Crystal aOS Data Processing Addendum

1 This version: 16 April 2026 v.1.0. Last updated: 16 April 2026 v1.0. Previous versions: None. Originally issued: 16 April 2026.

2 This Data Processing Addendum (**DPA**) supplements the Master Agreement (**Agreement**) entered into by and between the Client signing this DPA (**Client**) and Agentic Assets Ops (Aus) Pty Ltd (**Agentic**). By executing the DPA in accordance with clause 46 herein, Client enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below), if any. This DPA incorporates the terms of the Agreement, and any terms not defined in this DPA shall have the meaning set forth in the Agreement.

Definitions

3 **Affiliate** means:

a) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest,
b) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or
c) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

4 **Authorized Sub-Processor** means a third-party who has a need to know or otherwise access Client's Personal Data to enable Agentic to perform its obligations under this DPA or the Agreement, and who is either:

a) listed in **Exhibit B**; or

b) subsequently authorized under clause 23 of this DPA.

5 **Agentic Account Data** means personal data that relates to Agentic's relationship with Client, including the names or contact information of individuals authorized by Client to access Client's account and billing information of individuals that Client has associated with its account. Agentic Account Data also includes any data Agentic may need to collect for the purpose of managing its relationship with Client, identity verification, or as otherwise required by applicable laws and regulations.

6 **Agentic Usage Data** means Service usage data collected and processed by Agentic in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

7 **Data Exporter** means Client.

8 **Data Importer** means Agentic.

9 **Data Protection Laws** means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including:

a) the California Consumer Privacy Act (**CCPA**),

b) the General Data Protection Regulation (Regulation (EU) 2016/679) (**EU GDPR**) and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (**UK GDPR**) (together, collectively, the **GDPR**),

c) the Swiss Federal Act on Data Protection,

d) the UK Data Protection Act 2018,

e) the Privacy and Electronic Communications (EC Directive) Regulations 2003, and

f) the Australian Privacy Act 1988 including the Australian Privacy Principles (APPs);

in each case, as updated, amended or replaced from time to time. The terms Data Subject, Personal Data, Personal Data Breach, processing, processor, controller, and supervisory authority shall have the meanings set forth in the GDPR.

10 **EU SCCs** means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by clause 30 of this DPA.

11 **ex-EEA Transfer** means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (**EEA**), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

12 **ex-UK Transfer** means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (**UK**), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

13 **Services** shall have the meaning set forth in the Agreement.

14 **Standard Contractual Clauses** means the EU SCCs and the UK SCCs.

15 **UK SCCs** means the EU SCCs, as amended by the UK Addendum.

Relationship of the Parties; Processing of Data

16 The parties acknowledge and agree that with regard to the processing of Personal Data, Client may act either as a controller or processor and, except as expressly set forth in this DPA or the Agreement, Agentic is a processor. Client shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Client shall ensure that the processing of Personal Data in accordance with Client's instructions will not cause Agentic to be in breach of the Data Protection Laws. Client is solely responsible for the accuracy, quality, and legality of:

a) the Personal Data provided to Agentic by or on behalf of Client,

b) the means by which Client acquired any such Personal Data, and

c) the instructions it provides to Agentic regarding the processing of such Personal Data.

Client shall not provide or make available to Agentic any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Agentic from all claims and losses in connection therewith.

17 Agentic shall not process Personal Data:

a) for purposes other than those set forth in the Agreement and/or **Exhibit A**,

b) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Client, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which Agentic is subject; in such a case, Agentic shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or

c) in violation of Data Protection Laws.

Client hereby instructs Agentic to process Personal Data in accordance with the foregoing and as part of any processing initiated by Client in its use of the Services.

18 The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in **Exhibit A** to this DPA.

19 Following completion of the Services, at Client's choice, Agentic shall return or delete Client's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Agentic shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Client and Agentic have entered into Standard Contractual Clauses as described in Transfers of Personal Data (clauses 29-33), the parties agree that the certification of deletion of Personal Data that is described in clause 8.1(d) and clause 8.5 of the EU SCCs (as applicable) shall be provided by Agentic to Client only upon Client's request.

