Supplier Personal Data Processing Annex

THIS SUPPLIER DATA PROCESSING ANNEX ("**DPA**") forms part of any written or electronic agreement(s) between FIS or an FIS Affiliate and Supplier or a Supplier Affiliate for the purchase of services pursuant to which Supplier or a Supplier Affiliate processes Personal Data (the "**Agreement(s)**"). This DPA sets out obligations of FIS and Supplier with respect to data protection in relation to the Agreement(s).

Supplier enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Supplier Affiliates, if and to the extent Supplier or a Supplier Affiliate processes Personal Data for which FIS and/or such FIS Affiliates qualify as the Controller or Processor as detailed below. For the purposes of this DPA only, and except where indicated otherwise, the term "**Supplier**" shall include Supplier and Supplier Affiliates and the term "**FIS**" shall include FIS and/or where applicable FIS Affiliates.

1. **INTERPRETATION**.

1.1 In this DPA the following terms shall have the meanings set out in this Section 1, unless expressly stated otherwise:

(a) "**Aggregate Consumer Information**" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.

(b) "**CCPA**" means the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020.

(c) "**Cessation Date**" has the meaning given in Section 9.1.

(d) "**Client**" means a natural person or entity that receives products or services from FIS and/or any FIS Affiliate.

(e) "**Client Personal Data**" means any Personal Data originating from the Client and Processed by or on behalf of Supplier on behalf of FIS and/or any FIS Affiliate pursuant to or in connection with the Agreement.

(f) "**CPA**" means the Colorado Privacy Act.

(g) "**CTDPA**" means the Connecticut Personal Data Privacy and Online Monitoring Act.

(h) "**Data**" means any information or data to be processed or collected by Supplier pursuant to the Agreement(s), including any Personal Data, if applicable.

(i) "**Data Controller**" means the entity that determines the purposes and means of the Processing of Personal Data.

(j) "**Data Processor**" means any person or entity that Processes Personal Data on behalf of a Data Controller.

(k) "**Data Protection Laws**" 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.

(l) "**Deidentified Information**" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information.

(m) "**Depersonalized Information**" means Data provided by or on behalf of Client and/or Client's customers to FIS in connection with the Services, and all information derived from such Data, that has been cleansed to remove Client's name and any Personal Data;

(n) "**EEA**" means the European Economic Area.

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

(p) "**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.

(q) "**FADP**" means the Swiss Federal Act on Data Protection.

(r) "**FIS Affiliate**" means any companies which are controlled by FIDELITY INFORMATION SERVICES, LLC, which control FIS or which are under common control with FIS and either: (i) are Controllers of any Personal Data; and/or (ii) on whose behalf Supplier and/or any Subprocessor otherwise processes any Personal Data. For these purposes, "**control**" and its derivatives mean to hold, directly or indirectly, more than 50% of the respective shares with voting rights.

(s) "**FIS Personal Data**" means any Personal Data Processed by or on behalf of Supplier on behalf of FIS and/or any FIS Affiliate pursuant to or in connection with the Agreement.

(t) "**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**").

(u) "**MTCDPA**" means the Montana Consumer Data Privacy Act;

(v) "**ORCPA**" means the Oregon Consumer Privacy Act;

(w) "**Personal Data**" means any information relating to an identified or identifiable natural person ('data subject'). In this DPA, Personal Data refers to both Client Personal Data as well as FIS Personal Data.

(x) "**Personnel**" means a natural person's or entity's employees, agents, consultants or contractors.

(y) "**Process**" (and its derivatives) means any operation or set of operations performed upon Personal Data, whether or not by automatic means, including creating, collecting, aggregating, procuring, obtaining, accessing, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, making available, aligning, combining, restricting, erasing and/or destroying the information.

(z) "**Pseudonymized Information**" means the processing of Personal Data in a manner that renders the Personal Data no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data is not attributed to an identified or identifiable consumer.

(aa) "**Relevant Body**":

(i) in the context of the EU GDPR, means the European Commission;

(ii) in the context of the UK GDPR, means the UK Government (Secretary of State);

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

(iv) in the context of the CCPA, the California Privacy Protection Agency;

(v) in the context of the CPA, the Colorado Office of the Attorney General;

(vi) in the context of the CTDPA, the Connecticut Office of the Attorney General;

(vii) in the context of the MTCDPA, the Montana Office of the Attorney General;

(viii) in the context of the ORDPA, the Oregon Office of the Attorney General;

(ix) in the context of the TXDPSA, the Texas Office of the Attorney General;

(x) in the context of the UCPA, the Utah Office of the Attorney General; and/or

(xi) in the context of the VCDPA, the Virginia Office of the Attorney General.

