in the context of the direct business relationship between Service Provider and Company as set out in the Agreement, and as otherwise necessary for the business purposes and the performance of the Services as specified in the Agreement. Service Provider shall notify Company if it can no longer meet its obligations under this DPA.

6. ACCESS AND CONFIDENTIALITY

6.1 Service Provider shall limit access to Personal Data to those individuals with a need-to-know to fulfill the purpose(s) of the Agreement, and ensure that its personnel are subject to appropriate obligations of confidentiality that are consistent with the confidentiality provisions set forth in the Agreement.

7. SUB-PROCESSORS

7.1 Company provides general authorization to Service Provider to appoint sub-Processors in performing the Services, including any third-party service providers. As of the date of this DPA, a list of approved sub-Processors is set out in **Schedule 1** of this DPA.

7.2 Service Provider shall ensure that any sub-Processor is subject to obligations which are substantially similar to those set out in this DPA, and Service Provider shall be liable for the acts and omissions of its sub-Processors.

7.3 Service Provider will notify Company at least thirty (30) days in advance of allowing a new sub-Processor to Process Personal Data of Company. Where so provided by Data Protection Laws, Company may object to Service Provider's appointment of a new sub-Processor if Company reasonably believes that a proposed new sub-Processor will be unable to comply with this DPA or Data Protection Laws. Any such reasonable objection must be submitted to Service Provider in writing before the proposed new sub-Processor commences Processing Personal Data of Company. Service Provider's engagement of such new sub-Processor will otherwise be deemed authorized by Company. Upon receipt of an objection to a proposed sub-Processor, the Parties will cooperate in good faith to seek a mutually agreeable solution. If

after thirty (30) business days the Parties are unable to agree upon an alternative solution, Company may terminate the part of the Services that are dependent upon the proposed sub-Processor.

8. SECURITY

8.1 Service Provider shall maintain reasonable technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, alteration, unauthorized disclosure or access with respect to the Platform, and to provide a level of security appropriate to the risk, including as set forth in **Schedule 2**.

9. DATA SUBJECT REQUESTS

9.1 Where applicable, Company shall be responsible for responding to any requests from Data Subjects exercising their rights under Data Protection Laws ("**Data Subject Requests**").

9.2 Service Provider shall promptly notify Company if Service Provider receives a Data Subject Request concerning Personal Data Service Provider Processes in the provision of the Services to Company.

9.3 To the extent Company in its use of the Services does not have the ability to address a Data Subject Request, upon Company's request, Service Provider shall provide commercially reasonable efforts to assist Company in responding to such Data Subject Request, to the extent Service Provider is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws.

10. ASSISTANCE

10.1 Upon Company's request, Service Provider shall provide Company with reasonable cooperation and assistance needed to fulfil Company's obligations as a Controller, as required under Data Protection Laws, including to carry out a data protection impact assessment or other documentation related to Company's use of the Services and any related consultation with a competent Supervisory Authority, to the extent Company does not otherwise have access to the relevant information and such information is available to Service Provider.

11. PERSONAL DATA BREACH

11.1 Upon becoming aware of a Personal Data Breach, Service Provider shall notify Company without undue delay and in accordance with any specific timeframes required by Data Protection Law, and will cooperate with Company to promptly investigate and remediate the Personal Data Breach. Service Provider's notification of or response to a Personal Data Breach is not an acknowledgement by Service Provider of any fault or liability with respect to the Personal Data Breach. Company shall promptly notify Service Provider about any possible misuse of its accounts or authentication credentials or any security incident related to the Services.

12. DELETION

12.1 At the conclusion or termination of the Services, and upon Company's request, Service Provider shall delete Personal Data Processed under this DPA that has been shared or made accessible by Company.