20 **CCPA**. Except with respect to Agentic Account Data and Agentic Usage Data, the parties acknowledge and agree that Agentic is a service provider for the purposes of the CCPA (to the extent it applies) and is receiving personal information from Client in order to provide the Services pursuant to the Agreement, which constitutes a business purpose. Agentic shall not sell any such personal information. Agentic shall not retain, use or disclose any personal information provided by Client pursuant to the Agreement except as necessary for the specific purpose of performing the Services for Client pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA. The terms personal information, service provider, sale, and sell are as defined in section 1798.140 of the CCPA. Agentic certifies that it understands the restrictions of this clause 20.

Confidentiality

21 Agentic shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Agentic's confidentiality obligations in the

Agreement. Client agrees that Agentic may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Client.

Authorized Sub-Processors

22 Client acknowledges and agrees that Agentic may:

a) engage its Affiliates as well as the Authorized Sub-Processors on the List (defined below) to access and process Personal Data in connection with the Services; and

b) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data.

By way of this DPA, Client provides general written authorization to Agentic to engage sub-processors as necessary to perform the Services.

23 A list of Agentic's current Authorized Sub-Processors (**List**) is available to Client at https://www.crystalaos.com/policies/subprocessors. Such List may be updated by Agentic from time to time. Agentic will provide a mechanism to subscribe to notifications (which may include but are not limited to email notifications) of new Authorized Sub-Processors and Client, if it wishes, will subscribe to such notifications where available. If Client does not subscribe to such notifications, Client waives any right it may have to receive prior notice of changes to Authorized Sub-Processors. At least ten (10) days before enabling any third party other than existing Authorized Sub-Processors to access or participate in the processing of Personal Data, Agentic will add such third party to the List and notify subscribers, including Client, via the aforementioned notifications. Client may object to such an engagement by informing Agentic in writing within ten (10) days of receipt of the aforementioned notice by Client, provided such objection is in writing and based on reasonable grounds relating to data protection. Client acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Agentic from offering the Services to Client.

24 If Client reasonably objects to an engagement in accordance with clause 23 of this DPA, and Agentic cannot provide a commercially reasonable alternative or the matter cannot be resolved within thirty (30) days of Agentic providing Client with notice of the new Sub-Processor or material change, Client may discontinue the use of the affected Service by providing written notice to Agentic. Discontinuation shall not relieve Client of any fees owed to Agentic under the Agreement.

25 If Client does not object to the engagement of a third party in accordance with clause 23 of this DPA within ten (10) days of notice by Agentic, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.

26 Agentic will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Agentic under this DPA with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Agentic, Agentic shall remain liable to Client for the performance of the Authorized Sub-Processor's obligations under this DPA to the extent that such Sub-Processor performs those obligations on Agentic's behalf, as if Agentic were performing them directly.

27 If Client and Agentic have entered into Standard Contractual Clauses as described in Transfers of Personal Data (clauses 29-33):

a) the above authorizations will constitute Client's prior written consent to the subcontracting by Agentic of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and

b) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Agentic to Client pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Agentic beforehand, and that such copies will be provided by Agentic only upon request by Client.

Security of Personal Data.

28 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Agentic shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. **Exhibit C** sets forth additional information about Agentic's technical and organizational security measures.

Transfers of Personal Data

29 The parties agree that Agentic may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Client acknowledges that Agentic's primary processing operations take place in the United States and Australia, and that the transfer of Client's Personal Data to the United States and Australian is necessary for the provision of the Services to Client especially in cases where Client has not configured its account settings that deal with data storage and processing region preferences. If Agentic transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Agentic will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

30 **Ex-EEA Transfers**. The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

a) Module One (Controller to Controller) of the EU SCCs apply when Agentic is processing Personal Data as a controller pursuant to clause 44 of this DPA.

b) Module Two (Controller to Processor) of the EU SCCs apply when Client is a controller and Agentic is processing Personal Data for Client as a processor pursuant to clauses 16-20 of this DPA.

c) Module Three (Processor to Sub-Processor) of the EU SCCs apply when Client is a processor and Agentic is processing Personal Data on behalf of Client as a sub-processor.

For each module, where applicable the following applies:

d) The optional docking clause in Clause 7 of the EU SCCs does not apply.

e) In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in

clause 23 of this DPA.

f) In Clause 11 of the EU SCCs, the optional language does not apply.

g) All square brackets in Clause 13 of the EU SCCs are hereby removed.

h) In Clause 17 (Option 1) of the EU SCCs, the EU SCCs will be governed by Ireland law.

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

j) **Exhibit B** to this DPA contains the information required in Annex I and Annex III of the EU SCCs.

k) **Exhibit C** to this DPA contains the information required in Annex II of the EU SCCs.

l) By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

31 **Ex-UK Transfers**. The parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed in accordance with the UK Addendum, which is incorporated herein as **Exhibit D** of this DPA.

