PERSONAL DATA PROCESSING ANNEX

1. Defined Terms. As used in this Annex, the terms below (and their plural forms) have the following meanings:

1.1. "**Client Portal**" means a self-service portal made available to Client's designated representatives at Client's request at https://my.fisglobal.com/vendor-management offering specific Client resources to help better manage its relationship with FIS, including information about FIS' information security practices;

1.2. "**Data Protection Laws**" means, collectively: (i) the GDPR; and (ii) any legislation, and/or regulation implementing or made pursuant to them or which amends, replaces, re-enacts or consolidates any of them, and all other applicable laws relating to Processing of personal data and privacy that may exist in any relevant jurisdiction;

1.3. "**Data Subject Request**" means the exercise by a Data Subject of their rights under, and in accordance with, the GDPR in respect of Personal Data;

1.4. "**EEA**" means the European Economic Area;

1.5. "**EEA SCCs**" means the standard contractual clauses approved by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as set out in full at https://www.fisglobal.com/en/solutions-legal/fis-information-security;

1.6. "**GDPR**" means, as appropriate and as amended from time to time: (i) the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**");

1.7. "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Personal Data to any person to: (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission pursuant to Article 45 of the GDPR; and (ii) in the context of the UK, any country or territory outside the UK which does not benefit from an adequacy decision;

1.8. "**Security Statement**" means the FIS Security Statement found at https://www.fisglobal.com/solutions/legal/fis-information-security;

1.9. "**Services**" means any services provided by FIS to Client pursuant to the Agreement, including but not limited to Professional Services, support and/or maintenance services and hosting services;

1.10. "**Standard Contractual Clauses**" or "**SCCs**" means the EEA SCCs or UK SCCs, as appropriate;

1.11. "**Subprocessors**" means the relevant sub-processors listed in the GDPR section of the Client Portal;

1.12. **"Supervisory Authority"** means: (i) in the context of the EU GDPR, any authority within the meaning of Article 4(21) of the EU GDPR; and (ii) in the context of the UK GDPR, the UK Information Commissioner's Office;

1.13. "**UK**" means the United Kingdom;

1.14. "**UK SCCs**" means the standard contractual clauses approved by the European Commission pursuant to Commission Implementing Decision (EU) 2010/87, as set out in full at https://www.fisglobal.com/en/solutions-legal/fis-information-security; and

1.15. the terms, "**Binding Corporate Rules**", "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Processor**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

2. Controller and Processor. In the course of FIS providing the Services under the Agreement, Client may from time-to-time provide or make available Personal Data to FIS. The parties acknowledge and agree that, in relation to any such Personal Data provided or made available to FIS for Processing by Client under the Agreement, Client will be the Controller and FIS will be a Processor for the purposes of the Data Protection Laws.

3. Subject Matter. The Agreement determines the subject-matter and duration of FIS' Processing of Personal Data, and the obligations and rights of Client in relation to such Processing. The type of Personal Data, categories of Data Subjects and nature of FIS' Processing of Personal Data are set out in the Personal Data Attachment forming part of the Agreement.

4. Precedence. Except as expressly otherwise agreed, the provisions of this Annex shall supersede any contradicting provisions in the Agreement in relation to the subject matter of this Annex.

5. Instructions. FIS shall Process Personal Data on behalf of Client and only in accordance with the instructions given by Client from time to time as documented in, and in accordance with, the terms of the Agreement, or as required by applicable laws, in which case FIS shall to the extent not prohibited by such laws inform Client of that legal requirement before the relevant Processing of that Personal Data. FIS shall promptly inform Client if, in its opinion, an instruction infringes against applicable laws.

6. **Lawful Processing.** Client shall ensure that it is entitled to give access to the relevant Personal Data to FIS so that FIS may lawfully Process Personal Data in accordance with the Agreement on Client's behalf, which may include FIS Processing the relevant Personal Data outside the country where Client and/or the Data Subjects are located in order for FIS to provide the Services and perform its other obligations under the Agreement. Client shall (a) comply with its obligations under the Data Protection Laws which arise in relation to this Annex, the Agreement and the receipt of the Services and (b) not do or omit to do anything which causes FIS (or any sub-processor) to breach any of its obligations under the Data Protection Laws.

