DATA PROTECTION AGREEMENT

Customer and FuelTrust have agreed to this Data Protection Addendum ("**DPA**") as of the date of the Agreement into which it is incorporated thereto. This DPA applies to all Services provided by FuelTrust to Customer that involve the processing by FuelTrust of any Personal Data provided to FuelTrust under the Agreement on behalf of Customer pursuant to or in connection with the Services ("**Customer Personal Data**").

The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement. Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by and including this DPA. The following obligations shall only apply to the extent required by Data Protection Laws with regard to the relevant Customer Personal Data, if applicable.

1. **Definitions**

   1.1. In this DPA, the following terms shall have the meanings set out below..

      1.1.1. "**Data Protection Laws**" means, as applicable: (a) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "**GDPR**"); (b) the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 *et seq*. ("**CCPA**"); (c) United Kingdom ("UK") General Data Protection Regulation ("UK GDPR") and the UK Data Protection Act 2018; and (d) any other applicable data privacy and security laws and regulations.

      1.1.2. "**EEA**" means the European Economic Area.

      1.1.3. "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

      1.1.4. "**Standard Contractual Clauses**" means the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries (2010/87/EU) (the text of which is available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087), as amended from time to time.

      1.1.5. "**Subprocessor**" means any entity duly appointed by or on behalf of FuelTrust to Process Customer Personal Data in connection with the Services provided under Agreement.

   1.2. The terms "**Controller**," "**Data Subject**," "**Personal Data Breach**," "**Processing**," "**Processor**," and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

   1.3. The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. **Processing of Customer Personal Data**

   2.1. While providing the Services to Customer pursuant to the Agreement, FuelTrust may Process Customer Personal Data on behalf of Customer as per the terms of this DPA. The parties acknowledge and agree that, with regard to the Processing of Customer

Personal Data, Customer may be either the Controller or a Processor when it processes Personal Data of its clients ("**Clients**"). Consequently, FuelTrust is a Processor where Customer is a Controller, or a Subprocessor when Customer is acting as a Processor on behalf of its Clients. In some circumstances Customer may be a Processor, in which case Customer appoints FuelTrust as Customer's Subprocessor, which shall not change the obligations of either Customer or FuelTrust under this DPA, as FuelTrust will remain a Processor with respect to Customer in such event. FuelTrust shall only retain, use, or disclose Customer Personal Data as necessary for FuelTrust' performance of its obligations under the Agreement and only in accordance with Customer's instructions. FuelTrust shall not sell any Customer Personal Data as the term "selling" is defined in the CCPA. FuelTrust agrees to refrain from taking any action that would cause any transfers of Customer Personal Data to or from Customer to qualify as "selling personal information" under the CCPA.

2.2. FuelTrust shall not Process Customer Personal Data other than on Customer's documented (electronic) instructions unless Processing is required by Data Protection Laws to which FuelTrust is subject, in which case FuelTrust shall, to the extent permitted by Data Protection Laws, inform Customer of that legal requirement before Processing Customer Personal Data. For the avoidance of doubt, the Agreement, including any related Order entered into by Customer, shall constitute documented instructions for the purposes of this DPA. Customer shall be, or shall require Clients to be, responsible for: (a) giving adequate notice and making all appropriate disclosures to Data Subjects regarding Customer's use and disclosure and FuelTrust' Processing of Customer Personal Data; and (b) obtaining all necessary rights, and, where applicable, all appropriate and valid consents to disclose such Customer Personal Data to FuelTrust and to permit the Processing of such Customer Personal Data by FuelTrust for the purposes of performing FuelTrust's obligations under the Agreement or as may be required by Data Protection Laws. Customer shall notify FuelTrust of any changes in, or revocation of, the permission to use, disclose, or otherwise Process Customer Personal Data that would impact FuelTrust's ability to comply with the Agreement, or Data Protection Laws to which FuelTrust is subject.

