

DATA PROCESSING ADDENDUM

This DATA PROCESSING ADDENDUM (“**DPA**”) forms part of the Terms of Service between Provider and Client and, when executed, governs Provider’s Processing of Client Personal Data on behalf of Client in connection with Client’s use of the Services.

Any capitalized term used but not defined in this DPA shall have the meaning ascribed to such term in the Terms of Service. This DPA will take precedence over the provisions of the Terms of Service to the extent the provision conflicts or is inconsistent with this DPA solely with respect to the Processing of Client Personal Data. Provider and Client hereby agree as follows.

1. Defined Terms.

“**Compelled Disclosure**” means a disclosure of Personal Data that is compelled pursuant to applicable Data Protection Laws, as defined herein, or by any competent judicial, supervisory, or regulatory body that may arise through various means such as document subpoenas, oral questioning, interrogatories, requests for information, or similar processes aimed at disclosing any Personal Data.

“**Controller**” means Client.

“**CCPA**” means the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq. and its implementing regulations, as amended by the California Privacy Rights Act.

“**Data Protection Laws**” means legislation and regulations that relate to data protection and privacy and apply to Provider as a Processor of Client Personal Data in connection with the Terms of Service, including, without limitation, the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, the UK General Data Protection Regulation (UK GDPR), the UK Data Protection Act 2018, and the CCPA.

“**Data Subject**” means an identifiable natural person whose Client Personal Data is being Processed pursuant to the Terms of Service by Provider on behalf of Client in connection with the Services. For purposes of the CCPA, the term “Data Subject” includes the term “Consumer”.

“**Client Personal Data**” or “**Personal Data**” means any information or data relating to an identified or identifiable natural person that Client or a person acting on Client’s behalf provides to Provider or that Provider otherwise Processes on behalf of Client, in connection with the Services, and, as applicable, “Personal Information” as defined in Section 6 of this DPA. For clarity, Client Personal Data does not include Personal Data that Provider independently collects, licenses, maintains, or otherwise Processes for its own purposes as a Controller or Business (“**Provider Data**”), including Personal Data contained in Provider’s proprietary datasets, solely because such Provider Data is accessed, retrieved, analyzed, or otherwise used in connection with providing the Services to Client.

“**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.

“**Process**” or “**Processing**” means any operation or set of operations performed on Personal Data, including Personal Data collection, retention, archiving, structuring, alteration, retrieval, transmission, disclosure, restriction or erasure, or use of such data.

“**Processor**” means Provider, solely to the extent Provider Processes Client Personal Data on behalf of Client.

“**Standard Contractual Clauses**” or “**SCCs**” means the requisite contractual terms for Processors annexed to the European Commission’s Decision (EU) 2021/914 of 4 June 2021, available at https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en.

“**Subprocessor**” means a Processor engaged by Provider to Process Client Personal Data on behalf of Client in connection with the Services and identified in Exhibit F, excluding Provider personnel and contractors acting under Provider’s direct authority.

“**UK Addendum**” means the requisite contractual terms for Processors annexed to the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Commissioner under S119A(1) Data Protection Act 2018, available at <https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf>.

2. Client Obligations.

Client acknowledges that it is responsible for complying with all requirements that apply to it under the applicable Data Protection Laws with respect to the Processing of Client Personal Data and the instructions issued to Provider.

3. Provider Obligations.

(a) Provider will only Process Client Personal Data for the purposes described in this DPA and the Terms of Service, or as otherwise agreed within the scope of Client's lawful instructions, except to the extent otherwise required by applicable Data Protection Laws. Provider shall inform Client of such legal requirement before Processing unless applicable Data Protection Laws prohibit such information on important grounds of public interest. Provider will keep a record of how Provider Processes Client Personal Data and of the instructions it carries out on behalf of Client and, upon reasonable notice (and no more than once annually unless a Personal Data Breach has occurred), shall permit Client to review and audit Provider's Processing of Client Personal Data, including Provider's records, during normal business hours and at Client's expense, subject to Client's compliance with Provider's reasonable confidentiality requirements.

