PART A

General Terms and Conditions of Purchase

Release December 20th, 2021

1. Applicability

1.1. Orders, assignments and other agreements ("**Purchase Orders**") of Fidelity Information Services GmbH and Fidelity Information Services Operations GmbH ("**FIS**") shall be subject exclusively to the following General Terms and Conditions of Purchase ("**Purchase Conditions**"). These shall apply to all Deliverables and Services from the seller, Supplier and service Supplier ("**Supplier**") ordered by FIS under or in connection with purchase, work and service agreements, in particular to all goods and work Deliveries ("**Deliverables**") as well as to the production and processing of works and the provision of consulting, training, maintenance and other Services (collectively "**Services**"). Depending on the type of service, one or more Additional Conditions (Part B to Part G3) and Annexes may also apply.

1.2. Different terms and conditions of the Supplier, especially general terms and conditions of the Supplier, will not form part of the agreement, regardless of whether they have been expressly rejected by FIS or not, unless they have been expressly confirmed in writing by FIS. The unopposed acceptance or unconditional payment of Deliverables and Services does not constitute consent to the validity of different terms and conditions of the Supplier.

2. Order and Order Confirmation, change in performance

2.1. Orders by FIS must be made in writing in order to be effective and shall set out a clear description of the Services to be delivered,. Orders from FIS can also be validly issued with an electronic signature. The Supplier warrants that it will agree with FIS on appropriate service levels (in particular with regard to availability, maximum duration of individual failures, maximum number of failures, recovery time) for the services to be commissioned or commissioned and that it will allocate certain performance levels ("target values") to these in the service level agreements.

2.2. The transmission of a scanned signed document or an electronically signed document as an attachment by e-mail is sufficient.

2.3. Unless otherwise agreed, orders from FIS must be accepted by the Supplier within two weeks ("**Order Confirmation**"). Thereafter the transmission by e-mail of a scanned signed document or an electronically signed document as an attachment is sufficient. After two weeks FIS shall no longer bound to the respective order and shall be entitled to withdraw from the agreement.

2.4. Deviations, changes or additions to the order made by the Order Confirmation shall only become part of the agreement if they are confirmed in writing by FIS.

2.5. After conclusion of the agreement FIS may demand reasonable changes with regard to the agreed delivery or service from the Supplier until the agreed delivery or service has been rendered in full. The Supplier is obliged to review any change request by FIS without delay. If the Supplier is of the opinion that the change request made by FIS is erroneous, incomplete, ambiguous or non-executable, he shall immediately notify it recognisable consequences to FIS in writing and shall give FIS the opportunity to improve or confirm the change request ("**Complaint**"). Otherwise, the Supplier shall inform FIS within ten working days of receipt of the change request possible effects of the desired changes on the schedule, the payment and/or other contractual conditions. In the event of a Complaint about the original change request by the Supplier, the period shall run correspondingly from receipt of an improvement proposal or a confirmation of the original change request by FIS. If FIS decides to carry out the change, the parties shall with an amicably agreement arrange an appropriate adjustment of the delivery and/or service conditions agreed in the order, in particular with regard to any additional or reduced costs as well as any postponement of the delivery or service times.
If the Supplier recognizes that the delivery implementation or service changes or extension of delivery and service turn out to be necessary, the Supplier shall immediately inform FIS in writing. Changes or extensions to the scope of delivery or service require the prior written approval from FIS in order to become effective.

3. Delivery, service performance, risk transfer

3.1. Unless expressly otherwise agreed, Deliverables by the Supplier shall be made DPP (Incoterms 2020) to the shipping address specified by FIS. The risk shall pass to FIS at the time of delivery at the place of destination. Partial Deliverables and partial Services shall not be permitted without the prior written approval of FIS.

3.2. In the case of Services to be performed by the Supplier as well as in the case of Deliverables involving the assembly of the goods at the place of use, an acceptance shall take place in accordance with the provisions of section 8. In those cases, the risk passes to FIS at the moment of the written acceptance. The preceding paragraph does not apply insofar the acceptance is excluded by the nature and quality of the Services. In this case, the time of proof of complete performance of the service shall take the place of acceptance.

4. Dates and deadlines, delay

4.1. The Purchase Orders shall enter into force on the date of signature by both parties and shall be concluded for an indefinite period, unless a shorter term is agreed by the parties. Purchase Orders concluded for an indefinite period may be terminated by either party with three months' notice at the end of each year, at the earliest at the end of the calendar year following the conclusion of the agreement.

4.2. The dates or deadlines specified in the order for delivery or service are binding. The timeliness of Deliverables is determined by the receipt of the goods at the shipping address indicated by FIS. For the timeliness of Services or Deliverables, which include assembly or erection of the goods at the place of use, shall be decisive the date of written acceptance by FIS. This shall not apply if acceptance is excluded by the nature and quality of the Services. In this case, the timeliness depends on the time of the complete performance of the service.

4.3. If the Supplier is in delay with the delivery or the performance, FIS shall be entitled to demand to the Supplier a contractual penalty in the amount of 0.5% of the relevant delivery or performance value for each expired week of delay, but not more than a total of 5% of the respective delivery or performance value. The right of FIS to assert further damages shall remain unaffected; however, the contractual penalty shall be appropriate credited. The acceptance of the delayed delivery or service shall not constitute a waiver of the

assertion of the contractual penalty or other claims for compensation.

4.4. If Services are not performed by the Supplier within the agreed dates or deadlines, FIS shall be entitled, after expiry of a reasonable grace period granted to the Supplier, to perform the relevant Services itself or have them performed by third parties at the expense of the Supplier. Section 4.3. shall remain unaffected, but with the instruction that the delay shall be deemed to have ended in the event of successful self-execution. Sentence 1 of this section 4.4 shall apply mutatis mutandis if the Supplier does not perform Services in the way and manner owed under the contract; the right to assert further damages by FIS shall remain unaffected.

4.5. If the Supplier realises that the agreed dates or deadlines for the delivery or service cannot be kept, it shall immediately inform FIS in writing, stating the reasons and the expected duration of the delay. The validity of the agreed dates or periods for delivery or performance shall remain unaffected by the notification.

5. Cooperation between the contracting parties

5.1. FIS shall provide the Supplier the information FIS deems necessary for the performance of the Deliverables or Services owed. If the Supplier does not consider the information sufficient, it shall immediately notify FIS thereof in writing.

5.2. Within the framework of ongoing projects, the Supplier shall, upon request at any time, inform FIS in writing about the current status of the Deliverables or Services to an appropriate extent, grant FIS the access to its documents pertaining the performance of the Deliverables and/or Services owed and meet its team, employed in the respective project, at the registered office of FIS or at a location to be agreed in each case with FIS, in order to hold discussions regarding the status and scope of the owed Deliverables and/or Services. The Supplier shall provide a report of the meeting, which shall require the confirmation of FIS.

5.3. The Supplier shall perform the agreed Deliverables and Services in accordance with the current state of the art and by qualified personnel to perform the agreed Deliverables and Services. It will use the methods/processes and tools agreed with FIS or comparable developed methods and tools. The Supplier shall comply with the specifications, guidelines and/or manuals of FIS. The Supplier undertakes to comply with the “Supplier Security Terms” made available to the Supplier upon request and to impose a corresponding written obligation on its employees and any third parties involved in the execution with the agreement of FIS. FIS shall not be entitled to issue direct instructions to the Supplier's employees.

5.4. At FIS's request, the Supplier shall appoint a project manager who can provide the information required to carry out the agreed Deliverables or Services and who can either take or bring about decisions. A change of project manager requires the prior written agreement of FIS. The agreement may only be denied for important reasons.

6. Transfer of rights or granting of usage rights

6.1. If the Supplier during the performance of a delivery or a service for FIS provides, develops or produces works, creations, inventions or other tangible results (collectively "**Work Results**") which are protected by intellectual and industrial property rights or other trademark rights (collectively "**Intellectual Property Rights**"), the Supplier hereby assigns to FIS all Intellectual Property Rights to the Work Results. FIS accepts the transmission.

6.2. Insofar is a transfer not possible for legal reasons, the Supplier grants FIS the exclusive, worldwide, perpetual, transferable, and sub-licensable usage rights for the full exploitation of the Work Results, including the authority to process (while preserving the intellectual nature of the works), distribute, reproduce, renting, make publicly available and otherwise reproduce publicly of the Work Results, in the original or in processed form on any medium or other technical equipment in digital or analog form. The granting of rights also includes the right to use Work Results in the future for a type of use that is still technically unknown at the time of the order. FIS accepts the granting of rights of use.

6.3. The above transfer of rights or granting of usage rights also pertains to any preliminary and intermediate stages of the Work Results as well as to any design, training and documentation material.

6.4. Notwithstanding the preceding sections 6.1 to 6.3 the Supplier grants FIS the rights necessary for the contractual use and exploitation of other Deliverables or embodied performance results which are not Work Results ("**Other Results**"), but at least the non-exclusive, worldwide, perpetual, transferable and sub-licensable usage rights for the full exploitation of the Other Results, including the right of processing (while respecting the intellectual nature of the works), distribute, reproduce, rent, make available to the public or otherwise communicate to the public, in the original or edited form, on any medium or other technical device, in digital or analogue form.

6.5. The transfer of rights or granting of usage rights regulated in this section 6 shall be fully compensated by the agreed remuneration in the respective order.

6.6. The parties may make different provisions in the Purchase Order or transfer and/or granting of industrial property rights.

7. Open source software

The Supplier undertakes to ensure that the ordered Work Results and Other Results or Deliverables do not contain any open source software components, unless FIS has in advance expressly agreed to their use in writing. If the Supplier intends to integrate open source software components into the Work Results and/or Other Results, it shall immediately provide FIS with a list of all open source software components he intends to use, with a reference to the applicable open source software license terms, a description of the intended use and a copy of the complete license text. FIS shall inform the Supplier in writing within a reasonable period of time whether or not the intended use of the open source software components is approved. If no such information has been provided, approval shall be considered not granted.

8. Acceptance

8.1. Services provided by the Supplier shall be subject to an acceptance test after the results of the Services have been made available, unless an acceptance test is excluded due to the nature and quality of the Services. The Supplier shall announce in writing that the results of the Services are ready for acceptance no later than one week in advance. Partial acceptances shall not be carried out unless otherwise agreed in writing. At FIS's request, the Supplier shall support FIS free

of charge with its best efforts during the acceptance procedure. After conclusion of the acceptance test, FIS shall declare acceptance of the service provided if the service is free of defects. Acceptance shall be in writing.

8.2. If not only irrelevant defects of the Services are discovered during the acceptance test, FIS shall be entitled to refuse the acceptance. FIS shall inform the Supplier. The Supplier must remedy the defects in the service within a reasonable deadline at its own expense or provide its performance again free of defects and again make it available for acceptance. FIS will then carry out the acceptance test again. If the Supplier does not remedy the defects despite a reasonable deadline or if the Supplier fails to render the Services free of defects again, FIS may, without prejudice to other contractual rights, withdraw from the agreement and/or claim damages instead of performance. Further rights of FIS remain unaffected.

9. Warranty rights

9.1. FIS shall inspect the delivery for any deviations in quality and quantity within a reasonable deadline from receipt. The notification of any deviations, insofar as these are not obvious, is in any case considered timely, insofar it is given within a period of two weeks from the discovery of the deviation. If a longer statutory period exists for notification of deviations, this period shall apply.

9.2. If the Supplier fails to perform subsequent performance within a reasonable deadline set by FIS, FIS shall be entitled - notwithstanding any other statutory rights for defects - to perform the necessary actions to remedy the defect itself or get such a performance at the expense of the Supplier.

9.3. In the event of serial defects (defects of the same type occurring in at least 5% of the delivered goods inspected by random sampling), FIS shall be entitled to reject the entire delivery as defective and to assert the statutory claims for defects with respect to the entire delivery.

9.4. The Supplier shall bear all expenses necessary to the purpose of subsequent performance, especially transport, travel, labour and material costs as well as dismantling and installation costs. The place of performance for subsequent performance shall be the current designated location of the goods.

9.5. The limitation period for warranty rights is three years from delivery of the goods or acceptance of the work, unless a later limitation period results from §§ 438, 479 or § 634a BGB.

9.6. For newly delivered goods or newly produced works within the scope of subsequent performance, the limitation period shall begin to run anew from the moment of the replacement delivery or new production, unless subsequent performance appears minor in scope, duration and cost, or FIS had to assume, according to the conduct of the Supplier, that the Supplier did not feel obliged to take the measure, but acted only as a gesture of goodwill or similar reasons. The same shall apply in case of subsequent improvement if this concerns the same defect or the consequences of defective subsequent improvement.

10. Intellectual Property Rights

10.1. The Supplier shall ensure that the use and exploitation of the Work Results or Other Results by FIS does not conflict with any Intellectual Property Rights of third parties. This also applies in particular to the resale, leasing, licensing and/or use of the Work Results and Other Results domestically and abroad.

10.2. Insofar as the use and exploitation of the Work Results and/or Other Results violates the Intellectual Property Rights of third parties and the Supplier is responsible for such violation of Intellectual Property Rights, the Supplier shall indemnify FIS against all claims of third parties raised against FIS in and out of court arising from such violation of Intellectual Property Rights. The indemnity refers to all expenses and damages incurred by FIS as a result of or in connection with the claim by the third party, including any costs of a necessary and reasonable legal defence. Further statutory rights of FIS in the event of defects of title shall remain unaffected by the preceding provision.

11. Prices, payment according to expenditure

The prices stated in FIS's order are binding. All prices are understood inclusive of the statutory value added tax, unless this is shown separately. The agreed remuneration covers all Services to be rendered by the Supplier. In particular, in case of goods delivery, the costs for packaging, loading and transport to the shipping address specified by FIS are included (DPP (Incoterms 2020). The Supplier must insure the transport of the delivery at his own expense. For Services to be rendered by the Supplier as well as for Deliverables, which include the assembly of the goods at the place of use, the prices shall include all ancillary Services such as work equipment, materials and travel, unless otherwise agreed.

11.1. If payment is agreed on a time basis, the performance shall be provided and demonstrated on the basis of documentation sheets, which the Supplier shall agree with FIS in advance. FIS will only reimburse those times which can be proven in detail on monthly records and which have been countersigned by FIS. The Services rendered by the Supplier on a time and material basis shall be invoiced monthly in arrears on the basis of the countersigned documentation sheets to be attached to the invoice and under listing of other ancillary costs.

11.2. The daily rate agreed for payment on a time basis shall apply regardless on the days and the time in which the Services are performed. If in one day less than eight (8) hours are worked, the pro-rata remuneration shall correspond to the ratio of the hours worked to eight (8) hours per day and shall not exceed eight (8) hours. Overtime surcharges and break times are not remunerated.

11.3. Travel and accommodation costs shall be reimbursed to the Supplier if FIS has agreed to the assumption of the costs in advance in writing or in text form. In these cases, a refund will only be made upon submission of the original receipts and after deduction of of any pre-tax amounts to the following extent:

- Rail journeys (2nd class), flights (economy),
- Car use 0.30 EUR per kilometre driven;
- Accommodation costs up to 99,00 EUR gross per overnight stay;
- Travel and accommodation times, per diem expenses and meals shall not be reimbursed.

11.4. The Supplier shall agree in advance with FIS the details of travel and overnight accommodation (such as job site, dates or use of a car instead of rail or air travel).

11.5. The Supplier shall send invoices to FIS for the respective payments due, which indicate the travel and accommodation costs as well as separately the value added tax.

12. Invoicing, payment, default

12.1. Invoices are to be sent in duplicate to the invoice address stated in the order after dispatch of the delivery or performance of the service.

12.2. The respective valid value added tax shall be shown separately in the invoice.

12.3. Invoices must contain the purchase order references and the numbers for each individual item. Imprecise or incomplete invoices shall be considered not received until they are corrected or completed; in this case FIS shall notify the Supplier within a reasonable deadline. Copies of invoices shall be labelled as duplicates.

12.4. Unless otherwise agreed, payments shall occur within 60 days after complete delivery of the goods or after receipt and acceptance of the Services and receipt of a proper invoice, for payments within 14 days under deduction of 3% discount and for payments within 20 days under deduction of 2% discount. The supplier is not entitled to demand partial payments unless otherwise agreed in writing.

12.5. As far as the Supplier has to provide material certificates, reports including test reports, quality documents or other documents, the completeness of the delivery depends on the receipt of these documents.

12.6. Payments do not constitute an acknowledgement that the Deliverables or Services are as per the agreement, neither are they waiver of the Complaint according to § 377 HGB (German Commercial Code) or an approval of the delivery or service.

13. Awarding subcontracting

The involvement of third parties ("**Subcontractors**") for the performance of the contractually owed Deliverables and Services is not permitted without the prior written consent of FIS. In the event of unauthorized subcontracting, FIS shall be entitled to withdraw from the agreement in whole or in part and to claim damages.

14. Confidentiality

14.1. The Supplier shall treat all knowledge and experiences, documents, tasks, business processes and/or other information made available by FIS, including any Work Results as well as the existence and conditions of this agreement (collectively "**Confidential Information**") - even beyond the term of the agreement - as strictly confidential and shall keep them secret from third parties in connection with the provision of the Deliverables and/or Services owed. Without the prior written consent of FIS, Confidential Information may only be used for the purpose of providing the Deliverables and/or Services owed. Confidential Information may only be disclosed to Subcontractors engaged with the consent of FIS pursuant to section 13 if this is absolutely necessary for the performance of the Deliverables and/or Services owed and the Subcontractors engaged have previously been bound to confidentiality in a manner corresponding to this section 14.

14.2. The foregoing confidentiality obligations shall not apply to information (i) which are shared with affiliated companies of FIS, (ii) which was lawfully known to the Supplier without any obligation of confidentiality before having received them from FIS, (ii) which the Supplier has independently developed without recourse to or use of Confidential Information from FIS irrespective of the contractually owed delivery or service, (iii) which is generally known or publicly available at the time of receipt by the Supplier or which becomes so after receipt by the Supplier without breaching or violating this section 14 or any other provision protecting the Confidential Information of FIS, or (iv) which the Supplier is required by law, regulation or court order to disclose; in this case, the Supplier shall inform FIS prior to the disclosure and limit the scope of such disclosure as far as possible.

14.3. Any exchange of information between the Supplier and FIS customers concerning the subject matter of the agreement shall require the prior written consent of FIS in each individual case. FIS is entitled to share all confidential information with affiliated companies.

15. Quality assurance, audits, risk assessment

15.1. The Supplier is obliged to maintain a quality management system in its company which meets the requirements of ISO 9001. FIS has the right to carry out audits at the Supplier's premises in accordance with ISO 19011.

15.2. The Supplier shall grant FIS the right to audit the Supplier with regard to the performance of the Services for FIS and compliance with the agreements with FIS, provided that FIS announces the audit in writing within a reasonable deadline. The Supplier undertakes to assist with the audit, to support FIS to a reasonable extent, to provide all documents necessary for the performance of the audit and to grant FIS or third parties commissioned by FIS sufficient access to the relevant rooms, equipment and/or facilities during regular business hours, unless otherwise agreed.

15.3. The Supplier will cooperate with FIS in an appropriate manner and will provide FIS without delay at its request with the necessary information and documents to enable FIS to carry out an appropriate risk assessment with regard to the Supplier and his employees and, where applicable, subcontractors. To the extent permitted by law for the planned assignment for the provision of the services and reasonably requested by FIS, the Supplier will in particular provide certificates of good conduct for individual employees before they start work for FIS.

16. Data protection

16.1. The Supplier is obliged to observe the statutory provisions of data protection. In particular, all employees of the Supplier who come in contact with personal data of FIS shall be bound by data protection secrecy obligation. The Supplier shall also impose these obligations on its Subcontractors, if FIS has agreed to their engagement in accordance with section 13.

16.2. Insofar as the Supplier collects, processes and/or uses personal data on behalf of FIS within the scope of the performance of his contractually owed Services, the Supplier shall conclude an agreement with FIS on order data processing within according to Art. 28 GDPR. The Supplier undertakes to collect and use the personal data exclusively on behalf of and in accordance with the instructions of FIS. The Supplier shall take appropriate technical and organisational measures within the meaning of Art. 32 GDPR and shall design its internal organisation in such a way that it meets the special requirements of data protection and that the personal data is protected against misuse, unauthorised access, unauthorised alteration and/or loss.

16.3. If FIS grants the Supplier access to networks and data processing systems of FIS or its customers, this access and all personal data to which the Supplier has access may be

used exclusively for the purpose of fulfilling the contract. In this case, the Supplier undertakes to comply with the "Supplier Security Terms" made available to the Supplier upon request and to impose a corresponding written obligation on its employees and any third parties involved in the execution with the consent of FIS. Unless absolutely necessary for the performance of this agreement, the Supplier shall not be entitled to copy, store, evaluate, modify, delete or pass on to third parties any FIS data it has access without the prior written consent of FIS.

17. Disclosure and/or destruction of personal data and Confidential Information

The Supplier shall, at FIS's discretion, either surrender or destroy all personal data and Confidential Information of FIS, regardless of whether it is in electronic or embodied form, which it collects, receives and/or creates in connection with the agreed Deliverables and/or Services, including all copies, at FIS's discretion, immediately after delivery and/or acceptance of the delivery or service results, or if acceptance or handover is ruled out due to the nature or quality of the results, after complete performance of the agreed Services, or, if it is required to fulfil any claims based on defects, immediately after the end of the limitation period for the claims based on defects, unless statutory regulations on storage conflict with this. The Supplier must provide evidence of surrender or destruction. FIS may audit the complete surrender and/or destruction in accordance with section 15.2. FIS uses the findings of this audit solely to verify the complete release and/or destruction of data and Confidential Information.

18. Set-off and right of retention

FIS shall be entitled to set-off and retention rights as well as the defence of non-performance of the agreement to the full extent permitted by law. The offsetting or exercise of a right of retention by the Supplier due to disputed and not legally established counterclaims is excluded. The exercise of a right of retention by the supplier is also excluded insofar as counterclaims are not based on the same contractual relationship.

19. Assignment

The Supplier may transfer his rights and obligations only with the prior written consent of FIS. FIS will refuse consent only for important reasons. FIS is allowed to transfer its rights and obligations, in particular to affiliated companies within the meaning of section 15 AktG.

20. Termination (only valid for service agreement)

20.1. The termination of a service for which payment is measured in days or weeks is permissible,

- if the remuneration is calculated in hours or days, every day for the expiry of the following day;
- if the remuneration is calculated in weeks, no later than the first business day of a week for the end of the following Saturday.

If the remuneration is calculated according to months, quarters or longer periods of time or not calculated in periods of time, termination of the service by FIS with two weeks' notice is permissible.

20.2. Unless otherwise agreed, the above provision shall also apply if the duration of the service is determined or can be inferred from the nature or purpose of the Services.

20.3. The right of FIS to terminate the contract for good cause shall remain unaffected.

21. Compliance with the statutory minimum wage

21.1. In rendering the services, the Supplier undertakes to comply with all statutory provisions, in particular with the Act on the Regulation of a General Minimum Wage of 11.08.2014 (Minimum Wage Act - MiLoG) as amended, and shall pay its employees a salary at least equal to the respective statutory minimum wage.

21.2. For each culpable violation of the obligations of MiLoG by the Supplier or by subcontractors or lenders engaged by him FIS is entitled to charge a contractual penalty of 5% of the order value. In the event of a disproportionately high contractual penalty the contractor may demand a reduction of the contractual penalty from FIS.

21.3. The Supplier shall indemnify FIS in connection with its services from all claims in connection with § 1 MiLoG. This also applies to any necessary costs incurred by FIS due to the assertion of claims by employees or third parties (e.g. social security institutions). This also includes lawyer's fees according to the Lawyers' Fees Act (RVG) for any necessary extrajudicial and judicial legal defence.

21.4. The Supplier shall regularly provide FIS with monthly proof of payment of the minimum wage as well as documentation in accordance with § 17 (1) MiLoG, if requested by FIS. In doing so, the Supplier will, at FIS' request, provide an anonymised personnel deployment list showing the employees deployed, the hours worked by them and the wages paid in each case. The Supplier shall also provide FIS at its request with a corresponding list of other personnel employed (freelancers, trainees, interns, etc.). FIS undertakes to treat the documents as confidential and not to allow third parties to inspect them. (e.g. social security institutions). This also includes lawyers' fees in accordance with the Lawyers' Fees Act (RVG) for any necessary extrajudicial and judicial legal defence.

21.5. The Supplier undertakes to ensure that any subcontractors and lenders commissioned by him with the approval of FIS are also contractually obliged to comply with MiLoG and to pay the respective statutory minimum wage on time and regularly and to contractually agree this obligation if further subcontractors or lenders are employed. In the same way subcontractors must be obliged to submit confirmations in accordance with the obligation regulated above under 15.3.

