Digital Arbitrage, Inc. Data Processing Addendum

Last updated: February 1st, 2025

Addendum Background

Digital Arbitrage, Inc. dba Cloudbeds ("**Cloudbeds**," "**we**," or "**us**") is a software as a service provider. This Data Processing Addendum ("**Addendum**") supplements our Terms of Service, or other agreement in place between you ("**Client**" or "**you**") and Cloudbeds covering Client's use of the Services (the "**Agreement**"). Unless otherwise defined in this Addendum or in the Agreement, all capitalized terms used in this Addendum shall have the meanings set forth in the Definitions section below.

How to Execute this Addendum

1. We have pre-signed this Addendum, which includes both the main body of the Addendum and Schedule 4. Your signature is required:
    1. at the bottom of the main body of this Addendum [Page 6]
    2. at the bottom of Schedule 4 [Page 17]
2. Once you have signed in these four locations and submitted them through Hellosign, you will have a binding Addendum with us.

1. Scope and Term.

1.1. Roles of the Parties.

(a) *Client Personal Data*. Cloudbeds will Process Client Personal Data as Client's Processor in accordance with Client's instructions as outlined in Section 2.3 (Instructions).

(b) *Client Account Data*. Cloudbeds will Process Client Account Data as a Controller for the following purposes: (i) to provide and improve the Services; (ii) to manage the Client relationship (communicating with Client and Users in accordance with their account preferences, responding to Client inquiries and providing technical support, etc.), (iii) to facilitate security, fraud prevention, performance monitoring, business continuity and disaster recovery; and (iv) to carry out core business functions such as accounting, billing, and filing taxes.

(c) *Cloudbeds Usage Data*. Cloudbeds will Process Cloudbeds Usage Data as a Controller for the following purposes: (i) to provide, optimize, secure, and maintain the Cloudbeds Services; (ii) to optimize user experience; and (iii) to inform our business strategy.

(d) *Description of the Processing*. Details regarding the Processing of Client Personal Data by Cloudbeds are stated in Schedule 1 (Description of Processing).

1.2. Term of the Addendum. The term of this Addendum coincides with the term of the Agreement and terminates upon expiration or earlier termination of the Agreement (or, if later, the date on which Cloudbeds ceases all Processing of Client Personal Data).

1.3. Order of Precedence. If there is any conflict or inconsistency among the following documents, the order of precedence is: (1) the applicable terms stated in Schedule 4 (Region-Specific Terms including any transfer provisions); (2) the main body of this Addendum; and (3) the Agreement.

2. Processing of Client Personal Data.

2.1. Client Appointment. Client appoints Cloudbeds as its Data Processor (Service Provider) and agrees that all Client Personal Data provided to Cloudbeds pursuant to the Agreement and this Addendum complies with the collection, transmission and lawful processing requirements under Data Protection Laws to enable the Processing.

2.2. Obligations. Cloudbeds agrees to treat Client Personal Data as Client Confidential Information. Cloudbeds will not:

(a) Process Client Personal Data other than as set out in this Addendum and in the Agreement unless upon Client's further written instructions or as required by a Supervisory Authority;

(b) sell Client Personal Data; or

(c) share, use or disclose the Client Personal Data unless it is authorized in accordance with the Agreement, this Addendum, any Order, upon Client's further written instructions or as required by a Supervisory Authority.

2.3. Instructions. Client on behalf of itself and each Client Affiliate which is the Data Controller of the Client Personal Data instructs Cloudbeds:

(a) To Process Personal Data in accordance with the documented lawful instructions of Client as stated in the Agreement (including this Addendum) and respective Orders, as necessary to (i) enable the use of various features and functionalities in accordance with the Documentation (including as directed by Users through the Services, or (ii) comply with its legal obligations. Cloudbeds will notify Client if it becomes aware, or reasonably believes, that Client's instructions violate Data Protection Law; and

(b) Subject to the transfer requirements in Schedule 4 (Region-Specific Terms) transfer Client Personal Data to any country or territory, in each case as reasonably necessary for the provision of the Services and consistent with this Addendum.