2.3. Annex A to this DPA sets out certain information regarding FuelTrust' Processing of the Customer Personal Data.

3. **Security**

3.1. In accordance with its obligations under Data Protection Laws, FuelTrust shall take appropriate technical and organizational security measures ('TOMS') in Processing Customer Personal Data so as to ensure an appropriate level of security is adopted to mitigate the risks associated with the Processing of such Customer Personal Data, including unauthorized or unlawful Processing, accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or damage or access to the Customer Personal Data.

3.2. Information security policies of FuelTrust are reviewed at least annually and refined as necessary to keep current with modern threats and in line with updates to broadly accepted international standard ISO/IEC 27001. FuelTrust follows a mandated set of employment verification requirements for all new hires, including supplemental employees. These standards also apply to wholly owned subsidiaries and joint ventures. The requirements, which may be subject to change, include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each FuelTrust employee is responsible for implementing the above requirements in its hiring process as applicable and permissible under local law.

3.3. FuelTrust employees are required to complete security and privacy education annually and certify each year that they will comply with FuelTrust's ethical business conduct, confidentiality, and security requirements.

3.4. Security incidents are handled in accordance with FuelTrust's incident management and response policies, taking into account data breach notification requirements under Data Protection Laws.

3.5. The core functions of FuelTrust's cyber security incident management practice are conducted by FuelTrust's Computer Security Incident Response Team (CSIRT). CSIRT is managed by FuelTrust's Chief Information Security Office and is staffed with incident managers and outsourced forensic analysts. National Institute of Standards and Technology, United States Department of Commerce (NIST) and ISO guidelines for computer security incident handling have informed the development and remain the foundation of FuelTrust's incident management processes. CSIRT coordinates with other functions within FuelTrust to investigate suspected incidents, and if warranted, define, and execute the appropriate response plan. Upon determining that a Personal Data Breach, has occurred that affects Customer, FuelTrust will notify Customer, promptly, but not more than 72 hours, of being aware of the breach. The notification given will provide at least:

- Nature of the breach
- the date and time of occurrence of the breach
- the extent of the Customer Personal Data information ('PI') and data subjects affected by the breach
- the name and contact details of the Chief Information Security Office
- If known, the likely consequences of the breach
- The current measures taken or proposed to be taken to address the breach an mitigate its adverse effects.
- any other information that Customer shall legally or reasonably require in order to discharge its responsibilities under applicable Data Protection Laws in relation to such breach

3.6. Access, Intervention, Transfer and Separation Control

3.6.1. FuelTrust's architecture maintains logical separation of Customer Personal Data. Internal rules and measures separate data processing, such as reading, inserting, copying, amending, making available, deleting, and transferring Customer Personal Data, according to the contracted purposes. Access to Customer Personal Data is allowed only by authorized personnel in accordance with principles of segregation of duties, strictly controlled under identity and access management policies, and monitored in accordance with FuelTrust's internal privileged user monitoring and auditing program.

3.6.2. FuelTrust's privileged access authorization is individual, role-based, and subject to regular validation. Access to Customer Personal Data is restricted to the level required to deliver Services and support to Customer (i.e., least required privilege).

3.6.3. Transfer of Customer Personal Data within FuelTrust's network takes place on wired infrastructure and behind firewalls, without the use of wireless networking.

3.6.4. Upon expiration or cancellation of the Services, Customer Personal Data is rendered unrecoverable in conformity with NIST guidelines for media sanitization, or earlier upon Customer's request.

3.7. Service Integrity and Availability Controls

3.7.1. FuelTrust undergoes static and dynamic testing and vulnerability scanning prior to major production releases. Additionally, penetration testing, vulnerability scanning, is performed regularly by FuelTrust and authorized independent third parties. Modifications to operating system resources and application software are governed by FuelTrust change management policies.

3.7.2. FuelTrust maintains working network firewalls to protect data accessible via the internet and will keep all Customer Personal Data protected by the firewall at all times. Changes to network devices and firewall rules are also governed by the change management policies and are separately assessed for security risk prior to implementation.