(bb) "**Restricted Country**":

(i) in the context of the EEA, means a country or territory outside the EEA;

(ii) in the context of the UK, means a country or territory outside the UK; and

(iii) 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.

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

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

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

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

(dd) "**Security Requirements**" means the Supplier Information Security Requirements or other information security policies, procedures and measures included in the Agreement, as may be updated from time to time by mutual written agreement of the parties.

(ee) "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Supplier for FIS and/or any FIS Affiliate pursuant to the Agreement.

(ff) "**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 the Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

(gg) "**Subprocessor**" means any third party appointed by or on behalf of Supplier to Process Personal Data.

(hh) "**Supervisory Authority**":

(i) in the context of the EU GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR;

(ii) in the context of the UK GDPR, means the UK Information Commissioner's Office;

(iii) in the context of the FADP, the FDPIC;

(iv) in the context of the California CCPA, the California Privacy Protection Agency;

(v) in the context of the Colorado CPA, the Colorado Office of the Attorney General;

(vi) in the context of the Connecticut CTDPA, the Connecticut Office of the Attorney General;

(vii) in the context of the MTCDPA, the Montana Office of the Attorney General;

(viii) in the context of the ORDPA, the Oregon Office of the Attorney General;

(ix) in the context of the TXDPSA, the Texas Office of the Attorney General;

(x) in the context of the Utah UCPA, the Utah Office of the Attorney General; and/or

(xi) in the context of the Virginia VCDPA, the Virginia Office of the Attorney General.

(ii) "**TXDPSA"** means the Texas Data Privacy and Security Act;

(jj) "**UK**" means the United Kingdom of Great Britain and Northern Ireland;

(kk) "**UK GDPR**" means the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019).

(ll) "**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**").

(mm) "**UCPA**" means the Utah Consumer Privacy Act.

(nn) "**VCDPA**" means the Virginia Consumer Data Protection Act.

1.2 In this DPA:

(a) the terms, "**Controller**", "**Data Subject**", "**Personal Data Breach**", "**Processor**" and "**Process/Processing/Processed**" shall have the meaning ascribed to the corresponding terms in the GDPR;

(b) the terms, "**Business**" and "**Service Provider**" shall have the meaning ascribed to the corresponding terms in the CCPA;

(c) unless otherwise defined in this DPA, all capitalized terms in this DPA shall have the meaning given to them in the Agreement; and

(d) 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. PROCESSING OF PERSONAL DATA

2.1 In the course of Supplier providing the Services under the Agreement, Supplier may from time-to-time Process FIS Personal Data and/or Client Personal Data supplied to it by or on behalf of FIS or an FIS Affiliate. The parties acknowledge and agree that:

(a) In relation to any FIS Personal Data provided or made available to Supplier for Processing in connection with the Services, **FIS is the Controller** and **Supplier is either a Controller or a Processor**, depending on the Services Supplier provides pursuant to the Agreement;

(b) in relation to any Client Personal Data, **Client is the Controller**, **FIS is a Processor**, and **Supplier is an additional Processor**.

2.2 Supplier shall:

(a) comply with all applicable Data Protection Laws in Processing Personal Data; and

When acting as a Processor or additional Processor:

(b) only Process the Personal Data for the specific purpose(s) set out in the Data Processing Details Appendix that is incorporated into the Agreement as an appendix thereto.

(c) not Process Personal Data other than:

(i) for FIS Personal Data: on FIS' written instructions (including the instruction set out in Section 2.44); or

(ii) for Client Personal Data: on Client's written instructions as provided by FIS (including the instruction set out in Section 2.45); or

(iii) as otherwise strictly required by applicable laws.

When acting as a Controller:

(b) only Process the Personal Data for the specific purpose(s) set out in Data Processing Details Appendix. Supplier may only process the Personal Data for another purpose:

(i) where it has obtained the Data Subject's consent, or identified its own legal basis for the processing as a Controller;

(ii) where necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the Data Subject or of another natural person.