2.4. Description of Processing. Schedule 1 sets out the subject matter and other details regarding the Processing of the Client Personal Data contemplated as part of the Services, including Data Subjects, categories of Personal Data, special categories of Personal Data, Subprocessors and description of Processing.

2.5. Confidentiality. Cloudbeds will treat Client Personal Data as Client's confidential information under the Agreement. Cloudbeds will ensure that its personnel authorized to Process Client Personal Data are bound by written or other legally binding obligations of confidentiality.

3. Security.

3.1. Security. Cloudbeds has implemented and will maintain appropriate technical and organizational measures designed to protect the security, confidentiality, integrity and availability of Client Personal Data and protect against Security Incidents. Client is responsible for configuring the Services and using features and functionalities made available by Cloudbeds to maintain appropriate security in light of the nature of Client Data. Our current technical and organizational measures are described in Schedule 2 to this Addendum. Client acknowledges that these measures are subject to technical progress and development and that Cloudbeds may update or modify them from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services during Agreement.

3.2. Security Incident. Cloudbeds will notify Client without any undue delay, and in no event longer than 72 hours after becoming aware of a Security Incident. We will use commercially reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within our reasonable control. Upon Client's written request and taking into account the nature of the Processing and the information then-available to Cloudbeds, we will cooperate reasonably with you and provide you the information reasonably necessary for you to meet your Security Incident notification and other obligations under Data Protection Law. Except as required by law, Cloudbeds will not take action to notify Your Users of any Security Incident. Cloudbeds' notification of a Security Incident is not a statement or admission by Cloudbeds of fault or liability with respect to such Security Incident.

4. Subprocessing.

4.1. General Authorization. In the course of providing our Services, we may be required to contract with Subprocessors to perform a portion of the Services. We have included as Schedule 3 a list of the Subprocessors we currently use. By entering into this Addendum, Client authorizes Cloudbeds to engage the Subprocessors to Process Client Personal Data. Cloudbeds will (i) enter into a written agreement with each Subprocessor imposing data protection terms that require the Subprocessor to protect Client Personal Data to the standard required by Data Protection Law and to the same standard provided by this Addendum; and (ii) remain liable to Client if such Subprocessor fails to fulfill its data protection obligations with regard to the relevant Processing activities under the Agreement.

4.2. Notice of New Subprocessors. We will not add any additional Subprocessors without informing you of such Subprocessors by giving you at least thirty (30) days' notice before allowing any new Subprocessor to Process Client Personal Data ("**Subprocessor Notice Period**"). Client may object to Cloudbeds' appointment of a new Subprocessor during the Subprocessor Notice Period. If you object, Client may, as your sole and exclusive remedy, terminate the applicable Order for the affected Services.

5. Assistance and Cooperation Obligations

5.1. Data Subject Rights. Taking into account the nature of the Processing, Cloudbeds will provide reasonable and timely assistance to Client to enable you to (1) respond to requests for exercising data subject's rights (including rights of access, rectification, erasure, restriction, objection, and data portability) in respect to Client Personal Data. If any such requests or correspondence is received directly by us, we will forward you the request or correspondence and will wait for further direction from you before taking action. We will not communicate with authorities or Your Users without receiving your advance permission, except as required by applicable law. Upon documented request from you, we will correct, supplement, modify or delete any of Client Personal Data, except as required by applicable law.

5.2. Cooperation Obligations. Upon Client's reasonable request and taking into account the nature of the applicable Processing, Cloudbeds will provide reasonable assistance to Client in fulfilling Client's obligations under Data Protection Law (including data protection impact assessments and consultations with regulatory authorities), provided that Client cannot reasonably fulfill such obligations independently with help of available Documentation.

5.3. Regulatory Requests. Unless prohibited by Law, Cloudbeds will promptly notify Client of any valid, enforceable subpoena, warrant, or court order from law enforcement or public authorities compelling Cloudbeds to disclose Client Personal Data. Cloudbeds will follow its law enforcement guidelines in responding to such requests. In the event that Cloudbeds receives an inquiry or a request for information from any other third party (such as a regulator or data subject) concerning the Processing of Client Personal Data, Cloudbeds will redirect such inquiries to Client, and will not provide any information unless required to do so under applicable law.

