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 "**Customer**" means a client or customer of Client.

1.3 "**Data Protection Laws**" means means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data under the Agreement and this DPA, including without limitation European Data Protection Laws; in each case as amended, repealed, consolidated or replaced from time to time;

1.4 "**Data Subject Request**" means the exercise by a Data Subject of their rights under, and in accordance with Data Protection Laws in respect of Personal Data;

1.5 "**EEA**" means the European Economic Area;

1.6 "**Europe**" means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.;

1.7 "**European Data Protection Laws**" means data protection laws applicable in Europe, including the EU GDPR, the UK GDPR and the FADP, in each case, as may be amended, superseded or replaced;

1.8 "**FADP**" means Swiss Federal Act on Data Protection;

1.9 "**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**");

1.10 "**Personnel**" means a person's employees, agents, consultants or contractors;

1.11 "**Relevant Body**":

1.11.1 in the context of the EU GDPR, means the European Commission;

1.11.2 in the context of the UK GDPR, means UK Government (Secretary of State); and/or

1.11.3 in the context of the Swiss FADP, means the Federal Data Protection and Information Commissioner ("**FDPIC**");

1.12 "**Restricted Country**":

1.12.1 in the context of the EEA, means a country or territory outside the EEA;

1.12.2 in the context of the UK, means a country or territory outside the UK; and

1.12.3 in the context of Switzerland, means a country or territory outside Switzerland,

that the Relevant Body has not deemed to provide an 'adequate' level of protection for Personal Data pursuant to a decision made in accordance with applicable European Data Protection Laws;

1.13 "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Personal Data to any person located in:

1.13.1 in the context of the EEA, a Restricted Country outside the EEA (an "**EEA Restricted Transfer**");

1.13.2 in the context of the UK, a Restricted Country outside the UK (a "**UK Restricted Transfer**"); and/or

1.13.3 in the context of Switzerland, a Restricted Country outside Switzerland (a "**Swiss Restricted Transfer**");

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

1.15 "**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;

1.16 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries as approved by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914) of 4 June 2021;

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

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

1.19 "**UK**" means the United Kingdom;

1.20 "**UK Transfer Addendum**" means the template Addendum B.1.0 issued by the UK Information Commissioner's Office (ICO) and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the Mandatory Clauses included in Part 2 thereof (the "**Mandatory Clauses**"); and

1.21 In this DPA:

1.21.1 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; and

1.21.2 any reference to any statute, regulation or other legislation in this DPA shall be construed as meaning such statute, regulation or other legislation, together with any applicable judicial or administrative interpretation thereof (including any binding guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority).

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 by Client under the Agreement, Client may either act as a Controller or a Processor and FIS will be a (sub) 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 Data Protection 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; (b) inform Data Subjects that their Personal Data will be disclosed to FIS and, where applicable, request consent for the disclosure and/or cross-border transfer of their Personal Data; and (c) 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 The parties agree that, to the extent a) Client transfers Personal Data to FIS in a Restricted Country or b) FIS transfers Personal Data to Client in a Restricted Country, it shall be effecting a Restricted Transfer. To allow such Restricted Transfer to take place without breach of applicable Data Protection Laws, the parties agree as follows:

7.1.1 in the event of an EEA Restricted Transfer, the parties agree to incorporate the SCCs into this DPA, which SCCs are completed in accordance with Part 1 of Attachment 1 (*Population of SCCs*);

7.1.2 in the event of a UK Restricted Transfer, the parties agree to incorporate the SCCs into this DPA, which SCCs are varied to address the requirements of the UK GDPR in accordance with UK Transfer Addendum and completed in accordance with Part 2 of Attachment 1 (*Population of SCCs*);

7.1.3 in the event of a Swiss Restricted Transfer, the parties agree to incorporate the SCCs in this DPA, which SCCs are completed in accordance with Part 1 of Attachment 1 (*Population of SCCs*) and varied in accordance with Part 3 of Attachment 1; and

7.1.4 in the event of a Restricted Transfer, the parties agree to implement the "Supplementary Measures" set out in Attachment 2, in addition to the SCCs.

7.2 In the event of any conflict between the terms of this Annex and the terms of the applicable SCCs, the terms of the applicable SCCs shall prevail to the extent of such conflict.