3.7.3. FuelTrust's data center services within AWS support a variety of information delivery protocols for transmission of data over public networks, such as HTTPS, HSTS, SSH, and SSL. FuelTrust systematically monitors production data center resources 24×7. Internal and external vulnerability scanning is regularly conducted by authorized administrators to help detect and resolve potential exposures.

3.7.4. FuelTrust has business continuity and disaster recovery plans, which are developed, maintained, verified, and tested in compliance with the ISO 27001 Information Security Controls. Recovery point and time objectives for the Services are established according to their architecture and intended use. Backup data intended for off-site storage, if any, is encrypted prior to transport.

3.7.5. Security configuration and patch management activities are performed and reviewed regularly. FuelTrust's infrastructure is subject to emergency planning concepts, such as disaster recovery and multiple AWS servers available in regions throughout the country. Business continuity plans for FuelTrust' infrastructure are documented and regularly revalidated.

3.7.6. FuelTrust implements anti-virus software and scanning technologies, and regularly updated signature files, to ensure that all operating systems, software and other systems hosting, storing, processing, or that have access to Customer Personal Data and are known to be susceptible or vulnerable to being infected by or further propagating viruses, spyware and malicious code, are and remain free from such viruses, spyware and malicious code. FuelTrust will mitigate threats from all viruses, spyware, and other malicious code that should reasonably be detected.

3.8. **Activity Logging, Input Control.** FuelTrust policy requires administrative access and activity in the computing environments to be logged and monitored, and the logs to be archived and retained in compliance with FuelTrust' records management plan. Changes made to production are recorded and managed in compliance with FuelTrust change management policy.

3.9. Physical Security, Entry Control

3.9.1. FuelTrust requires its infrastructure providers to maintain physical security standards designed to restrict unauthorized physical access to offices. FuelTrust uses AWS and their data centers are limited controlled access and monitored by surveillance cameras. Access is allowed only by authorized personnel. See:

- *https://aws.amazon.com/compliance/iso-27001-faqs/* and
- *https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf*

3.9.2. Upon termination of employment, employees are removed from the access list and required to surrender their access credentials. Use of security tokens and fobs are logged.

3.10. **Compliance**. FuelTrust information security standards and management practices are aligned to the ISO/IEC 27001 standard for information security

management. Assessments and audits are conducted regularly by FuelTrust to track compliance with its information security standards. Additionally, independent third-party industry standard audits are performed annually on all FuelTrust production systems maintained in AWS data centers.

3.11. **Encryption**

3.11.1. FuelTrust maintains the following encryption standards:

- Accepted Encryption Algorithms for stored data;
- Public key encryption must use a 2048-bit (or larger) RSA public key;
- Symmetric encryption must use AES 256 bit, CBC mode;
- API servers must use TLS 1.2 SSL with SHA-256 and 2048-bit public keys;
- The SHA-2 family of hashes. PBKDF2 (SHA1 + HMAC), key derivation functions;
- random number generators

3.12. Customer confirms that the above measures provide an adequate level of protection for the Customer Personal Data.

4. **Data Sharing**

4.1. To the extent permitted by law, FuelTrust will inform Customer without delay of any Data Subject's requests for rectification, deletion, blocking of data, and enforcement of privacy rights in accordance with applicable law, complaints from Data Subjects, or objections from competent regulators. If Customer is obliged to provide information regarding Customer Personal Data to third parties (including Data Subjects or competent regulators), FuelTrust will provide reasonable support to Customer to the extent necessary, provided that (a) Customer has submitted its request for assistance to FuelTrust in writing; and (b) Customer agrees to pay the cost of any support (including internal resources) provided by FuelTrust or its Subprocessors) based on the rates set out in FuelTrust's price list for consulting services in excess of four hours per year.

4.2. FuelTrust will not disclose Customer Personal Data to any unauthorized third-party subject to mandatory law. If a government demands access to Customer Personal Data, FuelTrust will notify Customer in writing prior to disclosure unless prohibited by law.

