Data Protection Addendum

This data protection addendum (Addendum) is intended to supplement the underlying agreement between the Client and JTC (Agreement) under the terms of which JTC agrees to provide certain services to the Client (Services).

1. Definitions And Interpretation

In this Addendum, "Data Protection Legislation" means all applicable laws and regulations relating to the processing of personal data by the Client and/or JTC including, but not limited to, (i) the General Data Protection Regulation 2016/679 (GDPR), and any statutory instrument, order, rule or regulation made thereunder or national implementing laws, regulators or equivalent provisions, as from time to time amended, extended, re-enacted or consolidated, and (ii) the Personal Data Protection Act 2012 of Singapore (PDPA), including all amendments thereto and subsidiary legislation enacted thereunder, whether now or in the future. References to a provision of the GDPR shall be interpreted to mean the relevant provision of the equivalent Data Protection Legislation that applies to the Party.

The terms "controller", "processor", "data subject", "personal data breach", "process", "personal data" and "supervisory authority" shall have the meanings given to those terms or equivalent terms in the applicable Data Protection Legislation.

Unless defined otherwise in this Addendum or the Agreement, any defined terms shall have the same meaning as in the Agreement.

References in this Addendum to the "Client" shall mean any corporate body (wherever incorporated), foundation, individual, partnership (of whatever kind as permitted by the applicable law) or other association or body (whether or not incorporated) or trust or fund or other structure or arrangement to or in respect of which JTC provides Services and "JTC" shall mean the JTC entity or entities providing the Services under the Agreement, unless otherwise set out in the Agreement. JTC and the Client shall each be a "Party" and together shall be the "Parties".

2. General Obligations

2.1 The Parties acknowledge and agree that JTC, in performing the Services for the purposes described in the Agreement, will receive personal data from the Client (either directly or indirectly) and the Parties may share personal data in the course of providing the Services.

2.2 The Client and JTC shall at all times comply with the Data Protection Legislation in so far as it relates to the Services and to each Party, and in particular the Client and JTC each:

a) accept their separate responsibilities for ensuring that they comply with the Data Protection Legislation; and

b) agree to comply with any requirements which the other Party reasonably requires it to put in place in respect of the provision of the Services in order to ensure that the other Party's respective obligations under clause 2.2a above are discharged.

2.3 The Client shall ensure that the personal data supplied by it (or on its behalf) to JTC in relation to the Services will be:

a) obtained lawfully and in accordance with the Data Protection Legislation (to the extent that it applies to the Client) and that it has all necessary consents, approvals, notices and registrations in place to enable the lawful transfer of the personal data to JTC;

b) adequate, relevant and not excessive in relation to the purpose for which it is shared with JTC;

c) accurate at all relevant times (and the Client specifically agrees to keep the personal data up-to-date at all times during which JTC processes that personal data

and shall provide JTC with any revisions and updates to the relevant personal data); and

d) transferred between the Parties by a secure means.

2.4 Each Party shall not, by its acts or omissions, cause the other Party to breach its respective obligations under the Data Protection Legislation.

2.5 In the event that the Client instructs JTC to share personal data with a third party (other than a sub-processor appointed by JTC in accordance with clause 4.4 below), such as a banking services provider, regulator, clearing house or intermediary, the Client shall be responsible for ensuring such third party is an appropriate recipient of the personal data and JTC shall not be liable for any loss that may result from complying with such instruction in the event that the third party fails to comply with its obligations under the Data Protection Legislation. This shall include both: (i) the sharing of personal data held by JTC for the purpose of complying with KYC obligations (in accordance with clause 3.1a below) with a third party pursuant to a 'reliance' arrangement under anti-money laundering obligations and, (ii) requesting a Service from JTC that would, by its nature, require JTC to share personal data with a third party such as an intermediary, regulatory body or agency.

3. JTC as Controller

3.1 The Parties acknowledge that JTC processes personal data received from the Client in the capacity of sole controller and not as a processor nor as joint controller with the Client in the following circumstances:

a) where JTC is required to process the personal data for its own purposes in order to comply with a legal obligation that applies to it (for example, in order to meet JTC's own regulatory obligations by virtue of applicable "know your customer" (KYC) or anti-money laundering (AML) regulations);

b) where JTC provides Services which require it to act autonomously in relation to the personal data it receives from the Client and therefore determine the means and purposes of the processing (including but not limited to trustee Services, Money-Laundering Reporting Officer Services and where JTC acts as an Alternative Investment Fund Manager); and

c) where JTC processes the personal data of Client personnel in order to manage JTC's relationship or for marketing and business development purposes (subject always to having obtained any necessary consents).