(c) retain the Personal Data for no longer than necessary for the purpose(s) for which it is processed. Supplier shall put in place appropriate technical or organizational measures to ensure compliance with this obligation, including erasure or anonymization of the data and all back-ups at the end of the retention period;

(d) in order to enable Data Subjects to effectively exercise their rights pursuant to Data Protection Laws, inform them: i) of its identity and contact details; ii) of the categories of Personal Data processed and iii) where it intends to share the Personal Data with any third-parties: the recipients or categories of recipients and the purpose of such transfer. For Personal Data subject to the European Data Protection Laws, the information that Supplier shall provide to Data Subjects shall comply with the requirements set out in Articles 13 and 14 of the GDPR, or equivalent provisions of any other Data Protection Laws. All information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language as required by Data Protection Laws;

(e) deal with any enquiries and requests it receives from a Data Subject relating to the processing of his/her Personal Data and the exercise of his/her rights under Data Protection Laws without undue delay and at the latest within one month of the receipt of the enquiry or request. Supplier shall take appropriate measures to facilitate such enquiries, requests and the exercise of Data Subject rights. Any information provided to the Data Subject shall be in an intelligible and easily accessible form, using clear and plain language. Where Supplier processes the Personal Data for direct marketing purposes, it shall cease Processing for such purposes if the Data Subject objects to it;

(f) not make a decision based solely on the automated processing of the Personal Data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the Data Subject or similarly significantly affect him/her, unless with the explicit consent of the Data Subject or if authorized to do so under the laws of the country of destination, provided that such laws provide suitable measures to safeguard the Data Subject's rights and legitimate interests. In this case, Supplier shall, where necessary in cooperation with FIS: a) inform the Data Subject about the envisaged automated decision, the envisaged consequences and the logic involved; and b) implement suitable safeguards, at least by enabling the Data Subject to contest the decision, express his/her point of view and obtain review by a human being; and

(g) inform Data Subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point to handle complaints. Supplier shall deal promptly with any complaints it receives from a Data Subject.

2.3 To the extent permitted by applicable laws, Supplier shall inform FIS of:

(a) any Processing to be carried out under Section 2.2(c)(iii); and

(b) the relevant legal requirements that require it to carry out such Processing,

before the relevant Processing of that Personal Data.

2.4 FIS instructs Supplier to Process Personal Data to the limited extent strictly necessary for Supplier to provide the Services to FIS pursuant to and in accordance with the Agreement.

2.5 The Data Processing Details Appendix sets out certain information regarding Supplier's Processing of Personal Data. The parties may from time to time amend the Data Processing Details Appendix by mutual written agreement.

2.6 Where Supplier receives an instruction from FIS that, in its reasonable opinion, infringes any Data Protection Laws, Supplier shall immediately inform FIS.

2.7 **Applicable Data Protection Laws.** Supplier shall observe all Applicable Data Protection Laws with respect to the protection and Processing of Personal Data.

2.8 **Approvals.** Supplier will obtain and maintain throughout the term of the Agreement all necessary licenses, authorizations or approvals, as required by the Data Protection Laws.

2.9 **California Law Compliance**. Supplier is a Service Provider under the CCPA, and as may be amended from time to time. Supplier must not: (i) sell or share Personal Data of California Consumers to another business, person, or third party for monetary or other valuable consideration; (ii)retain, use or disclose Personal Data of California Consumers, except for the purpose of performing the Services specified in the Agreement or as otherwise permitted by applicable law; (iii) retain, use, or disclose Personal Data of California Consumers outside of the direct business relationship between FIS and Supplier; (iv) combine Personal Data of a California Consumer with Personal Data that Supplier receives from or on behalf of another person, or collects from its own interaction with the California Consumer, provided that Supplier may combine Personal Data of California Consumers to perform any business purpose permitted by the CCPA. FIS will notify Supplier within two (2) business days if it receives a verifiable request from a California Consumer to exercise privacy rights under the CCPA and Supplier agrees to assist FIS in meeting its CCPA compliance obligations. Supplier certifies that it understands and will comply with the requirements of this section and if Supplier is unable to meet the restrictions imposed by this subsection, it will provide notice to FIS promptly upon making such determination, in which case FIS may notify Supplier to stop the processing of Personal Data of California Consumers or coordinate in good faith with Supplier to ensure the Personal Data of California Consumers Personal Data is processed in accordance with the CCPA.

