WHITE-LABEL PLATFORM DATA PROCESSING ADDENDUM

This Data Processing Addendum (including its Appendices) ("**Addendum**") forms part of and is subject to the terms and conditions of the White Label Platform Exhibit (the "**White Label Platform Exhibit**") by and between Customer and Talos Trading, LLC ("**Talos**").

1. Subject Matter and Duration.

a) Subject Matter. This Addendum reflects the parties' commitment to abide by Data Protection Laws concerning the Processing of Customer Personal Data under the terms of the White Label Platform Exhibit. All capitalized terms that are not expressly defined in the White Label Platform Exhibit will have the meanings given to them in the White Label Platform Exhibit. If and to the extent language in this Addendum or any of its Exhibits conflicts with the White Label Platform Exhibit, this Addendum shall control.

b) Duration. This Addendum will become legally binding upon the date that the parties sign this Addendum. This Addendum will terminate automatically upon termination of the White Label Platform Exhibit.

2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) "**Customer Personal Data**" means Personal Data Processed by Talos under the White Label Platform Exhibit on behalf of Customer.

b) "**Data Protection Laws**" means all applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which the Customer Personal Data are subject. "Data Protection Laws" may include, but are not limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"); the EU General Data Protection Regulation 2016/679 ("**GDPR**") and its respective national implementing legislations; the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation; and the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time).

c) "**Personal Data**" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws, and will, at a minimum, mean any information relating to an identified or identifiable natural person.

d) "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or 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.

e) "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data attributable to Talos.

f) "**Services**" means the services that Talos performs under the White Label Platform Exhibit.

g) "**Subprocessor(s)**" means Talos's authorized vendors and third-party service providers that Process Customer Personal Data.

3. Processing Terms for Customer Personal Data.

a) Talos's Role under Data Protection Laws. Talos is a "Service Provider" and/or independent "Processor" of Customer Personal Data (as such terms are defined by Data Protection Laws). Under no circumstances shall the parties be considered joint "Controllers" under Data Protection Laws.

b) Talos's Processing of Customer Personal Data. Talos shall Process Customer Personal Data to provide the Services in accordance with the White Label Platform Exhibit, this Addendum, any applicable Statement of Work, and any instructions agreed upon by the parties. Talos will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and Applicable Law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions.

c) Authorization to Use Subprocessors. To the extent necessary to fulfill Talos's contractual obligations under the White Label Platform Exhibit, Customer hereby authorizes Talos to engage Subprocessors.

d) Talos and Subprocessor Compliance. Talos shall (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Customer Personal Data that imposes on such Subprocessors data protection requirements for Customer Personal Data that are consistent with this Addendum; and (ii) remain responsible to Customer for Talos's Subprocessors' failure to perform their obligations with respect to the Processing of Customer Personal Data.

e) Right to Object to Subprocessors. Where required by Data Protection Laws, Talos will notify Customer via email prior to engaging any new Subprocessors that Process Customer Personal Data and allow Customer ten (10) days to object. If Customer has legitimate objections to the appointment of any new Subprocessor, the parties will work together in good faith to resolve the grounds for the objection.

f) Confidentiality. Any person authorized to Process Customer Personal Data must contractually agree to maintain the confidentiality of such information or be under an appropriate statutory obligation of confidentiality.

g) Personal Data Inquiries and Requests. Where required by Data Protection Laws, Talos agrees to provide reasonable assistance and comply with reasonable instructions from Customer related to any requests from individuals exercising their rights in Customer Personal Data granted to them under Data Protection Laws.

h) Sale of Customer Personal Data Prohibited. Talos shall not sell Customer Personal Data as the term "sell" is defined by the CCPA.

i) Data Protection Impact Assessment and Prior Consultation. Where required by Data Protection Laws, Talos agrees to provide reasonable assistance at Customer's expense to Customer where, in Customer's judgment, the type of Processing performed by Talos requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

j) Demonstrable Compliance. Talos agrees to provide information reasonably necessary to demonstrate compliance with this Addendum upon Customer's reasonable request.