22. Insurance

22.1. In all cases, Supplier shall effect and maintain, at its own cost, all applicable insurances as required by law and to cover Supplier's responsibilities and liabilities under the Purchase Order. Supplier will be responsible to ensure that any subcontractors maintain in force coverage as required herein, or that coverage is extended under Supplier's policies. The required insurance coverage will in no way be interpreted as relieving Supplier of any other responsibility or liability hereunder or any applicable law, statute, regulation or order. Unless specified otherwise on the Purchase Order, the Insurance Requirements below set forth minimum amounts of certain types of insurance coverage and other requirements relating to such insurance and is part of the Purchase Order. Supplier and its sub-contractors, as

described above, will maintain such insurance and comply with such other obligations during the Term, at its own expense:

22.2. TYPES & MINIMUM AMOUNTS OF INSURANCE COVERAGE.

1. Commercial General Liability Insurance: including Premises & Operations, Products/Completed Operations, Contractual, Broad Form Property Damage, and Personal Injury with a combined single limit of at least One Million Dollars ($1,000,000) per occurrence and Two Million Dollars ($2,000,000) general aggregate.
2. Business Automobile Liability Insurance: for all owned, non-owned, borrowed, leased, and hired vehicles to be used in connection with the Purchase Order, with a combined single limit of at least One Million Dollars ($1,000,000) each accident.
3. Workers' Compensation: with Alternate Employer Endorsement and including at least One Million Dollars ($1,000,000) Employers Liability coverage.
4. Property Insurance: against all risks of physical loss or damage to any property of FIS in the care, custody, or control of Supplier.
5. Professional Liability: in an amount of at least Ten Million Dollars ($10,000,000) including coverage for Network Security Liability and Privacy Liability.
6. Commercial Crime: including employee Dishonesty coverage in an amount of at least Five Million Dollars ($5,000,000).
7. Cyber Liability: in an amount of at least Ten Million Dollars ($10,000,000).

22.3. OTHER INSURANCE OBLIGATIONS.

1. Prior to executing the Purchase Order and within ten (10) days of each subsequent policy renewal, Supplier will provide FIS with certificates of insurance evidencing that the coverage and policy endorsements required hereunder are maintained in force with insurance companies that have an adequate rating. .
2. Supplier or its insurers will provide thirty (30) days written notice to FIS prior to cancellation or material change of any such policy.
3. Except with respect to the gross negligence of FIS, Supplier's policies will be primary and non-contributing with respect to any other insurance or self-insurance which may be maintained by FIS.
4. FIS will be named as an additional insured under the Commercial General Liability, Automobile Liability, Umbrella and Professional Liability policies, as well as a Loss Payee under the Commercial Crime policy described above.
5. Supplier and its Insurance Carriers will waive subrogation with respect to the Workers' Compensation, Employers Liability, Commercial General Liability and Automobile Liability policies.

23. Additional agreements, additional provisions, written form

Side agreements, amendments and supplements to an order and/or these Terms and Conditions of Purchase must be made in writing in order to be effective. This formal requirement can only be waived in writing. §§ 126a, 127 para. 2 BGB do not apply.

24. Amendments; Authorized Representatives

The Purchase Order may only be modified only by a written instrument signed by duly authorized representatives of both parties.

25. Usage And Interpretation

a. ENGLISH LANGUAGE. English will be the language of the Purchase Order. Translation of the Purchase Order, its attachments, schedules, exhibits, correspondence, documents, invoices, notices or other communications related to the Purchase Order, or the transactions thereunder, into another language will be at the sole risk of the translating party. In the event any conflicts arise between the English version of the Purchase Order and a translated version, the English version will prevail. If permitted under local Law, all communications pursuant to the Purchase Order will be conducted in the English language. Unless the context clearly indicates otherwise, (i) references to a party's agreement, consent, notice, request or approval mean written and signed agreement, consent, notice or approval, (ii) the words "will" and "shall" have the same meaning, which is obligatory, and (iii) the word "including" means "including, without limitation" so that it does not limit the scope of the word or phrase to which it is applied.

b. WEB-BASED PROVISIONS, PASSIVE CONTRACTS, INVOICE TERMS. The effectiveness of the Purchase Order, or of any statement or other contract made under the Purchase Order, will not be conditioned upon FIS becoming bound by (i) a reference in the Purchase Order to one or more documents maintained by Supplier and made available to FIS at a Web page, by email distribution or in any other manner; (ii) a "click-through", "shrink wrap" or similar mechanism presented by Supplier (whether in the past, present or future) involving the use of an action other than actual signature or electronic signature (as recognized by Law) to cause agreement to terms and conditions presented by Supplier; or (iii) as part of an invoice or similar administrative document. The parties understand and agree that any such documents, terms and conditions will be only for (A) informational purposes or to set forth obligations of or rights granted by the Supplier or its Affiliates, (B) that neither FIS nor any FIS Affiliate will be bound by any contractual obligation that might otherwise arise from any such reference or mechanism, whether under or in connection with the Purchase Order or otherwise, and (C) that any such documents, terms and conditions will in any event be subject to the Purchase Order, including these terms.

c. WAIVER. Failure by FIS to enforce the performance of any of the provisions of the Purchase Order shall neither be deemed to be a waiver of its rights hereunder nor shall it affect the validity of the Purchase Order in any way. Any waiver by FIS to any breach of the Purchase Order shall be specific to such particular breach and shall not bind the parties in respect of any subsequent breach by Supplier, even if such subsequent breach is identical or similar.

26. Severability clause

Should any provision of these General Terms and Conditions of Purchase be or become invalid, this shall not affect the validity of the remaining provisions.

27. **Applicable law**
German law shall apply with the exception of the UN Convention on Contracts for the International Sale of Goods (CISG) and the conflict of law's provisions.

28. **Jurisdiction**
Exclusive place of jurisdiction is Munich (Landgericht München I). However, FIS shall also be entitled to sue the Supplier at its registered office.

Part B - Supplier Code of Conduct
Part C - Supplier Security Terms
Part D - Operational Continuity and Exit
Part E - Supplier Audit Terms
Part F - Central Outsourcing Management
Part G1 - FIS - Vendor C2P DPA
Part G2 - FIS - Vendor C2C DPA
Part G3 - FIS - Vendor P2SP DPA

FIS Supplier Code of Conduct

Table of Contents

PURPOSE AND INTENT

FIS is committed to the highest ethical, environmental, social and governance standards. We have established and set out our ethical standards in the FIS *Code of Business Conduct and Ethics*, which applies to all employees, officers, subcontractors and, to the extent relevant, directors of the Company. The *Code of Business Conduct and Ethics* incorporates standards that are an extension of FIS' core values and reflect our commitment to ethical business practices and legal compliance. The FIS *Code of Business Conduct and Ethics* can be found at: *http://www.investor.fisglobal.com/phoenix.zhtml?c=180304&p=irol-govconduct_pf.*

FIS' definition of good corporate ethics includes the standards set forth in this *Supplier Code of Conduct* as a supplement to the *Code of Business Conduct and Ethics*. FIS expects that its suppliers ("**Suppliers**") will share and embrace our commitments to integrity and ethics, health and safety, labor standards, environmental performance, and anti-corruption practices. We understand that Suppliers are independent entities; however, the business practices and actions of a Supplier may impact and/or reflect upon FIS. Therefore, FIS expects all Suppliers and their employees, agents, and subcontractors (Suppliers' employees, agents, and subcontractors shall hereinafter be referred to collectively as "**Representatives**") to adhere to this FIS *Supplier Code of Conduct* and the *Code of Business Conduct and Ethics* while they are conducting business with and/or on behalf of FIS. FIS Suppliers are responsible for delivering the appropriate communications to educate and train their Representatives to ensure they understand and comply with such requirements.

LEGAL, REGULATORY AND ETHICAL COMPLIANCE

FIS Suppliers and their Representatives are expected to conduct their business in compliance with the applicable laws and regulations of the countries where they conduct business with or on behalf of FIS. In addition to any specific obligations under any agreement with FIS, all FIS Suppliers are expected to comply with the following legal and ethical standards:

- To communicate with honesty and with full candor.
- Be forthright with FIS, FIS representatives, regulators and other government officials and never engage in misleading communications. This obligation does not require the Supplier to give up legal protections or legally privileged communication.
- To conduct business in compliance with local labor and employment standards.
- FIS expressly prohibits any such participation in, support of or association with the illegal and immoral practice of trafficking in persons, forced labor and slavery. FIS is committed to a high ethical standard in its daily business practices and will continue to act in accordance with all applicable laws. Our Code of Business Conduct and Ethics requires that FIS and its employees not only obey company policies and all laws in any country where FIS operates, but also all transnational doctrines concerning fundamental human rights
- To conduct business in full compliance with all applicable anti-bribery and anti-corruption laws and with the United States Foreign Corrupt Practices Act and the UK Bribery Act. Specifically, Suppliers agree to not

make any direct or indirect payments or promises of payments to employees of government agencies, state-owned or controlled businesses, government officials or any other person to induce the individual to misuse his or her position to obtain or retain business or any other improper advantage.

- To keep its books, records and accounts in reasonable detail, accurately and such that they fairly reflect all transactions and dispositions of assets as the record-keeping provisions of Anti-Corruption Laws require.
- Also, to prohibit the mischaracterization or omission of any transaction on a company's books or any failure to maintain proper accounting controls that result in such a mischaracterization or omission.
- Keeping detailed, accurate descriptions of all payments and expenses is crucial for compliance purposes as Anti-Corruption Laws require.
- Adhere to the FIS *Anti-Bribery Anti-Corruption Policy*, which can be found at: *http://www.investor.fisglobal.com/phoenix.zhtml?c=180304&p=irol-govconduct*
- To comply with all applicable trade control, export, re-export and import requirements. For the avoidance of doubt, trade control means any laws, administrative regulations and executive orders of any applicable legal jurisdiction relating to the control of imports and exports of commodities and technical data, use or remote use of software and related property or services, and embargo of goods or services, and includes the Export Administration Regulations of the U.S. Department of Commerce and the regulations and executive orders administered by the Office of Foreign Asset Control of the U.S. Department of the Treasury.
- While conducting business for or on behalf of FIS, Suppliers must not participate in any national or international boycott that is not sanctioned by the United States government.
- To conduct business in full compliance with fair competition laws.
- To conduct business in compliance with copyright protections including all international conventions and laws governing the rights of copyright owners.
- Suppliers will comply with applicable environmental laws and regulations regarding hazardous materials, air emissions, waste and wastewater discharges, including the manufacture, transportation, storage, disposal, and release to the environment of such materials. We encourage the Supplier's responsible use of raw materials and natural resources, and efforts to reduce the consumption of these materials.

BUSINESS PRACTICES

Suppliers and their Representatives are expected to conduct their business with integrity and in accordance with their obligations under any specific agreements with FIS or, if no such agreement exists, in accordance with *FIS Standard Terms and Conditions of Purchase*. In addition to any specific obligations under the Supplier's agreement with FIS, all FIS Suppliers are expected to comply with the following business practices:

Business Records

- Honestly and accurately record and report all business information, and comply with all applicable laws regarding their completion and accuracy.
- Create, retain, and dispose of business records in full compliance with all applicable legal and regulatory requirements.

Systems, Security, Technology & Property

- Protect and responsibly use both the physical and intellectual assets of FIS including property, supplies, consumables, and equipment when authorized by FIS to use such assets.
- Use FIS provided information technology and systems (including e-mail) only for authorized FIS business-related purposes. FIS strictly prohibits Suppliers and their Representatives from using FIS provided technology and systems to create, access, store, print, solicit, or send any material that is intimidating, harassing, threatening, abusive, sexually explicit or otherwise offensive or inappropriate and/or to send any false, derogatory, or malicious communications using FIS provided information assets and systems. Comply with the FIS *Acceptable Use Policy* to the extent FIS e-mail and internet is made available.
- Comply with all FIS requirements for maintenance of passwords, confidentiality, security, and privacy procedures as a condition of receiving access to FIS' internal corporate network, all systems and buildings. Unless otherwise explicitly stated in a Supplier Agreement, with FIS, all data stored or transmitted on FIS owned or leased equipment is to be considered private and is the property of FIS. Suppliers must inform its Representatives that FIS monitors all use of the corporate networks and all systems (including e-mail) and accesses all data stored or transmitted using the FIS network.
- Comply with the intellectual property ownership rights of FIS and others including but not limited to copyrights, trademarks, and trade secrets. Use software, hardware and content only in accordance with their associated license or terms of use. Prohibit the illegal use of copyrighted materials including the illegal download of music, internet games and movies.

Gifts and Entertainment

FIS selects its Suppliers based on cost, quality and service. Any exchange of gifts or entertainment - regardless of amount - that is intended or appears intended to buy influence with a FIS employee or representative will be viewed as a serious violation of this *FIS Supplier Code of Conduct*.

- Gifts offered to FIS employees or representatives should be rare and always modest in cost; only inexpensive business-related items are acceptable. Examples of acceptable gifts are an inexpensive writing pen, or inexpensive business card holder.
- Gifts in excess of the local buying equivalent of $US 75.00 are prohibited without prior approval having been obtained by the FIS employee or representative. Currency and currency equivalents such as gift vouchers, gift cards, and similar stored value cards are never permitted regardless of the value of the gift.
- Entertainment offered should never exceed the local buying equivalent of $US 75.00 per person without prior approval having been obtained by the FIS employee or representative. Suppliers must never provide entertainment that is sexually oriented or otherwise in bad taste or which would be embarrassing to FIS or inconsistent with FIS' brand image as a professional, ethical, and responsible corporate citizen. Examples of acceptable entertainment are, a business lunch at a local restaurant without alcohol, a business dinner with limited alcohol, and a local hosted cultural or social event lasting a few hours.
- The Supplier should be cognizant not to offer an excessive number of gifts within a calendar year even if they are at $US 75.00 or under.
- Contact your FIS representative to submit a request for review into our FIS Gift and Entertainment Registry if the proposed gift or entertainment exceeds $US 75,00 for a decision.
- Gift giving and entertainment practices may vary in different cultures, but the limits in the policy are applicable globally and regardless of local business culture.
- For further details, please consult the Gifts and Entertainment Standard within the FIS Anti-Bribery Anti-corruption Policy. NOTE: FIS Rules for China may have additional requirements. Please request guidance for this country from your FIS representative.

Suppliers and their Representatives must to report to FIS' Corporate Compliance Office and/or our FIS Ethics Hotline any request for or offer of a bribe, kickback, grease payment, facilitation payment or other offer intended to buy influence as well as conflicts of interest.

Report by email to *corporatecompliance@fisglobal.com*. For additional reporting mechanisms, please see the reporting section at the end of the policy for further details.

Conflict of Interest, Insider Trading & the Press

- Suppliers and their Representatives must take all appropriate action to avoid actual conflicts of interest and the appearance of conflicts of interests.
- Suppliers and their Representatives are not permitted to deal directly with any FIS representative whose spouse, domestic partner, or other family member or relative holds a significant financial interest in the Supplier. If such a relationship exists, the conflict of interest must be disclosed and resolved appropriately before the Supplier may become a supplier to FIS.
- Contact your FIS representative to submit the actual or potential conflict into our FIS Conflicts of Interest Registry for review and a decision.
- Supplier must prohibit insider trading of any company's stock when in the possession of information that is not available to the investing public and that could influence an investor's decision to buy or sell stock.
- No Supplier should speak to the press on FIS' behalf unless the expressly authorized to do so in writing by FIS.

Personal Data Privacy

- If Supplier processes or has access to any personal data regarding employees or other contractors of FIS, then Supplier shall treat such personal data as FIS' confidential information and only process it for legitimate purposes in accordance with all applicable laws. Such personal data shall not be used for any purpose except as necessary to implement, perform or enforce the Supplier's contract with FIS. Supplier must use the same reasonable efforts as it uses to protect its own confidential and proprietary information (but in any event not less than a reasonable standard of care) to protect the confidentiality and security of such personal data, and must delete or destroy the personal data when it is no longer needed in relation to the Supplier's relationship with FIS.
- FIS will apply the same standards with respect to any personal data regarding employees of Supplier that FIS may access or process with respect to its relationship with Supplier. See the *FIS Privacy Policy* and the *Controlled Personal Data Privacy Notice*, which can be found at https://www.fisglobal.com/privacy.

EMPLOYMENT AND LABOR PRACTICES

FIS Suppliers must share in FIS' commitment to human rights and equal opportunity in the workplace. FIS Suppliers shall conduct their employment practices in full compliance with local employment and labor laws and regulations.

In addition, all FIS Suppliers are expected to comply with the following:

- Provide employees with a workplace that is free of harassment and unlawful discrimination. Regardless of cultural differences, FIS Suppliers are expected to comply with all applicable labor and employment laws in hiring, compensation, access to training, promotion, termination, and retirement and Suppliers shall not discriminate based on race, color, national origin, religion, age, disability, gender, marital status, sexual orientation, gender identification, protected veteran status or any other protected category.
- Provide a safe and healthy work environment and fully comply with all applicable safety and health laws, regulations and practices.
- Prohibit the use of alcohol and the abuse of prescription medication while on FIS or FIS customer owned or leased property and while conducting FIS business.
- Prohibit use, manufacture, possession, distribution, and/or sale of illegal drugs.
- Prohibit the possession of weapons and dangerous substances on FIS or FIS customer owned or leased property.
- Provide a work environment that is free from human trafficking and slavery, which includes forced labor and unlawful child labor. Use only voluntary labor. The use of forced labor whether in the form of indentured labor, bonded labor, or prison labor by a FIS Supplier and/or its subcontractors is prohibited.
- Employees and people hired as contract or temporary labor should not be required to lodge "deposits" or their identity papers with their employer and are free to leave their employer after reasonable notice without penalty.
- Comply with all local minimum working age laws and requirements and under no circumstances use child labor in any capacity or employ people under the age of 16 years, or the legal minimum working age, whichever is higher. FIS supports legitimate workplace apprenticeship programs provided that the programs are for educational purposes and exclusively for the benefit of under-age people employed.
- Provide a workplace free from physical abuse or discipline, the threat of physical abuse, sexual or other harassment, verbal abuse or other forms of intimidation, or measures that compromise the individual's mental integrity.
- Pay all workers in accordance with the applicable wage laws.
- Strictly adhere to working hours or labor hour statutes. Overtime pay must be paid in accordance with applicable law. No employee shall be required to work more than the maximum hours permitted by applicable law.

- No deduction from wages not permitted by applicable law shall be permitted without the express permission of the worker concerned.
- All disciplinary measures should be recorded and administered in accord with applicable labor and employment law.
- Keep employee records in accordance with applicable law.

COMPLIANCE WITH THE FIS SUPPLIER CODE OF CONDUCT

It is the responsibility of the Supplier to ensure that its Representatives understand and comply with this *FIS Supplier Code of Conduct* and to inform its FIS contact,

the FIS Compliance Office at *corporatecompliance@fisglobal.com,* or a member of FIS Management if any situation develops that causes the Supplier to operate in violation of this *FIS Supplier Code of Conduct*.

- FIS Suppliers are expected to self-monitor their compliance with FIS' *Supplier Code of Conduct*. Provided the violation does not result in illegal conduct, a Supplier who self-reports a violation of this *Supplier Code of Conduct* will be permitted a reasonable time to correct its non-compliance.

In addition to any other rights FIS may have under its agreement with the Supplier, FIS may request the immediate removal of any Representative who behaves in a manner that is disruptive, unlawful, or inconsistent with this *Supplier Code of Conduct* or any other public FIS policy.

REPORTING COMPLIANCE FAILURES OR QUESTIONABLE BEHAVIOR

You are encouraged to work with your primary FIS contact to resolve any business-related issues. However, if you suspect a violation of policy or law, or suspected violation, compliance failures or any questionable behavior/misconduct you need to take immediate action to report the concern(s) to the Chief Compliance and Customer Advocacy Officer via *corporatecompliance@fisglobal.com.*

If you do not have internet access ─ send your concerns to:

Chief Compliance and Customer Advocacy Officer

Fidelity National Information Services, Inc.

601 Riverside Avenue

Jacksonville, Florida 32204

If you prefer to remain anonymous (with certain exceptions in some European countries), FIS provides toll-free Ethics Hotline numbers (877.364.7384 for U.S. or Canada) for each country and an Ethics Website www.fnisethics.com that are available 24 hours a day, 7 days a week. Toll-free numbers for each country are provided in Appendix A to the Code of Business Conduct and Ethics found externally on the FIS Global website Corporate Governance page: *http://www.investor.fisglobal.com/phoenix.zhtml?c=180304&p=irol-govHighlights*

You may also obtain the toll-free numbers from the Ethics Website.

FIS does not tolerate any retaliation against anyone who, in good faith, reports a violation of FIS policy or law or cooperates with an investigation.

PART C

Release December 20th, 2021

1. SAFETY AND SECURITY ON PREMISES. Supplier Personnel must comply with all FIS postings and notices regarding safety and security when on the premises of FIS, and with the postings and notices of Clients or their customers when on their premises. Supplier Personnel must not carry weapons or ammunition onto the premises of FIS, Clients or their customers and must not use or carry weapons or ammunition while attending FIS-sponsored events.

2. ACCESS PRIVILEGES AND RESTRICTIONS. In the event Supplier Personnel will receive access credentials for FIS's facilities, applications, systems or servers, those of its Affiliates or those of any Clientsor any of their customers, the following provisions will also apply:

   2.1. Supplier will require all Supplier Personnel that will be issued access credentials to submit to FIS's then current access requirements.
   2.2. Supplier will promptly, but in any event within twenty-four (24) hours, (i) confiscate each such access credential from Supplier Personnel when the Supplier Personnel's need to have such access in orderfor the Products to be provided is discontinued and (ii) notify FIS of any change in the status (includingany such suspension, termination or discontinuation) of Supplier Personnel for whom such a device oraccess credential has been requested or to whom such a device or access credential has been provided.
   2.3. Supplier will not request that such an access credential be provided, or provide such an access credential, to any individual who will not be directly engaged by or at the request of FIS to provide theProducts.
   2.4. FIS reserves the right to deny any access credential request or terminate any access credential that has been provided. Supplier will notify FIS within twenty-four (24) hours of any changes to the SupplierPersonnel for whom such an access credential has been requested or to whom such an access credential has been provided.
   2.5. Supplier will not permit any such access credential to be used by more than one individual.

3. INFORMATION SECURITY AND INTERNAL CONTROLS. In the event Supplier (i) stores any data of FIS,its Clients or their customers, otherwise has any such data in its possession or control, (ii) has access to any such data from outside the premises of FIS, its Clients or their customers, or (iii) has access to any networks of FIS, its Clients or their customers, the following provisions will apply to Supplier. Supplier will be considered to have access to such data in the event that a communications link (defined as a pre- established communications path from the customer premises, through a carrier network, to a network of FIS, its Clients or their customers) exists between any of Supplier's systems or servers and any systems orservers on which such data is stored. In the event a Supplier Affiliate or Contractor to Supplier does so, Supplier will ensure by contract and otherwise that the following provisions apply correspondingly to the Supplier Affiliate or Contractor for the benefit of FIS.
   3.1. Supplier will be responsible for establishing and maintaining an information security program to (i) ensure the security and confidentiality of such data, (ii) protect against any anticipated threats or hazards to the security or integrity of such data, and (iii) protect against unauthorized access to or use of such data that could result in substantial harm or inconvenience to FIS, its Clients or their customers. Such information security program shall include ongoing security awareness training for all Supplier personnel providing Products hereunder and shall be at least as stringent as the requirements of ISO 27001/27002. Supplier shall designate an individual to be responsible for the information security program. Such individual shall respond to FIS inquiries regarding computer security and to be responsible for notifying FIS-designated contact(s) if a breach or an incident occurs, as further described herein.
   3.2. Supplier will maintain security for its own systems, servers, and communications links as necessary to protect such data and networks. Supplier's security controls must include (i) anti-virus/malware devices, (ii) DMZ subnet and firewall controls, (iii) IDS/IPS controls, (iv) patch management controls,
   (v) physical security controls, and (v) change management controls.
   3.3. On FIS' request, Supplier will contract with an appropriately qualified third-party information security assurance vendor to perform, on a semi-annual basis, an information security assessment that includes intrusion testing. Supplier will forward results of these tests to FIS within ten (10) business days following the Supplier's receipt from the security assurance vendor. If, after reviewing such test results, FIS believes that additional testing is warranted, Supplier will discuss such additional testing with FIS in good faith.

   3.4. Supplier will notify FIS of any and all breaches to Supplier's information security as soon as practicablebut in no event longer than one (1) business day after the discovery of any such breach, and will work with FIS management to identify the root cause of the incident and the potential impact to FIS, its Clients or their

customers, as reasonably requested by FIS.

