GLOBAL RESEARCH PLATFORMS, LLC PROCESSING ADDENDUM (DPA)

Effective Date: 07/09/2026

GRP: Global Research Platforms, LLC ("GRP") 4110 Carillon Pt Kirkland, WA 98033	**Service Provider:** *WiseData LLC* *82 WENDELL AVE. STE 100, Pittsfield MA 01201*
GRP Contact: *Davina Inslee* *Secretary, Deputy GC* *(206) 331-1747* *legal@gatesventures.com*	**Service Provider Contact:** *Cheng Han* *Co-founder & CEO* *617-651-1886* *cheng@wisedata.ai*
Agreement(s) being amended/incorporating DPA: ☐ any agreement listed below *Master Services Agreement dated April 8, 2026, and Statement of Work No. 1 thereunder, each between Global Research Platforms, LLC and WiseData LLC.*	☒ any separate agreement signed by the parties and explicitly incorporating this DPA by reference All the foregoing as designated, including any applicable Statement of Work (**SOW**) attached thereto, collectively referred to as the **Agreement(s)**.

1 **Introduction.** GRP has entered into one or more Agreements described above. This DPA between GRP and Service Provider shall apply to all Processing of GRP Personal Data by Service Provider to provide the services as described and/or defined under the Agreement (**Services**).

2 **Order of Precedence.** Should there be a conflict between this DPA, and the Agreement or SOW, this DPA will govern. Should there be a conflict between data protection terms in the SOW and the Agreement, the SOW will govern.

3 **Definitions.** In this DPA, the following terms have the meanings set out below and cognate terms are defined accordingly:

3.1 **Applicable Laws** means all statutes, laws, rules, regulations, ordinances, and the like of any federal, international, city, state, provincial, or local government or governmental agency applicable to Services under the Agreement including without limitation Data Protection Laws.

3.2 **Data Protection Laws** means Applicable Laws relating to privacy, security, or protection of Personal Data (e.g., the EU General Data Protection Regulation (Regulation 2016/679) (**GDPR**); the UK GDPR as applicable as part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended) (**UK GDPR**); the California Consumer Protection Act (**CCPA**), and the amending California Privacy Rights Act (**CPRA**)) and any subsequent supplements, amendments, or replacements to the same.

3.3 **Confidential Information** is defined in the Agreement.

3.4 **GRP Personal Data** means any Personal Data Processed by Service Provider in connection with the Services, including Personal Data provided by or made available by GRP to Service Provider or collected by Service Provider on behalf of GRP.

3.5 **GRP Systems** means any hardware, software, networks, or other information technology resources owned or operated by, or on behalf of, GRP.

3.6 **Data Breach** means any unauthorized interference with the availability of, or any unauthorized, unlawful or accidental loss, misuse, destruction, alteration, acquisition of, access to, disclosure of, or damage to GRP Personal Data or any other non-public data or Confidential Information received from GRP, or any other unauthorized Processing of GRP Personal Data or unauthorized access to GRP Systems.

3.7 **Data Subject** means an identified or identifiable natural person about whom Personal Data is Processed under this Agreement or as otherwise defined (including under similar terms such as "consumer") under Data Protection Laws.

3.8 **Personal Data** means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household or with a particular individual's or household's device; or any inferences drawn therefrom. Personal Data includes, but is not limited to, name, alias, postal address, social security number, identification number, biometric identifiers, credit/debit card information, driver's license number (or other unique government identifier, such as passport or military ID), phone number, physical address, email address, details of orders and fulfilments, location data, employment or educational information, online identifiers such as internet protocol addresses, cookie or other unique identifiers, criminal background check, work authorization, or to one or more factors specific to the physical, physiological, genetic, mental, economic, financial, cultural, sexual orientation, union status, or social

identity of the individual, or as otherwise defined (including under similar terms such as personal information, Personal Data, personal health information, personally identifiable information, and sensitive personal information) under Data Protection Laws.

3.9 **Process, processed, or processing** means the collection, receipt, recording, organization, structuring, alteration, use, transmission, access, sharing, provision, disclosure, distribution, copying, transfer, storage, management, retention, deletion, combination, restriction, summarizing, aggregation, correlation, inferring, derivation, analysis, adaptation, retrieval, consultation, destruction, disposal, or other handling of Personal Data.