7.3 If required by any Supervisory Authority or the mandatory laws or regulatory procedures of any jurisdiction in relation to an EEA Restricted Transfer UK Restricted Transfer and/or Swiss Restricted Transfer, the parties shall upon request of either party execute or re-execute the applicable SCCs as separate documents setting out the proposed transfers of Personal Data in such manner as may be required.

7.4 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 from Client to FIS made in connection with the Agreement:

7.4.1 FIS shall notify Client of the same, and provide to Client a copy of its Binding Corporate Rules; and

7.4.2 from the date of such notification, all Restricted Transfers from Client to FIS made in connection with the Agreement shall be subject to such Binding Corporate Rules, and the relevant 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 Subprocessors 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 ten (10) business days 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.

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 confirms 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:

15.2 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;

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

15.4 describe the likely consequences of the Personal Data Breach; and

15.5 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.

15.6 Client, and/or its Customers, are solely responsible for complying with data breach notification laws applicable to Client and/or its Customers 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; and

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.

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.

Attachment 1

Population of SCCs

Notes:

- In the context of any EEA/Swiss Restricted Transfer, the SCCs completed in accordance with Part 1 of this Attachment 1 are incorporated by reference into and form an effective part of this Annex.

- In the context of any UK Restricted Transfer, the SCCs as varied by the UK Transfer Addendum and completed in accordance with Part 2 of this Attachment 1 are incorporated by reference into and form an effective part of this Annex.

- In the context of any Swiss Restricted Transfer, the SCCs as amended in accordance with Part 3 of this Attachment 1 are incorporated by reference into and form an effective part of the DPA.

PART 1: EEA AND SWISS RESTRICTED TRANSFERS

1. **SIGNATURE OF THE SCCs.** Where the SCCs apply in accordance with Section 7 of this Annex, each of the parties is hereby deemed to have signed the SCCs at the relevant signature block in the Agreement.

2. **APPLICABLE MODULE.**

- **Module 2** applies if Client acts as a Controller and transfers Personal Data from Europe to FIS, acting as Processor, in a Restricted Country.
- **Module 3** applies if Client acts as a Processor and transfers Personal Data from Europe to FIS, acting as Sub Processor, in a Restricted Country.
- **Module 4** applies if FIS, acting as Processor, transfers Personal Data from Europe to Client, acting as Controller, in a Restricted Country.

3. **POPULATION OF THE BODY OF THE SCCs**

3.1 Module 2 and Module 3 of the SCCs shall be completed as follows:

(a) The optional 'Docking Clause' in Clause 7 is not used and the body of that Clause 7 is left intentionally blank.

(b) the Parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 of the SCCs shall be provided by the data importer to the data exporter only upon data exporter's written request.

(c) Parties agree that the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 17 of this DPA.

(d) In Clause 9, OPTION 2: GENERAL WRITTEN AUTHORISATION applies, and the minimum time period for advance notice of the addition or replacement of Subprocessors shall be the advance notice period set out in Section 10 of this Annex.

(e) In Clause 11, the optional language is not used and is deleted.

(f) In Clause 13, all square brackets are removed and all text therein is retained.

(g) In Clause 17, OPTION 1 applies, and the parties agree that the SCCs shall be governed by the law of Ireland in relation to any EEA and Swiss Restricted Transfer.

(h) For the purposes of Clause 18, the parties agree that any dispute arising from the SCCs in relation to any EEA and Swiss Restricted Transfer shall be resolved by the courts of Ireland, and Clause 18(b) is populated accordingly.

3.2 Module 4 of the SCCs shall be completed as follows:

(a) The optional 'Docking Clause' in Clause 7 is not used and the body of that Clause 7 is left intentionally blank.

(b) In Clause 11, the optional language is not used and is deleted.

(c) For the purposes of Clause 17, the parties agree that the SCCs shall be governed by the law of Ireland in relation to any EEA and Swiss Restricted Transfers.

(d) For the purposes of Clause 18, the parties agree that any dispute arising from the SCCs in relation to any EEA and Swiss Restricted Transfer shall be resolved by the courts of Ireland.

4. POPULATION OF ANNEXES TO THE SCCs

4.1 Annex I to the Appendix to the SCCs is completed with the corresponding information detailed in the Personal Data Attachment, with – for module 2 and module 3 - Client being 'data exporter' and FIS being 'data importer' and – for module 4 – FIS being 'data exporter' and Client being 'data importer'.