(b) Client's activation, configuration, prompt, query, instruction, or use of agentic functionality through the Services constitutes Client's documented instruction to Process Client Personal Data as reasonably necessary to perform the applicable functionality in accordance with the Terms of Service and this DPA.

(c) Upon Client's request, Provider shall provide reasonable and timely assistance to Client in conducting and completing any necessary assessments required, including but not limited to assessments equivalent to the requirements stipulated in the applicable Data Protection Laws. Provider agrees to cooperate with Client in facilitating these assessments, taking into account the nature of the processing activities and the information available to Provider. Client shall reimburse Provider for reasonable costs incurred in providing such assistance.

(d) Provider must notify Client without undue delay (and in any event within seventy-two (72) hours) after Provider (or one or more of its personnel, agents, or Subprocessors) becomes aware of any Personal Data Breach involving Client Personal Data.

(e) Provider shall notify Client if Personal Data may not be Processed in accordance with Client's instructions due to a legal requirement under any applicable Data Protection Laws. In this event, Provider shall promptly notify Client of the conflicting legal requirement to the extent permitted by the applicable law and cooperate in good faith with Client to establish alternative instructions in accordance with applicable Data Protection Laws.

(f) Provider must take appropriate technical, organizational, and security measures to protect Client Personal Data against unauthorized or unlawful access, accidental loss, destruction, or damage, including but not limited to the measures set forth in Exhibit E.

(g) To the extent a Third-Party Model Provider Processes Client Personal Data as a Subprocessor, Provider will maintain written contractual or other commercially reasonable arrangements governing such Processing and prohibiting use of Client Personal Data for model-training purposes, except where Client affirmatively selects or authorizes a model or service whose disclosed terms provide otherwise. Provider will identify any such exception before Client's use of the applicable model or service.

(h) Provider shall limit access to Personal Data to those individuals who require access to the Personal Data to meet Provider's obligations with respect to the delivery of services to Client. Provider shall ensure that those individuals are informed in writing of the confidential or sensitive nature of the Personal Data. Provider shall ensure that any individuals authorized to Process Personal Data on behalf of Provider are subject to appropriate confidentiality obligations with respect to Personal Data in accordance with applicable Data Protection Laws and this DPA.

(i) Client authorizes Provider to transfer or provide (or provide access to) Personal Data only to the subcontractors, agents, or other third parties listed at Exhibit F of this DPA. Provider will ensure that the arrangement between Provider and Subprocessor is governed by a written contract that offers substantially the same level of protection for Client Personal Data as required by this DPA and Data Protection Laws. Provider shall notify Client at least thirty (30) days before Provider appoints a new Subprocessor to Process Personal Data, and Client may object to the appointment of a new Subprocessor within thirty (30) days of receiving such notice on reasonable grounds relating to data protection. Provider shall cooperate with Client in good faith to find an alternative means of Processing should Client object to the addition of a new

Subprocessor. If the parties are unable to resolve Client's objection within thirty (30) days, either party may terminate the affected services under the applicable Order Form upon written notice.

(j) Provider will comply without undue delay with any reasonable request from Client requiring Provider to amend, transfer, or delete any Personal Data, taking into account the nature of the Processing. Upon expiration or termination of the applicable Services, Provider shall delete or return Client Personal Data in accordance with Client's instructions, except to the extent retention is required by applicable law or expressly provided for in the Terms of Service, Documentation, or applicable Order Form. Any Client Personal Data retained pursuant to the foregoing will remain subject to this DPA for so long as it is retained.

(k) Provider shall provide relevant training to individuals authorized by Provider to Process Personal Data on behalf of Client. The training shall align with applicable Data Protection Laws and cover the nature and scope of Processing. Training sessions shall occur at least annually and within a reasonable period before such individuals commence Processing Personal Data.

(l) In the event that Provider receives a request for Compelled Disclosure, then, unless expressly prohibited by law, Provider shall: (i) promptly upon receiving notice of Compelled Disclosure, and prior to making any disclosure, notify Client in writing of such Compelled Disclosure and the conditions thereof; (ii) upon Client's request, and in accordance with Client's instructions, use reasonable efforts to oppose such disclosure, delay compliance with the Compelled Disclosure, and seek a protective order, or other limitations on disclosure, including providing all documentation related thereto, or other remedy on Client's behalf, at Client's cost and expense.