3.10 **Sell** or **selling** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data to another business or a third party for monetary or other valuable consideration.

3.11 **Share** or **sharing means** sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party, whether or not for monetary or other valuable consideration.

3.12 **Services** means services provided by Service Provider on behalf of GRP under the Agreements.

3.13 **Standard Contractual Clauses** or SCCs means the UK Information Commissioner ("UK ICO") (as they may apply for UK to Third Country transfers): means the International Data Transfer Addendum issued by the UK Information Commissioner in accordance with s.119A of the UK Data Protection Act 2018 (New UK SCCs).

3.14 **Sub-processor** means any person or entity engaged by Service Provider (or other Processor) that Processes GRP Personal Data to help provide the Services.

3.15 The terms **Controller** or **Data Controller** and **Processor** or **Data Processor and Business and Service Provider** shall have the same meaning as in applicable Data Protection Laws.

4 Data Ownership/Licenses

4.1 For purposes of this DPA, as between the parties, GRP retains all right, title, and interest in GRP Personal Data.

4.2 GRP grants to Service Provider limited right and license under applicable intellectual property laws to make, use, copy, distribute, display,

organize, create derivative works from, and otherwise Process, the GRP Personal Data, and to sublicense all the foregoing rights to approved Sub-processors, solely as necessary to perform the Services under the Agreement and subject to restrictions and obligations in this DPA.

5 General Compliance Obligations

5.1 Service Provider certifies that it understands the restrictions of this DPA and shall comply with, and assist GRP in complying with, obligations regarding GRP Personal Data under this DPA, the Data Protection Laws, and applicable and accepted industry standards, including any applicable self-regulatory programs.

5.2 Service Provider shall make available information necessary to demonstrate compliance with Data Protection Laws and such other information and documentation requested by GRP to demonstrate compliance with its obligations in this DPA.

5.3 Service Provider shall not engage in Processing of Personal Data, or any other activities, in connection with this Agreement in a way that may cause GRP to breach any of its obligations regarding GRP Personal Data under Data Protection Laws or obligations to GRP's customers.

5.4 Service Provider shall ensure that all Service Provider employees, agents, officers, consultants, Processors, Sub-processors and any third party authorized to Process GRP Personal Data are a) properly trained regarding obligations under this DPA and Data Protection Laws and b) subject to written confidentiality agreements that provide substantially the same level of protection for GRP Personal Data as provided in this DPA and as required by Data Protection Laws.

5.5 Service Provider will not Sell or Share GRP Personal Data, nor use, retain, or disclose GRP Personal Data outside of its direct business relationship with the GRP or for any other purpose except as required by law. Specifically, Service Provider shall not Share GRP Personal Data for the purposes of cross-contextual behavioural advertising.

5.6 Service Provider shall not combine GRP Personal Data with Personal Data which it receives from other sources and customers, including the information collected from Service Provider's independent interaction with the Data Subjects. This does not include combining GRP Personal Data solely in the context of the business purpose of providing the Services.

6 Scope of Processing

6.1 **Roles of Parties.** The parties acknowledge and agree that with respect to Processing of GRP Personal Data, Service Provider is a Processor and a Service Provider and GRP is a Controller and Business.

6.2 **Details of Processing.** Service Provider will provide to GRP in writing appropriate and accurate information regarding its Processing of GRP Personal Data Processed in connection with the Services including information about the categories of GRP Personal Data, how such data is collected and Processed, and the purposes for which such data is used, in a manner appropriate to allow GRP to meet its record keeping and notice and consent obligations under Data Protection Laws, including information as set forth in Exhibit 1 (Processing Details) or in a Statement of Work.

6.3 GRP **Instructions and Restrictions on Processing**

6.3.1 Service Provider will use, retain, and disclose GRP Personal Data solely for the specific business purpose of providing the Services and in accordance with GRP's instructions, including as described in the Agreement. Service Provider will inform GRP if any of GRP's instructions infringes any Data Protection Laws.