3.2 A privacy notice setting out how JTC will store, transfer, or otherwise process such personal data (Privacy Notice) is available online at the JTC Group Privacy Notice - JTC. The Client agrees to ensure that the information contained in the Privacy Notice is made readily available to any data subjects whose personal data is provided to JTC in connection with the Services.

3.3 Where consent to processing personal data is required under the applicable Data Protection Legislation or where processing or disclosing personal data for the purposes set out in the Privacy Notice are not considered a lawful basis under applicable Data Protection Legislation, the Client consents to any personal data provided to JTC for the purposes of the Agreement, being processed in accordance with the Privacy Notice. In the event that this includes the personal data of data subjects who are not party to the Agreement, the Client shall ensure that it has obtained the consent of such data subjects to the processing by JTC.

3.4 Each Party shall comply with their own obligations under the Data Protection Legislation in relation to the personal data for which they are controller including in responding to requests by a data subject to exercise their rights under the Data Protection Legislation and notifying personal data breaches. The Parties each agree to provide such assistance as is reasonably required to enable the other Party to comply with its

respective obligations under the Data Protection Legislation.

4. JTC as Processor

4.1 In the course of providing the Services to the Client (other than those set out in clause 3.1 above), JTC shall process personal data on behalf of the Client. The Parties acknowledge that JTC shall be acting as a processor in relation to such personal data.

4.2 The details of the processing operations for the applicable Services, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Client, are specified in Annex 1 to this Addendum unless otherwise specified in the Agreement or in writing with the Client.

4.3 In relation to the personal data that JTC processes on the Client's behalf, JTC shall:

a) process personal data only on documented instructions from the Client (which may be given by the Client throughout the duration of the processing of personal data and may be via email or verbally so long as such verbal instructions are recorded or subsequently documented in writing) unless otherwise required to do so by a law to which JTC is subject. In such circumstances, JTC shall inform the Client of that legal requirement before processing, unless the applicable law prohibits this. The Client acknowledges that JTC, as a regulated entity, is subject to local legislation and regulations that may require it to process personal data contrary to the instructions of the Client in limited circumstances such as sharing personal data with a Regulatory Body;

b) promptly inform the Client if, in JTC's opinion, instructions given by the Client infringe the Data Protection Legislation;

c) process the personal data only for the purpose of providing the Services and for the duration of the Agreement (subject to any applicable legal obligation to retain the personal data for longer) unless it receives further instructions from the Client;

d) implement the technical and organisational measures specified in Annex 2 to this Addendum to ensure the security of the personal data. This includes protecting the personal data against a personal data breach. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects;

e) grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for the Services and ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

f) apply specific restrictions and/or additional safeguards in the event that processing involves special category data (being such information designated as such under the Data Protection Legislation);

g) deal promptly and adequately with inquiries from the Client about its processing of personal data and make available all information reasonably necessary to demonstrate compliance with the obligations that are set out in this Addendum and stem directly from the Data Protection Legislation.

h) At the Client's request and cost, permit and contribute to audits at reasonable intervals (being no more than once every 12 months) and on reasonable notice or if there are indications of non-compliance. In deciding on a review or an audit, the Client shall take into account relevant certifications held by JTC. Where necessary, audits may also include inspections at the premises or physical facilities of JTC provided that they shall be carried out with reasonable notice and during normal office hours;

i) make the information referred to in clause 4.3g, including the results of any audits, available to the competent supervisory authority/ies on request;

j) promptly notify the Client of any request it has received from a data subject to exercise a right under the Data Protection Legislation. JTC shall not respond to the request and shall not be required to action the request or communicate with the data subject in relation to their request other than to inform them that JTC is not the controller of their personal data;

k) assist the Client, at the Client's cost, in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing that JTC undertakes. This shall be achieved by JTC responding to the Client's reasonable requests to provide copies of such personal data as is held by JTC on behalf of the Client or to editing or erasing such personal data that JTC holds on the Client's behalf provided that the Client does not have independent access to the relevant databases/storage in order to be able to obtain such copies/makes such changes themselves. In relation to objections to processing activities or requests to restrict the processing activities of JTC, JTC shall comply with the Client's reasonable instructions and shall not be liable for any loss that may arise in the event that such compliance results in a reduction in or inability to perform the Services; and

l) assist the Client, at the Client's cost, in ensuring compliance with the following obligations under the relevant Data Protection Legislation (where required under such Data Protection Legislation), taking into account the nature of the data processing by JTC and the information available to JTC:

m) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

n) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

o) the obligation to ensure that personal data is accurate and up to date, by informing the Client without delay if JTC becomes aware that the personal data it is processing is inaccurate or has become outdated; and

p) the security obligations in the Data Protection Legislation by implementing the technical and organisational measures set out in Annex 2 to this Addendum.