k) Service Optimization. Where permitted by Data Protection Laws, Talos may Process Customer Personal Data: (i) for its internal uses to build or improve the quality of its services; (ii) to detect Security Incidents; and (iii) to protect against fraudulent or illegal activity.

l) Aggregation and De-Identification. Talos may: (i) compile aggregated and/or de-identified information in connection with providing the Services provided that such information cannot reasonably be used to identify Customer or any data subject to whom Customer Personal Data relates ("**Aggregated and/or De-Identified Data**"); and (ii) use Aggregated and/or De-Identified Data for its lawful business purposes.

m) Information Security. Talos shall implement and maintain commercially reasonable technical and organizational measures designed to protect Customer Personal Data in accordance with the Technical and Organizational Measures attached hereto as **Appendix I**.

n) Security Incidents. Upon becoming aware of a Security Incident, Talos agrees to provide written notice without undue delay to Customer within the time frame required under Data Protection Laws to Customer's designated point of contact. Where possible, such notice will include all available details required under Data Protection Laws for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident

4. Cross-Border Transfers of Customer Personal Data.

a) Cross-Border Transfers of Customer Personal Data. Customer authorizes Talos and its Subprocessors to transfer Customer Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.

b) EEA, Swiss, and UK Standard Contractual Clauses. If Customer Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Customer to Talos in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by Module Two's obligations in the Annex to the Commission Implementing Decision (EU) 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 ("**Standard Contractual Clauses**") as supplemented by **Appendix 2** attached hereto, the terms of which are incorporated herein by reference. Each party's signature to this Order Form shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

5. Audits.

a) Customer Audit. Where Data Protection Laws afford Customer an audit right, Customer (or its appointed representative) may carry out an audit of Talos's policies, procedures, and records relevant to the Processing of Customer Personal Data. Any audit must be: (i) conducted during Talos's regular business hours; (ii) with reasonable advance notice to Talos; (iii) carried out in a manner that prevents unnecessary disruption to Talos's operations; and (iv) subject to reasonable confidentiality procedures. In addition, any audit shall be limited to once per year, unless an audit is carried out at the direction of a government authority having proper jurisdiction.

6. Customer Personal Data Deletion.

a) Data Deletion. At the expiry or termination of the White Label Platform Exhibit, Talos will delete all Customer Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with Talos's data retention schedule), except where Talos is required to retain copies under applicable laws, in which case Talos will isolate and protect that Customer Personal Data from any further Processing except to the extent required by applicable laws.

7. Customer's Obligations. Customer represents and warrants that: (i) it has complied and will comply with Data Protection Laws; (ii) it has provided data subjects whose Customer Personal Data will be Processed in connection with the White Label Platform Exhibit with a privacy notice or similar document that clearly and accurately describes Customer's practices with respect to the Processing of Customer Personal Data; (iii) it has obtained and will obtain and continue to have, during the term, all necessary rights, lawful bases, authorizations, consents, and licenses for the Processing of Customer Personal Data as contemplated by the White Label Platform Exhibit; and (iv) Talos's Processing of Customer Personal Data in accordance with the White Label Platform Exhibit will not violate Data Protection Laws or cause a breach of any agreement or obligations between Customer and any third party.

8. Processing Details.

a) Subject Matter. The subject matter of the Processing is the Services pursuant to the White Label Platform Exhibit.

b) Duration. The Processing will continue until the expiration or termination of the White Label Platform Exhibit.

c) Categories of Data Subjects. Data subjects whose Customer Personal Data will be Processed pursuant to the White Label Platform Exhibit.

d) Nature and Purpose of the Processing. The purpose of the Processing of Customer Personal Data by Talos is the performance of the Services.

e) Types of Customer Personal Data. Customer Personal Data that is Processed pursuant to the White Label Platform Exhibit.

APPENDIX 1 TO THE DATA PROCESSING ADDENDUM

TECHNICAL AND ORGANIZATIONAL MEASURES

This Appendix 1 forms part of the Addendum. Capitalized terms not defined in this Appendix 1 have the meaning set forth in Addendum.