6.3.2 Service Provider shall have rights to use GRP Personal Data solely (i) to the extent necessary or appropriate to (a) perform its obligations under the Agreement; (b) operate, manage, test, maintain, and enhance the Service including as part of its business operations; (c) to create and disclose aggregate statistics about GRP Personal Data and the Service in a manner that prevents individual identification of the GRP, or the individual subjects of GRP Personal Data; and/or (d) protect the Service from a threat to the Service, GRP Personal Data, and GRP's and Service Provider's systems; or (ii) if required by court order of a court or authorized governmental agency, provided that prior notice first be given to the GRP unless such notice is prohibited by law or court order; or (iii) as otherwise expressly authorized by the GRP. Service Provider shall not Share any information with or disclose any information to a third party without GRP's prior written consent.

7 **Data Security**

7.1 **Data Security Obligations.** Service Provider will implement and maintain commercially reasonable administrative, technical, and physical safeguards, including procedures and practices commensurate with the level of sensitivity of the GRP Data and the nature of its activities under the Agreement, to protect the security, confidentiality and integrity of any GRP Personal Data Processed by Service Provider or in its possession and control and GRP Systems including such safeguards (a) designed to ensure the security of systems upon which GRP Data is Processed and GRP Systems; and (b) designed to prevent any Data Breach. Any such measures shall include procedures and practices as described in Annex 2.

7.2 **Data Breach**

7.2.1 In addition to, and without limiting, any other right or remedy available to GRP under this Agreement or at law or equity, in the event of any actual or potential Data Breach, Service Provider shall immediately take reasonable and appropriate steps to: (a) notify GRP of such Data Breach after Service Provider discovers or learns of such Data Breach; (b) furnish to GRP full details of the Data Breach; (c) take appropriate steps without unreasonable delay to investigate, mitigate, and remedy the Data Breach and prevent further Breaches, including, if deemed appropriate by GRP, hiring qualified forensics investigators, approved and under contract of confidentiality with GRP, to assist with the same; (d) assist GRP in its investigation, mitigation, and remedying of the Data Breach; (e) assist GRP in preparing and providing notices to individuals affected by the Data Breach, and any others as deemed appropriate by GRP, to inform such persons of the facts and circumstance of the incident which may include, naming Service Provider in connection with Data Breach; (f) cooperate with GRP in any litigation or regulatory action related to the Data Breach; and (g) cooperate with GRP in any other reasonable action, step, or proceeding as may be deemed necessary by GRP in connection with the Data Breach and any dispute, inquiry or claim concerning the Data Breach. Service Provider agrees to completely remedy any breach no later than within thirty (30) days of discovery of a Data Breach and provide full details of steps Service Provider shall take to prevent such a Breach from reoccurring. Service Provider agrees to take the foregoing responsive measures, including cost of notice and, if applicable, costs of credit monitoring and repair services at its sole cost and expense if Service Provider's actions or omissions cause or contribute to the Data Breach. Service Provider's failure to remedy any Data Breach in a timely manner will be a material breach of the Agreement.

7.2.2 Unless prohibited by an applicable law or court order, Service Provider shall immediately notify GRP of any third-party legal process relating to any Data Breach, including, but not limited to, any legal process initiated by any governmental entity.

7.2.3 Service Provider's cooperation or obligation to report or respond to Data Breaches under this DPA shall not be deemed an acknowledgment by Service Provider of any fault or liability of Service Provider with respect to a Data Breach.

7.3 **Security Audit.** Service Provider will ensure that the facilities that process, handle, and/or store such information are audited annually against SOCII Type 2 (or its current equivalent) standards. The summary report of any security audit will be provided to GRP following the

completion of such audit. Service Provider will also inform GRP of any material vulnerabilities discovered by any audits and the nature of each vulnerability. Service Provider will promptly correct each such vulnerability and will certify same in writing to GRP upon written request**.**

7.4 During the term of the Agreement or so long as Service Provider maintains possession or control of Personal Information, whichever is longer, Service Provider will maintain cyber-security insurance sufficient to cover costs relating to Data Breaches caused by Service Providers acts or omissions with minimum limits of one million United States of America dollars ($1,000,000 USD). Such coverages shall be provided by insurance carriers with an A.M. Best rating of at least A VII, or such other insurance carriers approved in writing by GRP. Prior to the commencement of any services under this Agreement and upon each renewal of the insurances, Service Provider shall furnish GRP a copy of a certificate confirming the requisite insurance is in place. The minimum limit set forth above is not intended to and does not limit Service Provider's responsibilities. Service Provider acknowledges and agrees that its failure to provide the certificate of insurance as required hereunder will not be a waiver by GRP of Service Provider's contractual requirements to provide insurance.

