DATA PROCESSING ADDENDUM

This Data Processing Addendum (including its Appendices) ("**Addendum**") forms part of and is subject to the terms and conditions of the Order Form and Software Subscription Agreement (collectively, the "**Agreement**") by and between Customer (as defined in the Order Form) 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 Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, 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 Agreement.

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 Agreement.

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Data Protection Regulation; and the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time).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 Agreement.

3. Processing Terms for Customer Personal Data.

a) Talos's Role under Data Protection Laws. Talos is a "Business" and/or independent "Controller" 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 and in accordance with the Talos Privacy Policy available at: https://talos.com/privacy-policy/.

c) 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**.

d) Security Incidents. Upon becoming aware of a Security Incident, Talos agrees to provide written notice without undue delay to Customer. Talos shall be solely responsible for remediating the Security Incident, including the provision of any legally required notice to affected individuals required under Data Protection Laws.

4. Cross-Border Transfers of Customer Personal Data.

a) Cross-Border Transfers of Customer Personal Data. Customer authorizes Talos 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 One'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 Agreement shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

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. Personnel Security. 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 (a) limit access to Customer Personal Data to those employees and Subprocessors with a need-to-know, (b) promptly terminate its personnel's access to Customer Personal Data when such access is no longer required for performance under the Agreement; (c) ensure multifactor authentication is used to access all Customer Personal Data and network systems (d) log the details of any access to Customer Personal Data, and (e) be responsible for any "**Processing**" (as defined in the Addendum) of Customer Personal Data by its personnel. Talos agrees to employ reasonable tools and techniques to detect unauthorized access, copying, or leakage of sensitive information. Talos shall implement measures to prevent Customer Personal Data from being downloaded or otherwise copied to local drives or removable media.

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

5. Encryption. Using industry standard encryption tools, Talos will encrypt Customer Personal Data that Talos: (i) transmits or sends wirelessly or across public networks or within the Talos Systems; (ii) stores on laptops or storage media, and (iii) stores on portable devices or within the Talos System. Talos will safeguard the security and confidentiality of all encryption keys associated with encrypted information. Talos shall encrypt all Customer Personal Data while at rest and in transit.

6. Password Management. Talos will maintain a password management policy designed to ensure strong passwords consistent with industry standard practices. Multi-factor will be enforced for authentication to production systems by Talos staff.

7. Security Monitoring. Talos will provide security detection & monitoring for production systems with alerts evaluated and escalated 24x7x365 based on severity and impact.

8. Incident Response Plan. Talos will maintain an incident response plan to detect, respond to, contain, investigate, and remediate cybersecurity incidents, including all incidents that compromise the confidentiality, integrity, and availability of data, systems, networks, and services. The plan shall identify and assign roles and responsibilities to key stakeholders and decision-makers across the organization. Talos shall regularly test the incident response plan.

9. 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.

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

11. Third Party Assessment. Talos shall engage a qualified third-party assessment organization to conduct external penetration testing on at least an annual basis and shall remediate any findings classified as “critical” or “high” within 30 days.

12. Detection and Alerting. will proactively monitor, detect, and alert its internal security team regarding suspicious or malicious activity within Talos’s production and corporate environments.

13. Security Segmentation. Talos will use appropriate measures to monitor, detect and restrict the flow of information on a multilayered basis within the Talos Systems using tools such as firewalls, proxies, and network-based intrusion detection systems, where necessary.

14. Secure Software Development. Talos represents and warrants that any software used in connection with the Processing of Customer Personal Data is or has been developed using secure software development practices, including: (a) segregating development and production environments; (b) filtering out potentially malicious character sequences in user inputs; (c) using secure communication techniques, including encryption; (d) using sound memory management practices; (e) using web application firewalls to address common web application attacks such as cross-site scripting, SQL injection and command injection; (f) implementing the OWASP Top Ten recommendations, as applicable; (g) patching of software; (h) testing object code and source code for common coding errors and vulnerabilities using code analysis tools; (i) testing of web applications for vulnerabilities using web application scanners; and (j) testing software for performance under denial of service and other resource exhaustion attacks.

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 Switzerland and/or the United Kingdom. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss and/or United Kingdom law as it relates to transfers of personal data that are subject to such laws."; (ii) the optional text in Clause 7 is deleted; (iii) the measures Talos is required to take under Clause 8.5(d) of the Standard Contractual Clauses are those measures required of Talos under applicable Data Protection Laws; (iv) the optional text in Clause 11 is deleted; (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, in which case, the corresponding Processing of Customer Personal Data affected by such termination shall be discontinued unless otherwise agreed by the parties; (vi) notwithstanding anything to the contrary, Customer will reimburse Talos for all costs and expenses incurred by Talos in connection with the performance of Talos'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 Agreement; (vii) the information required under Clause 15.1(c) will be provided upon Customer's written request; and (viii) 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 Agreement.
Contact person's name, position, and contact details: As set forth in the Notices section of the Agreement.
Activities relevant to the data transferred under these Clauses: As set forth in the Agreement.
Role: Controller.

Data Importer: Talos.
Address: As set forth in the Notices section of the Agreement.
Contact person's name, position, and contact details: As set forth in the Notices section of the Agreement.
Activities relevant to the data transferred under these Clauses: As set forth in the Agreement.
Role: Controller.

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 Agreement 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 Agreement.

Purpose(s) of the data transfer and further processing: Talos provides software to help institutions 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.

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.

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

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