6. Deletion and Return of Client Personal Data.

6.1. During Term. During the term of the Agreement, Client and its Users may, through the features of the Services, access, retrieve or delete Client Personal Data.

6.2. Post Termination. Following expiration or termination of the Agreement, Cloudbeds must, in accordance with the Documentation, delete all Client Personal Data. Notwithstanding the foregoing, Cloudbeds may retain Client Personal Data (i) as required by Data Protection Law or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Cloudbeds will maintain the confidentiality of, and otherwise comply with the applicable provisions of this Addendum with respect to retained Client Personal Data and not further Process it except as required by Data Protection Law.

7. Review, Audit and Inspection Rights.

7.1. Audit Reports. Cloudbeds' data center service provider is regularly audited by independent third-party auditors and/or internal auditors, including as described at https://aws.amazon.com/compliance/soc-faqs /. If Client cannot reasonably verify Cloudbeds' compliance with the terms of this Addendum, Cloudbeds will provide written responses (on a confidential basis) to all reasonable requests for information made by Client related to its Processing of Client Personal Data, provided that such right may only be exercised no more than once every twelve (12) months.

7.2. On-site Audits. Only to the extent Client cannot reasonably satisfy Cloudbeds' compliance with this Addendum through the exercise of its rights under Section 7.1 above, or where required by Data Protection Law or a regulatory authority, Client, or its authorized representatives, may, at Client's expense, conduct audits (including inspections) during the term of the Agreement to assess Cloudbeds' compliance with the terms of this Addendum. Any audit must (i) be conducted during Cloudbeds' regular business hours, with reasonable advance written notice of at least sixty (60) calendar days (unless Applicable Data Protection Law or a regulatory authority requires a shorter notice period); (ii) be subject to reasonable confidentiality controls obligating Client (and its authorized representatives) to keep confidential any information disclosed that, by its nature, should be confidential; (iii) occur no more than once every twelve (12) months; and (iv) restrict its findings to only information relevant to Client.

8. **Region-Specific Terms.** To the extent Cloudbeds Process Client Personal Data protected by Data Protection Laws in one of the specific regions listed in Schedule 4 (Region-Specific Terms), the terms specified for the applicable regions will also apply, including the provisions relevant for international transfers of Personal Data (directly or via onward transfer).

9. **Definitions.**

"**Cloudbeds Account Data**" means Personal Data relating to Client's relationship with Cloudbeds, including: (i) Users' account information (e.g. name, email address, or Cloudbeds' account ID); (ii) billing and contact information of individual(s) associated with Client's Cloudbeds account (e.g. billing address, email address, or name); (iii) Users' device and connection information (e.g. IP address); and (iv) content/description of technical support requests (excluding attachments).

"**Cloudbeds Usage Data**" means Personal Data relating to or obtained in connection with the use, performance, operation, support or use of the Services. Cloudbeds Usage Data may include event name (i.e. what action Users performed), event timestamps, browser information, and diagnostic data. For clarity, Cloudbeds Usage Data does not include Client Personal Data.

"**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Client Personal Data**'' means Personal Data contained in Client Data and/or any Client Materials that Cloudbeds Processes under the Agreement solely on behalf of Client. For clarity, Client Personal Data includes any Personal Data included in the attachments provided by Client or its Users in any technical support requests.

"Data Protection Laws" means all laws applicable to the Processing of Personal Data under the Agreement.

"**Personal Data**" means information about an identified or identifiable natural person, or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

"**Processing**" (and "**Process**") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

“**Security Incident**'' means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data Processed by Cloudbeds and/or its Subprocessors.
“**Subprocessor**” means any third party (inc. Cloudbeds Affiliates) engaged by Cloudbeds to Process Client Personal Data.
“**Users**” means any individual that Client authorizes to use the Services. Users may include: (i) Client’s and its Affiliates’ employees, consultants, contractors and agents (ii) third parties with which Client or its Affiliates transact business (iii) individuals invited by Client’s users (iv) individuals under managed accounts, or (v) individuals interacting with a Services as Client’s customer.