8 **Data Protection Compliance Assistance.** Upon GRP request, Service Provider will provide reasonable assistance and information to GRP regarding its Processing of GRP Data, including for the following.

8.1 **Regulator Enquiries and Regulatory Consultation.** Service Provider will assist GRP in complying with its obligations relating to investigation or inquiries from government entities or regulators and any consultations with any supervisory or regulatory authority.

8.2 **Audits and assessments.** Upon request by GRP, in addition to Security Audits described in Section 7.3, Service Provider shall procure and make available to GRP audit and assessment reports conducted by a qualified independent third party approved by GRP to confirm Service Provider's compliance with its obligations under this DPA with regard to Processing GRP Personal Data. If the audit reveals any vulnerability or inadequacy, Service Provider shall correct any such vulnerability or inadequacy at its sole cost and expense and shall certify the same in writing to GRP. Service Provider shall use best efforts to correct or mitigate all vulnerabilities and inadequacies without unreasonable delay but no later than within thirty (30) days of completion of the audit, unless GRP agrees in writing otherwise. Service Provider's failure to procure audits or to complete corrections in a timely manner will be a material breach of the Agreement.

8.3 **Third Party Complaint or Inquiry.** Service Provider shall promptly notify GRP if it receives or learns of: (a) any complaint, inquiry, investigation, request, or any other communication relating an actual or alleged violation of privacy or data security relating to the Service, GRP Personal Data, or GRP Systems and (b) any request from a government entity or regulator provided such notice to GRP is not prohibited by law or court order. Service Provider shall provide GRP with full co-operation and assistance in relation to any such communication or request including by providing GRP with full details of any such communication or request, investigation of any actual or alleged violation, and information needed to further investigate any actual or alleged violation and respond to such communications or request. Service Provider shall comply with any instructions given by GRP regarding responding to such communications.

8.4 **Data Subject Rights.** Service Provider will immediately notify GRP in writing, and in any case without undue delay, if Service Provider receives (i) any requests from a data subject, with respect to GRP Personal Data, including individual opt-out requests, requests for access and/or deletion and all similar individual rights requests; or (ii) any complaint or inquiry relating to the Processing of GRP Personal Data, including allegations that the Processing infringes on any individual's or third party's rights. Service Provider will not respond to any such request or complaint unless expressly authorized to do so by GRP or required to respond under applicable Data Protection Laws. Service Provider shall comply with any instructions given by the GRP regarding responding to such requests, complaint or inquiries.

8.5 **DPIAs.** Service Provider will assist GRP in complying with its obligations under the applicable Data Protection Laws, including, without limitation, conducting data protection impact assessments and records of processing activities.

9 Sub-processors

9.1 Service Provider may only provide access to or transfer GRP Personal Data to a third party (including any affiliates, group companies, or subcontractors) with the express, prior, written consent of GRP. GRP consents to such access or transfer to Service Provider’s Sub-processors approved by GRP.

9.2 When requested by GRP, Service Provider will make available an up-to-date list of current Sub-processors (the current version of which is attached as Annex 3 and GRP authorizes Service Provider to use such Sub-processors to process GRP Personal Data unless GRP objects within 30 days of receipt to any such Sub-processors.

9.3 Service Provider will enter into written agreements with Service Provider's Sub-processors. Those agreements will contain obligations on those third parties that are no less protective of GRP Personal Data than the obligations on the Service Provider under this DPA.

9.4 Where a third party appointed by Service Provider to process GRP Personal Data in performance of the Services fails to fulfil its obligations under any sub-processing agreement or Data Protection Laws, Service Provider will remain fully liable to GRP for the fulfilment of its obligations under this DPA and the Agreement.

10 **Location of Processing** Service Provider may Process GRP Personal Data in the regions listed in Exhibit 1, (Approved Regions) provided Service Provider cooperates with the GRP to comply with applicable data transfer restrictions and obligations required by Data Protection Laws. Service Provider will not Process such GRP Personal Data outside of the Approved Regions without GRP's knowledge and written authorization (where GRP authorization received by email or other electronic means is acceptable).