3.5. Unless a more stringent standard applies, with regard to personal or financial information regarding FIS' (or its Clients' or Clients' customers') former, current or prospective clients, customers, directors, shareholders or employees ("Sensitive Data"): (a) Supplier shall not transmit any such Sensitive Data unencrypted over the internet or a wireless network, and shall not store any Sensitive Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry- standard encryption software approved by FIS; (b) all backup and archival media containing Sensitive Data must be encrypted and contained in secure, environmentally-controlled storage areas owned, operated, or contracted for by Supplier; and (c) destruction of any Sensitive Data must be by shredding in a secured area for Sensitive Data on paper, or for electronic storage, by wiping or degaussing for physical destruction or disposal, in a manner meeting forensic industry standards such as the NIST SP800-88 Rev. 1 Guidelines for Media Sanitization.

3.6. Not more frequently than once each quarter during the Term, and thereafter for so long as Supplier continues to provide the Service, Supplier will conduct, or have a third party conduct, vulnerability scans and penetration tests of those components of Supplier's environment required to support the Products and will promptly, and in any event not less than ten (10) business days following receipt from such third party, provide to FIS the results of any such scans and tests. In addition, Supplier will allow FIS or one of FIS's approved third-party security assurance vendors to perform periodic vulnerability scans and penetration tests of those components of Supplier's environment, if any, required to support any Product. FIS agrees to share the results of any scan or test it performs in Supplier's environment to assist Supplier in correcting any information security vulnerabilities identified. Supplier will correct any information security vulnerability identified in FIS's or Supplier's own scans and penetration tests within the applicable time periods below, based on the severity level of the vulnerability, and provide FIS a new scan report upon remediation:

3.6.1. High (CVSS great than 7) severity vulnerabilities will be corrected within thirty (30) business days;

3.6.2. Medium to Low (CVSS less than 7) severity vulnerabilities will be corrected within ninety (90) business days;

3.7. PCI DATA SECURITY STANDARD. If and to the extent Supplier or any Product is subject to the Payment Card Industry Data Security Standard requirements (as amended from time to time) ("PCI DSS"), Supplier will comply with said requirements. In addition, if and to the extent Supplier or any Product is subject to PCI DSS requirements:

3.7.1. Supplier will submit their Report of Compliance ("ROC") within ten (10) days of the execution of this Supplement and will have a ROC prepared, and provide to FIS such updated ROC, annually thereafter;

3.7.2. Supplier will publish to Visa' Global Service Supplier registry and maintain 'Green Status' in such registry throughout the duration of the Purchase Order; and

3.7.3. if Supplier fails to maintain 'Green Status' in the Visa Global Service Supplier registry, the following provisions shall apply:

3.7.1.1 If Supplier in in 'Yellow Status' in the Visa Global Service Supplier registry, Supplier will provide the Products free of charge until Supplier obtains 'Green Status'; and

3.7.1.2 If Supplier is in 'Red Status' or is not listed in the Visa Global Service Supplier registry: (i) Supplier will provide the Products free of charge free of charge until Supplier obtains 'Green Status' or the Purchase Order terminates, (ii) Supplier will refund to FIS the six (6) then most recent months of fees paid by FIS under the Purchase Order (excluding any period in which Supplier was providing the Products free of charge due to Supplier being in 'Yellow Status' or 'Red Status' pursuant to this provision); and (iii) FIS may, in addition to any other remedies FIS may have, terminate the Purchase Order with no financial obligation to Supplier arising from such termination.

4 BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY. Supplier will establish and maintain disaster recovery and business continuity plans designed to minimize the risks associated with a disaster affecting Supplier's ability to provide the Products or Services, which includes (if applicable to the Products or Services) off-site data storage and recovery infrastructure. Supplier will test its disaster recovery and business continuity plans, including call trees, not less frequently than annually, and will annually provide to FIS the disaster recovery and business continuity plans test results. FIS may share such disaster recovery plan and test results with Clients who have contracted for the Products or Services, if any, FIS's auditors, and FIS's regulators. Supplier will implement the applicable disaster recovery or

business continuity plan upon the occurrence of a disaster, and shall notify FIS promptly following such event. In the event of a disaster (as defined in the plan), Supplier will not charge fees higher than or in addition to the agreed fees under the Purchase Order. Supplier will notify of, and invite FIS to participate in (at no additional charge to FIS), Supplier's disaster recovery and business continuity plan test.

Supplier's recovery time objective for the Services ("RTO") under such plan shall be agreed in writing withFIS. Supplier will maintain adequate backup procedures in order to recover FIS's or if applicable any Client's data to the point of the last available good backup, with a recovery point objective ("RPO") as agreed in writing with FIS. If Supplier fails to meet the RTO and RPO in any annual test, Supplier shall perform a rootcause analysis of the cause of the failure to meet the RTO or RPO and will remediate the cause of such failure and retest within six (6) months of the failed test. If Supplier fails to meet the RTO or RPO in the retest, Supplier will have a second six (6) month period to remediate and retest. If Supplier fails a second time, FIS may request that the parties attempt to reach a mutually agreeable resolution, and if the parties are unable to agree upon a resolution within thirty (30) days of FIS's request, FIS may terminate the Purchase Order with no further financial obligation to Supplier.

5. THIRD PARTY SOFTWARE. In connection with the provision of Products to FIS, Supplier has not and shall not use, incorporate, or integrate any third party computer software except as set forth on the Purchase Order or with FIS's prior written consent.

6. ADDITIONAL DEFINITIONS.

(1) A "Destructive Element" is any computer code or other technological device which (i) is intentionally designed to disrupt, disable, harm or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of a Product, or any other associated software, firmware, hardware, computer system or network (sometimes referred to as "viruses" or "worms"), (ii) would disable a Product or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral (sometimes referred to as "time bombs," "time locks," or "drop dead" devices), (iii) would permit Supplier, any Supplier Personnel or any licensor or Contractor to Supplier to access a Product to cause such disablement or impairment (sometimes referred to as "traps," "access codes" or "trap door" devices), or (iv) contains any other similar harmful, malicious or hidden procedures, routines or mechanisms which would cause a Product or any other associated software, firmware, hardware, computer system or network to cease functioning or damage or corrupt data, storage media, programs, equipment or communications or otherwise interfere with operations.

(2) A "Force Majeure Event" is any force majeure event or other condition causing a performance delay to be excused under the Purchase Order.

7. BACKGROUND CHECKS. Subject to mandatory restrictions imposed by applicable Laws, Supplier shall perform background checks on all Supplier Personnel including temporary personnel who will be performing any Services under the Purchase Order. Background checks will consist of, subject to mandatory restrictions imposed by applicable Laws, screened checks for educational history, employment history verification for the past ten (10) years (or such shorter period permitted by Law), credit reference, criminal checks, and a financial/regulatory check including a check of U.S. Government Specially Designated National (OFAC) and export denial lists. Supplier will comply with all applicable Laws related to the background check, including required notices and applicable consents. In addition, Supplier will require the individual to report any criminal convictions. Supplier will not assign anyone to perform Services for FIS who has not authorized or otherwise been subject to a background investigation, or whose background investigation has revealed a negative result. Specifically, in the United States, any individual who has tested positive for drugs or whose background check findings do not meet the standards established by Supplier in accordance with all applicable Laws, including if there is a conviction or referral to a pretrial diversion program for a crime that is related to his or her duties shall not be assigned to the provision of the Products. Supplier acknowledges that under applicable banking Laws, an individual may not participate, directly or indirectly, in any manner in the conduct of the affairs of any insured depository institution without regulatory consent if he or she has a conviction, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution, of a crime involving dishonesty, breach of trust or money laundering, including any crime concerning the illegal manufacture, sale, distribution of or trafficking in controlled substances, unless the crime meets certain criteria for treating the crime as de minimis. The background check must be completed before assignment of an individual and periodically thereafter. Further, if requested by FIS for any reason, Supplier shall immediately remove a Supplier Personnel from the provisionof the Products.

The previous requirements are fulfilled, unless otherwise agreed between Supplier and FIS, if Supplier shares a current certificate of good conduct with FIS prior to the assignment of Supplier Personnel. At its sole discretion FIS has the right to make the start of the Services depending on the completion of the background check or on the submission of the certificate of good conduct.

8. SAFEGUARDING OF INFORMATION.

a. PROTECTION OF FIS CONFIDENTIAL INFORMATION. Supplier must protect all FIS Confidential Information with at least the same degree of care it uses to protect its own confidential information, but in no event will Supplier use less than a reasonable standard of care to protect any FIS Confidential Information.

(1) Supplier will (i) restrict the use and disclosure of FIS Confidential Information to Supplier Personnel and do so solely on a "need to know" basis in connection with Supplier's obligations to provide the Products, (ii) ensure Supplier Personnel who receive or have access to FIS Confidential Information are bound by confidentiality obligations at least as restrictive and as protective of the FIS Confidential Information as the provisions of this PART C, (iii) establish procedural, physical and electronic safeguards, designed to prevent the compromise or unauthorized disclosure of FIS Confidential Information and to achieve the objectives of the Guidelines (if applicable), (iv) not use or disclose any FIS Confidential Information except in accordance with the Purchase Order, (v) promptly investigate any security breach to determine whether such incident has resulted or is likely to result in misuse or unauthorized possession or disclosure of FIS Confidential Information; and (vi) promptly notify FIS of any Breach discovered by Supplier.

(2) In providing any notice of a Breach, Supplier will (i) provide notice in text form to FIS, within twelve (12) hours of discovering the Breach, and (ii) ensure and document that FIS has received the notice, and (iii) keep FIS informed as to the actual and anticipated effects of the Breach and the corrective actions taken or to be taken in response to the Breach. In addition, if the Breach results or is likely to result in misuse of Personal Data, NPI, PHI or payment card data, Supplier will (A) notify FIS as soon as possible and reasonably cooperate with FIS in its efforts to notify affected Clients and their customers and to mitigate the actual or potential harm resulting from the Breach and (B) reimburse FIS for its reasonable costs in notifying Clients or their customers of the Breach and making available to them any credit monitoring services and for any other costs FIS reasonably incurs with respect to the Breach.

(3) FIS Confidential Information will remain the property of FIS, its Affiliate or other party from or through whom it was provided.

(4) Except for Personal Data, NPI, PHI, other information protected by the Privacy Regulations, or any payment card data,

(a) the parties' respective confidentiality obligations under the Purchase Order do not apply to any information that: (i) was previously known by the party; (ii) is a matter of public knowledge; (iii) was or is independently developed by the party; (iv) is released for disclosure with written consent of the party; or (v) is received from a third party to whom it was disclosed without restriction.

(b) each party may disclose information notwithstanding its confidentiality obligations under the Purchase Order to the extent required (i) by Law, (ii) in connection with the tax treatment or tax structure of the Purchase Order; or (iii) in response to a valid order of a court or other governmental body, provided that the party provides the other party with written notice and the other party is afforded a reasonable opportunity to obtain a protective order with respect to the disclosure.

(5) At the end of the Term, or upon the prior termination of the Purchase Order, Supplier will destroy all FIS Confidential Information in a manner designed to preserve its confidentiality, or, at FIS's written request and expense, return it to FIS.

(6) FIS will have and retain all right, title and interest in all FIS Confidential Information, whether possessed by FIS prior to, or acquired or refined by FIS (either independently or in concert with Supplier) during, the Term of the Purchase Order.

(7) If Supplier and FIS are both located in the United States, Supplier will not, without the prior written consent of FIS, (i) provide the Services or access, store or process any FIS Confidential Information outside the United States, or (ii) export any FIS Confidential Information to anywhere outside the United States. These provisions apply without regard to where the Services are provided or FIS Confidential Information is accessed, stored or processed.

(8) If the Products include or contemplate the processing of any European Union Personal Data, Supplier agrees that it will perform such processing solely inside the European Economic Area and shall not process any such data outside of the European Economic Area without the express, specific, prior written consent of FIS. Supplier further acknowledges that additional contractual provisions may be required in such case.

b. CONSUMER INFORMATION AND PRIVACY. If, in connection with the Purchase Order, Supplier receives, stores

or accesses any Personal Data, NPI, PHI or other information or materials that are subject to the Privacy Regulations and Guidelines, Supplier will comply with the applicable requirements of the Privacy Regulations and Guidelines. Supplier acknowledges that the Guidelines include provisions regarding the safeguarding of consumer information, response programs and notice in the event of unauthorized access to consumer information, that FIS provides information processing services to Clients subject to the Guidelines, and that FIS may be required to notify Clients, their customers or other third parties of security incidents that result, or are likely to result, in misuse or unauthorized possession or disclosure of Personal Data, NPI, PHI, payment card data or other Confidential Information. Without limiting the foregoing, Supplier will (i) ensure the security and confidentiality of such information or materials, (ii) protect against any anticipated threats or hazards to the security or integrity of such records, (iii) detect unauthorized access to or use of such records or information, and (iv) protect against unauthorized access to or use of such records or information that would result in harm or inconvenience to any Client or any customer of a Client.

c. SPECIFIC PRECAUTIONS. Supplier represents and warrants that it has and will maintain in place commercially reasonable precautions to safeguard the confidentiality, security and integrity of FIS Confidential Information in a manner designed to meet the requirements of this PART C. These precautions will include but will not be limited to (i) contractual restrictions on access to the information by Contractors and Supplier's other vendors, (ii) intrusion detection systems on all information systems of FIS maintained or controlled by Supplier, and (iii) notification procedures for notifying FIS promptly in the event a security breach is detected or suspected, as well as other response programs when there is a suspected or detected Breach involving Personal Data, NPI, PHI or payment card data. These precautions will also include, as appropriate, (A) access controls to FIS information systems, including controls to identify and permit access only to authorized individuals and controls to prevent access to FIS Confidential Information through improper means, (B) Supplier Personnel controls and training, (C) physical access restrictions at locations where FIS Confidential Information is located, (D) encryption of electronic FIS Confidential Information when appropriate or legally required, and (E) a disaster recovery plan as appropriate and on FIS' request aligned with FIS to protect against loss or damage to FIS Confidential Information due to potential hazards such as fire or water damage or technological failures. Supplier will (1) monitor the foregoing measures with periodic audits or testing and (2) provide copies of the same sufficient to assure FIS or its regulatory authorities that Supplier is implementing these precautions, and (3) notify FIS immediately in the event there is any suspected or actual unauthorized access, use, disclosure or alteration to FIS Confidential Information. Supplier will indemnify FIS from, defend FIS against, and pay any final judgments awarded against FIS, resulting from any claim brought by a third party, including but not limited to a customer of FIS, against FIS based on any breach of such privacy Laws, rules or regulations by Supplier, including Supplier Personnel.

In addition to the foregoing, if Supplier processes or otherwise has access to any Personal Data or personal information on FIS's behalf, including FIS's staff Personal Data, in relation to the Purchase Order or when performing Supplier's obligations under the Purchase Order, Supplier shall only process such data or information on FIS's behalf and not for any other purposes, and Supplier shall process such data and information only in accordance with instructions given by FIS from time to time in accordance with the Purchase Order; likewise, Supplier shall take appropriate technical and organizational measures against unauthorized or unlawful processing of the Personal Data and personal information or its accidental loss, destruction or damage, in accordance with the Purchase Order. For clarity, the mentioned Personal Data shall be treated as FIS Confidential Information hereunder.

d. LOCATION. Supplier personnel will only work from Supplier's registered premises unless otherwise agreed with FIS.

e. CONTROLLED PERSONAL DATA NOTICE. FIS has a Controlled Personal Data Notice which is available for review at http://www.fisglobal.com/Privacy.

f. ADDITIONAL DEFINITIONS.

(1) A "Breach" is an actual or attempted unauthorized (i) access to or (ii) use, possession or release of FIS Confidential Information.

(2) "Personal Data" means any data that identifies an individual or relating to an identifiable individual; for the purposes of this definition, and identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his/her identity (physical, economic, social identity, etc.).

(3) "FIS Confidential Information" is information disclosed in any form in connection with the Purchase Order to Supplier, or to a Supplier Affiliate, any Supplier Personnel, or a Contractor to Supplier, by FIS, an FIS Affiliate or a Client, or by a customer of a Client, regardless of the manner of disclosure (including disclosure by giving access), that

either:

(a) constitutes or contains Personal Data, NPI, PHI, or payment card data, or FIS's employee records (including any FIS employee's name, address, phone number, salary, taxpayer or government identification number, date of birth, health records, bank account information or labor party), or

(b) constitutes or contains (i) FIS's business strategy and direction, (ii) FIS's operating or marketing plans, (iii) memos or other documents or communications pertaining to pending FIS litigation or contracts (including the Purchase Order), (iv) any information disclosed by FIS that is designated as "confidential" at or prior to disclosure, (v) other FIS data or information which is not generally known, including business information, specifications, research, software, trade secrets, discoveries, ideas, know-how, designs, drawings, flow charts, data, computer programs, marketing plans, budget figures, and other financial and business information, or (vi) information of the kind described by any of the foregoing categories that is of or disclosed by a Client, an FIS Affiliate, or a customer of a Client.

(4) The "Guidelines" are the standards and guidelines established pursuant to (i) the Gramm-Leach-Bliley Act of 1999 or a state law equivalent, relating to the protection of nonpublic personal information provided to financial institutions ("NPI"), (ii) the Health Insurance Portability and Accountability Act of 1996 or a state law equivalent, relating to the protection of protected health information ("PHI"), (iii) EU Data Protection Directive and General Data Protection Regulation, (iv) other relevant privacy Laws, or (v) PCI DSS, relating to cardholder data ("payment card data").

(5) The "Privacy Regulations" are the standards, guidelines and other regulations established by various federal or state regulatory agencies to protect the privacy and security of customer or patient information held by financial institutions, medical service Suppliers and other entities including but not limited to the Guidelines.

9. TERMINATION. FIS may terminate the Purchase Order, or any Products, lease or license thereunder, without penalty, (i) at any time upon giving Supplier no less than sixty (60) days prior written notice of its intent to do so or (ii) in the event of a Change in Control of Supplier, immediately upon written notice to Supplier. In the event of any termination by FIS pursuant to this Section d, FIS will be obligated to pay for the Products properly delivered and accepted and the Services successfully completed by Supplier through the effective date of such termination. A "Change in Control" of Supplier is any event or series of events by which (i) any person, entity or group of persons or entities acquires control of Supplier, where "control" is possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of Supplier, whether through record or beneficial ownership of voting securities, by contract or otherwise, or (ii) if Supplier is a corporation, limited liability company or other entity having a board of directors or other group of individuals having similar functions, during any period of twelve (12) consecutive months commencing before or after the date hereof, individuals who at the beginning of such twelve-month period were members of Supplier's board of directors or other such group cease for any reason to constitute a majority of the members.

The right to terminate the Purchase Order, or any Products, lease or license thereunder for good cause remains unaffected for both contracting parties. A good cause for termination may exist in favor of FIS on the basis of the regulatory provisions in particular in the following cases:

a. if the Supplier violates applicable law, legal provisions or contractual provisions; or
b. if obstacles are identified which may alter or prevent the performance of the Supplier or make it impossible to continue to receive the Services by FIS; or
c. if material changes occur that affect the Products or Services or the Supplier (e.g., an unauthorized onward transfer or a regulatory prohibition); or
d. where there are deficiencies in the handling and security of confidential, personal or otherwise sensitive data or information; and or
e. where instructions are issued by the relevant authority of FIS, for example where the relevant authority requires the termination or transfer of the service or is no longer able to monitor FIS or its clients as a result of the Products or Services arrangement.

10. TRAINING. All Supplier Personnel working with FIS' infrastructure have to check the inbox of the respective account every ten (10) business days and in case a training (provided through FIS' Regulatory University RegU or other tools) or a similar task is assigned, Supplier Personnel shall ensure to complete the training or the task within the due deadline. FIS has no obligations to reimburse the Supplier for completion of such trainings and tasks. FIS has the right to terminate the Order with immediate effect if Supplier Personnel fails to complete such trainings and tasks within the due deadline.

11. OBLIGATION TO INFORM. FIS may at its sole discretion and before the beginning of the Services or any time during the Services or up to three (3) years after the Services have ended request from the Supplier and Supplier shall without undue delay furnish FIS with information including but not limited to: FIS Vendor Risk Assessment Survey; Report for recent third party audit completed by organization e.g. ISO 27001:2013 certificate, SSAE 16 Report, etc.; Copy of Professional Indemnity insurance certificate; Background check report of vendor employee(s); latest copy of Balance Sheet along with Profit and Loss Statements; BCP/DR plan along with recent Disaster Recovery test report; Vulnerability Assessment and Penetration Testing Report. FIS has the right to terminate the Order with immediate effect if Supplier fails to inform FIS accordingly upon FIS' request without undue delay.

PART D

OPERATIONAL CONTINUITY AND EXIT

Release December 20th, 2021

1. Definitions.

"FIS Group" means FIS and FIS' Affiliates from time to time;

"Event" means:

(a) the application of any resolution power or resolution procedure to FIS by a Regulator under applicable legislation in force from time to time in order to safeguard public interests, including the continuity of the FIS' critical functions and/or financial stability; or

(b) the execution of any one or more of the options contained in the recovery plan for FIS or FIS' Affiliates submitted to the FIS' Regulator in accordance with such Regulator's rules and guidance.

"**Event Date**" means the date on which an Event occurs;

"**Recipient**" means a person to whom all or part of the business, assets, rights or liabilities of FIS has been transferred;

"Regulator" means a regulatory or quasi regulatory authority empowered by law which regulates FIS in connection with the Services performed by the Supplier, or any replacement or successor body in any relevant jurisdiction from time to time

"Services" (as defined also in Part A) means any services (including Professional Services and Maintenance) delivered by the Supplier under the terms of the Purchase Order.

2. Classification.

2.1. FIS shall notify the Supplier whether the Services performed by the Supplier are internally classified by FIS as per applicable regulations as outsourcing and whether the outsourcing is classified as outsourcing of a critical or important function (any such outsourcing referred to herein as "**Critical Services**"). FIS shall also notify the Supplier if the internal classification changes.

3. Recovery and Events.

3.1. If FIS was, immediately prior to the Event Date, entitled to receive Services pursuant to the Purchase Order and/or receive any other benefit of the Purchase Order (as applicable) (the "**Supply**") and is subject to an Event, then the Supplier shall:

3.1.1. provide all assistance and services required by FIS (or the Regulator) to give effect to and assist in the continuation of the Supply which FIS was receiving prior to the Event on the same terms as applicable immediately prior to the Event Date. FIS shall pay the Supplier for its reasonable costs (including for any time committed) in providing such assistance and services to the extent they are outside of the scope of the Services;

3.1.2. for a maximum period of 12 months from the Event Date (or such longer period specified by a Regulator), not terminate, suspend, withhold or materially alter any Supply provided pursuant to the Purchase Order (regardless of whether such right to terminate, suspend, withhold or materially alter has arisen but has not been exercised prior to the Event Date) unless:

3.1.2.1. the Regulator consents to the termination, suspension, withholding or alteration;

3.1.2.2. the Supplier has the permission of a court of competent jurisdiction; or

3.1.2.3. FIS fails to fulfil its payment obligations under and in accordance with the terms of the Purchase Order.

3.2. The Regulator shall be entitled to enforce the Purchase Order or part of it (as applicable) on behalf of FIS, and the Supplier and each Supplier Affiliate (if relevant) shall act upon directions and instructions given by the Regulator, as if the Regulator were FIS and those directions or instructions were given to the Supplier or the relevant Supplier's Affiliate by FIS.

3.3. If managing an Event involves a transfer of any part of the business of FIS to a Recipient, the terms of Section 4 (Divestment) shall apply.

3.4. FIS shall be entitled to, in accordance with the terms of Section 4 (Divestment), with the consent of the Supplier (such consent not to be unreasonably delayed), novate or transfer its rights and obligations under the Purchase Order to a Recipient (including a "bridge bank" to which the Regulator has directed the

Purchase Order be novated or transferred). The effect of such transfer shall be that the Purchase Order shall be treated as having been originally entered into between the Supplier and the Recipient and the Supplier shall enter into and execute any documentation required by FIS or any Regulator and any such Recipient for the purpose of novating or transferring the Purchase Order and otherwise for giving effect to such novation or transfer subject to Purchase Order of commercial terms (such commercial terms to be negotiated in good faith by the parties and to be in accordance with the Supplier then current standard commercial terms at the time) provided, however, that the Supplier will continue to provide such Services to the Divested Business in accordance with Section 3.1 (below) until the earlier of: (1) such time as the new Purchase Order has been signed; and (2) one year from the date the Divested Business is no longer within the FIS Group. The Supplier acknowledges that following the completion of such novation or transfer the Recipient shall be entitled to exercise any of its rights set out in this Section 2 (Recovery and Resolution) and Section 4 (Divestment).