CLIENT	**DIGITAL ARBITRAGE, INC.**
_____	Tony Vardiman _____
Client Legal Name: _____	By: Tony Vardiman
By: _____	Title: Data Protection Officer
Title: _____	

Schedule 1 Description of Processing

This Schedule forms part of the Addendum and the Clauses and must be completed and signed by the parties.

Categories of data subjects

- Prospects, customers, business partners and vendors of Controller (who are natural persons)
- Employees or contact persons of Controller prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Controller (who are natural persons)
- Client's Users authorized by Client to use the Services

Categories of data

The personal data Processed include, the following categories of data:

- First, Middle, and Last Name
- Title
- Position
- Employer
- Contact Information (Company, email, phone, physical home address)
- ID Data
- Professional Life data
- Personal Life data
- Connection data
- Financial Data (credit cards, banking information)
- Localization data

Special categories of data (if appropriate)

The personal data transferred include, but not limited to, the following special categories of data:

- No special categories of data are required for the Services (e.g., information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life). Client agrees not to submit such data unless explicitly required and agreed upon in advance.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- Client Personal Data: Cloudbeds will Process Client Personal Data as Processor in accordance with Client's instructions as set out in Section 2.3 (Client Instructions).
- Cloudbeds Account Data and Cloudbeds Usage Data: Cloudbeds will Process Cloudbeds Account Data and Cloudbeds Usage Data for the limited and specified purposes outlined in Section 1.1 (Roles of the Parties).

Nature of Processing

Cloudbeds will process personal information by handling, storing, sharing with Subprocessors, accessing and reviewing Personal Information for the Processing purposes set out in the Agreement, Orders and this Addendum. Additional information regarding the nature of the Processing (including transfer) is described in respective Orders for relevant Services and Documentation referring to technical capabilities and features, including but not limited to collection, structuring, storage, transmission, or otherwise making available of Personal Data by automated means.

Duration of Processing

Cloudbeds will process personal information as long as necessary for the purposes described in this Addendum, unless a longer retention is required by law.

Transfers to (Sub-)processors: Cloudbeds will transfer Client Personal Data to Subprocessors as permitted in Section 4 (Subprocessing).

Schedule 2
Security Measures

Cloudbeds utilizes Amazon Web Services ("**AWS**") and relies to a great extent on the technical security measures adopted by AWS. In addition to the security measures adopted by AWS, and to the extent data processing activities occur outside the AWS system, Cloudbeds has implemented the following technical and organizational measures to ensure the security of Client Personal Data:

1. Cloudbeds has adopted industry standard processes designed to ensure that unauthorized persons are prevented from gaining physical access to our premises and the rooms where data processing systems are located.
2. Employees are only allowed access to tasks assigned to them.
3. We use video surveillance and alarm devices with reference to access areas.
4. Personnel without access authorization (e.g. technicians, cleaning personnel) are accompanied all times.
5. Cloudbeds has processes and requirements designed to ensure that all computers processing personal data (including computers with remote access) are password protected, both after booting up and when left, even for a short period.
6. We assign individual user passwords for authentication.
7. We only grant system access to our authorized personnel and strictly limit their access to applications required for those personnel to fulfill their specific responsibilities.
8. We have implemented a password policy that prohibits the sharing of passwords, outlines procedures to follow after disclosure of a password, and requires that passwords be changed regularly.
9. We ensure that passwords are always stored in encrypted form.
10. We have adopted procedures to deactivate user accounts when an employee, agent, or administrator leaves Cloudbeds or moves to another responsibility within the company.
11. We use industry standard technologies to prevent the installation and use of unauthorized hardware and software in our premises.

12. We have established rules for the safe and permanent destruction of data that are no longer required.

13. Except as necessary for the provision of the Services, Client Personal Data cannot be read, copied, modified or removed without authorization during transfer or storage.

14. We encrypt data during any transmission.

15. We are able to retrospectively examine and establish whether and by whom Client Personal Data has been entered into data processing systems, modified or removed.

16. We log administrator and user activities.

17. We process the personal data received from different clients so that in each step of the processing the Controller can be identified and so that data is always physically or logically separated.