11 **Transfers to Third Countries.**

11.1 Transfers of European Area Personal Data (except UK Personal Data) by **GRP** to Vendor in Third Countries are subject to the Standard Contractual Clauses, Module Two ("Controller to Processor"), and attached to this DPA and incorporated by reference. The information required for the purposes of the SCCs is provided in Exhibit 1 ("Description of Processing and Transfer Details of GRP Personal Data") to this DPA. The Parties agree that the SCCs are incorporated into this DPA without further need for reference, incorporation, or attachment and that by executing this DPA, each party is deemed to have executed the SCCs.

11.2 <u>UK and Swiss Personal Data Transfers</u>. Where the **GRP** Personal Data is subject to the UK GDPR or the Swiss DPA, the SCCs above shall be read to be modified as follows as applicable:

11.2.1 References to "Regulation (EU) 2016/679" or "that Regulation" and any articles therefrom shall be interpreted to mean equivalent references to the UK GDPR or Swiss DPA.

11.2.2 References to "EU", "Union" and "Member State" shall be interpreted to mean references to the "UK" or "Switzerland".

11.2.3 To the extent that the Standard Contractual Clauses as modified in accordance with this Section 11 in compliance with UK GDPR are substituted or replaced, the parties agree to either promptly implement the same or agree to use another acceptable method for transfer of such data and promptly amend this DPA as necessary to comply with such requirements.

11.2.4 The information required for the purposes of UK data transfers is provided in Exhibit 1 ("Description of Processing and Transfer

Details of GRP Personal Data") and Exhibit 2 ("Technical and Organizational Measures").

11.3 Onward Transfers. In connection with the provision of the Services to GRP, Vendor may receive from or transfer and Process GRP Personal Data to Third Countries provided that its Sub-processors take measures to adequately protect such data consistent with applicable Data Protection Laws.

11.4 To the extent that any substitute or additional appropriate safeguards or mechanisms under any Data Protection Laws of Limited Transfer Regions are required to transfer GRP Personal Data from a Limited Transfer Region, as applicable, to any third country, the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA governing the parties' Processing of Limited Transfer Data.

12 **General Terms**

12.1 **Indemnification.** Service Provider shall indemnify, defend, and hold harmless GRP, and its directors, officers, employees, and agents (and successors, heirs, and assigns) (**Representatives**) against any liability, damage, loss, or expense (including reasonable attorneys' fees and costs) (**Liabilities**) incurred by GRP as a result of a claim arising from a breach of any obligations or restrictions of this DPA or other actions in connection with Processing of Personal Data by Service Provider or their Sub-processor (**Claim**). Service Provider will not enter into a settlement that would result in liability to GRP without GRP's prior written consent, which shall not be unreasonably withheld or delayed.

12.2 **Notices.** Unless expressly stated otherwise in the Agreement, all notices under this DPA will be in writing and delivered by email, certified mail (return receipt requested), or express courier (with confirmation of delivery). The notice will be deemed given and will be effective upon receipt: (a) when it is delivered to a party personally; (b) upon receipt, if sent certified mail, return receipt requested; or (c) when sent by a nationally recognized overnight courier service (with confirmation of delivery.

12.3 **Retention & Deletion of GRP Personal Data.** Upon GRP's request, or upon termination or expiration of the Agreement, Service Provider will delete all GRP Personal Data under Service Provider's possession or control or provide GRP ability to delete such GRP Personal Data directly through tools or functionality made available by Service Provider; excepting where deletion is not permitted under Applicable Laws (including Data Protection Laws) or the order of a governmental or regulatory body.

12.4 **Termination**

12.4.1 **Deletion or Return of GRP Personal Data.** Upon termination or expiration of the Agreement, Service Provider will, upon request of GRP prior to termination or expiration provide a copy of all GRP Personal Data in Service Provider's possession to the GRP. Upon written verification from GRP of GRP's receipt of such GRP Personal Data, or absent such request, Service Provider shall promptly destroy such data in a reasonably secure manner.

12.4.2 **Survival.** The provisions of this DPA that, by their terms, require performance after the termination or expiration of this DPA, or have application to events that may occur after the termination or expiration of this DPA, will survive the termination or expiration of this DPA, including Sections 2, 3, 4, 5, 7, 8, and 12.