4.4 JTC has the Client's general authorisation for the engagement of the authorised sub-processors set out at www.jtcgroup.com/sub-processors/, from time to time, provided that such sub-processors have been validly appointed in accordance with clause 4.6. JTC shall inform the Client of any material changes to the sub-processors relevant to the Services at least ten (10) days in advance.

4.5 In the event that the Client reasonably objects to a change to a sub-processor on data protection grounds, JTC shall provide the Client with a written description of commercially reasonable alternative(s), if any, to such change, including without limitation, modification to the Services. If JTC, in its sole discretion, cannot provide any such alternative(s), or if the Client does not agree to any such alternative(s) if provided, JTC may terminate the Agreement. Termination shall not relieve the Client of any fees owed to JTC under the Agreement. If the Client does not object to the change to a sub-processor within ten (10) days of notice provided by JTC, the sub-processor shall be deemed authorised.

4.6 Where JTC engages a sub-processor for carrying out specific processing activities (on behalf of the Client), it shall do so by way of a

contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on JTC in accordance with this Addendum. JTC shall remain fully responsible to the Client for the performance of the sub-processor's obligations in accordance with its contract with JTC.

4.7 Any transfer of personal data to a third country or an international organisation by JTC shall be carried out only for the purpose of providing the Services under the Agreement or in order to fulfil a specific requirement under law to which JTC is subject and shall take place in compliance with the international transfer requirements of the Data Protection Legislation.

4.8 In the event of a personal data breach concerning data processed by JTC on behalf of the Client, JTC shall notify the Client without undue delay after having become aware of the breach and shall cooperate with the Client and assist the Client in complying with its own obligations under the Data Protection Legislation, taking into account the nature of processing and the information available to JTC.

4.9 Following termination of the Agreement, JTC shall, at the choice of the Client, delete all personal data processed on behalf of the Client or return such personal data to the Client and delete existing copies unless an applicable law requires storage of the personal data. Notwithstanding the foregoing, the Client acknowledges that JTC, as a regulated entity, is subject to local legislation and regulations that may require it to retain personal data for a period beyond the termination of the Agreement. Until such personal data is deleted or returned to the client, JTC shall continue to hold it under the terms of this Addendum. In the absence of an instruction from the Client within 15 working days of termination of the Agreement, JTC may delete all personal data processed on behalf of the Client that is not required to be retained under an applicable law.

4.10 JTC is prohibited from Selling (as such term is defined in the California Consumer Privacy Act ("CCPA")) the personal data processed on the Client's behalf or retaining, using, or disclosing such personal data for any purposes other than the specific purposes of performing the Services. JTC hereby certifies that it has understood the restrictions set out in this clause and the CCPA in relation to Service Providers (as defined in the CCPA) and will comply with them.

5. JTC as Joint Controller

5.1 For the purposes of processing personal data in connection with the Services, the Parties may, in limited circumstances, act as joint controllers for the purposes of the Data Protection Legislation. Each Party shall notify the other Party in the event that they believe the Parties are acting as joint controllers.

5.2 Where the Parties act as joint controllers, they shall, unless otherwise agreed:

a) cooperate to ensure that their obligations as joint controllers under the Data Protection Legislation are complied with;
b) consult with each other about any notices given to data subjects in relation to the Personal Data and each be responsible for providing their own notice to data subjects;
c) promptly inform each other about the receipt of any data subject access request and, prior to responding to the request, cooperate to identify the most appropriate course of action for addressing such request;
d) provide each other with reasonable assistance in complying with any data subject access request;
e) assist each other, at the cost of the assisted Party, in ensuring compliance with their respective obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

f) notify each other without undue delay on becoming aware of any personal data breach that may impact the other Party. Unless otherwise agreed, the Party responsible for the personal data breach shall be required to comply with any relevant notification obligations in relation to such breach but shall, at all times, consult with the other Party prior to making such notifications or any public communications regarding the breach;

g) maintain complete and accurate records and information to demonstrate compliance with this clause and allow (at reasonable intervals and upon reasonable notice) for audits by the other Party or the other Party's designated auditor; and

h) provide each other with contact details of at least one employee as a point of contact and responsible manager for all issues arising out of the Data Protection Legislation. For JTC, this person shall be the Data Privacy Governance Officer (gdpr@jtcgroup.com) unless otherwise notified in writing.