18. We create back-up copies stored in protected environments.

19. We perform regular restore tests from our backups.

20. We have created business recovery strategies.

21. We do not use personal data for any purpose other than what we have been contracted to perform.

22. We do not remove Client Personal Data from our business computers or premises for any reason (unless you have specifically authorised such removal for business purposes).

23. Whenever a user leaves his or her desk unattended during the day and prior to leaving the office at the end of the day, he or she is required to place any documents containing Client Personal Data in a secure environment such as a locked desk drawer, filing cabinet, or other secured storage space.

24. We ensure that each computer system runs a current anti-virus solution.

25. We have designated a responsible person to perform the functions of a data protection officer.

26. We have obtained the written commitment of our employees to maintain confidentiality and to comply with our requirements under the Addendum and the GDPR.

27. We regularly train our staff on data privacy and data security.

Schedule 3

List of SubProcessors

Subprocessor	Services provided to Vendor	Location of the Processing (country)
Payment Processing Services		
Stripe Platform	Payment Processing	United States, Canada, Europe, Mexico, Asia Pacific, Hong Kong, Japan, Singapore and UAE
Stripe Direct	Payment Processing	46 countries globally
DLocal	Payment Processing	Thailand
PayPal	Payment Processing	United States
Adyen	Payment Processing	EU
PayU Latam	Payment Processing	Argentina, Brazil, Colombia, Mexico, Chile, Panama, and Peru
Ixopay	Payment Processing	United States, Canada, Puerto Rico, and Australia
MaxiPago!	Payment Processing	Brazil
Hosting and Storage Services		
Amazon AWS	Application and Data Hosting	United States
Communication and Collaboration Platforms		
G Suite (Google Workspace)	Productivity and Collaboration	United States
Office365	Productivity and Collaboration	United States
Slack	Communication and Support	United States
Zoom	Customer support and communication	United States
DialPad	Customer support and communication	United States
Jira	Collaboration and tracking services	United States
Sendgrid	Transactional email delivery	United States
Customer Support and Service Tools		
Zendesk	Customer Support	United States
Assembled	Customer Support Operations	United States
Forethought	Customer Support Operations	United States
N8N	Customer Support Operations	United States
Anthropic	Customer Support Operations	United States
Pinecone	Customer Support Operations	United States
Momentum	Customer Support Operations	United States
OpenAI	Customer Support Operations	United States
LangSmith	Customer Support Operations	United States
Security, Compliance and Monitoring		

Okta	Identity and Access Management	United States
DataDog	Cloud Monitoring and Performance	United States
Loki	Cloud Monitoring and Performance	United States
Tempo	Cloud Monitoring and Performance	United States
DocuSign	Digital transaction management	United States
Data Analysis, Data Enrichment and CRM Tools		
SnowFlake	Data Analysis	United States
Tableau	Data Analysis	United States
SalesForce	Sales Support	United States
Google Analytics	Application Advertising Analytics	United States
QuickInsight	Data Analytics	United States
Pendo	Data Analytics and Tracking	United States
Hotjar	Data Analytics and Tracking	United States
Salesloft	Data Analytics and Tracking	United States

Schedule 4 – Region-Specific Terms

Additional definitions are set out in Section 4.

1. Europe, United Kingdom and Switzerland.

1.1 Client Instructions. In addition to Section 2.3 (Client Instructions) of the Addendum above, Cloudbeds will Process Client Personal Data only on documented instructions from Client, including with regard to transfers of such Client Personal Data to a third country or an international organization, unless required to do so by Data Protection Laws to which Cloudbeds is subject; in such a case, Cloudbeds shall inform Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Cloudbeds will promptly inform Client if it becomes aware that Client's Processing instructions infringe Data Protection Laws.

1.2 European Transfers. Where Personal Data protected by the EU Data Protection Laws is transferred, either directly or via onward transfer, to a country outside of Europe that is not subject to an adequacy decision, the following applies:

(a) The EU SCCs are hereby incorporated into this Addendum by reference as follows:

(i) Client is the "data exporter"

(ii) Digital Arbitrage, Inc., (d/b/a Cloudbeds) is the "data importer". Cloudbeds is a hospitality management service in which the Services stores and processes personal information, guest information, business information, and employee information for the purposes of centralizing hospitality business data and services to the organization in accordance to the terms of the Agreement.