32 **Transfers from Switzerland**. The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

a) The terms General Data Protection Regulation or Regulation (EU) 2016/679 as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (**FADP**, and as revised as of 25 September 2020, the **Revised FADP**) with respect to data transfers subject to the FADP.

b) The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

c) Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner (**FDPIC**) of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Clause 13 shall be observed.

d) The term EU Member State as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

33 **Supplementary Measures**. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

a) As of the date of this DPA, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Client's Personal Data (**Government Agency Requests**);

b) If, after the date of this DPA, the Data Importer receives any Government Agency Requests, Agentic shall attempt to redirect the law enforcement or government agency to request that data directly from Client. As part of this effort, Agentic may provide Client's basic contact information to the government agency. If compelled to disclose Client's Personal Data to a law enforcement or government agency, Agentic shall give Client reasonable notice of the demand and cooperate to allow Client to seek a protective order or other appropriate remedy unless Agentic is legally prohibited from doing so. Agentic shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of the such Government Agency Requests; and

c) The Data Exporter and Data Importer will meet as needed to consider whether:

i. the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

ii. additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

iii. it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

d) If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

e) If either:

i. any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this DPA cease to be valid; or

ii. any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended,

then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

Rights of Data Subjects

34 Agentic shall, to the extent permitted by law, notify Client upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively **Data Subject Request(s)**). If Agentic receives a Data Subject Request in relation to Client's data, Agentic will advise the Data Subject to submit their request to Client and Client will be

responsible for responding to such request, including, where necessary, by using the functionality of the Services. Client is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Agentic, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

35 Agentic shall, at the request of the Client, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Client in complying with Client's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that:*

a) Client is itself unable to respond without Agentic's assistance; and

b) Agentic is able to do so in accordance with all applicable laws, rules, and regulations.

Client shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Agentic.

Actions and Access Requests; Audits

36 Agentic shall, taking into account the nature of the processing and the information available to Agentic, provide Client with reasonable cooperation and assistance where necessary for Client to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, *provided that* Client does not otherwise have access to the relevant information. Client shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Agentic.

37 Agentic shall, taking into account the nature of the processing and the information available to Agentic, provide Client with reasonable cooperation and assistance with respect to Client's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Client shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Agentic.

38 Agentic shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA, and retain such records for a period of three (3) years after the termination of the Agreement. Client shall, with reasonable notice to Agentic, have the right to review, audit and copy such records at Agentic's offices during regular business hours.

39 Upon Client's written request at reasonable intervals, and subject to reasonable confidentiality controls, Agentic shall, either:

a) make available for Client's review copies of certifications or reports demonstrating Agentic's compliance with prevailing data security standards applicable to the processing of Client's Personal Data, or

b) if the provision of reports or certifications pursuant to a) is not reasonably sufficient under Data Protection Laws, allow Client's independent third party representative to conduct an audit or inspection of Agentic's data security infrastructure and procedures that is sufficient to demonstrate Agentic's compliance with its obligations under Data Protection Laws, *provided that*:

i. Client provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Agentic's business;

ii. such audit shall only be performed during business hours and occur no more than once per calendar year; and

iii. such audit shall be restricted to data relevant to Client. Client shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Agentic for any time expended for on-site audits. If Client and Agentic have entered into Standard Contractual Clauses as described in Transfers of Personal Data (clauses 29-33), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this clause 39.

40 Agentic shall immediately notify Client if an instruction, in Agentic's opinion, infringes the Data Protection Laws or Supervisory Authority.

41 In the event of a Personal Data Breach, Agentic shall, without undue delay, inform Client of the Personal Data Breach and take such steps as Agentic in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Agentic's reasonable control).

42 In the event of a Personal Data Breach, Agentic shall, taking into account the nature of the processing and the information available to Agentic, provide Client with reasonable cooperation and assistance necessary for Client to comply with its obligations under the GDPR with respect to notifying:

a) the relevant Supervisory Authority; and

b) Data Subjects affected by such Personal Data Breach without undue delay.

43 The obligations described in clauses 41 and 42 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Client. Agentic's obligation to report or respond to a Personal Data Breach under clauses 41 and 42 will not be construed as an acknowledgement by Agentic of any fault or liability with respect to the Personal Data Breach.