6. International Transfers

6.1 In the event that the Services require the Parties to transfer personal data to each other in a manner that is restricted under Chapter V of the GDPR (or the equivalent international transfer provisions of the Data Protection Legislation) and no derogation or other transfer mechanism would apply to such a transfer, the Parties hereby agree to incorporate either of the following into the Agreement (as applicable):

a) the standard contractual clauses in the form adopted by the European Commission on 4 June 2021 under Implementing Decision 914/2021/EU, as from time to time amended, extended, re-enacted or consolidated ("EU SCCs") (together with any applicable addendum and/or consequential modifications to the EU SCCs as required by local Data Protection Legislation where relevant); or

b) the equivalent standard contractual clauses adopted by the applicable local Data Protection Legislation (such as the UK International Data Transfer Agreement or the Dubai International Financial Centre Standard Data Protection Contractual Clauses), as amended, extended, re-enacted or consolidated from time to time.

6.2 Where the EU SCCs apply, they shall be deemed completed as follows:

a) Module One – Controller-to-Controller terms apply where the Client is acting as a controller and data exporter (as defined in the EU SCCs) and JTC is acting as a controller and data importer.

b) Module Two – Controller-to-Processor terms apply where the Client is acting as controller and data exporter and JTC is acting as a processor and data importer.

c) Module Three – Processor-to-Processor terms apply for where the Client is acting as a processor and data exporter and JTC is acting as a sub-processor and data importer.

d) Module Four – Processor-to-Controller terms apply where the JTC is acting as a processor and data exporter and the Client is acting as a controller and data importer.

e) in Clause 7, the optional docking clause applies.

f) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with the Sub-Processor section of this Agreement.

g) in Clause 11, the optional language is deleted.

h) in Clause 17 and 18, the Parties agree that the governing law and forum for disputes for the EU Standard Contractual Clauses is as set out in the governing law clause of the Agreement.

i) The Annexes of the EU SCCs (or equivalent) will be deemed completed with the information set out in the Annexes to this Addendum and www.jtcgroup.com/sub-processors/ unless otherwise set out in the Agreement. The identity and contact details of the Client and JTC for the purposes of the EU SCCs are set out in the Agreement.

j) for the purposes of Annex I.C, the competent Supervisory Authority shall be the Luxembourg National Data Protection Commission (Commission Nationale pour la Protection des Données).

7. General Terms

7.1 In the event of a conflict between this Addendum regarding data protection matters and the provisions of the Agreement, this Addendum shall prevail.

7.2 JTC shall be entitled to terminate the Agreement insofar as it concerns processing of personal data under this Addendum where, after having informed the Client that its instructions infringe applicable legal requirements in accordance with clause 4.3b, the Client insists on compliance with the instructions.

7.3 Signature of the Agreement shall be automatically deemed to include signature of this Addendum and the EU SCCs (where applicable in accordance with clause 6.1).

7.4 Annexures 1 and 2 are an integral part of this Addendum.

7.5 JTC may, from time to time amend, substitute, delete or add to this Addendum without reference to the Client although JTC will endeavour to give reasonable notice to the Client, using commercially reasonable methods, of any material changes. The Client's continued use of the Services provided by JTC after such notice had been given and such amendments had come into effect shall constitute the Client's agreement to be bound by such amended Addendum.

Annex One

Details Of Data Processing

1. The subject matter, nature, scope, context and purpose of the processing of personal data:

To provide the Services as set out in the Agreement.

2. Duration of processing

The processing shall continue until the later of:

a) the Agreement being terminated in accordance with its terms and any notice period or transition period prescribed by the Agreement having expired; or

b) JTC no longer being subject to an applicable legal or regulatory requirement to continue to store the personal data.

3. The types / categories of personal data to be processed

The Services may involve JTC processing and retaining the following types of personal data to the extent necessary to provide the Services as well as such other personal data as may be required in order to provide the Services:

a) name;
b) contact details;
c) personal characteristics;
d) employment information;
e) official identification information;
f) customer due diligence information;
g) financial details;
h) statutory company records data;
i) transactional details; or
j) authentication data.

4. Categories of Data Subject

The categories of Data Subjects shall be those Data Subjects whose Personal Data is required to be processed by JTC in order to provide the requested Services. This may include the following where applicable:

a) the Client's employees (including, for the avoidance of doubt, current, former and future employees);

b) the Client's directors, shareholders and ultimate beneficial owners;

c) unitholders, pension plan or share scheme members or beneficiaries (e.g. in relation to administration services provided by JTC Employer Solutions);

d) investors in the Client's funds/investment vehicles or directors, shareholders and ultimate

beneficial owners of such investors (e.g. in relation to fund administration services);

e) key staff or people behind a target entity (e.g. in relation to operational due diligence);

f) suppliers, service providers or sellers of assets (where JTC is required to undertake due diligence on the Client's behalf as part of the Services).