7. **Restricted Transfers.**

7.1. To the extent required to ensure the legality of Restricted Transfers, the parties hereby agree to incorporate into this Annex by reference: (i) in the context of a Restricted Transfer originating in the EEA, the EEA SCCs; and (ii) in the context of a Restricted Transfer originating in the UK, the UK SCCs. In the event of any conflict or inconsistency between this Annex and the applicable SCCs, the terms of the applicable SCCs shall prevail.

7.2. Notwithstanding Section 7.1, to the extent FIS implements, at any time during the term of the Agreement, Binding Corporate Rules which may be relied on to legitimatise Restricted Transfers made in connection with the Agreement: (i) FIS shall notify Client of the same and provide to Client a copy of its Binding Corporate Rules; and (ii) from the date of such notification, all Restricted Transfers made in connection with the Agreement shall be subject to such Binding Corporate Rules, and the applicable SCCs shall cease to apply accordingly.

8. **FIS Personnel.** FIS shall ensure that all persons it authorizes to access Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9. **Personnel Compliance.** Each party shall take reasonable steps to ensure that any natural person acting under its authority who has access to Personal Data does not Process it except on instructions from it.

10. **Sub-processors.** Client hereby authorizes FIS to appoint the Subprocessors as additional Processors of Personal Data under the Agreement, provided that FIS shall: (i) impose upon such Processors data protection obligations that ensure at least the same level of data protection as set out herein; and (ii) be responsible for the acts and omissions of such Processors under the Agreement. FIS shall inform Client of any intended changes concerning the addition or replacement of other Processors not permitted hereunder, by making such information available to Client in the GDPR section of its Client Portal (and Client may subscribe to receive electronic notifications when such GDPR section changes). Client may object to such changes in writing setting out its reasonable concerns in detail within four (4) weeks from such notice. If Client does not respond to such changes, FIS shall have the right to continue to Process the Personal Data in accordance with the terms of this Annex, including using the relevant sub-processors. If Client objects, FIS shall consult with Client, consider Client's concerns in good faith and inform Client of any measures taken to address Client's concerns. If Client upholds its objection and/or demands significant accommodation measures which would result in a material increase in cost to provide the Services, FIS shall be entitled to increase the fees for the Services or, at its option, terminate the Agreement. Where necessary to legalize the use of any such other Processors, Client hereby authorizes FIS to conclude the SCCs in accordance with Section 7 with such Processors as agent on behalf of Client and (if required) Client's Affiliates. Each such conclusion of SCCs shall be considered a supplement to the Agreement and shall be subject to the terms and conditions set out therein.

11. **Technical and Organizational Measures.** FIS shall implement appropriate technical and organizational measures to protect Personal Data and ensure a level of security appropriate to the risk. FIS' measures comprise those documented in its Security Statement.

12. **Deletion.** Upon the date of termination or expiry of Services involving the Processing of Personal Data (the "**Cessation Date**"), FIS shall cease all Processing of Personal Data related to such Services except as set out in this Section. Client hereby acknowledges and agrees that, due to the nature of Personal Data Processed by FIS, return (as opposed to deletion) of Personal Data may require exceptional effort by FIS in some circumstances. Having regard to the foregoing, Client agrees that it is hereby deemed (at the Cessation Date) to have irrevocably selected deletion, in preference of return, of such Personal Data. As such, FIS shall delete all relevant Personal Data Processed on behalf of Client within 30 days of the Cessation Date, subject to FIS retaining any copies required by applicable laws (and in that case, for such period as may be required by such applicable laws).

13. **Assistance and Cooperation.** FIS shall, upon Client's reasonable written request, provide reasonable assistance to Client with its legal obligations under Data Protection Laws, including any data protection impact assessments and prior consultations with Supervisory Authorities which Client reasonably considers to be required of it by Data Protection Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing by, and information available to, FIS.

14. **Data Subject Requests.** FIS shall, upon Client's reasonable written request, provide Client with such assistance as may be reasonably necessary and technically possible in the circumstances to assist Client in fulfilling its obligation to respond to Data Subject Requests. Upon receipt of any Data Subject Request that relates to Personal Data that FIS Processes for Client, FIS shall promptly notify Client and not respond to such Data Subject Request except on the written instructions of Client. Client is solely responsible for responding to Data

Subject Requests. FIS' notification of or response to a Data Subject Request under this Section is not an acknowledgement by FIS of any fault or liability with respect to the Data Subject Requests.