4.2 Part C of Annex I to the Appendix to the SCCs is completed as below:

The competent Supervisory Authority shall be determined as follows:

- Where Client is established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of that EU Member State in which Client is established.
- Where Client is not established in an EU Member State, Article 3(2) of the GDPR applies and Client has appointed an EU representative under Article 27 of the GDPR: the competent Supervisory Authority shall be the Supervisory Authority of the EU Member State in which Client's EU representative relevant to the processing hereunder is based (from time-to-time).
- Where Client is not established in an EU Member State, Article 3(2) of the GDPR applies, but Client has not appointed an EU representative under Article 27 of the GDPR: the competent Supervisory Authority shall be the Supervisory Authority of the EU Member State notified in writing to FIS' contact point, which must be an EU Member State in which the Data Subjects whose Personal Data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located.

4.3 Annex II to the Appendix to the SCCs is completed by reference to the Security Statement.

PART 2: UK RESTRICTED TRANSFERS

Where relevant in accordance with Section 7 of this Annex, the SCCs also apply in the context of UK Restricted Transfers as varied by the UK Transfer Addendum in the manner described below:

(a) *Part 1 of the UK Transfer Addendum*. As permitted by Section 17 of the UK Transfer Addendum, the parties agree that:

(i) Tables 1, 2 and 3 of Part 1 of the UK Transfer Addendum are deemed completed with the corresponding details set out in the Personal Data Attachment and the foregoing provisions of Part 1 of Attachment 1 (subject to the variations effected by the Mandatory Clauses described in (b) unten); and

(ii) Table 4 of Part 1 of the UK Transfer Addendum is completed by the box labelled 'Data Importer' being deemed to have been ticked.

(b) *Part 2 of the UK Transfer Addendum*. The parties agree to be bound by the Mandatory Clauses of the UK Transfer Addendum.

(iii) In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in this Annex to the SCCs shall be read as a reference to those SCCs as varied in the manner set out in this Part 2.

PART 3: SWISS RESTRICTED TRANSFERS

Where relevant in accordance with Section 7 of this DPA, the SCCs apply to Swiss Restricted Transfers, subject to the following amendments and additional provisions:

(a) The term "EU Member State" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with the SCCs;

(b) The SCCs also protect the data of legal entities until the entry into force of the revised version of the FADP of 25 September 2020, which is scheduled to come into force in 2023 (“Revised FADP”); and

(c) The FDPIC shall act as the “competent supervisory authority” insofar as the relevant data transfer is governed by the FADP.

Attachment 2

Supplementary Measures

The parties have agreed to implement the following Supplementary Measures to the safeguards set out in the SCCs, in line with "Recommendations 01/2020 on measures thar supplement transfer tools to ensure compliance with the EU level of protection of personal data" as adopted on 18 June 2021 by the European Data Protection Board.

Technical measures

1. Physical Security: each FIS location that houses the physical components used to transfer information is controlled by security systems that restrict access and monitor activity. These areas are monitored 24x7 by Security Operations Centers.

2. Encryption: FIS uses industry standard encryption protocols for both in-transit and at-rest critical data.

3. DLP. Software is in place at numerous levels of FIS to alert and block the transfer of sensitive data outside of the organization. These issues are alerted and investigated in real time.

4. FIS enabled logging on all critical infrastructure that is used in the handling of Client data. These logs are monitored 24x7 by Cyber Fusion Centers that can respond in real time to any potential issues.

Further details of FIS' security program are summarized in the Security Statement found at:
https://www.fisglobal.com/solutions/legal/fis-information-security.

Contractual measures

5. FIS provides regular information – by publishing Transparency Reports - on government requests received by FIS from law enforcement and public authorities based in a third country outside Europe to access data relating to individuals in Europe. These Transparency Reports are available on the Client Portal (section Vendor Management, General Data Protection Regulation).

6. FIS declares that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or Personal Data, (2) it has not purposefully created or changed its business processes in a manner that facilitates access to Personal Data or systems, and (3) that national law or government policy does not require FIS to create or maintain back doors or to facilitate access to personal data or systems or for FIS to be in possession or to hand over the encryption key.

Organizational measures

7. Training: all FIS new hires must complete privacy awareness training within 30-60 days of their hire date. All employees are required to take privacy training annually, pass a quiz on the course, and confirm their willingness to comply with FIS policies and standards affiliated with privacy.