Talos shall use commercially reasonable efforts to implement and maintain reasonable administrative, technical, and physical safeguards designed to protect Customer Personal Data. Such safeguards shall include:

1. Information Security Policy. Talos shall maintain a written information security policy applicable to all authorized personnel.

2. Training. Talos will provide information security awareness training to all employees annually.

3. Access Control. Talos will maintain an access control policy, procedures, and controls consistent with industry standard practices. Talos will limit access to Customer Personal Data to those employees and Subprocessors with a need-to-know.

4. Logical Separation. Talos will ensure Customer Personal Data is logically separated from other Talos client data.

5. Encryption. Where appropriate, Customer Personal Data will be encrypted in-transit and at rest using industry standard encryption technologies.

6. Password Management. Talos will maintain a password management policy designed to ensure strong passwords consistent with industry standard practices.

7. Incident Response Plan. Talos will maintain an incident response plan that addresses Security Incident handling. Upon request, Talos will provide Customer with a copy of its incident response plan.

8. Backups of Customer Personal Data. Talos will maintain an industry standard backup system and backup of Customer Personal Data designed to facilitate timely recovery in the event of a service interruption.

9. Disaster Recovery and Business Continuity Plans. Talos will maintain disaster recovery and business continuity plans consistent with industry standard practices.

APPENDIX 2 TO THE DATA PROCESSING ADDENDUM

ADDITIONAL TERMS FOR THE STANDARD CONTRACTUAL CLAUSES

This Appendix 2 forms part of the Addendum and supplements the Standard Contractual Clauses. Capitalized terms not defined in this Appendix 2 have the meaning set forth in the Addendum.

The parties agree that the following terms shall supplement the Standard Contractual Clauses:

1. Supplemental Terms. The parties agree that the following terms shall supplement the Standard Contractual Clauses: (i) a new Clause 1(e) is added the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the applicable data protection laws of the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection."; (ii) the optional text in Clause 7 is deleted; (iii) a new Clause 1(f) is added to the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to the UK Data Protection Laws (as defined in Annex III); (iv) Option 1 in Clause 9 is struck and Option 2 is kept, and data importer must submit the request for specific authorization in accordance with Section 3(e) of the Addendum; (v) the optional text in Clause 11 is deleted; and (vi) in Clauses 17 and 18, the governing law and the competent courts are those of Ireland (for EEA transfers), Switzerland (for Swiss transfers), or England and Wales (for UK transfers).

2. Annex I. Annex I to the Standard Contractual Clauses shall read as follows:

A. List of Parties

Data Exporter: Customer.
Address: As set forth in the Notices section of the Software Subscription Agreement dated by and between Talos and Customer (the "**Main Agreement**").
Contact person's name, position, and contact details: As set forth in the Notice section of the Main Agreement.
Activities relevant to the data transferred under these Clauses: The Services as set forth in the White Label Platform Exhibit.
Role: Controller.

Data Importer: Talos.
Address: As set forth in the Notices section of the Main Agreement.
Contact person's name, position, and contact details: As set forth in the Notice section of the Main Agreement.
Activities relevant to the data transferred under these Clauses: The Services as set forth in the White Label Platform Exhibit.
Role: Processor.

B. Description of the Transfer:

Categories of data subjects whose personal data is transferred: Customer's personnel who are authorized users of the Services and Customer's customers.

Categories of personal data transferred: Customer Personal Data that is Processed under the White Label Platform Exhibit including, but not limited to, name and email address.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: To the parties' knowledge, no sensitive data is transferred.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Customer Personal Data is transferred on a continuous basis by virtue of an authorized user's use of the Services.

Nature of the processing: As set forth in the White Label Platform Exhibit.

Purpose(s) of the data transfer and further processing: Talos provides software to help institutions and their customers manage their full trade lifecycle of crypto, including: liquidity sourcing, direct market access, price discovery, algorithmic trade execution, transaction cost analysis (TCA), reporting, clearing, and settlement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Customer Personal Data will be retained in accordance with the Talos privacy policy available at: https://talos.com/privacy-policy/.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: The list of Talos's subprocessors can be provided upon Customer's request.