15. Personal Data Breaches.

15.1. If FIS becomes aware of any actual Personal Data Breach affecting Personal Data that FIS Processes for Client, FIS shall: (i) notify Client of such Personal Data Breach without undue delay; and (ii) take reasonable steps to mitigate the effects of the Personal Data Breach. The notification shall at least:

15.1.1. describe the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

15.1.2. communicate the name and contact details of the data protection officer or other contact point at FIS where more information can be obtained;

15.1.3. describe the likely consequences of the Personal Data Breach; and

15.1.4. describe the measures taken or proposed to be taken by FIS to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

15.2. Client is solely responsible for complying with data breach notification laws applicable to Client and fulfilling any third-party notification obligations related to any Personal Data Breach. FIS' notification of, or response to, a Personal Data Breach under this Section is not an acknowledgement by FIS of any fault or liability with respect to the Personal Data Breach.

16. Demonstration of Compliance. FIS shall, upon Client's reasonable written request, make available to Client all information reasonably necessary to demonstrate FIS' compliance with the obligations set out in this Annex in relation to Personal Data that FIS Processes for Client.

17. Audits. FIS and Client will use current certifications or other existing audit reports to minimize repetitive audits. If Client (acting reasonably and in good faith) considers that the information provided in accordance with Section 16 is not sufficient to demonstrate FIS' compliance with the obligations set out in this Annex, or where otherwise required by Data Protection Laws, Client may (at its cost) perform on-site audits at the FIS processing facility (or facilities) that provides the Services to Client, subject to the following:

17.1. on-site audits may only be carried out once per calendar year, unless a Supervisory Authority having jurisdiction over Client expressly requires more frequent audits (in which case the request for audit shall detail the applicable requirements under which the Supervisory Authority requires the audit and/or information from Client, including details of the relevant regulation or regulatory obligation which necessitates such request);

17.2. requests for on-site audit visits shall be made in writing by Client at least sixty (60) days in advance (unless shorter notice is given by the Supervisory Authority or specifically required by the relevant regulatory obligation, in which case Client will give as much advance notice as is possible in the circumstances and provide the reasoning for the shorter notice) and shall specify the scope of the information sought and the specific purpose of the audit;

17.3. on-site audits will be limited to a review of FIS' compliance with this Annex;

17.4. on-site audits shall be conducted during normal business hours for the facility and shall be coordinated with FIS so as to cause minimal disruption to FIS' business operations;

17.5. on-site audits must be reasonable in scope and duration, shall not last more than two (2) business days;

17.6. on-site audits shall be performed by Client's employees and/or a reputable third-party auditor agreed to by both parties, it being understood that Client (and its representatives) shall at all times be bound by the confidentiality provisions of the Agreement and shall be accompanied by a representative of FIS;

17.7. FIS may require on-site audits to be conducted remotely, if necessary, for health and safety reasons;

17.8. except as prohibited by applicable laws or the relevant Supervisory Authority, FIS shall receive and be entitled to comment on any report prepared by or on behalf of Client prior to that report being published or disseminated (such report to be FIS Confidential Information except to the extent it relates to the business or affairs of Client, which information will be Client Confidential Information), which publication or dissemination shall be done only pursuant to the confidentiality provisions of the Agreement;

17.9. when performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated;

17.10. FIS does not allow any form of direct security testing initiated by Client or on behalf of Client, including but not limited to, vulnerability scanning, penetration testing, application code scanning, dynamic testing, installation of audit software, direct access to systems, or ethical hacking of FIS systems, applications, databases, or networks, except as may otherwise be agreed by FIS' Chief Information Security Officer and/or designee in writing and signed by both parties; and

17.11. FIS will not acknowledge any results from any form of security testing that is not performed by FIS. FIS will provide Client and any Supervisory Authority with access to a summary of its annual vulnerability

assessment findings in accordance with the Section 'Patch and Vulnerability Management' in the Security Statement.

18. Reimbursement. Client shall reimburse FIS for time spent and any costs reasonably incurred by FIS at rates agreed between Client and FIS (or if none have been agreed, at FIS' standard professional services rate) in performing its obligations under Sections 12 to 17, in each case except to the extent that such costs were incurred as a result of any breach by FIS of its obligations under this Annex.