12.5 **Governing Law; Conflicts of Law; Severance.** The parties to this DPA agree to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement (without reference to its conflict of laws requirements), unless otherwise required by Data Protection Laws. To the extent any court or governmental entity with competent jurisdiction determines that a provision of this DPA is invalid or unenforceable, the parties agree and intend that such provision should be (a) amended solely as necessary to bring it back into force in a manner consistent with the parties' manifest intent, or if that is not possible (b) severed from the DPA in a manner to give maximum legal force and effect to the remaining provisions.

EXHIBIT 1

DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

1. ***Data Exporter –*** see page 1 of DPA

2. ***Data Importer –*** see page 1 of DPA

3. ***Activities relevant to the data transferred***

The activities relevant to the data transferred at the Services more fully described in the Agreement and applicable ordering documents.

4. **Processing information**

Subject matter and duration of the Processing of GRP Personal Data

The subject matter and duration of the Processing of the GRP Personal Data are set out in the Principal Agreement, this DPA, and in applicable Statements of Work.

The nature and purpose of the Processing of GRP Personal Data

Operation of Addie, an AI query assistant embedded on www.alzheimersdata.org: receiving user-submitted questions, generating answers grounded in GRP's published website content with citations, and logging interactions for quality assurance, answer-accuracy auditing, and aggregate usage reporting, and as may be described in applicable Statements of Work.

The types of GRP Personal Data to be Processed

User-submitted query text and conversation content (free text, which may incidentally contain personal data), and technical and usage metadata (timestamps, session identifiers, page context, and IP addresses processed transiently for security and rate limiting). The Addie widget is public and unauthenticated; no account data, names, or email addresses are collected by design. Additional types as may be described in applicable Statements of Work.

The Types of Sensitive GRP Personal Data to be Processed

None collected by design. Users are instructed not to submit personal health information; incidental inclusion in user-submitted free text is possible. Additional types, if any, as may be described in applicable Statements of Work.

Strict purpose limitation; no profiling and no use of GRP Personal Data for model training; access restricted to authorized personnel on a need-to-know basis; access and audit logging; onward transfers limited to the approved Sub-processors listed in Exhibit 3; deletion or anonymization upon GRP's instruction.

The categories of Data Subject to whom the GRP Personal Data relates

Visitors to the public website www.alzheimersdata.org who interact with the Addie query assistant, and as may be described in applicable Statements of Work.

The frequency of the transfer of GRP Personal Data from GRP to Service Provider

Continuous, for the duration of the Services.

Location of Processing of GRP Personal Data by Service Provider

United States (Google Cloud Platform and OpenAI).

See also Sub-processor list

The obligations and rights of GRP

The obligations and rights of **GRP** are set out in the Agreement and this DPA.

5. Standard Contractual Clauses Information

SCC Clause	GDPR	Swiss DPA	UK GDPR
Clause 2 – Effect and invariability of the Clauses			Delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679"
Clause 6 – Description of Transfer			The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in

			Exhibit I where UK Data Protection Laws apply to the data exporter's processing when making that transfer.
Clause 7 – Docking Clause	An entity that is not a party to these clauses may, with the agreement of the parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 1.A		
Clause 8.8(i) of Modules 2 and 3			replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
Clause 9(a) – use of sub-processors	SPECIFIC PRIOR AUTHORISATION: The data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific Written authorisation. The data importer shall submit the request for specific authorisation at least 15 days prior to the engagement of the subprocessor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.		
Clause 17 – Governing Law	These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.	These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.	These Clauses shall be governed by the law of England and Wales.
Clause 18 – Choice of Forum and Jurisdiction	(b) The parties agree that those shall be the courts of Ireland.	The parties agree that those shall be the competent courts of Switzerland.	The parties agree that those shall be the courts of England and Wales.

Annex 1A – List of Parties	The name, address, and contact person's name, position, and contact details, and each party's role in processing personal data are provided in Section 1, 2, and 3 above		
Annex 1B – Description of Transfer	This information can be found in Section 4 above. To the extent applicable, the descriptions of safeguards applied to the special categories of Personal Data can be found in Exhibit 2 to the DPA.		
Clause 13 and Annex 1C – Competent Supervisory Authority	Identify the competent supervisory authority/ies in accordance with Clause 13: Irish Data Protection Commission	Identify the competent supervisory authority/ies in accordance with Clause 13: FDPIC	Identify the competent supervisory authority/ies in accordance with Clause 13: UK Information Commissioner
Annex II – Technical and Organizational Measures	The description of technical and organization measures designed to ensure the security of Personal Data is described more fully in Exhibit 2 to the DPA.		
Annex II – Technical and Organizational Measures – Sub-Processors	The description of technical and organization measures designed to ensure the security of Personal Data processed by Sub-processors is described more fully in Exhibit 2 to the DPA.		
Annex III – List of Sub-Processors	See Exhibit 3.		