Agentic's Role as a Controller

44 The Parties acknowledge and agree that with respect to Agentic Account Data and Agentic Usage Data, Agentic is an independent controller, not a joint controller with Client. Agentic will process Agentic Account Data and Agentic Usage Data as a controller:

a) to manage the relationship with Client;

b) to carry out Agentic's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes;

c) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Client;

d) for identity verification purposes;

e) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Agentic is subject; and

f) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement.

Agentic may also process Agentic Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by Agentic as a controller shall be in accordance with Agentic's privacy policy set forth at https://www.crystalaos.com/policies/privacy.

Conflict

45 In the event of any conflict or inconsistency among the following documents, the order of precedence will be:

a) the applicable terms in the Standard Contractual Clauses;

b) the terms of this DPA;

c) the Agreement; and

d) Agentic's privacy policy.

Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Execution of this DPA

46 Agentic has pre-signed this DPA, in the signature block below and in each of the main body, and **Exhibit B** (as the data importer). To complete this DPA, Client must:

a) complete the information requested in the signature block below and sign there,

b) complete the information requested of the data exporter on **Exhibit B**, and

c) send the completed and signed Addendum to Agentic by email to support@crystalaos.com.

Upon receipt of the validly completed Addendum by Agentic at this email address, this DPA will become legally binding.

Client	**Agentic Assets Ops (Aus) Pty Ltd**
Signature:_____ Client Legal Name:_____	Signature:_____

Print Name:_____	Print Name: Joni Pirovich
Title:_____	Title: Director
Date:_____	Date:_____

Exhibit A Details of Processing

1 **Nature and Purpose of Processing**. Agentic will process Client's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Client's instructions as set forth in this DPA. The nature of processing includes, without limitation:

a) receiving data, including collection, accessing, retrieval, recording, and data entry;
b) protecting data, including restricting, encrypting, and security testing;
c) holding data, including storage, organization, and structuring;
d) erasing data, including destruction and deletion;
e) analyzing data, including product usage assessment; and
f) sharing data, including disclosure to subprocessors as permitted in this DPA.

2 **Duration of Processing:** Agentic will process Client's Personal Data as long as required:

a) to provide the Services to Client under the Agreement;
b) for Agentic's legitimate business needs; or
c) by applicable law or regulation.

Agentic Account Data and Agentic Usage Data will be processed and stored as set forth in Agentic's privacy policy.

3 **Categories of Data Subjects:** Client's employees, consultants, contractors, agents, and/or end customers, users or clients.

4 **Categories of Personal Data:** Agentic processes Personal Data contained in Agentic Account Data, Agentic Usage Data, and any Personal Data provided by Client (including any Personal Data Client collects from its end users and processes through its use of the Services) or collected by Agentic in order to provide the Services or as otherwise set forth in the Agreement or this DPA. Categories of Personal Data include name, email, job title, username, Agentic device identifiers (e.g. serial number), IP address for Agentic device, installed applications for Agentic device, background check verification records (at discretion of Controller), security training records.

5 **Sensitive Data or Special Categories of Data:** Clients are prohibited from providing sensitive personal data or special categories of data to Agentic, including without limitation, any data which discloses the criminal history, unless Client has obtained prior written consent from Agentic and engaged in good faith with Agentic as to the appropriateness of existing controls and necessity of new controls prior to providing sensitive personal data or special categories of data to Agentic.

Exhibit B Information Required by EU SCCs and UK Addendum

1 The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

2 The Parties

Data exporter(s):

Name:

Trading Name (if different):

Address: ;

Official Registration Number (if any) (Agentic number or similar identifier):

Contact person's name, position and contact details: , ,

Activities relevant to the data transferred under these Clauses: As described in Section 2 of the DPA.

Signature and date:

Role (controller/processor): Controller

Data importer(s):

Name: Agentic Assets Ops (Aus) Pty Ltd

Trading Name (if different): N/A

Address and contact information: 805 / 220 Collins St, Melbourne VIC 3000; support@crystalaos.com

Official Registration Number (if any) (Company number or similar identifier): ABN 34 672 615 851

Activities relevant to the data transferred under these Clauses: As described in clauses 16-20 of the DPA.

Signature and date:

Role (controller/processor): As described in clauses 16-20 of the DPA.