(m) If Client waives compliance or, after providing the notice and assistance required under Section 3(l) of this DPA, Provider remains clearly and unambiguously required by applicable law to disclose Personal Data, Provider shall (i) use reasonable efforts to protect the confidentiality of Personal Data; (ii) disclose only that portion of the Personal Data that Provider is legally required to disclose; and (iii) use reasonable efforts to obtain written assurances from the applicable court or other applicable presiding authority that such Personal Data will be (A) afforded the highest standard of confidential treatment; (B) disclosed solely to Provider's attorneys, and in any event, strictly in accordance with confidentiality obligations not less onerous than the confidentiality obligations protecting Personal Data required herein; (C) disclosed to such attorneys on a strict need-to-know basis; and (D) in addition to (A), (B), and (C), stored in IT systems subject to the most stringent industry data security standards.

4. Liability

Notwithstanding Section 14.2 of the Terms of Service, Provider's aggregate liability arising from Provider's material breach of this DPA, a Personal Data Breach resulting from Provider's breach of this DPA, or Provider's material violation of applicable Data Protection Laws in its capacity as a Processor will be subject to the limitation of liability applicable to breaches of confidentiality under Section 14.3 of the Terms of Service.

5. Data Subject Rights

Taking into account the nature of the Personal Data Processing, Provider shall:

- (i) not respond to a Data Subject or consumer request related to Client Personal Data itself, or through a Subprocessor, unless to verify the Data Subject or consumer, or as required by Data Protection Laws, and in such case, only after notifying Client of Provider's intention to respond to the extent reasonably feasible and not otherwise permitted by Data Protection Laws;
- (ii) notify Client without undue delay if Provider or any Subprocessor receives a request from a Data Subject or consumer under any Data Protection Laws in respect of Client Personal Data.

6. Additional CCPA Terms of Service

(a) All capitalized terms in this Section 6 that are not defined in Section 1 of this DPA or the Terms of Service shall be interpreted in accordance with the definitions provided by the CCPA.

(b) Provider understands, acknowledges, and agrees that, in connection with its obligations under the Terms of Service, Provider or its affiliates may receive information from Client that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked with, either directly or indirectly, a

particular individual or household in California, or otherwise Process such information on behalf of Client at any time in anticipation of, in connection with, or incidental to, the performance of the Terms of Service (collectively, “**Personal Information**” or “**Client Personal Information**”). Provider shall comply with the CCPA and agrees that any Personal Information that Client discloses to Provider is provided for a Business Purpose. Client represents and warrants that it does not Sell or Share Personal Information disclosed to Provider.

(c) Provider shall not under any circumstances do the following:

- (i) Sell or Share Personal Information;
- (ii) Process Personal Information for any purpose other than as necessary for the specific Business Purpose specified in the Terms of Service or otherwise permitted by the CCPA or its regulations;
- (iii) Process Personal Information outside of the direct relationship with Client; or
- (iv) combine the Personal Information that Provider receives from Client with Personal Information that Provider receives from, or on behalf of, another person or persons, or that it collects from its own interaction with Consumers unless expressly permitted by the CCPA.

(d) Client may take any reasonable and appropriate steps to ensure that Provider Processes Client Personal Information in a manner consistent with Client's obligations herein. Provider shall promptly notify Client in writing of any determination that Provider can no longer meet its obligations set forth herein. Provider shall cooperate with Client to take reasonable and appropriate steps to remediate or stop any unauthorized Processing of Personal Information.

(e) Provider hereby agrees that it will act solely as a Service Provider in relation to Personal Information. Provider acknowledges its obligations under the CCPA and hereby certifies its commitment to comply with the provisions outlined in the CCPA and this DPA.