EXHIBIT 2

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF COMPANY PERSONAL DATA

Service Provider will implement and maintain commercially reasonable administrative, technical**,** and physical safeguards, including procedures and practices commensurate with the level of sensitivity of the GRP Personal Data and the nature of its activities under the Agreement, to protect the security, confidentiality**,** and integrity of GRP Personal Data Processed by Service Provider or in its possession and control including such safeguards (a) to protect the security of systems upon which such data is Processed; and (b) designed to prevent a Data Breach.

Service Provider's personnel will not process GRP Personal Data without authorization. Personnel are obligated to maintain the confidentiality of any GRP Personal Data and this obligation continues even after their engagement ends.

Detailed description of the technical and organizational measures implemented by Service Provider (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

Encryption and transmission security. All data in transit is protected with TLS 1.2 or higher; the Addie API is served exclusively over HTTPS with origin checking and a CSP/CORS posture and API domain allowlist is restricted to two URLs provided by Gates Ventures IT. Data at rest is encrypted using Google Cloud's default AES-256 encryption (Cloud Storage, Firestore).

Confidentiality, integrity, and availability. Processing runs on segregated Google Cloud Run services within a dedicated GCP project. The public API endpoint is protected by Google Cloud Armor, per-origin rate limiting, and a daily spend circuit-breaker that bounds abuse impact. Front-end delivery uses script-tag versioning so production behavior cannot change silently.

Restoration and resilience. Infrastructure uses managed, redundant Google Cloud services. The content index is rebuilt automatically from canonical CMS sources via publish webhooks, allowing full restoration of the knowledge base from source-of-truth content at any time.

Testing and evaluation. Release candidates pass regression gates including a standing answer-accuracy evaluation harness (citation fidelity, refusal calibration) that is re-run before any behavioral change ships to production.

Identification and authorization. Least-privilege IAM roles govern personnel access to the GCP project; access is limited to authorized personnel on a need-to-know basis and logged. The public widget itself is unauthenticated and maintains no user accounts.

Storage protection and data minimization. Only query text and technical metadata are processed. Audit records exclude direct identifiers by design (the user

email field remains unpopulated in the public widget); no personal data is collected by default and no account or contact data exists in the system.

Event logging and accountability. Structured interaction and audit logs map each answer to its cited sources, providing a per-response record of what was asked, what was retrieved, and what was answered.

Retention, erasure, and portability. Interaction records are keyed and individually deletable; data is retained per Exhibit 1 and applicable Statements of Work and deleted or anonymized upon GRP's instruction or at termination.

EXHIBIT 3
SUB PROCESSORS

This list identifies the Sub-processors authorized to access GRP Personal Data to perform the Services. Service Provider should clearly indicate which Sub-Processors apply to each transfer/set of transfers.

Describe for each Sub-Processor:				
Sub-Processor Name	Contact person's name, position, & contact details	Sub-Processor address (location(s) of processing)	Services provided (description of subject matter, nature of Processing of GRP Personal Data including clear delimitation of responsibilities)	Duration of Processing of GRP Personal Data
OpenAI, L.L.C.	Privacy Team — privacy@openai.com	San Francisco, CA, USA (processing in the United States)	Large language model API serving as the generation layer for Addie: receives user query text and retrieved website content to produce grounded, cited answers. API data is not used for model training. WiseData remains responsible for orchestration, retrieval, and logging.	N/A
Google LLC (Google Cloud Platform)	Google Cloud Privacy Team — cloud.google.com/privacy	United States	Cloud infrastructure hosting Addie's retrieval API, content index, and audit logs: Cloud Run (compute), Cloud Storage	N/A

			(content assets), Firestore (metadata and audit records), Cloud CDN and Cloud Armor (delivery and protection).	
Microsoft Corporation (Azure)	Microsoft Privacy — microsoft.com/privacy	United States	Cloud infrastructure and hosting	N/A