3 Description of the Transfer

Data Subjects	As described in Exhibit A of the DPA
Categories of Personal Data	As described in Exhibit A of the DPA
Special Category Personal Data (if applicable)	As described in Exhibit A of the DPA
Nature of the Processing	As described in Exhibit A of the DPA
Purposes of Processing	As described in Exhibit A of the DPA

Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the DPA
Frequency of the transfer	As necessary to provide perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA
Recipients of Personal Data Transferred to the Data Importer	Agentic will maintain a list of Authorized Sub-Processors at: https://www.crystalaos.com/policies/subprocessors.

4 **Competent Supervisory Authority**. The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

Exhibit C Description of the Technical and Organizational Security Measures implemented by the Data Importer

1 The following includes the information required by Annex II of the EU SCCs and Annex II of the UK Addendum.

Technical and Organizational Security Measure	**Details**
Measures of pseudonymisation and encryption of personal data	Agentic has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive Client data are encrypted at rest. Agentic uses only recommended secure cipher suites and protocols to encrypt all traffic in transit and Client Data is securely encrypted with strong ciphers and configurations when at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Agentic's Client agreements contain strict confidentiality obligations. Additionally, Agentic requires every downstream Sub-Processor to sign confidentiality provisions that are substantially similar to those contained in Agentic's Client agreements. Agentic has undergone a SOC 2 Type 2 audit that includes the Security, Confidentiality and Availability Trust Service Criteria.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Daily backups of production datastores are taken each day for thirty-five (35) days, and an annual backup is taken and held for 366 days. Backups are periodically tested in accordance with information security and data management policies.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Agentic has undergone a SOC 2 Type 2 audit that includes the Security, Confidentiality, and Availability Trust Service Criteria.
Measures for user identification and authorization	Agentic uses secure access protocols and processes and follows industry best-practices for authentication, including Multifactor Authentication and Single Sign On (SSO). All production access requires the use of two-factor authentication, and network infrastructure is securely configured to vendor

	and industry best practices to block all unnecessary ports, services, and unauthorized network traffic.
Measures for the protection of data during transmission	Agentic has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Agentic uses only recommended secure cipher suites and protocols to encrypt all traffic in transit (i.e. TLS 1.2+)
Measures for the protection of data during storage	Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by AWS.
Measures for ensuring physical security of locations at which personal data are processed	All Agentic processing occurs in physical data centers that are managed by AWS. https://aws.amazon.com/compliance/data-center/controls/
Measures for ensuring events logging	Agentic monitors access to applications, tools, and resources that process or store Client Data, including cloud services. Monitoring of security logs is managed by the security and engineering teams. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	Agentic adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. All production changes are automated through CI/CD tools to ensure consistent configurations.
Measures for internal IT and IT security governance and management	Agentic maintains an ISO 27001-compliant risk-based information security governance program. The framework for Agentic's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Client Data.
Measures for certification/assurance of processes and products	Agentic undergoes annual SOC 2 Type II and ISO 27001 audits, as well as ISO 42001 audits.
Measures for ensuring data minimisation	Agentic's Clients unilaterally determine what data they route through the Services. As such, Agentic operates on a shared

	responsibility model. Agentic gives Clients control over exactly what data enters Crystal aOS. Additionally, Agentic has built in self-service functionality to the Services that allows Clients to delete and suppress data at their discretion and configure data storage, processing and retention settings.
Measures for ensuring data quality	Agentic provides several technical, procedural and governance measures to ensure data quality. These measures include: (i) human-in-the-loop governance for adding documents and data to Knowledge Sets, (ii) use of Retrieval-Augmented Generation (RAG) pipeline to retrieve data before it is sent to a language model with the query to return a response, with citations that hyperlink to the source document(s), (iii) an evals model to ensure outputs from AI can be reviewed by both humans–in-the-loop and LLM(s)-as-a-judge, with strict mode that immediately halts a workflow where outputs fall below acceptance scores for eval criteria. Agentic ensures that data quality is maintained from the time a Client sends Client Data into the Services and until that Client Data is presented or exported through measures such as ACID-compliance of our production database(s), encryption and quality assurance testing throughout feature development.
Measures for ensuring limited data retention	Clients unilaterally determine what data they route through the Services. As such, Agentic operates on a shared responsibility model. If a Client is unable to delete Personal Data via the self-services functionality of the Services, then Agentic deletes such Personal Data upon the Client's written request, within the timeframe specified in this DPA and in accordance with Applicable Data Protection Law. All Personal Data is deleted from the Services following service termination.
Measures for ensuring accountability	Agentic has adopted measures for ensuring accountability, such as implementing data protection and information security policies across the business, recording and reporting Personal Data Breaches, and formally assigning roles and responsibilities for information security and data privacy functions. Additionally, Agentic conducts regular third-party audits to ensure