(f) For clarity, this Section 6 applies only to Client Personal Information that Provider Processes on behalf of Client as a Service Provider or Contractor. Nothing in this DPA changes Provider's role with respect to Provider Data that Provider Processes independently as a Business or Controller, provided that Provider will comply with applicable Data Protection Laws in connection with such independent Processing.

7. International Data Transfers

(a) Client acknowledges and agrees that Provider may access and Process Personal Data as necessary to provide the Services, and, in particular, that Personal Data may be transferred to, and Processed by, Provider and its Subprocessors within the United States and other jurisdictions in accordance with this DPA and applicable Data Protection Laws.

(b) Where Personal Data is transferred from the EEA to a jurisdiction that has not been determined to provide an adequate level of data protection by the EU Commission for Personal Data protection, the Standard Contractual Clauses (EU) 2021/914 (available at https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en) will be incorporated into this DPA and shall apply as follows:

- (i) Provider will be the data importer and Processor of Client Personal Data;
- (ii) Client will be a Controller of Client Personal Data;
- (iii) Module 2 (Controller to Processor) shall apply;
- (iv) Clause 7 (Docking Clause) does not apply;
- (v) The parties choose Option 2 of Clause 9.
- (vi) The option in Clause 11(a) (Redress) does not apply;
- (vii) The parties choose Option 2 of Clause 17; and
- (viii) For the avoidance of doubt, for purposes of the Standard Contractual Clauses, Exhibits B, C and D of this DPA shall serve as Annex I, Exhibit E shall serve as Annex II, and Exhibit F shall serve as Annex III. In the event of any conflict or inconsistency among or between the terms and conditions of any such SCCs and this DPA, the terms of the SCCs shall prevail.

(c) Where Personal Data is transferred from the United Kingdom to a jurisdiction that has not been determined to provide an adequate level of data protection by the Information Commissioner's Office for Personal Data protection, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

(available at <https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf>) will be incorporated into this DPA and shall apply as follows:

- (i) Provider will be the data importer and Processor of Client Personal Data.
- (ii) Client will be a Controller of Client Personal Data.
- (iii) Module 2 (Controller to Processor) shall apply.
- (iv) Clause 7 (Docking Clause) does not apply.
- (v) The parties choose Option 2 of Clause 9.
- (vi) The option in Clause 11(a) (Redress) does not apply.
- (vii) The parties choose Option 2 of Clause 17.
- (viii) For the avoidance of doubt, for purposes of the UK Addendum, Exhibits B, C and D of this DPA shall serve as Annex I, Exhibit E shall serve as Annex II, and Exhibit F shall serve as Annex III. In the event of any conflict or inconsistency among or between the terms and conditions of any such UK Addendum and this DPA, the terms of the UK Addendum shall prevail.

The Terms of Service, applicable Order Form, this DPA, and Client's use, configuration, activation, prompts, queries, and instructions through the Services constitute Client's documented instructions to Provider for the Processing of Client Personal Data. Provider will Process Client Personal Data in accordance with such instructions, unless otherwise required by applicable Data Protection Laws.

[signature page follows]

IN WITNESS WHEREOF, the parties have executed this DPA as of the Effective Date of the Terms of Service.

PROVIDER

By: _____

Name: _____

Title: _____

Date: _____

CLIENT: _____

By: _____

Name: _____

Title: _____

Date: _____

***THIS DPA IS NOT EFFECTIVE UNTIL EXECUTED BY BOTH PARTIES
PLEASE RETURN THE COMPLETED AND SIGNED DPA TO PRIVACY@DATASITE.COM***

EXHIBIT A

DESCRIPTION OF PROCESSING OF CLIENT PERSONAL DATA

This Exhibit A includes certain details of the Processing of Client Personal Data as required by Article 28(3) GDPR.

Subject matter, nature and duration of the Processing of Client Personal Data

The subject matter of the Processing is the provision of Agentic and Artificial Intelligence functionality through the Grata platform. The duration of the Processing is for the term of the Terms of Service and any post-termination period during which Provider is permitted or required to retain Client Personal Data.