C. Competent Supervisory Authority: The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

D. Additional Data Transfer Impact Assessment Questions: Data importer agrees that the responses to the data transfer impact assessment questions below are true, complete, and accurate.

Will data importer process any personal data under the Clauses about a non-United States person that is "foreign intelligence information" as defined by 50 U.S.C. § 1801(e)? Not to data importer's knowledge.

Is data importer subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where personal data is stored or accessed from that would interfere with data importer fulfilling its obligations under the Standard Contractual Clauses? For example, FISA Section 702. If yes, please list these laws: As of the effective date of the Addendum, no court has found Talos to be eligible to receive process issued under the laws contemplated by Question 10, including FISA Section 702 and no such court action is pending.

Has data importer ever received a request from public authorities for information pursuant to the laws contemplated by the question above? If yes, please explain: No.

Has data importer ever received a request from public authorities for personal data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain: No.

E. Data Transfer Impact Assessment Outcome: Taking into account the information and obligations set forth in the Addendum and, as may be the case for a party, such party's independent research, to the parties' knowledge, the personal data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the Standard Contractual Clauses to a country that has not been found to provide an adequate level of protection under applicable data protection laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable data protection laws.

F. Clarifying Terms: The parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Standard Contractual Clauses will be provided upon data exporter's written request; (ii) the measures data importer is required to take under Clause 8.6(c) of the Standard Contractual Clauses will only cover data importer's impacted systems; (iii) the audit described in Clause 8.9 of the Clauses shall be carried out in accordance with Section 7 of the Addendum; (iv) where permitted by applicable data protection laws, data importer may engage existing subprocessors using European Commission Decision C(2010)593 Standard Contractual Clauses for Controllers to Processors and such use of subprocessors shall be deemed to comply with Clause 9 of the Standard Contractual Clauses; (v) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Standard Contractual Clauses will be limited to the termination of the Standard Contractual Clauses; (vi) unless otherwise stated by data importer, data exporter will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Standard Contractual Clauses; (vii) the information required under Clause 15.1(c) of the Standard Contractual Clauses will be provided upon data exporter's written request; and (viii) notwithstanding anything to the contrary, data exporter will reimburse data importer for all costs and expenses incurred by data importer in connection with the performance of data importer's obligations under Clause 15.1(b) and Clause 15.2 of the Standard Contractual Clauses without regard for any limitation of liability set forth in the Main Agreement or the White Label Exhibit.

3. Annex II. Annex II of the Standard Contractual Clauses shall read as follows:

Data importer shall implement and maintain appropriate technical and organisational measures designed to protect personal data in accordance with the Addendum.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the Addendum.

4. Annex III. A new Annex III shall be added to the Standard Contractual Clauses and shall read as follows:

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK Addendum to the EU Commission Standard Contractual Clauses

Date of this Addendum:

1. The Standard Contractual Clauses are dated as of the same date as the Addendum.

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors. This Addendum forms part of and supplements the Standard Contractual Clauses to which it is attached. If personal data originating in the United Kingdom is transferred by data exporter to data importer in a country that has not been found to provide an adequate level of protection under UK Data Protection Laws, the Parties agree that the transfer shall be governed by the Standard Contractual Clauses as supplemented by this Addendum.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Standard Contractual Clauses
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021
UK Data Protection Laws	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	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that it fulfills the intention for it to provide the appropriate safeguards as required by Article 46 UK GDPR.

5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. 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 this Addendum has been entered into.

Hierarchy

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the Standard Contractual Clauses or other related agreements between the Parties, existing at the time this

Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

a. for 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 transfer; and

b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 8 above, include (without limitation):

a. References to the "Clauses" means this Addendum as it incorporates the Standard Contractual Clauses

b. Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfer(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."

c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.

d. References to Regulation (EU) 2018/1725 are removed.

e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK."

f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner.

g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales."

h. Clause 18 is replaced to state:

"Any dispute arising from these Standard Contractual 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."