4.3. FuelTrust shall require that all individuals employed or contracted by FuelTrust that process Customer Personal Data, or are subject to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality. FuelTrust shall further ensure that any of its subprocessors (as defined by the GDPR) shall have the same or substantially similar obligations to the same.

5. **Personal Data Breach.** Upon determining that a Personal Data Breach has occurred that affects Customer, FuelTrust will notify Customer promptly, but not more than 48 hours, after becoming aware of a breach of security in respect of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored, or otherwise processed by FuelTrust. FuelTrust will thereafter promptly (a) provide Customer with all such information as Customer reasonably requests in connection with a Personal Data Breach; (b) take commercially reasonable steps Customer requires it to take to mitigate the detrimental effects of any such Personal Data Breach on any of the data subjects and/or on Customer and provide evidence of such mitigation to Customer; and (c) otherwise cooperate with Customer in investigating and dealing with such Personal Data Breach and its consequences.

6. **Subprocessors.** FuelTrust may engage the Subprocessors listed in the applicable Data Processing Exhibit ("DPE") for the Services, and any other such Subprocessors as FuelTrust considers reasonably appropriate for the Processing of Customer Personal Data in accordance with this DPA, provided that FuelTrust shall notify Customer of the addition or replacement of such Subprocessor and Customer may, on reasonable grounds, object to a Subprocessor by notifying FuelTrust in writing within 10 days of receipt of FuelTrust's notification, giving reasons for Customer's objection. Upon receiving such objection, FuelTrust shall: (a) work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and (b) where such change cannot be made within 10 days of FuelTrust's receipt of Customer's notice, Customer may by written notice to FuelTrust with immediate effect terminate the portion of the Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor. This termination right is Customer's sole and exclusive remedy to Customer's objection of any Subprocessor appointed by FuelTrust. FuelTrust shall require all Subprocessors to enter into an agreement with equivalent effect to the Processing terms contained in this DPA. FuelTrust shall be solely responsible for complying with Data Protection laws in terms of its on-going sub-contracting.

7. **Audit**

7.1. FuelTrust and its Subprocessors have obtained the standard security certifications and personal data seals and marks listed at the following Web pages for FuelTrust Services:

- https://aws.amazon.com/compliance/iso-27001-faqs/
- https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf
- https://fueltrust.io/trustcenter/CCMReport/

7.2. Upon Customer's written request, FuelTrust will provide Customer with the most recent certifications or summary audit reports concerning the security measures for the FuelTrust computing environment used to provide the Services. FuelTrust will reasonably cooperate with Customer by providing available additional information to help Customer better understand such security measures. To the extent it is not possible to otherwise satisfy an audit obligation mandated by applicable law, only the legally mandated entity (such as a governmental regulatory agency having oversight of Customer's operations) or legally mandated functions within such entity (such as the internal controls function) may conduct an onsite visit of the facilities used to provide the Services, and only in a manner that causes minimal disruption to FuelTrust' business. Unless mandated by law, no audits are allowed within an AWS data center for security and compliance reasons.

7.3. Audits may only occur during normal business hours, and only after reasonable notice to FuelTrust (not less than 20 days' advance written notice). Audits will be conducted in a manner that does not have any adverse impact on FuelTrust's normal business operations. Customer shall comply with FuelTrust's standard safety, confidentiality, and security procedures in conducting any such audits. Any records, data, or information accessed by Customer in the performance of any such audit will be deemed to be the Confidential Information of FuelTrust. If an audit is requested, Customer agrees to pay the costs of any support provided by FuelTrust (including internal resources) based on a mutually agreed to Order Document.

7.4. The FuelTrust obligations stated in this Section 7 (and, as applicable, in Clause 12 paragraph 2 of the Standard Contractual Clauses) shall be replaced and superseded in their entirety by the FuelTrust or its Subprocessors obtaining a personal data protection seal or mark, or by the adherence to a certification mechanism or a code of conduct, considered by the European Data Protection Board or the Supervisory Authorities as an element to demonstrate sufficient guarantees of appropriate safeguards.