	compliance with our privacy and security standards.
Measures for allowing data portability and ensuring erasure	Personal Data submitted to the Services by Client may be deleted by the Client or at the Client's request. Personal Data is incidental to Agentic's Services. Based on Privacy by Design and Data Minimization principles, Agentic severely limits the instances of Personal Data collection and processing within the Services. Most use cases for porting Personal Data from Agentic are not applicable. However, Agentic will respond to all requests for data porting in order to address Client needs.
Technical and organizational measures of sub-processors	Agentic enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this DPA.

Exhibit D UK Addendum, International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

1 Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Client	Agentic
Key Contact	*See* Exhibit B of this DPA	*See* Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by clause 30 of the DPA.

Table 3: Appendix Information

Appendix Information means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

a)	Annex 1A: List of Parties	b)	As per Table 1 above
c)	Annex 2B: Description of Transfer	*d)*	*See Exhibit B of this DPA*
e)	Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	*f)*	*See Exhibit C of this DPA*
g)	Annex III: List of Sub processors (Modules 2 and 3 only):	*h)*	*See Exhibit B of this DPA*

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

a) **[SELECT OPTION]** [*Note: This provision permits the selected party (if any) to terminate the UK Addendum if the ICO changes the approved UK Addendum which directly results in a substantial, disproportionate, and demonstrable increase in (a) its direct costs of performing its obligations under the UK Addendum or (b) its risk under the UK Addendum.]*

Ending this UK Addendum when the Approved UK Addendum changes	x Importer x Exporter ☐ Neither Party

Entering into this UK Addendum:

2 Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.

3 Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

4 Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

UK Addendum	means this International Data Transfer Addendum incorporating the EU SCCs, attached to the DPA as Exhibit D.
EU SCCs	means the version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information
Appendix Information	shall be as set out in Table 3
Appropriate Safeguards	means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making an ex-UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	means the template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under clause 19 of this UK Addendum.
Approved EU SCCs	means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).
ICO	means the Information Commissioner of the United Kingdom.

ex-UK Transfer	shall have the same definition as set forth in the DPA .
UK	means the United Kingdom of Great Britain and Northern Ireland
UK Data Protection Laws	means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	shall have the definition set forth in the DPA.

5 The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfills the Parties' obligation to provide the Appropriate Safeguards.

6 If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.

7 If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws will apply.

8 If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

9 Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.

Hierarchy

10 Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for ex-UK Transfers, the hierarchy in clause 11 below will prevail.

11 Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.

12 Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

Incorporation and Changes to the EU SCCs:

13 This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:

a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b) clauses 10-12 above override clause 6 of the EU SCCs; and

c) the UK Addendum (including the EU SCCs incorporated into it) is:

i. governed by the laws of England and Wales; and

ii. any dispute arising from it is resolved by the courts of England and Wales.

14 Unless the parties have agreed alternative amendments which meet the requirements of clause 13 of this UK Addendum, the provisions of clause 16 of this UK Addendum will apply.

15 No amendments to the Approved EU SCCs other than to meet the requirements of clause 13 of this UK Addendum may be made.

16 The following amendments to the EU SCCs (for the purpose of clause 13 of this UK Addendum) are made:

a) references to the "Clauses" means this UK Addendum, incorporating the EU SCCs;

b) in Clause 2, 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",

c) Clause 6 (Description of the transfer(s)) is replaced with: "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 Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d) Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e) Clause 8.8(i) of Modules 2 and 3 is 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;"

f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g) References to Regulation (EU) 2018/1725 are removed;

h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i) The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j) Clause 13(a) and Part C of Annex I are not used;

k) The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l) In Clause 16(e), subsection (i) is replaced with: “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m) Clause 17 is replaced with: “These Clauses are governed by the laws of England and Wales”;

n) Clause 18 is replaced with: “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales.” A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts.”; and

o) The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to the UK Addendum

17 The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

18 If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

19 From time to time, the ICO may issue a revised Approved UK Addendum which:

a) makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

b) reflects changes to UK Data Protection Laws;

The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

20 If the ICO issues a revised Approved UK Addendum under clause 19 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

a) its direct costs of performing its obligations under the UK Addendum; and/or

b) its risk under the UK Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

21 The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.