4. Divestment

4.1. If FIS sells, transfers or otherwise disposes off, as a result of an Event, any Affiliate of FIS or any part of the business of any Affiliate of FIS that is directly receiving the benefit of the Services (the "**Divested Business"**) at the date of the sale or disposal ("**Disposal Date"**) to a Recipient which is not and is not intended to become an Affiliate of FIS, then the Supplier shall at the request and choice of FIS or the Regulator (if applicable) either:-

4.1.1. provide all assistance and services (including signing all documents) required by FIS (or the Regulator) to give effect to and assist in the continuation of the Supply which the Divested Business was receiving prior to the Disposal Date for a period requested by FIS and/ or the Regulator not exceeding one year. During that period and subject to the payment by FIS to the Supplier of Supplier's reasonable costs in providing such assistance and services to the Divested Business to the extent that the services and assistance are outside of the scope of the Services, the Divested Business will be entitled to receive the Services on the same terms as applicable immediately prior to the Disposal Date; or

4.1.2. promptly enter into a direct agreement with the Divested Business subject to agreement of commercial terms (such commercial terms to be negotiated in good faith by the parties and to be in accordance with Supplier's then current standard commercial terms at the time) for a separate Software License and the supply of Services on operational terms that are the same as the Purchase Order mutatis mutandis provided, however, that the Supplier will continue to provide such Services to the Divested Business in accordance with sub-Section 4.1.1 above until the earlier of: (1) such time as the new agreement has been signed; and (2) one year from the Disposal Date;

4.2. Under Section 4.1.1, the Divested Business shall continue to enjoy the rights and benefits it is entitled to under the Purchase Order as if it were still a part of the FIS' business or an Affiliate of FIS, provided that whilst the Divested Business is deemed to remain a member of FIS' Group, FIS shall remain fully liable for the acts and omissions of the Divested Business and shall be responsible for the compliance of such Divested Business with the terms and conditions of the Purchase Order, as if such Divested Business were a party hereunder and the Divested Business shall not itself be entitled to enforce the Purchase Order against the Supplier.

4.3. In order to achieve the efficient and effective transition of the Divested Business to a Recipient, subject to payment by FIS of all reasonable fees as agreed between the parties, the Supplier shall provide all assistance and services reasonably requested by FIS with respect to such transition, which shall include such assistance as FIS (or the Regulator) may consider to be appropriate in the circumstances.

4.4. The Purchase Order shall remain in full force and effect in respect of any part of the business of any Affiliate of FIS which is not divested pursuant to this Section 4 (Divestment).

4.5. The parties may disclose to any Recipient any Confidential Information which relates to the performance of the Services to the extent necessary for the Recipient to use or receive the Services pursuant to this Section 4 (Divestment).

5. Audit.

5.1. **Outsourcing Generally**. The Supplier will cooperate with FIS to meet its responsibilities to perform due diligence and assess the Supplier as its third-party technology service provider. This includes cooperating with Regulators, including other persons appointed by them. FIS shall at all times have regard to the principle of proportionality and take a risk-based approach to exercising the rights set out in this Section 5.

5.2. **ISAE 3402/IDW PS 951Audit**. The Supplier shall cause an independent public accounting firm to perform the audits (generally ISAE 3402) with respect to the Solution being provided under the Purchase Order

which the Supplier has agreed to be in scope for such audits. The Supplier shall make available to FIS a copy of the resulting independent audit report(s) relevant to the Purchase Order. The Supplier shall promptly address and resolve any mutually agreed upon deficiencies identified in such audit report(s).

5.3. **Governmental Access**. The Supplier shall permit Regulators to examine Supplier's books and records to the same extent as if the Solution was being performed by FIS on its own premises, subject to Supplier's confidentiality and security policies and procedures.

5.4. **Client Questionnaires**. Questionnaires may be submitted to the Supplier for completion no more than once annually and contain fifty (50) or less questions in total. Additional questionnaires or questionnaires exceeding fifty (50) questions will incur an additional fee based on the time spent by the Supplier answering the additional questions, at Supplier's then prevailing Professional Services fee rates.

5.5. **Dedicated Audit Visit**. FIS shall be entitled to conduct a non-duplicative, dedicated on-site audit visit annually in accordance with Supplier's then current on-site audit guidelines, which include the following:

FIS may visit the Supplier processing facility that provides the Solution to FIS once per calendar year, unless the audit visit serves to verify the remediation of a previous adverse audit finding or unless a Regulator expressly (in writing) requires more frequent visits.

Requests for any on-site audit visit shall be made in writing by FIS at least sixty (60) days in advance (unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective or if shorter notice is given by the Regulator or specifically required by the relevant regulatory obligation, in which case FIS 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 visit. Where the audit is due to a Regulator requirement, the request for audit shall also detail the applicable requirements under which the Regulator requires the visit and/or information from FIS, including details of the relevant regulation or regulatory obligation which necessitates such request.

On-site audit visits shall be conducted during normal business hours for the facility and shall be coordinated with the Supplier so as to cause minimal disruption to the Supplier's business operations.

All on-site audit visits must be reasonable in scope and duration, shall not last more than two (2) business days, and shall be conducted at the expense of FIS. In addition, FIS shall bear the cost of all of Supplier's' representatives' time and out-of-pocket costs incurred for assisting FIS or Regulator in such audit.

Any FIS initiated on-site audit visit shall be performed by FIS' employees and/or a reputable third-party auditor agreed to by both parties, it being understood that FIS (and its representatives) shall at all times be bound by the confidentiality provisions of this Purchase Order and shall be accompanied by a representative of FIS.

Due to COVID-19, the on-site audit may be held virtually.

Except as prohibited by applicable law or the relevant Regulator, the Supplier shall receive and be entitled to comment on any report prepared by or on behalf of FIS prior to that report being published or disseminated (such report to be Supplier's Confidential Information except to the extent it relates to the business or affairs of FIS, which information will be FIS Confidential Information), which publication or dissemination shall be done only pursuant to the confidentiality provisions of this Purchase Order.

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. The Supplier does not allow any form of direct security testing initiated by clients or on behalf of clients, 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 Supplier systems, applications, databases, or networks, except as may otherwise be agreed by the Supplier Chief Information Security Officer and/or designee in writing and signed by both Parties. The Supplier will not acknowledge any results from any form of security testing that is not performed by the Supplier. The Supplier will provide FIS and any Regulator with access to a summary of its annual vulnerability assessment findings as per the Section "Patch and Vulnerability Management" in the Supplier Information Security and Data Protection Statement.

5.6. **Access to Data**. In case of insolvency, resolution or discontinuation of business operations of the Supplier, the possibility for FIS to access the data owned by FIS shall be ensure. To do so the Supplier shall notify FIS without delay the insolvency, the resolution or the discontinuation of business operations and shall do everything necessary on its part to ensure FIS' ability to access or migrate the data.

5.7. **Access in relation to Critical Services**. In addition, in relation to Critical Services, the Supplier shall grant to FIS and its Regulators (a) full access to all relevant business premises (e.g. head offices and operation centers), including the relevant devices, systems, networks, information and data used for providing the Critical Services, including related financial information, personnel and the service provider's external

auditors reports; and (b)unrestricted rights of inspection and auditing related to the outsourcing arrangement, to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

5.8. **Principle of Proportionality**. FIS shall at all times have regard to the principle of proportionality and take a risk-based approach to exercising any of the rights set out in this Section (Audit).

5.9. **Compliance with FIS Policies**. While exercising the access and audit rights under this Section (Audit), Supplier shall comply with FIS' reasonable confidentiality and security policies and procedures.

5.10. **Cost of Audits**. All access and audit rights under this Section (Audit) shall be conducted at the expense of FIS. In addition, FIS shall bear the cost of all of Supplier's representatives' time and out-of-pocket costs incurred for assisting FIS or its Regulators in exercising such access and audit rights.

6. Monitoring.

6.1. FIS has the right to monitor Supplier's performance of Services on an ongoing basis.

7. Supplier's obligation to inform.

7.1. The Supplier shall assume the duty of ongoing, internal control (identification, testing and elimination of errors/defects; "ongoing control") of the outsourced area. The Supplier will inform FIS without undue delay after it becomes aware that a development may have a material impact on Supplier's ability to effectively provide Services that constitute a critical or import function for FIS in line with agreed service levels, applicable laws and regulatory requirements. The Supplier shall report significant errors/defects ("significant defects") and their processing/elimination to the FIS without delay. In addition, the contractor shall report any other developments that may affect the proper completion of the outsourced activities and processes.

8. Location information.

8.1. As at the Order Effective Date, the Solution will be hosted by the Supplier and Supplier's subcontractor's datacentres from the following locations:

8.2. Upon written request from FIS for details of the same, the Suppliers shall notify FIS of any change or addition to the locations stipulated above, however, the Supplier shall not change the location of the hardware infrastructure from which any Hosting Services, ASP Solution, BPaaS Solution or SaaS Solution element of the Services are provided ("**Hosting Services Infrastructure**") without providing prior notice to FIS. If the location of the Hosting Services Infrastructure is to change to a location outside the: (i) United Kingdom; or (ii) European Economic Area, and FIS objects to such change in location (by notice in writing to the Supplier): (i) on the basis of a need to comply with the requirements of a Regulator; and (ii) within thirty (30) days of notification from the Supplier of such change, the parties shall work together in good faith to address the objection. If the parties cannot agree on a resolution to the objection or if a Regulator determines that the relevant Services still do not meet the requirements of the Regulator, then either party may terminate the Purchase Order or relevant part thereof by providing at least thirty (30) days' prior written notice to the other party.

9. Termination on instruction from a Regulator.

9.1. If a Regulator instructs FIS to terminate the Purchase Order or relevant part thereof then FIS may terminate the Purchase Order, or relevant part thereof, subject to: (i) providing at least thirty (30) days' (or such shorter period as dictated by the Regulator) prior written notice to the Supplier; (ii) providing to the Supplier full details of the Regulator's instruction to terminate along with reasonably detailed evidence to support such instruction; and (iii) receipt by the Supplier of payment by FIS of all fees that otherwise would have been due under the Purchase Order had termination not occurred pursuant to this Section 9.

10. Termination

10.1 In the event of a full or partial termination of the Purchase Order by one of the parties, whether by notice of termination or by rescission, FIS may demand the continuation of the performance of the Services under the contractual conditions.

In the event of termination by the Supplier, FIS must exercise this right within one month of receipt of his declaration of termination. Within a further period of up to three months before the termination takes effect, FIS shall notify the Supplier of the date by which the Supplier must provide its Services.

In the event of termination by FIS, FIS shall declare at the same time as the termination whether and, if so, until what time it requires the Services of the Supplier beyond the time of the effectiveness of the termination.

The Supplier shall continue to provide its Services for a maximum of one year after the termination date.

10.2 In the event of termination the Supplier shall furthermore:

a. facilitate a transfer of the outsourced activities to another outsourcing company or a transfer back to FIS and support FIS in doing so,

b. avoid interruptions or other impairments of the FIS' business operations during the transfer of the outsourced activities to another outsourcing company or a transfer back to FIS.

c. promptly designate a contact person for the issues arising in connection with the transfer of the outsourced activities to another outsourcing company or a transfer back to FIS; and

d. conclude a corresponding agreement with FIS on the services to be provided by the Supplier in connection with the transfer of the outsourced activities to another outsourcing company or a transfer back to FIS ("**Termination Support**").

10.3 Upon termination the Supplier shall also be obliged to make the application data stored by FIS and, if applicable, any other stored data available to FIS or to a third party designated by FIS on a permanently readable mobile and audit-proof data carrier or by way of remote data transmission in a data format to be agreed between the parties. At FIS' request, the Supplier shall irrevocably delete all of the FIS' remaining data files. In addition, the Supplier shall, within a period of up to three months after the termination, instruct the employees of FIS or the third party with regard to the outsourced service.

10.4 The Supplier reserves the right to charge FIS for the necessary and proven costs and expenses incurred by it for the Termination Support. The costs for the Termination Support shall be determined in accordance with the purchase order. In the event of termination by the Supplier, the Supplier shall provide termination support up to 20 person days free of charge for FIS.

PART E

Release December 20th, 2021

1. Access, information and audit rights

The Supplier grants the right to gather information and the power to investigate to competent authorities and resolution authorities under Article 63(1)(a) of Directive 2014/59/EU and Article 65(3) of Directive 2013/36/EU.

The Supplier grants FIS and FIS' Clients and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, full access to all relevant business premises (e.g. head offices and operation centers), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service Supplier's external auditors ('access and information rights'); and unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

Nothing in the Purchase Order or any other agreement between FIS and Supplier shall impede or limit the effective exercise of the access and audit rights by FIS, FIS' Clients, competent authorities or third parties appointed by them to exercise these rights.
FIS or FIS' Clients may use pooled audits organized jointly with other Clients of FIS, and performed by FIS and Clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organizational burden on both FIS', the Clients and the Supplier; and third-party certifications and third-party or internal audit reports made available by the Supplier. The activities of the internal audit with regard to the outsourced area including the examination of the proper implementation of the ongoing control shall be carried out by the Supplier. The Supplier grants FIS the right to carry out its own audits by its internal audit department or an auditor appointed by FIS in the Supplier's company. The Supplier grants FIS' auditor an unrestricted right of audit in relation to the outsourced area. The Supplier assures to comply with the current and future principles for the organization of internal auditing to be observed under banking supervisory law in the organization of its internal auditing (in particular in accordance with the Minimum Requirements for Risk Management - MaRisk - of BaFin in their respective version) and undertakes to align the assigned auditing activities with these principles and to provide FIS with corresponding evidence on an annual basis.

The Supplier shall grant FIS the right to monitor the Supplier's performance on an ongoing basis (at least quarterly). The Supplier shall be obliged to prepare and send a report to FIS within the scope of its performance. The form and the interval of the reporting are regulated between the parties. The Supplier undertakes to provide FIS with
- findings of the internal audit on material deficiencies without being requested to do so and without delay, and
- information on the rectification of identified material deficiencies or deficiency rectification plans in a form and within a period appropriate to the respective deficiency without being requested to do so.
- and to make the aforementioned documents available to BaFin and the bank's auditor - in each case upon request.

In addition, the internal audit of the Supplier shall inform the internal audit of FIS annually about relevant audit activities (if applicable/planning) and any material results regarding the outsourced area, if applicable in summarized form. FIS shall also have the right to carry out security penetration testing to assess the effectiveness of implemented cyber and ICT security measures and processes.

Moreover, the Supplier shall assume the duty of ongoing, internal control (identification, testing and elimination of errors/defects; "ongoing control") of the outsourced area. The Supplier shall as well report significant errors/defects and their processing/elimination to FIS without delay. In addition, the Provides shall report any other developments that may affect the proper completion of the outsourced activities and processes.

FIS shall before a planned on-site visit, provide reasonable notice to the Supplier, unless this is not practicable or not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.

2. Sub-outsourcing

Sub-outsourcing of critical or important tasks or functions is not permitted without prior specific written authorization from FIS.

The Supplier informs FIS of any planned sub-outsourcing, or material changes thereof, where that might affect the

ability of the Supplier to meet its responsibilities under the Purchase Order. This includes planned significant changes of sub- contractors and at least a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect.

FIS has the contractual right to terminate the Purchase Order in the case of undue sub-outsourcing, e.g. wherethe sub-outsourcing materially increases the risks for FIS or FIS' Clients or where the Supplier sub-outsourceswithout notifying FIS.

FIS shall agree to sub-outsourcing only if the sub-contractor undertakes to comply with all applicable laws, regulatory requirements and contractual obligations; and grants FIS and FIS' Clients and competent authority the same contractual rights of access and audit as those granted by the Supplier.

3. Place of Performance

The performance of a critical or essential function takes place exclusively in Germany.
The storage or processing of the data takes place exclusively within the European Union. In case the place of performance of a critical or essential function or the storage or processing of the data is not in the European Union the Supplier shall ask the written consent of FIS.

FIS shall be informed in good time prior to the execution of a change of location at which critical or essential functions are performed or data are stored and/or processed.

The storage or processing of the data takes place exclusively within the European Union.

4. Termination rights

FIS has the right to terminate the Purchase Order, in accordance with the Purchase Order Terms and applicable law, including in the following situations:

a. where the Supplier is in a breach of applicable law, regulations or contractual provisions;

b. where impediments capable of altering the performance of the outsourced function are identified;

c. where there are material changes affecting the Purchase Order or the Supplier (e.g. sub-outsourcing or changes of sub-contractors);

d. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and

e. where instructions are given by the FIS' or FIS' Client's competent authority, e.g. in the case that the competent authority is, caused by the Services provided by Supplier, no longer in a position to effectively supervise FIS' Client.

The Supplier is obliged to support FIS in the orderly transfer of Services in the event of the termination of thePurchase Order.

PART F

Central Outsourcing Management

Release December 20th, 2021

ADDITIONAL REQUIREMENTS RELATING TO OUTSOURCING - GERMANY

In the event that the FIS classifies the services provided by the Supplier to the FIS in accordance with the terms of this Purchase Order as Outsourcing Services pursuant to **Circular 10/2017 – Regulatory requirements for IT – BAIT** and **10/2021 (- Minimum Requirements for Risk Management - MaRisk ("Circular 10/2017-10/2021")** ("Outsourcing"), the parties agree that the following additional provisions shall apply to such Outsourcing. For the avoidance of doubt, the parties agree that (1) the procurement of software, including any third party software or updates and services thereof and (2) the procurement of hardware and (3) third party services not qualified as Sub-Outsourcing Service Providers (as defined below) do not fall within the scope of the Material Outsourcing and therefore the provisions of Part E below do not apply.

1. Performance description

The Services that may be considered as Substantial Outsourcing are described in detail in the context of this Part F, including all Purchase Order.

2. Appropriate outsourcing control by the Supplier

The Supplier will use reasonable efforts to assist FIS in its outsourcing control obligations with respect to the services provided by the Supplier that may be classified as Material Outsourcing ("Outsourcing Control") by providing FIS with access to the information described in more detail in this Section 2.

a) To request an Audit, FIS must provide the Supplier with at least six (6) weeks prior to the proposed Audit date, submit a detailed Audit plan in writing. The audit plan must show the proposed scope, duration and start date of the Audit, as well as an estimate of Supplier's contribution (resources, effort, etc.). The Supplier will review the audit plan and provide FIS with any concerns or questions (e.g., requests for information that may affect the Supplier's security, privacy, employment, or other relevant policies). The Supplier will work with FIS to agree on a final audit plan. The Supplier will not unreasonably reject the final Audit plan.

b) If FIS engages an external auditor (such as an independent auditor or appointed auditors of the relevant regulatory authority as defined in Circular 10/2017-10/2021 ("Regulatory Authority") or any other relevant authority) to conduct the Audit, the parties must agree in advance (at least six (6) weeks prior to the proposed Audit Date) on such external auditor and such external auditor must enter into a confidentiality agreement acceptable to the Supplier prior to conducting the Audit.

c) The Audit must be conducted during regular business hours at the respective office, always in full attendance, in compliance with Supplier's policies, and must not unreasonably interfere with Supplier's business activities.

d) FIS will provide the Supplier with all Audit reports generated in connection with an Audit under this Section 2, unless prohibited by law. FIS may use the Audit Reports only for the purpose of fulfilling its obligations pursuant to the Outsourcing Control. The Audit Reports shall be treated as confidential information of the Parties for purposes of this Part F.

3. Unlimited information and review rights of the regulatory authority

To the extent required under this Part F, the Supplier shall grant the relevant Regulatory Authority an unrestricted right to information and review. Supplier agrees to tolerate without restriction any information gathering, investigative powers and examination measures of BaFin and other competent supervisory and resolution authorities as well as bodies appointed by them to conduct examinations with regard to the outsourced area. If Supplier has its registered office or the place of performance in a country which is not a member of the European Union, Supplier undertakes to recognize the aforementioned rights and powers also outside the European Union. Unless otherwise agreed in writing by the parties, the parties consider the following approach, taking into account the scope of the Material Outsourcing, to be appropriate:

a) To request an Audit, the Regulator shall submit a detailed Audit plan in writing to the Supplier within a reasonable period of time prior to the proposed audit date (typically six (6) weeks, which shall be considered reasonable). The audit plan should ideally identify the proposed scope, duration and start date of the Audit, as well as an estimate of Supplier's contribution (resources, effort, etc.).

The Regulator may grant Supplier the right to review the Audit Plan and communicate any concerns or issues (e.g., requests for information that may affect Supplier's security, privacy, employment or other relevant policies) to the Regulator. Supplier will work with the Regulator to agree a final Audit plan.

b) The Audit must be conducted during regular business hours at the respective office, always in full attendance, in compliance with Supplier's policies, and must not unreasonably interfere with Supplier's business activities.

c) Supplier or the Regulatory Authority shall make available to FIS any Audit reports generated in connection with an Audit under this Section 3, unless prohibited by law. Supplier may use the Audit reports only for the purpose of complying with its regulatory Audit requirements and/or to comply with the requirements of this Part E. The Audit reports shall be treated as confidential information of the parties within the meaning of this Part E.

4. Rights of instruction

Within the scope of their management decisions and duties relevant under banking supervision law, FIS shall have the right to issue instructions to the Supplier. The Supplier shall carry out these instructions accordingly.

5. Data protection compliance

The Parties agree that the provisions of the Data Protection Agreement (Part G1/G2/G3) adequately and sufficiently address all applicable data protection and security requirements that may apply to the Material Outsourcing.

6. Termination rights and reasonable notice periods

In addition to the termination rights set forth in the Part D, Section 7(c) (below) applies to the Material Outsourcing.

7. Subcontracting

a) FIS agrees that the Supplier shall have the right to subcontract or subcontract the Purchase Order (or any part thereof) previous FIS' prior written consent with FIS under the restriction of Part E-2, provided that the Supplier has entered into written agreements with such subcontractors that enable the Supplier to perform its obligations according to the same standards and in the same quality as agreed between FIS and the Supplier. This requires, in particular, that the subcontractors contractually assume the duties of the contractor to such an extent that FIS, its internal audit, auditor or BaFin can, if necessary, directly assert their rights granted under the agreements between FIS and the Supplier. In the event of a further transfer, the Supplier shall continue to be obliged to report to FIS. FIS shall be informed in writing at least (8) eight weeks prior to the execution of a transfer to a subcontractor, stating the suitability and reliability of the subcontractor as well as a precise description of the activities to be transferred. FIS may request further information from the Supplier for the purpose of assessment. Furthermore, the Supplier shall expressly state which of the following reasons for outsourcing apply:
   - optimisation of business functions and processes,
   - cost savings,
   - expertise of the appointed subcontractor in the field of administration or in certain markets or with certain assets or access of the appointed party (subcontractor) to global trading opportunities.

b) The Supplier will maintain a list of such subcontractors whose service is considered a Material Outsourcing within the meaning of Circular 10/2017-10/2021 ("Sub- Outsourcing Service Provider"), which may be accessed by FIS in accordance with the terms of the Purchase Order.

c) If FIS raises a reasonable objection in writing to the Supplier against a Sub-Outsourcing Service Provider, the Supplier shall be entitled to continue to engage such Sub-Outsourcing Service Provider irrespective of such objection and without any liability to FIS. However, FIS reserves the right to terminate the Purchase Order upon at least three (3) months' written notice to the end of the year, subject to payment of a 50% termination fee for the remainder of the term during which ordinary termination is not possible.

d) In the event of further outsourcing, Supplier shall also be obliged to obtain corresponding service provider reports from the sub-service providers commissioned by it for the commissioned further outsourcing and to make them available to FIS. For the purpose of an overall risk assessment of the outsourced service, the report on the activity of the sub-service provider should be included in the service provider report of Supplier.

8. Information obligations of the Supplier

To the extent reasonable, the Supplier will inform FIS without undue delay if the Supplier is no longer able to perform the agreed services in accordance with the Purchase Order.

PART G1

Vendor Data Processing Addendum
Controller to Processor

THIS DATA PROCESSING ADDENDUM is entered into as of the Addendum Effective Date by and between: (1) [INSERT FIS ENTITY] with an address at [INSERT ADDRESS] ("**FIS**"); and (2) [INSERT VENDOR ENTITY] with an address at [INSERT ADDRESS] ("**Vendor**").

1. INTERPRETATION

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

(a) **"Addendum Effective Date"** means [the effective date of the Agreement] **OR** [INSERT SPECIFIC EFFECTIVE DATE].

(b) "**Agreement**" means the [INSERT TITLE OF AGREEMENT] entered into by and between the parties on [DATE] **OR** [or around the date of execution of this Data Processing Addendum].