8. **FuelTrust Privacy Contact.** The FuelTrust privacy contact can be contacted via email at privacy@fueltrust.io.
9. **Return or Deletion of Customer Personal Data.** Unless otherwise required by applicable law, or where FuelTrust does not have the technical permissions to perform such, FuelTrust will render Customer Personal Data unreadable and unrecoverable within a 90 (ninety) day period following the termination or expiration of the Agreement. Upon a mutually agreed to Order, FuelTrust will return Customer Data in a reasonable and common format upon receiving written instructions from the Customer prior to termination or expiration, provided that the Customer Personal Data is available to FuelTrust. Subject to the terms of the Master SaaS Agreement by and between the Parties, FuelTrust will acquire no rights or interest in or to the Customer Personal Data. In the event that any applicable law does not permit FuelTrust to comply with the return or deletion of the Customer Personal Data, FuelTrust warrants that it will ensure the confidentiality of the Customer Personal Data and that it will not use or disclose any Customer Personal Data at or after the termination or expiration of the DPA.
10. **Transborder Data Processing.** If Personal Data originates from the EEA, U.K., or Switzerland, and is transferred by Customer to FuelTrust for Processing in a country not subject to an adequacy decision in accordance with the GDPR ("**Data Transfer**"), the parties will conduct such Data Transfer in accordance all applicable laws. The parties hereby agree to the Standard Contractual Clauses (which will be deemed executed by the parties as of the effective date of this DPA), and the following terms will apply: (a) Customer will be referred to as the "Data Exporter" and FuelTrust will be referred to as the "Data Importer" in such clauses with relevant company name and address details from the Agreement being used accordingly; (b) details in Annex A to this DPA will be used to complete Appendix 1 of those clauses; (c) details in Section 3 (Security) of this DPA will be used to complete Appendix 2 of those clauses; and (d) if there is any conflict between this DPA or the Agreement and the Standard Contract Clauses, the Standard Contract Clauses will prevail. Fuel Trust will properly execute Standard Contractual Clauses with FuelTrust's authorized Subprocessor or any of FuelTrust's affiliated entities, if legally necessary, prior to any Data Transfer or making available any Customer Personal Data to FuelTrust's authorized Subprocessor or another of FuelTrust's affiliated entities.

11. Nothing in this DPA relieves either party of its own direct responsibilities and liabilities under applicable Data Protection laws.

-the rest of this page is intentionally blank-

ANNEX A: Details of the Processing

Description of the Controller:
Customer and/or its respective Clients shall be the Controller of certain Personal Data provided to FuelTrust to provide the Services.

Nature of Services provided by FuelTrust:
FuelTrust provides cloud applications, including an API integration and analysis platform that enables Customer to process and receive business trade information, trade analytics, verification and validation of information, and the data collaboration of trade information with Customer's Clients and trade counterparties. FuelTrust also provides cloud-based services for Customer to integrate their data and applications with the ecosystem of cloud applications used by their customers and partners, in a normalized fashion.

Type(s) of Personal Data processed, for example but not exhaustively:
Identification and contact data (name, title, address, phone number, email address); usage information, location information, IP addresses, professional certification information.

Special categories of data (if applicable), for example but not exhaustively:
Not Applicable

Categories of Individuals:

- Customer's Clients' end-users authorized to use the Services
- Customer's employees and contractors (who are natural persons)
- Prospects, customers, business partners and vendors of Customer's Clients (who are natural persons).
- Employees, clients or contact persons of Customer's prospects, customers, business partners and vendors.

Nature of Processing Operations:
The Personal Data processed by FuelTrust or its Subprocessors will be subject to the processing activities described in the Agreement, SOWs, or purchase orders for the Services subject to this DPA. Personal Data may be Processed only to comply with Customer's instructions issued in accordance with this DPA.

Subprocessor List:
Amazon Web Services – infrastructure services
IBM Cloud Platform – AI Platform services, encryption key authority and issuance services
BlockApps – Blockchain cloud management services
Hubspot – customer support and communications