13. INTERNATIONAL DATA TRANSFERS

1.1 Where Service Provider and Company are located in different jurisdictions and there is a Restricted Transfer of Personal Data from Company to Service Provider, the Data Exporter (Company) and the Data Importer (Service Provider) shall transfer and Process Personal Data in accordance with **Schedule 3**. In the event and to the extent of any conflict between this DPA and any of the terms incorporated by reference into Schedule 3 to comply with Data Protection Laws, the terms in Schedule 3 shall prevail. With respect to any jurisdiction not listed in **Schedule 3**, where required by Data Protection Laws, upon either Party's request, the Parties shall cooperate in good faith to implement any further steps that may be required by Data Protection Laws to ensure the lawfulness of such transfers (including the entry into any additional transfer agreement or terms).

14. INFORMATION AND AUDIT

14.1 Service Provider shall provide such information as Company may reasonably request to demonstrate compliance with this DPA and Data Protection Laws.

14.2 Upon Company's reasonable and prior written request, and no more frequently than once every twelve (12) months, Service Provider shall make available to Company evidence of the most recent third-party audit or certifications setting out Service Provider's conformity in relation to Personal Data Processing activities pursuant to this DPA.

14.3 Any information provided under this section is Service Provider's confidential information, and shall be subject to the confidentiality terms of the Agreement or such other terms as Service Provider may require. Company may not provide such information to any third party or use such information for any purpose other than to verify Service Provider's compliance with this DPA without Service Provider's prior written consent.

14.4 If Company can reasonably demonstrate that the information provided is not sufficient to demonstrate compliance with this DPA, Service Provider shall reasonably consider any further requests for information from Company to demonstrate compliance with this DPA and Data Protection Laws.

15. CHANGES

15.1 Company acknowledges and agrees that Service Provider may from time to time update this DPA, including to ensure compliance with Data Protection Laws.

15.2 Where Service Provider makes such changes, Service Provider shall use reasonable endeavors to notify Company of such changes, which may include publishing such changes on Service Provider's website. If Company, acting reasonably, considers that such changes would have a material adverse effect on Company's ability to comply with Data Protection Laws, Company may, within thirty (30) days of the date of such change, terminate this DPA by providing written notice to Service Provider. Company acknowledges that Service Provider will not be required to provide the Services if such termination occurs.

SCHEDULE 1: Description of the Processing and Sub-Processors

Processor/ Data Importer	Processor Legal Entity Name: Navu, Inc. Address: 415 Cambridge Ave Suite 14, Palo Alto CA Privacy Point of Contact: Carl Hubbard Activities relevant to the Personal Data Processor and/or Transferred under this DPA: Providing the Services as specified in the Agreement.
Controller/ Data Exporter	Controller Legal Entity Name: [TO BE COMPLETED BY Company] Address: [TO BE COMPLETED BY Company] Privacy Point of Contact: [TO BE COMPLETED BY Company] Activities relevant to the Personal Data Processor and/or Transferred under this DPA: Receiving the Services as specified in the Agreement.
Data subjects:	Individuals whose Personal Data is included in the Customer Data; Customer's employees
Categories of Personal Data:	● Personal Data included in Customer Data (if any) ● Support and communications data, including Personal Data contained in Customer and individual inquiries or feedback ● Customer employees' Personal Data, including contact information
Special category ("sensitive") Personal Data and applied restrictions or safeguards:	Navu does not process any special category or sensitive Personal Data
Nature and purpose of the Processing and transfer (as applicable):	Processing operations are limited to the extent necessary to provide the services as specified under the Agreement.
Frequency and Duration of Processing, period for which the Personal Data will be retained and/or the criteria for determining that period:	Ongoing or the duration of the Services and thereafter as necessary to fulfill obligations set out in this DPA.
Approved Sub-Processors:	Amazon AWS (Email delivery, data backups & infrastructure) Stripe (Payment processing) Google (Oauth-based user authentication)

	IPData (Reverse IP lookup for visitor attribution) OpenAI (LLM for AI-powered Retrieval-Augmented Generation (RAG) services) Google Gemini (LLM for AI-powered Retrieval-Augmented Generation (RAG) services) Anthropic Claude (LLM for AI-powered analysis and report generation)

SCHEDULE 2: Technical and Organizational Security Measures

The below provides a non-exhaustive list of the high-level, minimum security requirements that Service Provider implements as part of its technical and organizational measures:

SECURITY CONTROL	DESCRIPTION
Access Control Management	● Processes designed to ensure that access to information, systems and applications is restricted to authorized users and is granted in accordance with "Need-To-Know" and "Least-Privilege" principles.
Data/Media Destruction	● Processes designed to ensure that access to data on media is rendered unlikely for a given effort via different actions such as clear, purge and destroy. ● On a case-by-case basis, the correct method of destruction is chosen depending on the desired outcome.
Acceptable Use	● Processes designed to ensure acceptable use of electronic devices and network resources. ● Computer devices, networks and other electronic information systems need to be managed in order to ensure confidentiality, integrity and availability of information assets.
Monitoring and Logging	● Processes which ensure that systems are designed and configured to generate and store security logs.
Encryption	● Unless technically infeasible or impractical, all private, confidential and regulated information shall be encrypted at rest and in transit according to industry best-practices.
Backup & Continuity	● Processes designed to ensure that information is backed up according to business, legal and regulatory requirements and considering the potential loss of the specific type of information.
Software Development Lifecycle (SDLC)	● Processes designed to ensure that security software development practices are implemented accordingly.
Vulnerability Management	● Processes designed to ensure that vulnerabilities identified in critical information systems are assessed and remediated in a timely manner.
Physical Controls	● Processes designed to implement facility access controls and to ensure workstation, device and information assets' security.

SCHEDULE 3: **International Data Transfers**

1. **Definitions**. For the purposes of this **Schedule 3**, the following definitions shall apply:

   (a) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

   (b) "**SCCs**" means the Controller-Processor (Module 2) of Standard Contractual Clauses published by the European Commission, as applicable, the latest version of which were published pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

   (c) "**UK Addendum**" means template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

2. **European Economic Area**. Where Company transfers Personal Data that is subject to the GDPR to Service Provider, and Service Provider is located in a country that does not ensure an adequate level of protection within the meaning of the GDPR, the SCCs shall apply as follows:

   (a) The SCCs shall be incorporated into this DPA by reference and be considered duly executed between Company and Service Provider upon the entry into force of this DPA.

   (d) Clause 7 (*docking clause* – optional) shall not apply.

   (e) Option 2 (*general authorization*) under Clause 9(a) (*use of sub-Processors*) of the SCCs shall apply and "[Specify time period]" shall be replaced with "thirty (30) days".

   (f) The optional text under Clause 11 (redress) shall not apply.

   (g) For the purposes of Clause 13(a) (supervision) of the SCCs, the Data Exporter shall be considered as the Company established in an EU Member State.

   (h) Option 1 under Clause 17 (governing law) of the SCCs shall apply, and the governing law shall be the law of the country of the Data Exporter.

   (i) Any disputes arising from the SCCs shall be resolved by courts of the supervisory authority of the Data Exporter (Clause 18 (choice of forum and jurisdiction)).

   (j) For the purposes of Annex I.A, Company and Service Provider can be contacted as set out in **Schedule 1** of this DPA. The activities relevant to the transfer under the SCCs relate to the reception and provision of the Services under the Agreement, as applicable.

   (k) Annex I.B to the SCCs shall be interpreted in accordance with the descriptions in this DPA.

   (l) The Supervisory Authority of the Data Exporter shall be the competent Supervisory Authority for the purposes of Annex I.C to the SCC

   (m) Annex II to the SCCs shall be interpreted in accordance with **Schedule 2** of this DPA.

3. **United Kingdom**. Where Company transfers Personal Data that is subject to the Data Protection Laws of the United Kingdom to Service Provider, and Service Provider is located in a country that does not ensure an adequate level of protection within the meaning of those Data Protection Laws, Company and Service Provider agree to the terms of Part 2: Mandatory Clauses of the UK Addendum. The information included in Part 1 of the UK Addendum is as set out in section 12.2 of this DPA. Either Company or Service Provider may end the UK Addendum as set out in Section 19 of the UK Addendum.