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

(d) "**Data Protection Laws**" means: (i) the GDPR; and (ii) to the extent applicable, the data protection or privacy laws of any other country.

(e) "**Data Subject**" means the identified or identifiable natural person to whom FIS Personal Data relates.

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

(g) "**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

(h) "**FIS Affiliates**" means any companies which are controlled by FIS, which control FIS or which are under common control with FIS and either: (i) are Controllers of any FIS Personal Data; and/or (ii) on whose behalf Vendor and/or any Subprocessor otherwise processes any FIS 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.

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

(j) "**GDPR**" means the UK GDPR and/or EU GDPR (as applicable), together with any applicable implementing or supplementary legislation in any member state of the EEA or the UK (including the UK Data Protection Act 2018). References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(k) "**Personal Data Breach**" means any actual or reasonably suspected 'personal data breach' (as defined in Article 4(12) of the GDPR).

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

(m) "**Relevant Body**":

(i) in the context of the UK GDPR, means the UK Information Commissioner's Office; and/or

(ii) in the context of the EU GDPR, means the European Commission.

(n) "**Restricted Country**":

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

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

that the Relevant Body has not deemed to provide an 'adequate' level of protection for Personal Data pursuant to a decision made in accordance Article 45(1) of the GDPR.

(o) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Personal Data to any person in a Restricted Country, which would be prohibited without a legal basis therefor under Chapter V of the GDPR.

(p) "**Security Requirements**" means FIS' information security policies and procedures for its suppliers attached hereto as Annex 3 (*Security Standards*), as may be updated from time to time by mutual agreement of the Parties.

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

(r) "**Standard Contractual Clauses**":

(i) in the context of a Restricted Transfer originating in the UK, means the standard contractual clauses approved by the European Commission pursuant to Commission Implementing Decision (EU) 2010/87, as set out in full in Annex 4 (*Standard Contractual Clauses For Restricted Transfers Originating in the UK*); and

(ii) in the context of a Restricted Transfer originating in the EEA, 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 in Annex 5 (*Standard Contractual Clauses For Restricted Transfers Originating in the EEA*).

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

(t) "**Supervisory Authority**":

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

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

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

(v) "**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).

1.2. In this Data Processing Addendum:

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

(b) unless otherwise defined in this Data Processing Addendum, all capitalised terms in this Data Processing Addendum shall have the meaning given to them in the Agreement; and

(c) any reference to any statute, regulation or other legislation in this Data Processing Addendum 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 FIS PERSONAL DATA

2.1. In the course of Vendor providing the Services under the Agreement, Vendor may from time-to-time Process FIS Personal Data supplied to it by or on behalf of FIS or an FIS Affiliate. The parties acknowledge and agree that, in relation to any FIS Personal Data provided or made available to Vendor for Processing in connection with the Services, **FIS is the Controller** and **Vendor is a Processor** for the purposes of the GDPR.

2.2. Vendor shall:

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

(b) not Process FIS Personal Data other than:

(i) on FIS' written instructions (including the instruction set out in Section 2.4); or

(ii) as otherwise strictly required by applicable laws.

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

(a) any Processing to be carried out under Section 2.2(b)(ii); and

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

before the relevant Processing of that FIS Personal Data.

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

2.5. Annex 1 (*Data Processing Details*) sets out certain information regarding Vendor's Processing of FIS Personal Data as required by Article 28(3) of the GDPR. The parties may from time to time amend Annex 1 (*Data Processing Details*) by mutual agreement.

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

3. VENDOR PERSONNEL

Vendor shall take reasonable steps to ensure the reliability of any Vendor's Personnel who may Process FIS Personal Data, including ensuring:

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

(b) that all such individuals have been vetted by Vendor 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, Vendor shall implement appropriate technical and organisational measures in relation to FIS Personal Data to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2. In assessing the appropriate level of security, Vendor shall take 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 4.1 and 4.2, Vendor shall, and shall cause each Subprocessor to, comply with the Security Requirements.

4.4. On FIS' request, Vendor shall (promptly following such request) provide to FIS written information describing in reasonable detail the technical and organisational measures taken by Vendor in relation to FIS Personal Data pursuant to Section 4.1.

5. SUBPROCESSING

5.1. Vendor may continue to use those Subprocessors already engaged by Vendor as at the date of this Data Processing Addendum which are listed in Annex 2 (*Subprocessors*), subject to Vendor meeting or having met the obligations set out in Section 5.3.

5.2. Subject to Section 5.1, Vendor shall not appoint any new Subprocessors without obtaining FIS' prior approval in writing (such approval not to be unreasonably withheld or delayed).

5.3. With respect to each Subprocessor appointed by Vendor, Vendor shall:

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

(b) ensure that the arrangement between Vendor and the Subprocessor is governed by a written contract including terms which offer at least the same level of protection for FIS Personal Data as those set out in this Data Processing Addendum.

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

(a) a list of the then-current Subprocessors engaged by Vendor, together with all relevant information relating to each such Subprocessor as shown in Annex 2 (*Subprocessors*); and

(b) written certification that the arrangements between Vendor and such Subprocessors meet the requirements set out in Section 5.3.

5.5. Vendor shall be liable for the acts and omissions of all Subprocessors under or in connection with this Data Processing Addendum.

6. DATA SUBJECT RIGHTS

6.1. Taking into account the nature of the Processing, Vendor shall assist FIS by implementing appropriate technical and organisational measures to enable FIS 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).

6.2. Vendor shall:

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

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

7. PERSONAL DATA BREACH

7.1. Vendor shall notify FIS without undue delay (and in any event within forty-eight (48) hours) upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting FIS Personal Data, providing FIS with sufficient information to allow it 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 Vendor to FIS pursuant to Section 7.1 shall include (to the extent available to Vendor 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. Vendor shall provide regular updates to FIS in respect of the resolution of any Personal Data Breach.

7.4. Vendor 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 each such Personal Data Breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Vendor shall provide reasonable assistance to FIS with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which FIS 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 FIS Personal Data by, and taking into account the nature of the Processing by, and information available to, Vendor.

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 FIS Personal Data (the "**Cessation Date**"), Vendor shall immediately cease all Processing of the FIS Personal Data for any purpose other than for storage in accordance with this Section 9.

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

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

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

9.3. Vendor 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 FIS Personal Data returned pursuant to Section 9.2(a), Vendor shall delete, and procure the deletion of, all other copies of FIS Personal Data Processed by Vendor and/or any Subprocessor.

9.5. Vendor and any Subprocessor may retain certain FIS 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 Vendor shall:

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

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

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

(d) ensure that such FIS 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, Vendor 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, Vendor shall make available to FIS all information reasonably necessary to demonstrate Vendor's compliance with the obligations laid down in this Data Processing Addendum and applicable Data Protection Laws. This could be in the form of mutually agreed third party certifications of industry standard.

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

10.3. FIS shall give Vendor reasonable notice of any audit or inspection to be conducted under Section 10.1, and Vendor 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(b)(i) or (ii) below), and FIS has given notice to Vendor 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 Vendor 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 Vendor's compliance with this Data Processing Addendum (including follow-up audits); or

(ii) FIS is required or requested to carry out 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 Vendor has failed to comply with its obligations under this Data Processing Addendum, FIS shall notify Vendor and Vendor 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 Vendor and/or any Subprocessor failed to comply in any material respect with the provisions of this Data Processing Addendum, in which case Vendor shall reimburse all reasonable and documented costs incurred by FIS in connection with such inspection or audit.

11. RESTRICTED TRANSFERS

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

11.2. Notwithstanding the generality of Section 11.1, the parties agree that to the extent FIS transfers FIS Personal Data to Vendor 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 relevant Standard Contractual Clauses shall be entered into by and between FIS as the "data exporter" and Vendor as the "data importer" with effect from the Addendum Effective Date.

12. CHANGE IN LAWS

12.1. FIS may propose any variations to this Data Processing Addendum which are necessary to address the changing requirements of any Data Protection Laws (including any updates to the Standard Contractual Clauses 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 that FIS considers (acting reasonably) that any failure to agree its proposed variations to this Data Processing Addendum may cause FIS to be in material breach of Data Protection Laws, FIS may terminate the Agreement in its entirety upon written notice to Vendor with immediate effect and without liability to Vendor.

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

13. INCORPORATION AND PRECEDENCE

13.1. This Data Processing Addendum 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 Data Processing Addendum and the Agreement, this Data Processing Addendum shall prevail; or

(b) any Standard Contractual Clauses entered into pursuant to Section 10.5 and this Data Processing Addendum and/or the Agreement, those Standard Contractual Clauses shall prevail.

Signed by _____	Signed by _____
for and on behalf of **[INSERT FIS ENTITY]**	for and on behalf of **[INSERT VENDOR ENTITY]**
Date: _____	**Date:** _____

Annex 1

Data Processing Details

Vendor's activities

[INSERT DESCRIPTION OF VENDOR'S ACTIVITIES RELEVANT TO THE SERVICES]

Subject matter and duration of the Processing of FIS Personal Data

The subject matter and duration of the Processing of the FIS Personal Data are set out in the Agreement and the Data Processing Addendum.

The nature and purpose of the Processing of FIS Personal Data

Vendor will process the FIS Personal Data to deliver the Services pursuant to the Agreement.

The types of FIS Personal Data to be Processed

☐ Contact data (e.g. name, email address, postal address)

☐ Identification data (e.g. date of birth, nationality, social security number)

☐ Solution log in and usage data

☐ Bank account data

☐ Financial data

☐ Contract and deal data (e.g. contractual/legal/financial relationship information)

☐ Billing and payments data

☐ Disclosed information from third parties (e.g. credit reference agencies or from public directories)

☐ Other; please specify: _____

The categories of Data Subjects to whom the FIS Personal Data relates

☐ FIS' and FIS Affiliates' employees

☐ FIS' and FIS Affiliates' customers

☐ FIS' and FIS Affiliates' potential customers

☐ FIS' and FIS Affiliates' suppliers

☐ Contact persons

☐ Other; please specify: _____

Authorised Subprocessors

FIS authorises Vendor to appoint the Subprocessors listed in Annex 2 (*Subprocessors*).

Data retention

Vendor will delete the FIS Personal Data from its systems on expiry or termination of the Services in accordance with Section 9 of the Data Processing Addendum.

Annex 2

Subprocessors

Subprocessor (full legal entity name)	Processing activities	Categories of FIS Personal Data	Location (full address)
[INSERT]	[INSERT]	[INSERT]	[INSERT]

Annex 3

Security Standards

[If the Security Standards are already set out in the MSA, please delete the Security Standards below and insert "As described in Section [x] (Information Security Requirements) of the Master [Service] Agreement."]

1. **DEFINITIONS.**

An "**Affiliate**" of a party is an entity which, directly or indirectly, controls, is controlled by, or is under common control with that party, where "control" of the party or other entity means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the party or other entity, whether through record or beneficial ownership of voting securities, by contract, or otherwise.

"**Business Days**" means any day from Monday to Friday on which FIS is open for business at the applicable FIS location(s) under the Agreement.

A "**Change in Control**" of Vendor is any event or series of events by which (i) any person, entity or group of persons or entities acquires control of Vendor, where "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of Vendor, whether through record or beneficial ownership of voting securities, by contract, or otherwise, or (ii) if Vendor is a corporation, limited liability company or other entity having a board of directors or other group of individuals having similar functions, during any period of twelve (12) consecutive months commencing before or after the date hereof, individuals who at the beginning of such twelve-month period were members of Vendor's board of directors or other such group cease for any reason to constitute a majority of the members.

A "**Claim**" is any action, litigation, or claim for which a party is subject to an indemnification obligation under the Agreement.

A "**Client**" is any current or prospective client or customer of FIS or an FIS Affiliate.

The "**Confidential Information**" of a party is any information received from the party that is of a confidential nature or is designated as 'confidential' at or prior to disclosure.

A "**Contractor**" to a party is any individual (other than the party or an employee of the party), corporation or other entity providing services to or on behalf of the party, including any direct or indirect independent contractor or subcontractor to the party.

"**Control**" of a legal entity is the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity, whether through record or beneficial ownership of voting securities, by contract or otherwise.

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

The "**Deliverables**" are any tangible or intangible products or services and other outcomes and outputs of the Services provided by Vendor to FIS or a FIS Affiliate under and as more particularly described and identified in the Agreement.

"**Designated End User**" shall mean the authorized employee(s) or agent(s) or Client(s) of FIS that are permitted to access and use the Software as contemplated under the Agreement.

A "**Destructive Element**" is any computer code or other technological device which (i) is intentionally designed to disrupt, disable, harm or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of a software, firmware, hardware, computer system or network (sometimes referred to as "viruses" or "worms"), (ii) would disable a Deliverable or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral (sometimes referred to as "time bombs," "time locks," or "drop dead" devices), (iii) would permit Vendor, any Vendor Personnel or any licensor or Contractor to Vendor to access a Deliverable to cause such disablement or impairment (sometimes referred to as "traps," "access codes" or "trap door" devices), or (iv) contains any other similar harmful, malicious or hidden procedures, routines or mechanisms which would cause a Deliverable or any other software, firmware, hardware, computer system or network to cease functioning or damage or corrupt data, storage media,

programs, equipment or communications or otherwise interfere with the operations of FIS, Clients or their customers.

"**Documentation**" means the user manuals, training materials, specifications, release notes, and other written documentation, as applicable, made available by Vendor from time to time to FIS in connection with and/or related to the Software.

The "**Effective Date**" is the date of effectiveness specified in the Agreement. If no date of effectiveness is specified in the Agreement, the Effective Date is the date FIS signs the Agreement, as determined by the date indicated for its signature.

The "**Engagement**" is the engagement of Vendor by Fidelity Information Services, LLC or its Affiliate to provide Software or Services under the Agreement.

A "**Force Majeure Event**" is an event that prevents a party's performance of an obligation under the Agreement and is beyond the reasonable control of the party, such as a natural disaster, strike, riot, earthquake, epidemic, terrorist action, war, fire, flood, unavailability of communications or electrical service provided by a third party, or governmental regulations imposed after the fact.

"**FIS**" is Fidelity Information Services, LLC. However, if a FIS Affiliate enters into the Agreement with Vendor, "FIS" refers to that FIS Affiliate for purposes of the Agreement.

"**GDPR**" means the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

"**Good Industry Practice**" means the exercise of that degree of professionalism, skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same type of activity under the same or similar circumstances;

The "**Guidelines**" are the standards and guidelines established pursuant to (i) the Gramm-Leach-Bliley Act of 1999 or a state law equivalent, relating to the protection of NPI, (ii) the Health Insurance Portability and Accountability Act of 1996 or a state law equivalent, relating to the protection of PHI, (iii) other relevant privacy Laws, or (iv) PCI DSS, relating to Payment Card Data.

An "**Information Breach**" is any actual or attempted unauthorized intrusion or other breach to the network, systems, or security of or under the management or control of Vendor affecting FIS data, including any actual or attempted access to or use, possession or release of Personal Data, NPI, PHI, Payment Card Data or other FIS Confidential Information.

"**Inventions**" are any discoveries, improvements, copyrights, programs, trademarks, processes, and systems relating to the Deliverables and the business of FIS and applications thereof, that Vendor may conceive, discover or make solely or jointly at any time during the Engagement, whether or not patentable or eligible to be copyrighted, and whether or not using the time, facilities, equipment or personnel of FIS.

"**Law**" means applicable laws collectively, including statutes, codes, rules, regulations, ordinances and orders of governmental authorities.

"**Losses**" means liabilities, claims, proceedings, judgments, damages, demands, actions, costs, charges, expenses, penalties, fines, settlements and any other loss of whatever nature, including court costs, legal counsel costs and legal fees.

A "**Notice of Contract Breach**" is a notice by one party to the other to notify the other of a material breach of the Agreement by the other party, describing why the notifying party believes the other party has committed a breach, including the applicable provision(s) of the Agreement and the applicable date(s) of the other party's act(s) or omission(s), and the cure or other relief the notifying party is requesting.

"**NPI**" is "nonpublic personal information" protected under the Gramm-Leach-Bliley Act of 1999 or a state law equivalent.

"**Payment Card Data**" is cardholder data protected under the Payment Card Industry Data Security Standard (PCI DSS).

"**PHI**" is "protected health information" protected under the Health Insurance Portability and Accountability Act of 1996 or a state law equivalent.

The "**Privacy Regulations**" are the standards, guidelines and other regulations established by various federal or state regulatory agencies to protect the privacy and security of customer or patient information held by financial institutions, medical service providers and other entities.

A "**Service**" is a service provided under the Agreement for data processing, software hosting, software as a service, a knowledge or information service, provision of work or workers on an outsourced basis, production management, customization or other custom development, training and support, and various other matters as requested by FIS and as more particularly described in the Agreement.

"**Software**" means the Vendor's software licensed to FIS under the Agreement including any subsequent modifications, enhancements, patches, versions, or updates thereto supplied by Vendor to FIS.

The "**Term**" is the term of the Agreement, including any extensions or renewals.

The phrase "**under the Agreement**" means under the Agreement directly or indirectly, such as through a statement of work or other contract made under the Agreement for the purchase of one or more Services or Software, and the phrase "with the Agreement" refers to the Agreement and any such other contract.

"**Use**" or "**use**" means FIS' and Designated End Users' right to (a) perform, display, copy, load into a computer's memory, and test the Software, (b) maintain copies of the Software and Documentation for back-up or archival purposes, (c) allow FIS' Contractors to utilize the Software exclusively for the purpose of processing FIS' or its Designated End User's data.

"**Vendor**" is the party identified as such in the Agreement.

"**Vendor Personnel**" are individuals who are assigned to perform a Service under the Agreement, including employees of Vendor or its Affiliates, employees of any Contractor to Vendor, and if an individual, Vendor or any Contractor to Vendor.

The terms, "**Controller**," "**Personal Data**," "**Processing**," and "**Processor**" shall have the same meaning as in the GDPR as it may be amended from time to time, and their related terms shall be construed accordingly for purposes of this Agreement.

2. **SAFETY AND SECURITY**.

2.1 ON PREMISES OF FIS AND ITS CLIENTS. All Vendor Personnel must comply with all FIS postings and notices regarding safety and security when on the premises of FIS, and with the postings and notices of Clients or their customers when on their premises. Without limitation of the foregoing, in all events Vendor Personnel must not carry weapons or ammunition onto the premises of FIS, Clients, or their customers and must not use or carry weapons or ammunition while attending FIS-sponsored events.

2.2 ACCESS PRIVILEGES AND RESTRICTIONS. In the event Vendor Personnel will receive access credentials for FIS' facilities, applications, systems or servers, those of its Affiliates or those of any Clients or any of their customers, the following provisions will also apply:

2.2.1 Vendor will require all Vendor Personnel that will be issued access credentials to submit to FIS' then current access credentialing process.

2.2.2 Vendor will promptly, but in any event within twenty-four (24) hours, (i) confiscate each such access credential from Vendor Personnel when the Vendor Personnel's need to have such access in order for the Services to be performed is discontinued and (ii) notify FIS of any change in the status (including any such suspension, termination or discontinuation) of Vendor Personnel for whom such a device or access credential has been requested or to whom such a device or access credential has been provided.

2.2.3 Vendor will not request that such an access credential be provided, or provide such an access credential, to any individual who will not be directly engaged by or at the request of FIS to provide Services.

2.2.4 FIS reserves the right to deny any access credential request or terminate any access credential that has been provided. Vendor will notify FIS within twenty-four (24) hours of any changes to the Vendor Personnel for whom such an access credential has been requested or to whom such an access credential has been provided.

2.2.5 Vendor will not permit any such access credential to be used by more than one individual.

2.3 INFORMATION SECURITY AND INTERNAL CONTROLS. In the event Vendor (i) stores any data of FIS, its Clients or their customers, otherwise has any such data in its possession or control, (ii) has access to any such data from outside the premises of FIS, FIS Affiliates, Clients or customers of Clients, or (iii) has access to any networks of FIS, FIS Affiliates, Clients or customers of Clients, the following provisions will apply to Vendor. In the event an entity other than Vendor does so under a contract with Vendor or otherwise for or on behalf of Vendor, Vendor will ensure by contract or otherwise that the following provisions apply correspondingly to the other entity for the benefit of FIS.

2.3.1 Vendor will be responsible for establishing and maintaining an information security program to (i) ensure the security and confidentiality of such data, (ii) protect against any anticipated threats or hazards to the security or integrity of such data, and (iii) protect against unauthorized access to or use of such data that could result in substantial harm or inconvenience to FIS, FIS Affiliates, Clients or customers of Clients.

2.3.2 The Vendor will implement and operate:

(a) Where technically possible, up to date anti-virus software upon all systems and networks used in the provision of the Services;

(b) The Services upon supported technologies which are kept up to date with the latest versions;

(c) A patch management process, which ensures patches are appropriately tested and deployed to rectify security vulnerabilities in a reasonable timeframe with critical or urgent patches deployed within thirty (30) days of release;

(d) A vulnerability management program that is undertaken on a frequent basis (at least quarterly) that includes (a) scanning the networks, infrastructure, applications and websites used in the provision of the Services, (b) validating any vulnerabilities found, and determining their criticality based upon industry recognized methods such as CVSS, and (c) creating and undertaking a plan to remediate the discovered vulnerabilities, based upon their criticality, at its own cost and in a timely manner;

(e) Standards to ensure that its systems are configured in a secure state, in line with industry recognized best practices, such as the National Institute of Standards and Technology ("**NIST**") or the Center of Internet Security;

(f) Robust processes to ensure that access to FIS data under its control is restricted to those individuals whom are explicitly authorized to access such data in the course of delivering the Services. Access shall be limited to those with a business need for such access and to those privileges needed to fulfil that need only. Access shall be assigned using unique logon credentials to ensure accountability is maintained;

(g) A robust and enforceable password policy in place that mandates the use of complex passwords and forces users to periodically change their password;

(h) Strong authentication methods (two-factor authentication) for those Vendor Personnel who work remotely and for those with administrative privileges upon systems used to provide the Deliverables or Services. Such access must be via encrypted communications;

(i) Multi-factor authentication for all internet facing systems storing and processing FIS data;

(j) Mechanisms to prevent the unauthorized removal of FIS data from the Vendor's networks via technologies such as removable media devices, the internet, email or instant messaging services;

(k) Strong encryption technologies (in line with industry standards such as NIST approved) to protect logon credentials, and FIS data during transmission and storage;

(l) The Vendor will implement and operate application level encryption ("**ALE**") technologies to protect sensitive data in-scope for FIS data at rest. ALE is defined as 1) the encryption of in-scope data by the application 2) encryption must occur before being written to a data store or being consumed by the application, 3) encryption must not be dependent on any underlying transport and/or other at-rest encryption including but not limited to the Vendor's use of native cloud encryption technologies and 4) ALE algorithms must meet strong encryption technologies (in line with industry standards such as NIST approved);

(m) Encryption technologies upon portable devices such as laptops, PDAs and smartphones, in order to protect any FIS information shared via, or stored upon, such technologies;

(n) Physical controls to mitigate the risk of unauthorized intrusion to Vendor's premises, networks and systems including, without limitation, (a) an auditable electronic access system that requires physical access tokens (such as swipe cards, biometric token, keys or fobs) to achieve access, (b) closed circuit television ("**CCTV**") coverage of all entry points, (c) intruder detection systems and burglar alarms, (d) processes to grant access only to authorized individuals, (e) processes to revoke physical access when no longer required, and (f) processes to manage visitors are authorized and supervised;

(o) Logical controls to mitigate the risk of unauthorized intrusion to Vendor's premises, networks and systems including, without limitation, (a) appropriately configured and maintained firewalls, (b) up to date intrusion detection systems, (c) centralized logging systems that records networks and systems activity and retains the ability

to inspect these logs in the event of a suspected or realized security breach, (d) the monitoring and inspection of such logs by persons separate from those responsible for administration of networks and systems;

(p) Systems and software development processes to ensure that commonly known security flaws (such as those defined by the Open Web Application Security Project) are not introduced into systems used to supply the Services. Such controls must include: (i) sufficient training for its software developers to ensure that the probability of security flaws being introduced is minimalized, and (ii) the testing of application and website code to eliminate security flaws;

(q) Separate environments between test and production systems and will ensure that no production data of FIS is used in test systems;

(r) Robust processes to ensure that changes to the premises, networks, systems and software used to supply the Services are appropriately evaluated, tested and implemented to limit the potential of service degradation;

(s) Processes to continually monitor its networks and systems for potential or actual security breaches;

(t) Processes to ensure that any FIS data is retained in accordance with a data retention policy which complies with FIS' requirements, and applicable legal or regulatory requirements;

(u) Processes to promptly return and/or erase all data in Vendor's possession or control, at the request and option of FIS, in a manner that maintains its confidentiality and integrity, as agreed between the parties;

(v) Processes to ensure that all information pertaining to, provided by, or owned by FIS is securely destroyed to beyond the point of recovery (once approved by FIS) as soon as it is outside the agreed retention policy or no longer required for a valid business purpose, including electronic and physical information assets. Certificates of destruction will be retained for audit purposes;

(w) Training in accordance good industry practice on secure software development at least annually for Vendor Personnel involved in the architecture and design, and development and testing of FIS software;

(x) Secure development lifecycle ("**SDLC**") processes based on Good Industry Practice; and

(y) Automated or manual analysis of the security of any code developed, remediation of any vulnerabilities prior to deployment to FIS, and the provision of reports of such analysis to FIS.