2.10 **FIS Obligations**. FIS will not instruct Supplier to perform any Processing of Personal Data that violates any Data Protection Law. Subject to the cooperation of Supplier as specified in this DPA, FIS will be solely responsible for safeguarding the rights of Data Subjects, including determining the adequacy of the security measures in relation to Personal Data which FIS uploads to the Services and providing any necessary notice to or obtaining any necessary consent from Data Subjects regarding the Processing. FIS shall have sole responsibility for the accuracy, quality, and legality of Personal Data provided to Supplier for Processing and the means by which FIS acquired Personal Data.

3. **SUPPLIER PERSONNEL**. Supplier shall take reasonable steps to ensure the reliability of any Supplier's Personnel who may Process Personal Data, including ensuring:

(a) that access is strictly limited to those individuals who need to know or access the relevant Personal Data for the purposes described in this DPA and the Agreement;

(b) that all such individuals have been vetted by Supplier in accordance with applicable laws; and

(c) that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. **SECURITY**.

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk (which may be of varying likelihood and severity) for the rights and freedoms of natural persons, Supplier shall implement appropriate technical and organizational measures in relation to Personal Data to ensure a level of security appropriate to that risk.

4.2 In assessing the appropriate level of security, Supplier shall take into account in particular of the risks presented by the Processing, in particular from a potential Personal Data Breach.

4.3 Without limiting the generality of Sections 4 and 4.2, Supplier shall, and shall cause each Subprocessor to, comply with the Security Requirements set out in the Agreement.

4.4 On FIS' request, Supplier shall (promptly following such request) provide to FIS written information describing in reasonable detail the technical and organizational measures taken by Supplier in relation to Personal Data pursuant to Section 4.

5. **SUBPROCESSING**

5.1 Supplier may continue to use those (Sub)processors already engaged by Supplier as at the date of this DPA which are listed in the Subprocessors Appendix, subject to Supplier meeting or having met the obligations set out in Section 5.3. The Subprocessor Appendix is incorporated into the Agreement as an appendix thereto.

5.2 Supplier may appoint new (Sub)processors Subject to Section 5.1 and in compliance with the Agreement.

5.3 With respect to each (Sub)processor appointed by Supplier, Supplier shall:

(a) before the (Sub)processor first Processes Personal Data, carry out adequate due diligence to ensure that the (Sub)processor is capable of providing the level of protection for Personal Data required by this DPA; and

(b) ensure that the arrangement between Supplier and the (Sub)processor is governed by a written contract including terms which offer at least the same level of protection for Personal Data as those set out in this DPA.

5.4 On FIS' request, Supplier shall (promptly following such request) provide to FIS:

(a) a list of the then-current (Sub)processors engaged by Supplier, together with all relevant information relating to each such Subprocessor as shown in the Subprocessor Appendix; and

(b) written certification that the arrangements between Supplier and such (Sub)processors meet the requirements set out in Section 5.3.

5.5 Supplier shall be liable for the acts and omissions of all (Sub)processors under or in connection with this DPA.

6. DATA SUBJECT RIGHTS

6.1 When Processing Personal Data as a Processor, Supplier shall assist FIS by implementing appropriate technical and organizational measures to enable FIS (and for Client Personal Data: the Client) to fulfil its obligations to respond to and otherwise address Data Subject's exercise of their rights under the Data Protection Laws (including those set out in Chapter III of the GDPR, or equivalent provisions of any other Data Protection Laws).

6.2 Supplier shall:

(a) promptly notify FIS if it, or any (Sub)processor, receives a request from a Data Subject under any Data Protection Laws in respect of Personal Data; and

(b) ensure that neither it, nor any (Sub)processor, responds to that request except on the written instructions of FIS or as required by applicable law to which it, or such (Sub)processor, is subject, in which case Supplier shall to the extent permitted by applicable law inform FIS of that legal requirement before it, or any (Sub)processor, responds to the request.

7. PERSONAL DATA BREACH

When acting as a Processor or additional Processor:

7.1 Supplier shall notify FIS without undue delay (and in any event within twenty-four (24) hours) upon Supplier or any of its Subprocessor becoming aware of a Personal Data Breach affecting Personal Data, providing FIS with sufficient information to allow it (and for Client Personal Data: the Client) to meet any obligations under the Data Protection Laws to inform affected Data Subjects and/or Supervisory Authorities of the Personal Data Breach.

7.2 At a minimum, any notification made by Supplier to FIS pursuant to Section 7.1 shall include (to the extent available to Supplier at the relevant time):

(a) a description of the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

(b) a description of the likely consequences of the Personal Data Breach; and

(c) a description of the measures taken or proposed to be taken to address the Personal Data Breach.