Purpose for which the Personal Data is Processed on behalf of Client group member

Provider may Process Client Personal Data as necessary to provide the Services, including receiving and processing prompts, queries, and instructions; receiving, hosting, and processing Client-provided content or data from Client-authorized integrations; indexing, organizing, searching, retrieving, and analyzing information; generating embeddings or other machine-readable representations; retrieving context relevant to Client instructions; transmitting minimized data to authorized AI/model Subprocessors where necessary; generating analyses, summaries, responses, and other outputs; performing Client-authorized agentic actions; executing code and processing files in temporary execution environments to carry out Client instructions; maintaining workflow state and intermediate artifacts as necessary to perform Client-authorized workflows; and recording and retaining security and audit logs to secure the Services and document access, Processing, and actions performed on Client's behalf; and providing related support and professional services.

Categories of Personal Data Processed

Client Personal Data may include names; business and personal contact details; professional or employment information; identifiers and account information; information contained in prompts, queries, Client-provided documents or datasets, and Client-authorized integrations; and other Personal Data that Client elects to submit or make available through the Services. For the avoidance of doubt, Client shall not provide special categories of data (as defined in Article 9 GDPR) to Provider unless expressly agreed in writing.

Categories of Data Subjects whose Personal Data is Processed

Employees, contractors, and other personnel of Client and its customers; business contacts and other individuals whose Client Personal Data is submitted or made available by or on behalf of Client through the Services.

EXHIBIT B

LIST OF PARTIES

	Data Exporter	Data Importer
Name	Client: _____	Provider
Address	As specified in the Terms of Service	As specified in the Terms of Service
Contact:	Name: _____ Title: _____ Email: _____	Name: <u>Matthew Steinhilber</u> Title: <u>Chief Legal Officer, General Counsel</u> Email: <u>Matthew.Steinhilber@datasite.com</u>
Activities relevant to the data transferred under these Clauses	As specified in Exhibit C to this DPA and the Terms of Service.	As detailed in Exhibit C to this DPA and the Terms of Service.
Role	Controller	Processor

EXHIBIT C

DESCRIPTION OF TRANSFER OF CLIENT PERSONAL DATA

Categories of Data Subjects whose Personal Data is transferred.

As outlined in Exhibit A to this DPA under "Categories of Data Subjects whose Personal Data is Processed".

Categories of Personal Data transferred.

As outlined in Exhibit A to this DPA under "Categories of Personal Data Processed".

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Relevant Personal Data is processed on a continuous basis, for the duration of the term of the applicable Services and any post-termination retention period permitted under the Terms of Service, Documentation, applicable Order Form, this DPA, or applicable law.

Nature of the Processing.

Depending on the nature and scope of the Services, Processing may include collection, receipt, access, hosting, storage, organization, indexing, retrieval, analysis, use, transmission to authorized Subprocessors, generation of outputs, performance of Client-authorized agentic actions, support, return, and erasure of Client Personal Data.

Purpose(s) of the data transfer and further Processing.

As outlined in Exhibit A to this DPA under "Purpose for which the Personal Data is Processed on Behalf of Client".

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period.

Client Personal Data will be retained for the period necessary to provide the Services and as otherwise specified in the Terms of Service or applicable retention schedule, subject to legal retention requirements.

For transfers to (Sub-)processors, also specify subject matter, nature and duration of the Processing.

As set forth above.

EXHIBIT D

COMPETENT SUPERVISORY AUTHORITY

Where Provider Processes Client Personal Data originating in the EEA, the competent supervisory authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses.

Where Provider Processes Client Personal Data originating in the UK, the competent supervisory authority shall be the UK Information Commissioner's Office.

EXHIBIT E

INFORMATION SECURITY STANDARDS

Provider maintains the following administrative, technical, and physical safeguards designed to protect Client Confidential Information and Client Materials processed through the Platform.

Provider may update or modify these safeguards from time to time, provided that Provider will not materially decrease the overall level of security provided for Client Confidential Information and Client Materials during the applicable Order Form term.

1. Information Security Program

Provider maintains a written information security program that includes administrative, technical, and physical safeguards appropriate to the nature of the Platform and the Client Confidential Information and Client Materials processed through the Platform.