2.3.3 The Vendor will implement and operate regular penetration tests ("**Vendor Security Tests**") upon the networks, infrastructure, applications and websites used in the provision of the Services, no less than once per calendar year and share the results of the Vendor Security Tests with FIS on request. If after reviewing such test results, FIS believes that additional testing is warranted, FIS and Vendor will discuss such additional testing in good faith. Vendor shall also permit FIS or a security consultant selected and approved by FIS to carry out penetration tests ("**FIS Security Tests**") on the Vendor's systems. The Vendor shall provide FIS with all reasonable assistance to enable FIS to perform the FIS Security Tests. FIS agrees to share the results of any vulnerability scan or penetration test it performs on Vendor's environment to assist Vendor in correcting any information security vulnerabilities identified. Vendor will correct (at its own cost) any information security vulnerability identified in the Vendor Security Tests or the FIS Security Tests within the applicable time periods below, based on the severity level of the vulnerability:

- Critical (CVSS Score: 9 - 10) severity vulnerabilities will be corrected within fourteen (14) days.
- High (CVSS Score: 7 - 8.9) severity vulnerabilities will be corrected within forty-five (45) days.
- Medium (CVSS Score: 4 – 6.9) severity vulnerabilities will be corrected within ninety (90) days
- Low (CVSS Score: less than 4) severity vulnerabilities will be corrected within one hundred and twenty (120) days

2.3.4 Where all, or part of, the Services are provided using online services (i.e. accessible via the internet), the Vendor must ensure that adequate protection is in place to mitigate the risk of denial-of-service (DoS) threats.

2.3.5 Vendor shall ensure that processes employed in the provision of the Services are staffed in such manner as to prevent conflicts of interest, fraud or error by invoking appropriate separation of duties.

2.3.6 Vendor shall ensure that information security awareness and training programs are provided for those responsible for handling FIS data, upon hire and on at least an annual basis.

2.3.7 Vendor will promptly notify FIS of any and all breaches to Vendor's information security within twenty-four (24) hours of discovering the Information Breach and work with FIS management to identify the root

cause of the incident and the potential impact to FIS, its Clients or their customers, as reasonably requested by FIS.

2.3.8 If and to the extent Vendor or any Service is subject to the Payment Card Industry Data Security Standard requirements (as amended from time to time) ("**PCI DSS**"), Vendor will comply with said requirements. In addition, if and to the extent Vendor or any Service is subject to PCI DSS requirements: (i) Vendor will submit their Attestation of Compliance ("**AOC**") and Vendor Responsibility Matrix within ten (10) days of the execution of this Agreement and will have an AOC and Vendor Responsibility Matrix prepared, and provide to FIS such updated AOC and Vendor Responsibility Matrix, annually thereafter; (ii) Vendor will publish to 'Visa' Global Service Vendor registry and maintain 'Green Status' in such registry throughout the duration of the Agreement; and (iii) if Vendor fails to maintain 'Green Status' in the Visa Global Service Vendor registry, the following provisions shall apply: (A) If Vendor in 'Yellow Status' in the Visa Global Service Vendor registry, Vendor will provide the Services free of charge until Vendor obtains 'Green Status'; and (B) If Vendor is in 'Red Status' or is not listed in the Visa Global Service Vendor registry: (a) Vendor will provide the Services free of charge free of charge until Vendor obtains 'Green Status' or the Agreement terminates, (b) Vendor will refund to FIS the six (6) then most recent months of fees paid by FIS under the Agreement (excluding any period in which Vendor was providing the Services free of charge due to Vendor being in 'Yellow Status' or 'Red Status' pursuant to this provision), and (c) FIS may, in addition to any other remedies FIS may have, terminate the Agreement with no financial obligation to Vendor arising from such termination.

2.4 BACKGROUND CHECKS. Vendor will perform the background check, as described herein, and also timely cooperate in good faith with FIS' performance of a background check, as described herein, for each individual who is performing any Services under the Agreement and has access to the facilities, records or data of FIS, any Affiliate, any Client or any customer of a Client. Where permitted by applicable Law, the background check will consist of, at a minimum, verification of the highest level of education completed, verification of employment for the past ten (10) years, social security number trace and validation, and a check of U.S. Government Specially Designated National (OFAC) and export denial lists. In addition, to the extent permitted by Law, the background check will include a 9-panel drug test and criminal record search. For the drug test, all specimens will be tested at a Department of Health and Human Services/Substance Abuse Mental Health Services Administration certified lab, and the screening service will include confirmation of all positive test results. The criminal record search will include, to the maximum extent permitted by Law, a federal, state and county check, and a National Criminal File check, for felony and misdemeanor convictions for the last ten (10) years in all locations where the individual has resided for the last ten (10) years. Vendor will comply with all applicable Laws related to the background check, including required notices and applicable consents. In addition, Vendor will require the individual to report any criminal convictions. Vendor will not assign anyone to perform Services for FIS who has tested positive for drugs or whose background check findings do not meet the standards established by Vendor in accordance with all applicable Laws, including without limitation if there is a conviction or referral to a pretrial diversion program for a crime that is related to his or her duties. Vendor acknowledges that under the banking Laws, an individual may not participate, directly or indirectly, in any manner in the conduct of the affairs of any insured depository institution without regulatory consent if he or she has a conviction, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution, of a crime involving dishonesty, breach of trust or money laundering, including any crime concerning the illegal manufacture, sale, distribution of or trafficking in controlled substances, unless the crime meets certain criteria for treating the crime as de minimis. The background check must be completed before assignment of an individual and periodically thereafter. FIS also reserves the right to request that Vendor provide an attestation confirming a background check as required by this provision has been completed and no disqualifying information has been identified on an annual basis during the Term of an Engagement. Upon five (5) Business Days' prior written notice, FIS may verify Vendor's compliance with this Section. Such verification will be conducted in a manner that minimizes disruption to Vendor's business. FIS may use an independent auditor to assist with such verification, provided that FIS has a written confidentiality agreement in place with such independent auditor. FIS will notify Vendor in writing if any such verification indicates that Vendor is not in compliance with this Section and Vendor will promptly remediate any issues of non-compliance discovered by FIS as part of such verification.

2.5 All FIS' audit rights of the Agreement including without limitation to examine Vendor's records (which must include auditable records of all financial and non-financial transactions relating to Products and Services) may, to the extent required by the regulators of FIS and/or its Clients, be exercised by FIS, FIS' Clients, and its and their regulators.

2.6 DESTRUCTIVE ELEMENTS. Vendor represents, warrants and covenants that it will not introduce or allow any Destructive Elements into the Services, any Products or Deliverables, or into the systems of FIS or any of FIS

Clients or their customers. Without limitation of the foregoing, Vendor warrants and covenants that it will use best efforts to avoid the coding or introduction of Destructive Elements into any systems used to provide Services, Products or Deliverables. Vendor will assist FIS with mitigation of any loss of operational efficiency or loss of data caused by such Destructive Elements. Upon learning of or discovering a cyber or information-security threat or vulnerability to FIS systems or to FIS Clients or their customers (including without limitation notifications received from security researchers, industry resources, or bug bounty programs), Vendor will promptly notify and cooperate with FIS and take all reasonable and necessary steps to isolate, mitigate, and remediate such known or suspected threat or vulnerability.

3. **SAFEGUARDING INFORMATION**

3.1 CONSUMER INFORMATION AND PRIVACY. If, in connection with the Agreement, Vendor receives, stores or accesses any Personal Data, NPI, PHI, Payment Card Data, or other information or materials that are subject to the Privacy Regulations and Guidelines, Vendor will comply with the applicable requirements of the Privacy Regulations and Guidelines. Vendor acknowledges that the Guidelines include provisions regarding the safeguarding of consumer information, response programs and notice in the event of unauthorized access to consumer information, that FIS provides information processing services to Clients subject to the Guidelines, and that FIS may be required to notify Clients, their customers or other third parties of security incidents that result, or are likely to result, in misuse or unauthorized possession or disclosure of Personal Data, NPI, PHI, Payment Card Data or other Confidential Information. Without limiting the foregoing, and in addition to its confidentiality and security obligations as otherwise set forth in the Agreement, Vendor will (i) ensure the security and confidentiality of such information or materials, (ii) protect against any anticipated threats or hazards to the security or integrity of such records, (iii) detect unauthorized access to or use of such records or information, and (iv) protect against unauthorized access to or use of such records or information that would result in harm or inconvenience to any Client or any customer of a Client. Vendor represents and warrants that it has and will maintain in place commercially reasonable precautions to safeguard the confidentiality, security and integrity of FIS Confidential Information in a manner designed to meet the requirements of this Section. These precautions will include but will not be limited to (i) contractual restrictions on access to the information by Contractors and Vendor's other vendors, (ii) intrusion detection systems on all information systems of FIS maintained or controlled by Vendor, and (iii) notification procedures for notifying FIS promptly in the event a security breach is detected or suspected, as well as other response programs when there is a suspected or detected Breach involving Personal Data, NPI, PHI or Payment Card Data. These precautions will also include, as appropriate, (A) access controls to FIS information systems, including controls to identify and permit access only to authorized individuals and controls to prevent access to FIS Confidential Information through improper means, (B) Vendor Personnel controls and training, (C) physical access restrictions at locations where FIS Confidential Information is located, (D) encryption of electronic FIS Confidential Information when appropriate or legally required, and (E) a disaster recovery plan as appropriate to protect against loss or damage to FIS Confidential Information due to potential hazards such as fire or water damage or technological failures. Vendor will (1) monitor the foregoing measures with periodic audits or testing and (2) provide copies of the same sufficient to assure FIS or its regulatory authorities that Vendor is implementing these precautions, and (3) notify FIS immediately in the event there is any suspected or actual unauthorized access, use, disclosure or alteration to FIS Confidential Information. Vendor will indemnify FIS from, defend FIS against, and pay any final judgments awarded against FIS, resulting from any claim brought by a third party, including but not limited to a customer of FIS, against FIS based on any breach of such privacy Laws, rules or regulations by Vendor, including Vendor Personnel.

3.1.1 Vendor will also use the information security safeguards described in Section 3.1 to protect any Confidential Information of FIS and FIS Clients comprising technical data, technical schematics, and any infrastructure, hardware, and/or software and systems information of FIS and FIS Clients that, if disclosed publicly, could enable or facilitate unauthorized access to such Confidential Information.

3.2 PROTECTION OF CONFIDENTIAL INFORMATION. Each party must protect the other's Confidential Information with the same degree of care used to protect its own Confidential Information, but in no event may either party use less than a reasonable standard of care be in connection with the preservation of the other's Confidential Information. FIS designates as its Confidential Information (i) the Agreement, (ii) any information obtained from or related to any Client of FIS including FIS Client business strategy, direction and contract information, (iii) any Personal Data, NPI, PHI, or Payment Card Data (iv) FIS' employee records (name, address, phone number, salary, taxpayer or government identification number, date of birth, health records, bank account information, labor party), (v) any business strategies and directions, operating or marketing plans, intellectual capital or trade secrets, (vi) memos or other documents or communications pertaining to pending FIS litigation or contracts (including the Agreement), (vii) any information disclosed by FIS that is designated as "confidential" at or

prior to disclosure, (viii) other FIS data or information which is not generally known, including business information, specifications, research, software, trade secrets, discoveries, ideas, know-how, designs, drawings, flow charts, data, computer programs, marketing plans, budget figures, and other financial and business information, and (ix) information of the kind described by any of the foregoing categories that is of or disclosed by a Client, an FIS Affiliate, or a customer of a Client. Vendor will (A) restrict the use and disclosure of the FIS' Confidential Information to its Vendor Personnel and do so solely on a "need to know" basis in connection with Vendor's obligations to provide Software or to perform Services in accordance with the Agreement, (B) ensure Vendor Personnel who receive or have access to FIS Confidential Information are bound by confidentiality obligations at least as restrictive and as protective of the FIS Confidential Information as the provisions of this Section, (C) require its Vendor Personnel to protect and restrict the use of the FIS' Confidential Information, (D) establish procedural, physical and electronic safeguards, designed to prevent the compromise or unauthorized disclosure of FIS Confidential Information and to achieve the objectives of the Guidelines (if applicable), (E) promptly investigate any security breach to determine whether such incident has resulted or is likely to result in misuse or unauthorized possession or disclosure of FIS Confidential Information and (F) not use or disclose FIS' Confidential Information except in accordance with the Agreement.

3.3 In providing any notice of an Information Breach, Vendor will use commercially reasonable efforts to (i) provide notice to one or more FIS managers generally responsible for security matters relating to the FIS Confidential Information affected by the Information Breach, within twenty-four (24) hours of discovering the Information Breach, and (ii) keep FIS informed as to the actual and anticipated effects of the Information Breach and the corrective actions taken or to be taken in response to the Information Breach. In addition, if the Information Breach results or is likely to result in misuse of Personal Data, NPI, PHI or Payment Card Data, Vendor will (A) notify FIS as soon as possible and reasonably cooperate with FIS in its efforts to notify affected Clients and their customers and to mitigate the actual or potential harm resulting from the Information Breach and (B) reimburse FIS for its reasonable costs in notifying Clients or their customers of the Information Breach and making available to them any credit monitoring services and for any other costs FIS reasonably incurs with respect to the Information Breach.

3.4 Confidential Information will remain the property of the party from or through whom it was provided. Except for NPI, PHI, Payment Card Data, or other information protected by the Guidelines, the parties' respective confidentiality obligations under the Agreement do not apply to any information that: (i) was previously known by the party; (ii) is a matter of public knowledge; (iii) was or is independently developed by the party; (iv) is released for disclosure with written consent of the party; or (v) is received from a third party to whom it was disclosed without restriction.

3.5 Each party may disclose information notwithstanding its confidentiality obligations under the Agreement to the extent required (i) by Law, (ii) in connection with the tax treatment or tax structure of the Agreement; or (iii) in response to a valid order of a U.S. court or other governmental body, provided that the party provides the other party with written notice and the other party is afforded a reasonable opportunity to obtain a protective order with respect to the disclosure.

3.6 Upon termination of the Agreement, Vendor will destroy all FIS Confidential Information in a manner designed to preserve its confidentiality, or, at the other party's written request and expense, return it to FIS. Upon FIS' written request, Vendor shall, at FIS' choice, delete or return all Personal Data Processed on behalf of FIS to FIS after the end of the provision of Services relating to Processing, subject to Vendor retaining any copies required by applicable EU member state law.

3.7 FIS will have and retain all right, title and interest in all of FIS' Confidential Information, whether possessed by FIS prior to, or acquired or refined by FIS (either independently or in concert with Vendor) during the Term.

3.8 Vendor will not, without the prior written consent of FIS, (i) provide the Software or Services or access, store or process any of FIS' Confidential Information outside the United States or (ii) export any of FIS' Confidential Information to anywhere outside the United States. The provisions of the Agreement apply without regard to where the Software or Services are provided or FIS Confidential Information is accessed, stored or processed.

3.9 EU GDPR Compliance. If Vendor shall process any Personal Data from FIS or a Client as part of the Services under the Agreement regarding individuals domiciled in countries outside of the United States (or to which the GDPR is otherwise applicable), such processing shall be in compliance with the Data Protection Addendum attached hereto as Appendix A and incorporated herein by this reference.

4. **SUBCONTRACTORS.**

4.1 Vendor will not utilize any Contractor to perform Services or provide any part of a Deliverable, without the prior written consent of FIS. Vendor will notify FIS of its intention to so engage another party not less than thirty (30) days prior to the entity commencing performance of any Services or to provide any part of the Deliverable. Vendor will provide such information and documentation concerning any such proposed party as FIS requests. Vendor will ensure that any such Contractor complies with all obligations of Vendor under the Agreement. Vendor is responsible for all of its obligations under the Agreement regardless of where performed or whether performed by any Contractor, and Vendor will be liable for the acts and omissions of any Contractor that Vendor uses to perform Services or provide any part of any Deliverable.

4.2 SERVICES PERFORMED BY PROVIDER PERSONNEL IN UK. If Vendor shall assign Vendor Personnel that are located in the United Kingdom to perform any part of the Services under the Agreement, then such performance shall be in compliance with the UK Services Terms attached hereto as **Appendix B** and incorporated herein by this reference.

5. Vendor may not engage sub-Processors under the Agreement or give access to or transfer any Personal Data to any third party (including any affiliates, group companies or sub-contractors) without the prior written consent of FIS and the relevant FIS Affiliates. If FIS consents to the use of third parties as sub-Processors Vendor shall (i) impose in writing upon such sub-Processors the same data protection obligations as set out herein and as are required by applicable Data Protection Legislation and (ii) be responsible for the acts and omissions of such sub-Processors under the Agreement. Where prior written consent given by FIS pursuant to this clause authorizes a class of third party to Process Personal Data, the Vendor shall notify FIS of any intended changes concerning the addition or replacement of any sub-Processors within such class, and FIS shall have the right to object to, and prevent, any such addition or replacement of sub-Processors within such class.

5.1 **COMPLIANCE WITH LAWS.** In all circumstances, Vendor will comply with, and will ensure that all Software, Services and Deliverables comply with all Law, including Law relating to export and import, privacy, use, disclosure or transfer of personal information, or security, and Law relating to the employment, health, safety and payment of Vendor Personnel. Vendor will perform an on-going review of Law applicable to Vendor's performance under the Agreement, including Law enacted or amended after the effective date of the Agreement. Vendor will identify and procure all permits, certificates, approvals, licenses, and inspections necessary for Vendor's performance under the Agreement other than such permits, certificates, approvals, licenses and inspections that FIS is directly responsible for obtaining under the Agreement. Without limiting any other obligation of Vendor under the Agreement, Vendor will at all times comply with all Law relating to trade sanctions, export controls, the U.S. Foreign Assets Control Regulations, the U.S. Export Administration Regulations, and the U.S. International Traffic in Arms Regulations.

6. **DATA PROTECTION TECHNICAL AND ORGANISATIONAL MEASURES**

6.1 In the course of Vendor providing Services under the Agreement(s), FIS may from time-to-time provide or make available Data to Vendor. The Agreement(s) determines the subject matter and the duration of Vendor's Processing of Personal Data, as well as the nature and purpose of any collection, use, and other Processing of Personal Data and the rights and obligations of FIS.

6.2 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 of varying likelihood and severity for the rights and freedoms of natural persons, Vendor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. As a minimum, these should include the requirements required under applicable Data Protection Legislation and the requirements set out in the Agreement. Upon request, Vendor shall provide a written description of the technical and organizational measures the Vendor employs for Processing Personal Data.

6.3 Vendor must cooperate upon FIS' reasonable request in order to assist FIS with its compliance with applicable privacy laws, including FIS' handling of Data Subject rights requests.

6.4 Where Vendor is acting as a Processor under the Agreement, at FIS' written request, Vendor shall make available to FIS all information reasonably necessary to demonstrate Vendor's compliance with the obligations agreed to in the Agreement(s), applicable privacy laws, and any data protection addenda.

6.5 Unless Vendor needs identifiable information in order to provide the product or service, Vendor will deidentify or pseudonymize FIS' data unless there is a need for the data to be identifiable.

6.6 Vendor must consider data protection issues as part of the default configuration of its systems, services, products, and business practices. Vendor's default configuration will follow privacy by default principles, including

data quality, minimization, and accountability. Vendor will Process FIS data in accordance with FIS instructions and only when relevant, minimal, and not excessive.

6.7 Vendor will provide certification and assurance of its processes and products pursuant to the GDPR.

7. **BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY**. To the extent applicable to the Services, Vendor will establish and maintain disaster recovery and business continuity plans designed to minimize the risks associated with a disaster affecting Vendor's ability to provide the Services, which includes off-site data storage and recovery infrastructure. Vendor's recovery time objective for the Services ("**RTO**") under such plan is [INSERT TIMEFRAME] hours/minutes. Vendor will maintain adequate backup procedures in order to recover FIS' or if applicable any Client's data to the point of the last available good backup. Vendor's recovery point objective ("**RPO**") is [INSERT TIMEFRAME] hours/minutes. Vendor will test its disaster recovery and business continuity plans, including call trees, not less frequently than annually, will annually provide to FIS disaster recovery and business continuity plans test results. If Vendor fails to meet the RTO and RPO in any annual test, Vendor shall perform a root cause analysis of the cause of the failure to meet the RTO or RPO and will remediate the cause of such failure and retest within six (6) months of the failed test. If Vendor fails to meet the RTO or RPO in the retest, Vendor will have a second six (6) month period to remediate and retest. If provider fails a second time, FIS may request that the parties attempt to reach a mutually agreeable resolution, and if the parties are unable to agree upon a resolution within thirty (30) days of FIS' request, FIS may terminate the Agreement with no further financial obligation to Vendor. Vendor will provide its disaster recovery plan and test results to FIS and FIS may share such disaster recovery plan and test results with Clients who have contracted for the Services, if any, FIS' auditors, and FIS' regulators. Vendor will implement the applicable disaster recovery or business continuity plan upon the occurrence of a disaster, and shall notify FIS promptly following such event. In the event of a disaster (as defined in the plan), Vendor will not charge fees higher than or in addition to the agreed fees under the Agreement. Vendor will notify of, and invite FIS to participate in (at no additional charge to FIS), Vendor's disaster recovery and business continuity plan test.

Annex 4

Standard Contractual Clauses for Restricted Transfers Originating in the UK

Clause 1

Definitions

For the purposes of the Clauses:

(a) *"personal data", "special categories of data", "process/processing", "controller", "processor", "data subject"* and *"supervisory authority"* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) "*the data exporter"* means the controller who transfers the personal data;

(c) *"the data importer"* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *"the subprocessor"* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) "*the applicable data protection law"* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *"technical and organisational security measures"* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result

of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions

received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue

a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the laws of the jurisdiction in which the data exporter is established (being either a jurisdiction within the United Kingdom or a Member State of the EEA).

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the laws of the jurisdiction in which the data exporter is established (being either a jurisdiction within the United Kingdom or a Member State of the EEA).

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1
Particulars of the Transfer

Data exporter	FIS.
Data importer	Vendor.
Categories of Data Subjects	As set out in Annex 1 (*Data Processing Details*).
Categories of Data	As set out in Annex 1 (*Data Processing Details*).
Special categories of data	As set out in Annex 1 (*Data Processing Details*).
Processing Operations	Storing, copying, accessing, sharing, modifying.

APPENDIX 2
Data Security

The technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are those set out in Annex 3 (*Security Standards*).

Annex 5

Standard Contractual Clauses for Restricted Transfers Originating in the EEA

SECTION 1

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Unused (Optional)

SECTION II – O BLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least four (4) weeks in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex I

Particulars Of The Transfer

A. LIST OF PARTIES

Data exporter	FIS.
Data importer	Vendor.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects	As set out in Annex 1 (*Data Processing Details*).
Categories of Data	As set out in Annex 1 (*Data Processing Details*).
Sensitive Data	As set out in Annex 1 (*Data Processing Details*).
Frequency of Transfer	Continuous for the term of the Agreement.
Nature of Processing	Storing, copying, accessing, sharing, modifying.
Purposes of the Transfer	The provision of the Services by data importer to data exporter.
Data Retention	Data importer will delete the personal data from its systems on expiry or termination of the services in accordance with its usual data retention practices.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority should be the authority in the country where the data exporter is established.

Annex II

Technical And Organisational Measures Including Technical And Organisational Measures To Ensure The Security Of The Data

As set out in Annex 3 (*Security Standards*).

PART G2

Vendor Data Processing Addendum
Independent Controller to Controller

THIS DATA PROCESSING ADDENDUM is entered into as of the Addendum Effective Date by and between: (1) [INSERT FIS ENTITY] with an address at [INSERT ADDRESS] ("**FIS**"); and (2) [INSERT VENDOR] with an address at [INSERT ADDRESS] ("**Vendor**").

1. INTERPRETATION

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

(a) **"Addendum Effective Date**" means [the effective date of the Agreement] **OR** [INSERT SPECIFIC EFFECTIVE DATE].