7.3 Supplier shall provide regular updates to FIS in respect of the resolution of any Personal Data Breach.

7.4 Supplier shall (at its own cost) co-operate with FIS and take (and procure that any applicable Subprocessor shall take) such reasonable steps as are reasonably directed by FIS to assist in the investigation, mitigation and remediation of such Personal Data Breach.

When acting as a Controller:

7.5 In the event of a Personal Data Breach concerning FIS Personal Data, Supplier shall take appropriate measures to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

7.6 In case of a Personal Data Breach that is likely to result in a risk to the rights and freedoms of natural persons, Supplier shall without undue delay notify both FIS and the competent supervisory authority. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for Supplier to provide all the information at the same time, it may do so in phases without undue further delay.

7.7 In case of a Personal Data Breach that is likely to result in a high risk to the rights and freedoms of natural persons, Supplier shall also notify, without undue delay, the Data Subjects concerned of the Personal Data Breach and its nature, if necessary, in cooperation with FIS, unless Supplier has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, Supplier shall instead issue a public communication or take a similar measure to inform the public of the Personal Data Breach.

7.8 Supplier shall document all relevant facts relating to the Personal Data Breach, including its effects and any remedial action taken, and keep a record thereof.

8. **DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION**. For Services that Supplier provides as a Processor, Supplier shall provide reasonable assistance to FIS (and for Client Personal Data: Client) with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which FIS (and for Client Personal Data: the Client) reasonably considers to be required of it by Article 35 or Article 36 of the GDPR or equivalent provisions of any other 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, Supplier.

9. DELETION OR RETURN OBLIGATIONS

9.1 Subject to Sections 9.2 and 9.5, upon the date of cessation of those Services involving the Processing of Personal Data (the "**Cessation Date**"), Supplier shall immediately cease all Processing of the Personal Data for any purpose other than for storage in accordance with this Section 99.

9.2 Subject only to Section 9.5, FIS may in its absolute discretion by written notice to Supplier at any time after the Cessation Date require Supplier to:

(a) return a complete copy of all Personal Data to FIS by secure file transfer in such format as is reasonably notified by FIS to Supplier; or

(b) delete, and procure the deletion of, all copies of Personal Data Processed by Supplier and/or any Subprocessor.

9.3 Supplier shall comply with any request made pursuant to Section 9.2 within fourteen (14) days thereof.

9.4 Promptly (and in any event within seven (7) days) following FIS' confirmation of receipt of all Personal Data returned pursuant to Section (a), Supplier shall delete, and procure the deletion of, all other copies of Personal Data Processed by Supplier and/or any Subprocessor.

9.5 Supplier and any Subprocessor may retain certain Personal Data if and as required by applicable law, and then only to the extent and for such period as required by such applicable law, and always provided that Supplier shall:

(a) to the extent permitted by applicable law, inform FIS of that legal requirement;

(b) ensure the ongoing confidentiality of all such Personal Data;

(c) Process such Personal Data in compliance with the Security Requirements;

(d) ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable law requiring its storage and for no other purpose; and

(e) act as a Controller in its own right in connection with such purposes, and shall comply with applicable obligations under Data Protection Laws in relation thereto.

9.6 Upon request from FIS, Supplier shall provide written certification to FIS that it has fully complied with this Section 9.

10. COMPLIANCE INFORMATION AND AUDIT RIGHTS

10.1 At FIS' written request, Supplier shall make available to FIS all information reasonably necessary to demonstrate Supplier's compliance with the obligations laid down in this DPA and applicable Data Protection Laws. This could be in the form of mutually agreed third party certifications of industry standard.

When acting as a Processor or additional Processor:

10.2 Supplier shall allow for and contribute to audits, including inspections, by FIS or an auditor mandated by FIS in relation to the Processing of Personal Data by Supplier and any Subprocessors.

10.3 FIS shall give Supplier reasonable notice of any audit or inspection to be conducted under Section 10.1, and Supplier need not give access to its premises for the purposes of such an audit or inspection:

(a) outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis (pursuant to Sections 10.3(i) or (ii) below), and FIS has given notice to Supplier that this is the case before attendance outside those hours begins; or

(b) for the purposes of more than one (1) audit or inspection, in respect of Supplier and each Subprocessor, in any calendar year, except for any additional audits or inspections which:

(i) FIS reasonably considers necessary because of genuine concerns as to Supplier's compliance with this DPA (including follow-up audits); or

(ii) FIS is required or requested to conduct by Data Protection Laws, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory.