5. The sensitive data processed / transferred and the applied safeguards:

The Services may involve JTC processing limited sensitive data where it is necessary for the Services. This may be in the form of criminal offence data and political opinions (for example, in relation to suspicious activity reports or customer due diligence checks). Health related data may also be processed in limited circumstance (for example, where pension fund distributions are linked to ill-health) and race and ethnicity data in the form of nationality and citizenship information.

6. The processing activities / operations relevant to the data transfer under the EU SCCs (where applicable) shall be:

Carrying out any operation or set of operations on the personal data, as necessary for the Services including:

a) organising, adapting or altering the information or data;

b) retrieving, consulting or using the information or data;

c) disclosing the information or data by transmission, dissemination or otherwise making it available; or

d) aligning, combining, blocking, erasing or destroying the information or data.

7. For processing by / transfers to (sub-) processors, the following specify subject matter, nature and duration of the processing shall apply:

As above at paragraphs 1 and 2 of this Annex 1 to the extent such information is provided to sub-processors for the purposes of providing the Services and as further detailed in the agreement with the sub-processor.

Annex Two

Technical And Organisational Measures

JTC is aligned to the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and International Organisation of Standardisation (ISO27001). JTC shall implement the following types of security measures and shall update those measures in accordance with industry best practice.

1. Physical access control

Measures in place to prevent unauthorised physical access to premises and facilities holding personal data such as locked doors, alarm system; video surveillance. Logging of facility exits/entries.

2. Systems Access Control

Measures in place to prevent unauthorised access to IT systems including:

a) central management of system access;

b) password procedures (including minimum length and complexity, lock out, history, and forced change of password);

c) ISO27001 certified tier III data centres, firewall controls monitoring inbound and outbound traffic against a pre-established set of permissible traffic flows;

d) intrusion detection;

e) prevention and response capabilities monitoring network traffic for malicious patterns and traffic anomalies; and

f) ability to detect and respond to direct and distributed denial of service attacks through network routing and DNS controls, incident response frameworks, standards and plans in place, external facing network penetration tests, testing against known vulnerabilities and exploits.

3. Data Access Control

Measures in place to prevent authorised users from accessing data beyond their authorised access rights and prevent the unauthorised input, reading,

copying, removal, modification or disclosure of data including:

a) access rights granted on a 'need to know' and 'least privileged' basis;
b) automated log of user access via IT systems;
c) measures to prevent the use of automated data-processing systems by unauthorised persons using data communication equipment;
d) remote access to internal corporate networks and consoles requiring multi-factor authentication through a secure remote access solution; and
e) data loss prevention software monitoring for the movement of data through our perimeter.

4. Disclosure Control

Measures in place to prevent the unauthorised access, alteration, or removal of data during transfer, and to ensure that all transfers are secure and are logged including:

a) secure network connections;
b) corporate devices such as laptops are full-disk encrypted to protect against data incidents through theft or loss;
c) prohibition of removable media;
d) data transfer audit trails and logging.

5. Awareness, Education and Training

JTC staff shall receive security training including:

a) mandatory security induction training for all new employees;
b) periodic and regular ethical phishing campaigns;
c) mandatory annual training for all existing employees; and
d) annual Employee Declaration (AED) attestation for all employees.

6. Availability Control

Measures in place to ensure that data is protected against accidental destruction or loss including:

a) ensuring that installed systems may, in the case of interruption, be restored;
b) ensuring systems are functioning, and that faults are reported;
c) ensuring stored personal data cannot be corrupted by means of a malfunctioning of the system; uninterruptible power supply (UPS);
d) Business Continuity procedures;
e) Remote data storage; and
f) Anti-virus/firewall systems.

7. Segregation Control

Measures in place to allow data collected for different purposes to be processed separately including:

a) restriction of access to data stored for different purposes according to staff duties;
b) where possible and required segregation of business IT systems;
c) Segregation of production, testing and disaster recovery environments.

8. Audit

Measures in place to ensure proper functioning of controls including:

a) audits in multiple global locations across JTC jurisdictions;
b) audits throughout the year by external clients as part of their own internal risk management processes;
c) audits through internal risk management processes by internal audit teams for application security, vulnerability assessments, and network security.