(b) "**Agreement**" means the [INSERT TITLE OF AGREEMENT] entered into by and between the parties on [DATE] **OR** [or around the date of execution of this Data Processing Addendum].

(c) "**Business Day**" means any day other than a Saturday, Sunday or public holiday in England.

(d) "**Data Protection Laws**" means: (i) the GDPR; and (ii) to the extent applicable, the data protection or privacy laws of any other country.

(e) "**Data Receiving Party**" has the meaning set out in Section 2.6.

(f) "**Data Subject**" means the identified or identifiable natural person to whom Shared Personal Data relates.

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

(h) "**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

(i) "**GDPR**" means the UK GDPR and/or EU GDPR (as applicable), together with any applicable implementing or supplementary legislation in any member state of the EEA or the UK (including the UK Data Protection Act 2018). References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(j) "**Personal Data Breach**" means any actual or reasonably suspected 'personal data breach' (as defined in Article 4(12) of the GDPR).

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

(l) "**Relevant Body**" means:

(i) in the context of the UK GDPR, the UK Information Commissioner's Office; and/or

(ii) in the context of the EU GDPR, the European Commission.

(m) "**Restricted Country**":

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

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

that the Relevant Body has not deemed to provide an 'adequate' level of protection for Personal Data pursuant to a decision made in accordance Article 45(1) of the GDPR.

(n) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Personal Data to any person in a Restricted Country, which would be prohibited without a legal basis therefor under Chapter V of the GDPR.

(o) "**Shared Personal Data**" means any Personal Data Processed pursuant to or in connection with the Agreement.

(p) "**Standard Contractual Clauses**":

(i) in the context of a Restricted Transfer originating in the UK, means the standard contractual clauses for the transfer of personal data to controllers established in third countries which do not ensure an adequate level of protection pursuant to Commission Decision C(2004)5721 of 5 February 2010, as set out in full in Annex 2 (*Standard Contractual Clauses For Restricted Transfers Originating in the UK*); and

(ii) in the context of a Restricted Transfer originating in the EEA, means the standard contractual clauses for the transfer of personal data to controllers established in third countries which do not ensure an adequate level of protection pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as set out in full in Annex 3 (*Standard Contractual Clauses For Restricted Transfers Originating in the EEA*);

(q) "**Supervisory Authority**":

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

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

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

(s) "**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).

1.2. In this Data Processing Addendum:

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

(b) unless otherwise defined in this Data Processing Addendum, all capitalised terms in this Data Processing Addendum shall have the meaning given to them in the Agreement; and

(c) any reference to any statute, regulation or other legislation in this Data Processing Addendum 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 SHARED PERSONAL DATA

2.1. In the course of performing their obligations under the Agreement, the parties may from time-to-time Process Shared Personal Data supplied by or on behalf of the other party. The parties acknowledge and agree that, in relation to any Shared Personal Data, **each party is an independent Controller** for the purposes of the GDPR and shall independently determine the purposes and means of such Processing.

2.2. The nature and scope of the Processing of Shared Personal Data by the parties is set out in Annex 1 (*Data Processing Details*).

2.3. Each party shall (at its own cost):

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

(b) on request, provide the other party with reasonable assistance, information and cooperation to ensure compliance with their respective obligations under Data Protection Laws.

2.4. Each party acknowledges, confirms and represents for its own part that, as a Controller of any Shared Personal Data:

(a) all personal data collected or sourced by it or on its behalf for Processing in connection with the Agreement, or which is otherwise provided or made available to the other party, shall comply with and have been collected or otherwise obtained in compliance with Data Protection Laws; and

(b) all instructions given in respect of the Shared Personal Data shall be in accordance with Data Protection Laws.

2.5. The parties will work together in good faith to ensure the information referred to in Data Protection Laws (including Articles 13 and 14 of the GDPR) is made available to relevant Data Subjects in relation to the Processing by either party when acting as a Controller, and the information is in a concise, transparent, intelligible and easily accessible form, using clear and plain language as required by Data Protection Laws.

2.6. If either party (the "**Data Receiving Party**") receives any complaint, notice or communication from a Supervisory Authority which relates directly or indirectly to the other party's: (i) Processing of the Shared Personal Data; or (ii) a potential failure to comply with Data Protection Laws, the Data Receiving Party shall (at its own cost and to the extent permitted by applicable law) promptly forward the complaint, notice or communication to the other party and provide the other party with reasonable co-operation and assistance in relation to the same.

3. PERSONNEL

Each party shall take reasonable steps to ensure the reliability of any Personnel who may Process Shared Personal Data, including ensuring:

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

(b) that all such individuals have been vetted by the relevant party 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, each party shall implement appropriate technical and organisational measures in relation to Shared Personal Data to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

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

5. DATA SUBJECT RIGHTS

5.1. If a Data Subject makes a written request to a party to exercise their rights in relation to the Shared Personal Data that concerns Processing in respect of which another party is the Controller, that party shall (at its own cost):

(a) forward the request to the other party promptly and in any event within five (5) Business Days from the date on which it received the request; and

(b) upon the other party's reasonable written request, provide that other party with reasonable co-operation and assistance in relation to that request to enable the other party to respond to such request and meet applicable timescales set out under Data Protection Laws.

6. PERSONAL DATA BREACH

6.1. Each party shall notify the other party without undue delay (and in any event within forty-eight (48) hours) upon becoming aware of a Personal Data Breach affecting Shared Personal Data, providing the other party with sufficient information to allow it to meet any obligations under the Data Protection Laws to inform affected Data Subjects and/or Supervisory Authorities of the Personal Data Breach.

6.2. At a minimum, any notification made by a party pursuant to Section 6.1 shall include (to the extent available 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.

6.3. Each party shall provide regular updates to the other party in respect of the resolution of any Personal Data Breach.

6.4. Each party shall (at its own cost) co-operate with the other party to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7. RESTRICTED TRANSFERS

7.1. The parties agree that to the extent either party transfers Shared Personal Data to the other party 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 relevant Standard Contractual Clauses shall be entered into by and between the sending party as the "data exporter" and the receiving party as the "data importer" with effect from the Addendum Effective Date.

7.2. Notwithstanding Section 7.1, to the extent FIS implements, at any time during the term of this Data Processing Addendum, Binding Corporate Rules which may be relied on to legitimatise Restricted Transfers from Vendor to FIS made in connection with the Agreement:

(a) FIS shall notify Vendor of the same, and provide to Vendor a copy of its Binding Corporate Rules; and

(b) from the date of such notification, all Restricted Transfers from Vendor to FIS made in connection with the Agreement shall be subject to such Binding Corporate Rules, and the relevant Standard Contractual Clauses shall cease to apply accordingly.

8. CHANGE IN LAWS

8.1. Either party may propose any variations to this Data Processing Addendum which it reasonably considers necessary to address the requirements of any Data Protection Laws (including any updates to the Standard Contractual Clauses to reflect any future decisions of a Relevant Body in relation to the subject matter thereof, or any updates necessary to implement Binding Corporate Rules as a lawful mechanism for Restricted Transfers).

8.2. If a party gives notice under Section 8.1, 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 the notice without undue delay.

8.3. In the event that either party considers (acting reasonably) that any failure to agree its proposed variations to this Data Processing Addendum may cause it to be in material breach of Data Protection Laws, that party may terminate the Agreement in its entirety upon written notice to the other party with immediate effect and without liability.

8.4. The parties agree that a party shall be deemed to be "acting reasonably" for the purposes of Section 8.3 in the event that the other party fails to execute the revised form of any Standard Contractual Clauses issued or approved by a Relevant Body from time to time promptly following a request.

9. INCORPORATION AND PRECEDENCE

9.1. This Data Processing Addendum shall be incorporated into and form part of the Agreement with effect from the Addendum Effective Date.

9.2. In the event of any conflict or inconsistency between:

(a) this Data Processing Addendum and the Agreement, this Data Processing Addendum shall prevail; or

(b) any Standard Contractual Clauses entered into pursuant to Section 7 and this Data Processing Addendum and/or the Agreement, those Standard Contractual Clauses shall prevail.

Signed by _____	Signed by _____
for and on behalf of **[INSERT FIS ENTITY]**	for and on behalf of **[INSERT VENDOR ENTITY]**
Date: _____	**Date:** _____

Annex 1

Data Processing Details

Subject matter and duration of the Processing of Shared Personal Data

The subject matter and duration of the Processing of the Shared Personal Data are set out in the Agreement and the Data Processing Addendum.

The nature and purpose of the Processing of Shared Personal Data

The parties will process the Shared Personal Data to perform their obligations under the Agreement.

The types of Shared Personal Data to be Processed

☐ Contact data (e.g. name, email address, postal address)

☐ Identification data (e.g. date of birth, nationality, social security number)

☐ Solution log in and usage data

☐ Bank account data

☐ Financial data

☐ Contract and deal data (e.g. contractual/legal/financial relationship information)

☐ Billing and payments data

☐ Disclosed information from third parties (e.g. credit reference agencies or from public directories)

☐ Other; please specify: _____

The categories of Data Subjects to whom the Shared Personal Data relates

☐ FIS' and FIS Affiliates' employees

☐ FIS' and FIS Affiliates' customers

☐ FIS' and FIS Affiliates' potential customers

☐ FIS' and FIS Affiliates' suppliers

☐ Contact persons

☐ Other; please specify: _____

Annex 2

Standard Contractual Clauses for Restricted Transfers Originating in the UK

Definitions

For the purposes of the clauses:

(a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) "the data exporter" shall mean the controller who transfers the personal data;

(c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

(d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorizes to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorized or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions (1) of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data (2), or

(iii) the data processing principles set forth in Annex A.

(i) It will not disclose or transfer the personal data to a third-party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and:

(i) the third-party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third-party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

III. Liability and third-party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third-party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs, then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Annex A

Data Processing Principles

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

    a. such decisions are made by the data importer in entering into or performing a contract with the data subject, and (ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties; or

    b. where otherwise provided by the law of the data exporter.

Annex B
Description of the Transfer

Data Subjects	As set out in Annex 1 (*Data Processing Details*).
Purposes of the Transfer	The provision of the Services by data importer to data exporter.
Categories of Data	As set out in Annex 1 (*Data Processing Details*).
Recipients	Data importer's affiliates and service providers.
Sensitive Data	As set out in Annex 1 (*Data Processing Details*).

Annex 3

Standard Contractual Clauses for Restricted Transfers Originating in the EEA

SECTION 1

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5(e) and Clause 8.9(b);

(iii) Clause 12(a) and (d);

(iv) Clause 13;

(v) Clause 15.1(c), (d) and (e);

(vi) Clause 16(e);

(vii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Unused (Optional)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence 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.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(a) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(b) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(c) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. 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 the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer 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, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9 – Unused

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall 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 these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer 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.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall 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 authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) 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.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the EU Member State in which the data exporter is established.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex I

Particulars Of The Transfer

A. LIST OF PARTIES

Data exporter	FIS.
Data importer	Vendor.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects	As set out in Annex 1 (*Data Processing Details*).
Categories of Data	As set out in Annex 1 (*Data Processing Details*).
Sensitive Data	As set out in Annex 1 (*Data Processing Details*).
Frequency of Transfer	Continuous for the term of the Agreement.
Nature of Processing	Storing, copying, accessing, sharing, modifying.
Purposes of the Transfer	The provision of the Services by data importer to data exporter.
Data Retention	Data importer will delete the personal data from its systems on expiry or termination of the services in accordance with its usual data retention practices.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority should be the authority in the country where the data exporter is established.

Annex II

Technical And Organisational Measures Including Technical And Organisational Measures To Ensure The Security Of The Data

[If the Security Measures are already set out in the MSA, please delete the Security Measures below and insert "As described in Section [x] (Information Security Requirements) of the Master [Service] Agreement."]

1. **DEFINITIONS.**

An "**Affiliate**" of a party is an entity which, directly or indirectly, controls, is controlled by, or is under common control with that party, where "control" of the party or other entity means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the party or other entity, whether through record or beneficial ownership of voting securities, by contract, or otherwise.

"**Business Days**" means any day from Monday to Friday on which FIS is open for business at the applicable FIS location(s) under the Agreement.

A "**Change in Control**" of Vendor is any event or series of events by which (i) any person, entity or group of persons or entities acquires control of Vendor, where "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of Vendor, whether through record or beneficial ownership of voting securities, by contract, or otherwise, or (ii) if Vendor is a corporation, limited liability company or other entity having a board of directors or other group of individuals having similar functions, during any period of twelve (12) consecutive months commencing before or after the date hereof, individuals who at the beginning of such twelve-month period were members of Vendor's board of directors or other such group cease for any reason to constitute a majority of the members.

A "**Claim**" is any action, litigation, or claim for which a party is subject to an indemnification obligation under the Agreement.

A "**Client**" is any current or prospective client or customer of FIS or an FIS Affiliate.

The "**Confidential Information**" of a party is any information received from the party that is of a confidential nature or is designated as 'confidential' at or prior to disclosure.

A "**Contractor**" to a party is any individual (other than the party or an employee of the party), corporation or other entity providing services to or on behalf of the party, including any direct or indirect independent contractor or subcontractor to the party.

"**Control**" of a legal entity is the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity, whether through record or beneficial ownership of voting securities, by contract or otherwise.

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

The "**Deliverables**" are any tangible or intangible products or services and other outcomes and outputs of the Services provided by Vendor to FIS or a FIS Affiliate under and as more particularly described and identified in the Agreement.

"**Designated End User**" shall mean the authorized employee(s) or agent(s) or Client(s) of FIS that are permitted to access and use the Software as contemplated under the Agreement.

A "**Destructive Element**" is any computer code or other technological device which (i) is intentionally designed to disrupt, disable, harm or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of a software, firmware, hardware, computer system or network (sometimes referred to as "viruses" or "worms"), (ii) would disable a Deliverable or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral (sometimes referred to as "time bombs," "time locks," or "drop dead" devices), (iii) would permit Vendor, any Vendor Personnel or any licensor or Contractor to Vendor to access a Deliverable to cause such disablement or impairment (sometimes referred to as "traps," "access codes" or "trap door" devices), or (iv) contains any other similar harmful, malicious or hidden procedures, routines or mechanisms which would cause a Deliverable or any other software, firmware, hardware, computer system or network to cease functioning or damage or corrupt data, storage media, programs, equipment or communications or otherwise interfere with the operations of FIS, Clients or their customers.

"**Documentation**" means the user manuals, training materials, specifications, release notes, and other written documentation, as applicable, made available by Vendor from time to time to FIS in connection with and/or related to the Software.

The "**Effective Date**" is the date of effectiveness specified in the Agreement. If no date of effectiveness is specified in the Agreement, the Effective Date is the date FIS signs the Agreement, as determined by the date indicated for its signature.

The "**Engagement**" is the engagement of Vendor by Fidelity Information Services, LLC or its Affiliate to provide Software or Services under the Agreement.

A "**Force Majeure Event**" is an event that prevents a party's performance of an obligation under the Agreement and is beyond the reasonable control of the party, such as a natural disaster, strike, riot, earthquake, epidemic, terrorist action, war, fire, flood, unavailability of communications or electrical service provided by a third party, or governmental regulations imposed after the fact.

"**FIS**" is Fidelity Information Services, LLC. However, if a FIS Affiliate enters into the Agreement with Vendor, "FIS" refers to that FIS Affiliate for purposes of the Agreement.

"**GDPR**" means the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

"**Good Industry Practice**" means the exercise of that degree of professionalism, skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same type of activity under the same or similar circumstances;

The "**Guidelines**" are the standards and guidelines established pursuant to (i) the Gramm-Leach-Bliley Act of 1999 or a state law equivalent, relating to the protection of NPI, (ii) the Health Insurance Portability and Accountability Act of 1996 or a state law equivalent, relating to the protection of PHI, (iii) other relevant privacy Laws, or (iv) PCI DSS, relating to Payment Card Data.

An "**Information Breach**" is any actual or attempted unauthorized intrusion or other breach to the network, systems, or security of or under the management or control of Vendor affecting FIS data, including any actual or attempted access to or use, possession or release of Personal Data, NPI, PHI, Payment Card Data or other FIS Confidential Information.

"**Inventions**" are any discoveries, improvements, copyrights, programs, trademarks, processes, and systems relating to the Deliverables and the business of FIS and applications thereof, that Vendor may conceive, discover or make solely or jointly at any time during the Engagement, whether or not patentable or eligible to be copyrighted, and whether or not using the time, facilities, equipment or personnel of FIS.

"**Law**" means applicable laws collectively, including statutes, codes, rules, regulations, ordinances and orders of governmental authorities.

"**Losses**" means liabilities, claims, proceedings, judgments, damages, demands, actions, costs, charges, expenses, penalties, fines, settlements and any other loss of whatever nature, including court costs, legal counsel costs and legal fees.

A "**Notice of Contract Breach**" is a notice by one party to the other to notify the other of a material breach of the Agreement by the other party, describing why the notifying party believes the other party has committed a breach, including the applicable provision(s) of the Agreement and the applicable date(s) of the other party's act(s) or omission(s), and the cure or other relief the notifying party is requesting.

"**NPI**" is "nonpublic personal information" protected under the Gramm-Leach-Bliley Act of 1999 or a state law equivalent.

"**Payment Card Data**" is cardholder data protected under the Payment Card Industry Data Security Standard (PCI DSS).

"**PHI**" is "protected health information" protected under the Health Insurance Portability and Accountability Act of 1996 or a state law equivalent.

The "**Privacy Regulations**" are the standards, guidelines and other regulations established by various federal or state regulatory agencies to protect the privacy and security of customer or patient information held by financial institutions, medical service providers and other entities.

A "**Service**" is a service provided under the Agreement for data processing, software hosting, software as a service, a knowledge or information service, provision of work or workers on an outsourced basis, production

management, customization or other custom development, training and support, and various other matters as requested by FIS and as more particularly described in the Agreement.

"**Software**" means the Vendor's software licensed to FIS under the Agreement including any subsequent modifications, enhancements, patches, versions, or updates thereto supplied by Vendor to FIS.

The "**Term**" is the term of the Agreement, including any extensions or renewals.

The phrase "**under the Agreement**" means under the Agreement directly or indirectly, such as through a statement of work or other contract made under the Agreement for the purchase of one or more Services or Software, and the phrase "with the Agreement" refers to the Agreement and any such other contract.

"**Use**" or "**use**" means FIS' and Designated End Users' right to (a) perform, display, copy, load into a computer's memory, and test the Software, (b) maintain copies of the Software and Documentation for back-up or archival purposes, (c) allow FIS' Contractors to utilize the Software exclusively for the purpose of processing FIS' or its Designated End User's data.

"**Vendor**" is the party identified as such in the Agreement.

"**Vendor Personnel**" are individuals who are assigned to perform a Service under the Agreement, including employees of Vendor or its Affiliates, employees of any Contractor to Vendor, and if an individual, Vendor or any Contractor to Vendor.

The terms, "**Controller**," "**Personal Data**," "**Processing**," and "**Processor**" shall have the same meaning as in the GDPR as it may be amended from time to time, and their related terms shall be construed accordingly for purposes of this Agreement.

2. **SAFETY AND SECURITY**.

2.1 ON PREMISES OF FIS AND ITS CLIENTS. All Vendor Personnel must comply with all FIS postings and notices regarding safety and security when on the premises of FIS, and with the postings and notices of Clients or their customers when on their premises. Without limitation of the foregoing, in all events Vendor Personnel must not carry weapons or ammunition onto the premises of FIS, Clients, or their customers and must not use or carry weapons or ammunition while attending FIS-sponsored events.

2.2 ACCESS PRIVILEGES AND RESTRICTIONS. In the event Vendor Personnel will receive access credentials for FIS' facilities, applications, systems or servers, those of its Affiliates or those of any Clients or any of their customers, the following provisions will also apply:

2.2.1 Vendor will require all Vendor Personnel that will be issued access credentials to submit to FIS' then current access credentialing process.

2.2.2 Vendor will promptly, but in any event within twenty-four (24) hours, (i) confiscate each such access credential from Vendor Personnel when the Vendor Personnel's need to have such access in order for the Services to be performed is discontinued and (ii) notify FIS of any change in the status (including any such suspension, termination or discontinuation) of Vendor Personnel for whom such a device or access credential has been requested or to whom such a device or access credential has been provided.

2.2.3 Vendor will not request that such an access credential be provided, or provide such an access credential, to any individual who will not be directly engaged by or at the request of FIS to provide Services.

2.2.4 FIS reserves the right to deny any access credential request or terminate any access credential that has been provided. Vendor will notify FIS within twenty-four (24) hours of any changes to the Vendor Personnel for whom such an access credential has been requested or to whom such an access credential has been provided.

2.2.5 Vendor will not permit any such access credential to be used by more than one individual.

2.3 INFORMATION SECURITY AND INTERNAL CONTROLS. In the event Vendor (i) stores any data of FIS, its Clients or their customers, otherwise has any such data in its possession or control, (ii) has access to any such data from outside the premises of FIS, FIS Affiliates, Clients or customers of Clients, or (iii) has access to any networks of FIS, FIS Affiliates, Clients or customers of Clients, the following provisions will apply to Vendor. In the event an entity other than Vendor does so under a contract with Vendor or otherwise for or on behalf of Vendor, Vendor will ensure by contract or otherwise that the following provisions apply correspondingly to the other entity for the benefit of FIS.

2.3.1 Vendor will be responsible for establishing and maintaining an information security program to (i) ensure the security and confidentiality of such data, (ii) protect against any anticipated threats or hazards to the

security or integrity of such data, and (iii) protect against unauthorized access to or use of such data that could result in substantial harm or inconvenience to FIS, FIS Affiliates, Clients or customers of Clients.

2.3.2 The Vendor will implement and operate:

(a) Where technically possible, up to date anti-virus software upon all systems and networks used in the provision of the Services;

(b) The Services upon supported technologies which are kept up to date with the latest versions;

(c) A patch management process, which ensures patches are appropriately tested and deployed to rectify security vulnerabilities in a reasonable timeframe with critical or urgent patches deployed within thirty (30) days of release;

(d) A vulnerability management program that is undertaken on a frequent basis (at least quarterly) that includes (a) scanning the networks, infrastructure, applications and websites used in the provision of the Services, (b) validating any vulnerabilities found, and determining their criticality based upon industry recognized methods such as CVSS, and (c) creating and undertaking a plan to remediate the discovered vulnerabilities, based upon their criticality, at its own cost and in a timely manner;

(e) Standards to ensure that its systems are configured in a secure state, in line with industry recognized best practices, such as the National Institute of Standards and Technology ("**NIST**") or the Center of Internet Security;

(f) Robust processes to ensure that access to FIS data under its control is restricted to those individuals whom are explicitly authorized to access such data in the course of delivering the Services. Access shall be limited to those with a business need for such access and to those privileges needed to fulfil that need only. Access shall be assigned using unique logon credentials to ensure accountability is maintained;

(g) A robust and enforceable password policy in place that mandates the use of complex passwords and forces users to periodically change their password;

(h) Strong authentication methods (two-factor authentication) for those Vendor Personnel who work remotely and for those with administrative privileges upon systems used to provide the Deliverables or Services. Such access must be via encrypted communications;

(i) Multi-factor authentication for all internet facing systems storing and processing FIS data;

(j) Mechanisms to prevent the unauthorized removal of FIS data from the Vendor's networks via technologies such as removable media devices, the internet, email or instant messaging services;

(k) Strong encryption technologies (in line with industry standards such as NIST approved) to protect logon credentials, and FIS data during transmission and storage;

(l) The Vendor will implement and operate application level encryption ("**ALE**") technologies to protect sensitive data in-scope for FIS data at rest. ALE is defined as 1) the encryption of in-scope data by the application 2) encryption must occur before being written to a data store or being consumed by the application, 3) encryption must not be dependent on any underlying transport and/or other at-rest encryption including but not limited to the Vendor's use of native cloud encryption technologies and 4) ALE algorithms must meet strong encryption technologies (in line with industry standards such as NIST approved);

(m) Encryption technologies upon portable devices such as laptops, PDAs and smartphones, in order to protect any FIS information shared via, or stored upon, such technologies;

(n) Physical controls to mitigate the risk of unauthorized intrusion to Vendor's premises, networks and systems including, without limitation, (a) an auditable electronic access system that requires physical access tokens (such as swipe cards, biometric token, keys or fobs) to achieve access, (b) closed circuit television ("**CCTV**") coverage of all entry points, (c) intruder detection systems and burglar alarms, (d) processes to grant access only to authorized individuals, (e) processes to revoke physical access when no longer required, and (f) processes to manage visitors are authorized and supervised;

(o) Logical controls to mitigate the risk of unauthorized intrusion to Vendor's premises, networks and systems including, without limitation, (a) appropriately configured and maintained firewalls, (b) up to date intrusion detection systems, (c) centralized logging systems that records networks and systems activity and retains the ability to inspect these logs in the event of a suspected or realized security breach, (d) the monitoring and inspection of such logs by persons separate from those responsible for administration of networks and systems;

(p) Systems and software development processes to ensure that commonly known security flaws (such as those defined by the Open Web Application Security Project) are not introduced into systems used to supply the Services. Such controls must include: (i) sufficient training for its software developers to ensure that the probability of security flaws being introduced is minimalized, and (ii) the testing of application and website code to eliminate security flaws;

(q) Separate environments between test and production systems and will ensure that no production data of FIS is used in test systems;

(r) Robust processes to ensure that changes to the premises, networks, systems and software used to supply the Services are appropriately evaluated, tested and implemented to limit the potential of service degradation;

(s) Processes to continually monitor its networks and systems for potential or actual security breaches;

(t) Processes to ensure that any FIS data is retained in accordance with a data retention policy which complies with FIS' requirements, and applicable legal or regulatory requirements;

(u) Processes to promptly return and/or erase all data in Vendor's possession or control, at the request and option of FIS, in a manner that maintains its confidentiality and integrity, as agreed between the parties;

(v) Processes to ensure that all information pertaining to, provided by, or owned by FIS is securely destroyed to beyond the point of recovery (once approved by FIS) as soon as it is outside the agreed retention policy or no longer required for a valid business purpose, including electronic and physical information assets. Certificates of destruction will be retained for audit purposes;

(w) Training in accordance good industry practice on secure software development at least annually for Vendor Personnel involved in the architecture and design, and development and testing of FIS software;

(x) Secure development lifecycle ("**SDLC**") processes based on Good Industry Practice; and

(y) Automated or manual analysis of the security of any code developed, remediation of any vulnerabilities prior to deployment to FIS, and the provision of reports of such analysis to FIS.