10.4 If it is established during an audit that Supplier has failed to comply with its obligations under this DPA, FIS shall notify Supplier and Supplier shall take all measures necessary to ensure its compliance as soon as reasonably practicable.

10.5 FIS shall bear its own third-party costs in connection with such inspection or audit, **unless** the findings of the audit show that Supplier and/or any Subprocessor failed to comply in any material respect with the provisions of this DPA, in which case Supplier shall reimburse all reasonable and documented costs incurred by FIS in connection with such inspection or audit.

11. RESTRICTED TRANSFERS

11.1 Supplier shall not make (nor instruct, permit or suffer a Subprocessor to make) a Restricted Transfer of any Personal Data except with the prior written consent of FIS (and for Client Personal Data: the Client) and in accordance with Section 11.2.

11.2 Notwithstanding Section 11.1, the parties agree that, to the extent FIS transfers Personal Data to Supplier 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:

(a) 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 Annex 1 (*Population of SCCs*);

(b) 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 Annex 1 (*Population of SCCs*); and

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

(d) in the event of a Restricted Transfer, Supplier agrees to implement the "Supplementary Measures" set out in Annex 2, in addition to the SCCs.

Conflicts

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

Provision of full-form SCCs

11.4 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 Transfers, 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.

12. CHANGE IN LAWS

12.1 FIS may propose any variations to this DPA which are necessary to address the changing requirements of any Data Protection Laws (including any updates to the SCCs to reflect any future decisions of a Relevant Body in relation to the subject matter thereof).

12.2 If FIS gives notice under Section 12.1, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in FIS' notice without undue delay.

12.3 In the event FIS considers (acting reasonably) that any failure to agree its proposed variations to this DPA may cause FIS (or for Client Personal Data: the Client) to be in material breach of Data Protection Laws, FIS may terminate the Agreement in its entirety upon written notice to Supplier with immediate effect and without liability to Supplier.

12.4 The parties agree that FIS shall be deemed to be "acting reasonably" for the purposes of Section 12.3 in the event Supplier fails to execute the revised form of any SCCs issued or approved by a Relevant Body from time to time promptly following FIS' request.

13. INCORPORATION AND PRECEDENCE

13.1 This DPA shall be incorporated into and form part of the Agreement with effect from the Addendum Effective Date.

13.2 In the event of any conflict or inconsistency between:

(a) this DPA and the Agreement, this DPA shall prevail; or

(b) any SCCs entered into pursuant to Section 11.2 and this DPA and/or the Agreement, those SCCs shall prevail.

Annex 1

Population of SCCs

Notes:

- In the context of any EEA/Swiss Restricted Transfer, the SCCs completed in accordance with Part 1 of this Annex 1 are incorporated by reference into and form an effective part of the DPA.
- 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 Annex 1 are incorporated by reference into and form an effective part of the DPA.
- In the context of any Swiss Restricted Transfer, the SCCs as amended in accordance with Part 3 of this Annex 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 11 of this DPA, each of the parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs.

2. **APPLICABLE MODULE**

- Module One of the SCCs shall apply to any EEA and Swiss Restricted Transfer where Supplier is processing FIS Personal Data in a capacity as Controller;
- Module Two of the SCCs shall apply to any EEA and Swiss Restricted Transfer where Supplier is processing FIS Personal Data in a capacity as Processor.
- Module Three of the SCCs shall apply to ant EEA and Swiss Restricted Transfer where Supplier is processing Client Personal Data in a capacity as (sub) Processor.

3. POPULATION OF THE BODY OF THE SCCs

The SCCs shall be populated as follows:

MODULE ONE:

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

(b) Clause 9 shall be deemed inapplicable.

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

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

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

(f) 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 completed accordingly.

(g) The parties agree the certification of deletion of Personal Data 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.

(h) Parties agree that the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 10 of this DPA.

MODULE TWO:

(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 9, OPTION 1: SPECIFIC PRIOR AUTHORISATION applies.

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

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

(e) 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.

(f) 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 completed accordingly.

(g) The Parties agree the certification of deletion of Personal Data 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.

(h) Parties agree that the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 10 of this DPA.