Provider maintains written information security policies and an incident response program designed to identify, respond to, mitigate, and recover from security incidents. Such policies and procedures are reviewed and updated periodically, as appropriate.

2. Access and Personnel Security

Provider maintains access controls designed to limit access to Client Confidential Information and Client Materials to authorized personnel with a legitimate business need. Access privileges are assigned based on role and the principle of least privilege and are periodically reviewed.

Provider maintains authentication controls, including multi-factor authentication where appropriate, and logging or auditing controls for access to systems containing Client Confidential Information or Client Materials.

Provider maintains personnel security and access-management processes appropriate to personnel roles and responsibilities, which may include background screening where permitted by applicable law and appropriate to the role. Provider maintains processes designed to modify or revoke access in a timely manner following termination of employment or changes in personnel responsibilities.

Personnel with access to Provider systems receive information security and privacy training upon hire and periodically thereafter, as appropriate to their roles and responsibilities.

3. Data and Infrastructure Security

Provider maintains administrative and technical controls designed to protect systems and environments used to process Client Confidential Information and Client Materials.

Provider uses industry-standard encryption designed to protect Client Confidential Information and Client Materials in transit and at rest, where appropriate to the nature of the applicable system and information.

Provider maintains logical access and segregation controls designed to prevent one client from accessing another client's Client Confidential Information or Client Materials, except where expressly authorized by the applicable client.

Provider also maintains controls designed to protect credentials, access tokens, encryption keys, secrets, and similar authentication information from unauthorized access or disclosure.

4. Application and Development Security

Provider maintains secure software-development and change-management practices designed to protect the confidentiality, integrity, and availability of the Platform.

Provider uses appropriate development, testing, and production controls and maintains processes for reviewing, approving, and tracking material production changes.

Provider maintains security monitoring and vulnerability-management practices designed to identify malicious activity, unauthorized access, and security vulnerabilities affecting the Platform. Identified vulnerabilities are assessed, prioritized, and remediated based on risk.

Provider conducts periodic penetration testing or comparable security assessments of the Platform and supporting infrastructure.

5. Third-Party Security

Provider maintains a risk-based process for evaluating third-party service providers that process Client Confidential Information or Client Materials or otherwise materially support the Platform.

Provider evaluates such providers based on factors including the nature of their access to information and Provider's operational dependency on their services.

Provider's use of subprocessors in connection with personal data is subject to the applicable data processing addendum.

6. Business Continuity and Resiliency

Provider maintains business-continuity and disaster-recovery measures appropriate to the Platform and periodically reviews or tests such measures.

Provider maintains measures designed to support the availability and resiliency of systems used to provide the Platform.

Any service-level, recovery-time, or recovery-point commitments will apply only if expressly set forth in an Order Form or other written agreement between the parties.

7. Security Assessments and Documentation

Provider will maintain independent security assessment or audit documentation applicable to the Platform.

Upon Client's reasonable written request and subject to appropriate confidentiality protections, Provider will make available its then-current independent security audit report or other reasonable security documentation customarily provided to similarly situated clients.

EXHIBIT F

LIST OF SUBPROCESSORS

The Controller has authorized the Provider to use the following Subprocessors identified below to Process Client Personal Data in connection with the Services.

1. Amazon Web Services (US, EU): Cloud infrastructure, hosting, storage, AI models
2. Microsoft (US, EU): Cloud email, storage, hosting, infrastructure, AI services
3. OpenAI (US, EU): Cloud-based AI models
4. Anthropic (US): Cloud-based AI models
5. Google Cloud / Google AI (US, EU): Cloud-based AI models
6. Perplexity AI (US): Cloud-based AI models
7. xAI / Grok (US, EU): Cloud-based AI models for certain clients
8. Mistral AI (EU): Cloud-based AI models for certain clients
9. GroqCloud (US, EU): Cloud-based AI inference services
10. TurboPuffer (US, EU): Vector database / retrieval infrastructure
11. SendGrid (US, EU): Email delivery services
12. Pendo (US, EU): Product analytics and user adoption