(iii) Module One (Controller to Controller) applies where Cloudbeds is Processing Cloudbeds Account Data or Cloudbeds Usage Data.

(iv) Module Two (Controller to Processor) applies where Client is a Controller of Client Personal Data and Cloudbeds is Processing Client Personal data as a Processor.

(v) Module Three (Processor to Processor) applies where Client is a Processor of Client Personal Data and Cloudbeds is Processing Client Personal Data as another Processor.

(vi) By entering into this Addendum and signature below, each party is deemed to have signed the EU SCCs as of the commencement date of the Agreement.

(b) For each Module, where applicable:

(i) In Clause 7, the optional docking clause does not apply.

(ii) In Clause 9, Option 2 applies, and the time period for prior notice of Subprocessor changes is stated in Section 4 (Subprocessing) of this Addendum.

(iii) In Clause 11, the optional language does not apply.

(iv) In Clause 17, Option 1 applies, and the EU SCCs are governed by Irish law.

(v) In Clause 18(b), disputes will be resolved before the courts of Ireland.

(vi) The Appendix of EU SCCs is populated as follows:

- The information required for Annex I(A) is located in the Agreement and/or relevant Orders.

- The information required for Annex I(B) is located in Schedule 1 (Description of Processing) of this Addendum.
- The competent supervisory authority in Annex I(C) will be determined in accordance with the Data Protection Laws; and
- The information required for Annex II is located in Schedule 3 (Technical and Organizational Measures) of this Addendum.

1.3 Swiss Transfers. Where Personal Data protected by the Swiss FADP is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the EU SCCs apply as stated in in Section 1.2 (European Transfers) above with the following modifications:
(a) All references in the EU SCCs to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss FADP; all references to the EU Data Protection Law in this Addendum will be interpreted as references to the FADP.
(b) In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

(c) In Clause 17, the EU SCCs are governed by the laws of Switzerland.

(d) In Clause 18(b), disputes will be resolved before the courts of Switzerland.
(e) All references to Member State will be interpreted to include Switzerland and Data Subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

1.4 United Kingdom Transfers. Where Personal Data protected by the UK Data Protection Laws is transferred, either directly or via onward transfer, to a country outside of the United Kingdom that is not subject to an adequacy decision, the following applies:
(a) The EU SCCs apply as set forth in Section 1.2 (European Transfers) above with the following modifications:

(i) By signature below, each party shall be deemed to have signed the UK Addendum.
(ii) For Table 1 of the UK Addendum, the parties' key contact information is located in the Agreement and/or relevant Orders.
(iii) For Table 2 of the UK Addendum, the relevant information about the version of the EU SCCs, modules, and selected clauses which this UK Addendum is appended to is located above in Section 1.2 (European Transfers) of this Schedule.
(iv) For Table 3 of the UK Addendum:

- The information required for Annex 1A is located in the Agreement and/or relevant Orders.
- The Information required for Annex 1B is located in Schedule 1 (Description of Processing) of this Addendum.
- The information required for Annex II is located in Schedule 3 (Technical and Organizational Measures).
- The information required for Annex III is located in Section 4 (Sub-processing) of this Addendum.

(b) In Table 4 of the UK Addendum, both the data importer and data exporter may end the UK Addendum.

2. US State Privacy Laws

The following terms apply where Cloudbeds Processes Personal Data subject to the US State Privacy Laws:

2.1. To the extent Client Personal Data includes personal information protected under US State Privacy Laws that Cloudbeds Processes as a Service Provider (as defined under US State Privacy Laws) or Processor, on behalf of Customer, Cloudbeds will Process such Client Personal Data in accordance with the US State Privacy Laws, including by complying with applicable sections of the US State Privacy Laws and providing the same level of privacy protection as required by US State Privacy Laws, and in accordance with Client's written instructions, as necessary for the limited and specified purposes identified in Section 1.1(a) (Client Personal Data) and Schedule 1 (Description of Processing) of this Addendum. Cloudbeds will not:

(a) retain, use, disclose or otherwise Process such Client Personal Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related Order, or as otherwise permitted under US State Privacy Laws;

(b) "sell" or "share" such Client Personal Data within the meaning of the US State Privacy Laws; and

(c) retain, use, disclose or otherwise Process such Client Personal Data outside the direct business relationship with Client and not combine such Client Personal Data with personal information that it receives from other sources, except as permitted under US State Privacy Laws.