MODULE THREE

(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 9, OPTION 1: SPECIFIC PRIOR AUTHORISATION applies.

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

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

(e) 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.

(f) 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 completed accordingly.

(g) The Parties agree the certification of deletion of Personal Data 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.

(h) Parties agree that the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 10 of this DPA.

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 Data Processing Details Appendix to the Agreement, with FIS being 'data exporter' and Supplier 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 FIS is established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of that EU Member State in which FIS is established.
- Where FIS is not established in an EU Member State: the Supervisory Authority in Ireland:

  DATA PROTECTION COMMISSION
  21 FITZWILLIAM SQUARE SOUTH
  DUBLIN 2
  D02 RD28
  IRELAND

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

PART 2: UK RESTRICTED TRANSFERS

Where relevant in accordance with Section 11 of this DPA, 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 Data Processing Details Appendix to the Agreement and the foregoing provisions of Part 1 of Annex 1 (subject to the variations effected by the Mandatory Clauses described in (b) below); 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.

(c) In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in this DPA 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 11.2 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.

Annex 2

Supplementary Measures

Background:

- In judgment C-311/18 (Schrems II) the Court of Justice of the European Union (CJEU) indicated that Controllers or Processors, acting as data exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the data importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Standard Contractual Clauses (SCCs);
- The CJEU refers to recital 109 of the GDPR, encouraging Controllers and Processors to implement - where appropriate and required - supplementary measures to ensure compliance with the level of protection required under European Data Protection Laws;
- This Annex 2 provides such additional supplementary measures, drawing on the recommendations contained in the *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of Personal Data*, Version 2.0, adopted by the European Data Protection Board on 18 June 2021.

In the event of a conflict between this Annex 2 and the SCCs, the SCCs prevail.

1. BACK DOORS AND SIMILAR PROGRAMMING

1.1 Supplier confirms that:

(a) it has not purposefully created back doors or similar programming that could be used to access the system(s) that the Supplier uses for processing of the transferred Personal Data and/or the transferred Personal Data themselves;

(b) it has not purposefully created or changed its business processes in a manner that facilitates access to Personal Data or systems by public authorities; and

(c) that, the best of its knowledge, national law or government policy does not require the Supplier to create or maintain back doors or to facilitate access to Personal Data or systems or for the Supplier to be in possession or to hand over the encryption key.

For the sake of clarity, a back door or similar programming refers to an intentionally created undisclosed or hidden access to a system, an application or to Personal Data. A back door does not include regular support access, management access or access for the purpose of maintenance. Vulnerabilities not known at the time of the release do not constitute a 'back door'.

1.2 FIS is entitled to terminate the Agreement in those cases in which Supplier does not reveal the existence of 1) a back door or similar programming, 2) manipulated business processes or 3) any requirement to create or maintain any of these.

1.3 In circumstances where the Supplier disclosed Personal Data transferred in violation of the commitments contained in provision 1.1 above, Supplier shall compensate Data Subjects for any material and non-material damage suffered as a result of such violation.

2. **AUDITS OR INSPECTIONS TO VERIFY IF DATA WAS DISCLOSED TO PUBLIC AUTHORITIES**. FIS may exercise its power to require that the Supplier submit its processing facilities and other documentation and files to audit or inspection pursuant to the SCCs by giving short notice to the Supplier to verify if Personal Data was disclosed to public authorities. Supplier shall ensure that FIS is in a position to verify whether the transferred Personal Data was disclosed to public authorities and under which conditions they were disclosed. In particular, access logs and other similar trails must be tamper-proof (e.g. they should be made inalterable using state of the art encryption techniques, such as hashing, and also systematically transmitted to the exporter on a periodic basis) so that auditors are in a position to find evidence of disclosure. Access logs and other similar trails must also distinguish between accesses due to regular business operations and accesses due to orders or requests for access. When carrying out its obligations under this provision, Supplier will in all circumstances cooperate with FIS and the competent supervisory authority in a timely fashion.

3. MONITORING CHANGES IN LEGISLATION OR PRACTICE. Supplier shall monitor any legal or policy developments (such as changes in the legislation or practice in the countries where the data is transferred) which might

lead to its inability to comply with its obligations under the SCCs. In particular, Supplier shall make reasonable efforts to inform FIS of legal or policy developments ahead of their implementation to enable FIS to recover the Personal Data from the Supplier (either by returning the data to the FIS or by deleting or securely encrypting the data).