2.2. Cloudbeds must inform Client if it determines that it can no longer meet its obligations under US State Privacy Laws within the timeframe specified by such laws, in which case Client may take reasonable and appropriate steps to prevent, stop, or remediate any unauthorized Processing of such Client Personal Data.

2.3. To the extent Client discloses or otherwise makes available Deidentified Data to Cloudbeds or to the extent Cloudbeds creates Deidentified Data from Client Personal Data, in each case in its capacity as a Service Provider, Cloudbeds will:

(a) adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(b) publicly commit to maintain and use such Deidentified Data in a de-identified form and to not attempt to re-identify the Deidentified Data, except that Cloudbeds may attempt to re-identify such data solely for the purpose of determining whether its de-identification processes are compliant with the US State Privacy Laws; and

(c) before sharing Deidentified Data with any other party, including Subprocessors, contractors, or any other persons ("**Recipients**"), contractually obligate any such Recipients to comply with all requirements of this Section 2.3 (including imposing this requirement on any further Recipients).

3. South Korea

3.1. Customer agrees that it has provided notice and obtained all consents and rights necessary under

Data Protection Laws for Cloudbeds to Process Cloudbeds Account Data and Cloudbeds Usage Data pursuant to the Agreement (including this DPA).

3.2. To the extent Client discloses or otherwise makes available Deidentified Data to Cloudbeds, Cloudbeds will:

(a) maintain and use such Deidentified Data in a de-identified form and not attempt to re-identify the Deidentified Data; and

(b) before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons ("**Recipients**"), contractually obligate any such Recipients to comply with all requirements of this Section 3.2 (including imposing this requirement on any further Recipients).

4. Definitions.

4.1 Where Personal Data is subject to the laws of one the following regions, the definition of "**Data Protection Laws**" includes:

(a) **Australia**: the Australian Privacy Act;

(b) **Brazil**: the Brazilian Lei Geral de Proteção de Dados (General Personal Data Protection Act);

(c) **Canada**: the Canadian Personal Information Protection and Electronic Documents Act;

(d) **Europe**: (i) the Regulation 2016/679 of the European Parliament and of the Council 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, or GDPR) and (ii) the EU e-Privacy Directive (Directive 2002/58/EC) as amended, superseded or replaced from time to time ("**EU Data Protection Law**");

(e) **Japan**: the Japanese Act on the Protection of Personal Information;

(f) **Singapore**: the Singapore Personal Data Protection Act;

(g) **South Korea**: the South Korean Personal Information Protection Act ("**PIPA**") and the Enforcement Decrees of PIPA;

(h) **Switzerland**: the Swiss Federal Act on Data Protection and its implementing regulations as amended, superseded, or replaced from time to time ("Swiss FADP");

(i) **The United Kingdom**: the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 as amended, superseded or replaced from time to time ("**UK Data Protection Law**"); and

(j) **The United States**: all state laws relating to the protection and Processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations ("**CCPA**"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act ("**US State Privacy Laws**").

4.2. "**Deidentified Data**" means data that cannot reasonably be used to infer information about, or otherwise be linked to, a data subject.

4.3. "**Europe**" includes, for the purposes of this DPA, the Member States of the European Union and European Economic Area.

4.4. "**EU SCCs**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, superseded, or replaced from time to time.

4.5. "**Service Provider**" has the same meaning as given in the CCPA.

4.6. "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as amended, superseded or replaced from time to time.

CLIENT	**DIGITAL ARBITRAGE, INC.**
_____	Tony Vardiman _____
Client Legal Name: _____	By: Tony Vardiman
By: _____	Title: Data Protection Officer
Title: _____	