2.3.3 The Vendor will implement and operate regular penetration tests ("**Vendor Security Tests**") upon the networks, infrastructure, applications and websites used in the provision of the Services, no less than once per calendar year and share the results of the Vendor Security Tests with FIS on request. If after reviewing such test results, FIS believes that additional testing is warranted, FIS and Vendor will discuss such additional testing in good faith. Vendor shall also permit FIS or a security consultant selected and approved by FIS to carry out penetration tests ("**FIS Security Tests**") on the Vendor's systems. The Vendor shall provide FIS with all reasonable assistance to enable FIS to perform the FIS Security Tests. FIS agrees to share the results of any vulnerability scan or penetration test it performs on Vendor's environment to assist Vendor in correcting any information security vulnerabilities identified. Vendor will correct (at its own cost) any information security vulnerability identified in the Vendor Security Tests or the FIS Security Tests within the applicable time periods below, based on the severity level of the vulnerability:

- Critical (CVSS Score: 9 - 10) severity vulnerabilities will be corrected within fourteen (14) days.
- High (CVSS Score: 7 - 8.9) severity vulnerabilities will be corrected within forty-five (45) days.
- Medium (CVSS Score: 4 – 6.9) severity vulnerabilities will be corrected within ninety (90) days
- Low (CVSS Score: less than 4) severity vulnerabilities will be corrected within one hundred and twenty (120) days

2.3.4 Where all, or part of, the Services are provided using online services (i.e. accessible via the internet), the Vendor must ensure that adequate protection is in place to mitigate the risk of denial-of-service (DoS) threats.

2.3.5 Vendor shall ensure that processes employed in the provision of the Services are staffed in such manner as to prevent conflicts of interest, fraud or error by invoking appropriate separation of duties.

2.3.6 Vendor shall ensure that information security awareness and training programs are provided for those responsible for handling FIS data, upon hire and on at least an annual basis.

2.3.7 Vendor will promptly notify FIS of any and all breaches to Vendor's information security within twenty-four (24) hours of discovering the Information Breach and work with FIS management to identify the root

cause of the incident and the potential impact to FIS, its Clients or their customers, as reasonably requested by FIS.

2.3.8 If and to the extent Vendor or any Service is subject to the Payment Card Industry Data Security Standard requirements (as amended from time to time) ("**PCI DSS**"), Vendor will comply with said requirements. In addition, if and to the extent Vendor or any Service is subject to PCI DSS requirements: (i) Vendor will submit their Attestation of Compliance ("**AOC**") and Vendor Responsibility Matrix within ten (10) days of the execution of this Agreement and will have an AOC and Vendor Responsibility Matrix prepared, and provide to FIS such updated AOC and Vendor Responsibility Matrix, annually thereafter; (ii) Vendor will publish to 'Visa' Global Service Vendor registry and maintain 'Green Status' in such registry throughout the duration of the Agreement; and (iii) if Vendor fails to maintain 'Green Status' in the Visa Global Service Vendor registry, the following provisions shall apply: (A) If Vendor in 'Yellow Status' in the Visa Global Service Vendor registry, Vendor will provide the Services free of charge until Vendor obtains 'Green Status'; and (B) If Vendor is in 'Red Status' or is not listed in the Visa Global Service Vendor registry: (a) Vendor will provide the Services free of charge free of charge until Vendor obtains 'Green Status' or the Agreement terminates, (b) Vendor will refund to FIS the six (6) then most recent months of fees paid by FIS under the Agreement (excluding any period in which Vendor was providing the Services free of charge due to Vendor being in 'Yellow Status' or 'Red Status' pursuant to this provision), and (c) FIS may, in addition to any other remedies FIS may have, terminate the Agreement with no financial obligation to Vendor arising from such termination.

2.4 BACKGROUND CHECKS. Vendor will perform the background check, as described herein, and also timely cooperate in good faith with FIS' performance of a background check, as described herein, for each individual who is performing any Services under the Agreement and has access to the facilities, records or data of FIS, any Affiliate, any Client or any customer of a Client. Where permitted by applicable Law, the background check will consist of, at a minimum, verification of the highest level of education completed, verification of employment for the past ten (10) years, social security number trace and validation, and a check of U.S. Government Specially Designated National (OFAC) and export denial lists. In addition, to the extent permitted by Law, the background check will include a 9-panel drug test and criminal record search. For the drug test, all specimens will be tested at a Department of Health and Human Services/Substance Abuse Mental Health Services Administration certified lab, and the screening service will include confirmation of all positive test results. The criminal record search will include, to the maximum extent permitted by Law, a federal, state and county check, and a National Criminal File check, for felony and misdemeanor convictions for the last ten (10) years in all locations where the individual has resided for the last ten (10) years. Vendor will comply with all applicable Laws related to the background check, including required notices and applicable consents. In addition, Vendor will require the individual to report any criminal convictions. Vendor will not assign anyone to perform Services for FIS who has tested positive for drugs or whose background check findings do not meet the standards established by Vendor in accordance with all applicable Laws, including without limitation if there is a conviction or referral to a pretrial diversion program for a crime that is related to his or her duties. Vendor acknowledges that under the banking Laws, an individual may not participate, directly or indirectly, in any manner in the conduct of the affairs of any insured depository institution without regulatory consent if he or she has a conviction, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution, of a crime involving dishonesty, breach of trust or money laundering, including any crime concerning the illegal manufacture, sale, distribution of or trafficking in controlled substances, unless the crime meets certain criteria for treating the crime as de minimis. The background check must be completed before assignment of an individual and periodically thereafter. FIS also reserves the right to request that Vendor provide an attestation confirming a background check as required by this provision has been completed and no disqualifying information has been identified on an annual basis during the Term of an Engagement. Upon five (5) Business Days' prior written notice, FIS may verify Vendor's compliance with this Section. Such verification will be conducted in a manner that minimizes disruption to Vendor's business. FIS may use an independent auditor to assist with such verification, provided that FIS has a written confidentiality agreement in place with such independent auditor. FIS will notify Vendor in writing if any such verification indicates that Vendor is not in compliance with this Section and Vendor will promptly remediate any issues of non-compliance discovered by FIS as part of such verification.

2.5 All FIS' audit rights of the Agreement including without limitation to examine Vendor's records (which must include auditable records of all financial and non-financial transactions relating to Products and Services) may, to the extent required by the regulators of FIS and/or its Clients, be exercised by FIS, FIS' Clients, and its and their regulators.

2.6 DESTRUCTIVE ELEMENTS. Vendor represents, warrants and covenants that it will not introduce or allow any Destructive Elements into the Services, any Products or Deliverables, or into the systems of FIS or any of FIS

Clients or their customers. Without limitation of the foregoing, Vendor warrants and covenants that it will use best efforts to avoid the coding or introduction of Destructive Elements into any systems used to provide Services, Products or Deliverables. Vendor will assist FIS with mitigation of any loss of operational efficiency or loss of data caused by such Destructive Elements. Upon learning of or discovering a cyber or information-security threat or vulnerability to FIS systems or to FIS Clients or their customers (including without limitation notifications received from security researchers, industry resources, or bug bounty programs), Vendor will promptly notify and cooperate with FIS and take all reasonable and necessary steps to isolate, mitigate, and remediate such known or suspected threat or vulnerability.

3. **SAFEGUARDING INFORMATION**

3.1 CONSUMER INFORMATION AND PRIVACY. If, in connection with the Agreement, Vendor receives, stores or accesses any Personal Data, NPI, PHI, Payment Card Data, or other information or materials that are subject to the Privacy Regulations and Guidelines, Vendor will comply with the applicable requirements of the Privacy Regulations and Guidelines. Vendor acknowledges that the Guidelines include provisions regarding the safeguarding of consumer information, response programs and notice in the event of unauthorized access to consumer information, that FIS provides information processing services to Clients subject to the Guidelines, and that FIS may be required to notify Clients, their customers or other third parties of security incidents that result, or are likely to result, in misuse or unauthorized possession or disclosure of Personal Data, NPI, PHI, Payment Card Data or other Confidential Information. Without limiting the foregoing, and in addition to its confidentiality and security obligations as otherwise set forth in the Agreement, Vendor will (i) ensure the security and confidentiality of such information or materials, (ii) protect against any anticipated threats or hazards to the security or integrity of such records, (iii) detect unauthorized access to or use of such records or information, and (iv) protect against unauthorized access to or use of such records or information that would result in harm or inconvenience to any Client or any customer of a Client. Vendor represents and warrants that it has and will maintain in place commercially reasonable precautions to safeguard the confidentiality, security and integrity of FIS Confidential Information in a manner designed to meet the requirements of this Section. These precautions will include but will not be limited to (i) contractual restrictions on access to the information by Contractors and Vendor's other vendors, (ii) intrusion detection systems on all information systems of FIS maintained or controlled by Vendor, and (iii) notification procedures for notifying FIS promptly in the event a security breach is detected or suspected, as well as other response programs when there is a suspected or detected Breach involving Personal Data, NPI, PHI or Payment Card Data. These precautions will also include, as appropriate, (A) access controls to FIS information systems, including controls to identify and permit access only to authorized individuals and controls to prevent access to FIS Confidential Information through improper means, (B) Vendor Personnel controls and training, (C) physical access restrictions at locations where FIS Confidential Information is located, (D) encryption of electronic FIS Confidential Information when appropriate or legally required, and (E) a disaster recovery plan as appropriate to protect against loss or damage to FIS Confidential Information due to potential hazards such as fire or water damage or technological failures. Vendor will (1) monitor the foregoing measures with periodic audits or testing and (2) provide copies of the same sufficient to assure FIS or its regulatory authorities that Vendor is implementing these precautions, and (3) notify FIS immediately in the event there is any suspected or actual unauthorized access, use, disclosure or alteration to FIS Confidential Information. Vendor will indemnify FIS from, defend FIS against, and pay any final judgments awarded against FIS, resulting from any claim brought by a third party, including but not limited to a customer of FIS, against FIS based on any breach of such privacy Laws, rules or regulations by Vendor, including Vendor Personnel.

3.1.1 Vendor will also use the information security safeguards described in Section 3.1 to protect any Confidential Information of FIS and FIS Clients comprising technical data, technical schematics, and any infrastructure, hardware, and/or software and systems information of FIS and FIS Clients that, if disclosed publicly, could enable or facilitate unauthorized access to such Confidential Information.

3.2 PROTECTION OF CONFIDENTIAL INFORMATION. Each party must protect the other's Confidential Information with the same degree of care used to protect its own Confidential Information, but in no event may either party use less than a reasonable standard of care be in connection with the preservation of the other's Confidential Information. FIS designates as its Confidential Information (i) the Agreement, (ii) any information obtained from or related to any Client of FIS including FIS Client business strategy, direction and contract information, (iii) any Personal Data, NPI, PHI, or Payment Card Data (iv) FIS' employee records (name, address, phone number, salary, taxpayer or government identification number, date of birth, health records, bank account information, labor party), (v) any business strategies and directions, operating or marketing plans, intellectual capital or trade secrets, (vi) memos or other documents or communications pertaining to pending FIS litigation or contracts (including the Agreement), (vii) any information disclosed by FIS that is designated as "confidential" at or

prior to disclosure, (viii) other FIS data or information which is not generally known, including business information, specifications, research, software, trade secrets, discoveries, ideas, know-how, designs, drawings, flow charts, data, computer programs, marketing plans, budget figures, and other financial and business information, and (ix) information of the kind described by any of the foregoing categories that is of or disclosed by a Client, an FIS Affiliate, or a customer of a Client. Vendor will (A) restrict the use and disclosure of the FIS' Confidential Information to its Vendor Personnel and do so solely on a "need to know" basis in connection with Vendor's obligations to provide Software or to perform Services in accordance with the Agreement, (B) ensure Vendor Personnel who receive or have access to FIS Confidential Information are bound by confidentiality obligations at least as restrictive and as protective of the FIS Confidential Information as the provisions of this Section, (C) require its Vendor Personnel to protect and restrict the use of the FIS' Confidential Information, (D) establish procedural, physical and electronic safeguards, designed to prevent the compromise or unauthorized disclosure of FIS Confidential Information and to achieve the objectives of the Guidelines (if applicable), (E) promptly investigate any security breach to determine whether such incident has resulted or is likely to result in misuse or unauthorized possession or disclosure of FIS Confidential Information and (F) not use or disclose FIS' Confidential Information except in accordance with the Agreement.

3.3 In providing any notice of an Information Breach, Vendor will use commercially reasonable efforts to (i) provide notice to one or more FIS managers generally responsible for security matters relating to the FIS Confidential Information affected by the Information Breach, within twenty-four (24) hours of discovering the Information Breach, and (ii) keep FIS informed as to the actual and anticipated effects of the Information Breach and the corrective actions taken or to be taken in response to the Information Breach. In addition, if the Information Breach results or is likely to result in misuse of Personal Data, NPI, PHI or Payment Card Data, Vendor will (A) notify FIS as soon as possible and reasonably cooperate with FIS in its efforts to notify affected Clients and their customers and to mitigate the actual or potential harm resulting from the Information Breach and (B) reimburse FIS for its reasonable costs in notifying Clients or their customers of the Information Breach and making available to them any credit monitoring services and for any other costs FIS reasonably incurs with respect to the Information Breach.

3.4 Confidential Information will remain the property of the party from or through whom it was provided. Except for NPI, PHI, Payment Card Data, or other information protected by the Guidelines, the parties' respective confidentiality obligations under the Agreement do not apply to any information that: (i) was previously known by the party; (ii) is a matter of public knowledge; (iii) was or is independently developed by the party; (iv) is released for disclosure with written consent of the party; or (v) is received from a third party to whom it was disclosed without restriction.

3.5 Each party may disclose information notwithstanding its confidentiality obligations under the Agreement to the extent required (i) by Law, (ii) in connection with the tax treatment or tax structure of the Agreement; or (iii) in response to a valid order of a U.S. court or other governmental body, provided that the party provides the other party with written notice and the other party is afforded a reasonable opportunity to obtain a protective order with respect to the disclosure.

3.6 Upon termination of the Agreement, Vendor will destroy all FIS Confidential Information in a manner designed to preserve its confidentiality, or, at the other party's written request and expense, return it to FIS. Upon FIS' written request, Vendor shall, at FIS' choice, delete or return all Personal Data Processed on behalf of FIS to FIS after the end of the provision of Services relating to Processing, subject to Vendor retaining any copies required by applicable EU member state law.

3.7 FIS will have and retain all right, title and interest in all of FIS' Confidential Information, whether possessed by FIS prior to, or acquired or refined by FIS (either independently or in concert with Vendor) during the Term.

3.8 Vendor will not, without the prior written consent of FIS, (i) provide the Software or Services or access, store or process any of FIS' Confidential Information outside the United States or (ii) export any of FIS' Confidential Information to anywhere outside the United States. The provisions of the Agreement apply without regard to where the Software or Services are provided or FIS Confidential Information is accessed, stored or processed.

3.9 EU GDPR Compliance. If Vendor shall process any Personal Data from FIS or a Client as part of the Services under the Agreement regarding individuals domiciled in countries outside of the United States (or to which the GDPR is otherwise applicable), such processing shall be in compliance with the Data Protection Addendum attached hereto as Appendix A and incorporated herein by this reference.

4. **SUBCONTRACTORS.**

4.1 Vendor will not utilize any Contractor to perform Services or provide any part of a Deliverable, without the prior written consent of FIS. Vendor will notify FIS of its intention to so engage another party not less than thirty (30) days prior to the entity commencing performance of any Services or to provide any part of the Deliverable. Vendor will provide such information and documentation concerning any such proposed party as FIS requests. Vendor will ensure that any such Contractor complies with all obligations of Vendor under the Agreement. Vendor is responsible for all of its obligations under the Agreement regardless of where performed or whether performed by any Contractor, and Vendor will be liable for the acts and omissions of any Contractor that Vendor uses to perform Services or provide any part of any Deliverable.

4.2 SERVICES PERFORMED BY PROVIDER PERSONNEL IN UK. If Vendor shall assign Vendor Personnel that are located in the United Kingdom to perform any part of the Services under the Agreement, then such performance shall be in compliance with the UK Services Terms attached hereto as **Appendix B** and incorporated herein by this reference.

5. Vendor may not engage sub-Processors under the Agreement or give access to or transfer any Personal Data to any third party (including any affiliates, group companies or sub-contractors) without the prior written consent of FIS and the relevant FIS Affiliates. If FIS consents to the use of third parties as sub-Processors Vendor shall (i) impose in writing upon such sub-Processors the same data protection obligations as set out herein and as are required by applicable Data Protection Legislation and (ii) be responsible for the acts and omissions of such sub-Processors under the Agreement. Where prior written consent given by FIS pursuant to this clause authorizes a class of third party to Process Personal Data, the Vendor shall notify FIS of any intended changes concerning the addition or replacement of any sub-Processors within such class, and FIS shall have the right to object to, and prevent, any such addition or replacement of sub-Processors within such class.

5.1 **COMPLIANCE WITH LAWS.** In all circumstances, Vendor will comply with, and will ensure that all Software, Services and Deliverables comply with all Law, including Law relating to export and import, privacy, use, disclosure or transfer of personal information, or security, and Law relating to the employment, health, safety and payment of Vendor Personnel. Vendor will perform an on-going review of Law applicable to Vendor's performance under the Agreement, including Law enacted or amended after the effective date of the Agreement. Vendor will identify and procure all permits, certificates, approvals, licenses, and inspections necessary for Vendor's performance under the Agreement other than such permits, certificates, approvals, licenses and inspections that FIS is directly responsible for obtaining under the Agreement. Without limiting any other obligation of Vendor under the Agreement, Vendor will at all times comply with all Law relating to trade sanctions, export controls, the U.S. Foreign Assets Control Regulations, the U.S. Export Administration Regulations, and the U.S. International Traffic in Arms Regulations.

6. **DATA PROTECTION TECHNICAL AND ORGANISATIONAL MEASURES**

6.1 In the course of Vendor providing Services under the Agreement(s), FIS may from time-to-time provide or make available Data to Vendor. The Agreement(s) determines the subject matter and the duration of Vendor's Processing of Personal Data, as well as the nature and purpose of any collection, use, and other Processing of Personal Data and the rights and obligations of FIS.

6.2 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 of varying likelihood and severity for the rights and freedoms of natural persons, Vendor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. As a minimum, these should include the requirements required under applicable Data Protection Legislation and the requirements set out in the Agreement. Upon request, Vendor shall provide a written description of the technical and organizational measures the Vendor employs for Processing Personal Data.

6.3 Vendor must cooperate upon FIS' reasonable request in order to assist FIS with its compliance with applicable privacy laws, including FIS' handling of Data Subject rights requests.

6.4 Where Vendor is acting as a Processor under the Agreement, at FIS' written request, Vendor shall make available to FIS all information reasonably necessary to demonstrate Vendor's compliance with the obligations agreed to in the Agreement(s), applicable privacy laws, and any data protection addenda.

6.5 Unless Vendor needs identifiable information in order to provide the product or service, Vendor will deidentify or pseudonymize FIS' data unless there is a need for the data to be identifiable.

6.6 Vendor must consider data protection issues as part of the default configuration of its systems, services, products, and business practices. Vendor's default configuration will follow privacy by default principles, including

data quality, minimization, and accountability. Vendor will Process FIS data in accordance with FIS instructions and only when relevant, minimal, and not excessive.

6.7 Vendor will provide certification and assurance of its processes and products pursuant to the GDPR.

7. **BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY**. To the extent applicable to the Services, Vendor will establish and maintain disaster recovery and business continuity plans designed to minimize the risks associated with a disaster affecting Vendor's ability to provide the Services, which includes off-site data storage and recovery infrastructure. Vendor's recovery time objective for the Services ("**RTO**") under such plan is [INSERT TIMEFRAME] hours/minutes. Vendor will maintain adequate backup procedures in order to recover FIS' or if applicable any Client's data to the point of the last available good backup. Vendor's recovery point objective ("**RPO**") is [INSERT TIMEFRAME] hours/minutes. Vendor will test its disaster recovery and business continuity plans, including call trees, not less frequently than annually, will annually provide to FIS disaster recovery and business continuity plans test results. If Vendor fails to meet the RTO and RPO in any annual test, Vendor shall perform a root cause analysis of the cause of the failure to meet the RTO or RPO and will remediate the cause of such failure and retest within six (6) months of the failed test. If Vendor fails to meet the RTO or RPO in the retest, Vendor will have a second six (6) month period to remediate and retest. If provider fails a second time, FIS may request that the parties attempt to reach a mutually agreeable resolution, and if the parties are unable to agree upon a resolution within thirty (30) days of FIS' request, FIS may terminate the Agreement with no further financial obligation to Vendor. Vendor will provide its disaster recovery plan and test results to FIS and FIS may share such disaster recovery plan and test results with Clients who have contracted for the Services, if any, FIS' auditors, and FIS' regulators. Vendor will implement the applicable disaster recovery or business continuity plan upon the occurrence of a disaster, and shall notify FIS promptly following such event. In the event of a disaster (as defined in the plan), Vendor will not charge fees higher than or in addition to the agreed fees under the Agreement. Vendor will notify of, and invite FIS to participate in (at no additional charge to FIS), Vendor's disaster recovery and business continuity plan test.

PART G3

Vendor Data Processing Addendum
Processor to Subprocessor

THIS DATA PROCESSING ADDENDUM is entered into as of the Addendum Effective Date by and between: (1) [INSERT FIS ENTITY] with an address at [INSERT ADDRESS] ("**FIS**"); and (2) [INSERT VENDOR ENTITY] with an address at [INSERT ADDRESS] ("**Vendor**").

1. INTERPRETATION

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

(a) **"Addendum Effective Date**" means [the effective date of the Agreement] **OR** [INSERT SPECIFIC EFFECTIVE DATE].

(b) "**Agreement**" means the [INSERT TITLE OF AGREEMENT] entered into by and between the parties on [DATE] **OR** [or around the date of execution of this Data Processing Addendum].

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

(d) "**Client**" means a client of FIS who supplied the Client Personal Data.

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

(f) "**Data Protection Laws**" means: (i) the GDPR; and (ii) to the extent applicable, the data protection or privacy laws of any other country.

(g) "**Data Subject**" means the identified or identifiable natural person to whom Client Personal Data relates.

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

(i) "**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

(j) "**FIS Affiliates**" means any companies which are controlled by FIS, which control FIS or which are under common control with FIS and either: (i) are Controllers of any Client Personal Data; and/or (ii) on whose behalf Vendor and/or any Subprocessor otherwise processes any Client 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.

(k) "**GDPR**" means the UK GDPR and/or EU GDPR (as applicable), together with any applicable implementing or supplementary legislation in any member state of the EEA or the UK (including the UK Data Protection Act 2018). References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(l) "**Personal Data Breach**" means any actual or reasonably suspected 'personal data breach' (as defined in Article 4(12) of the GDPR).

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

(n) "**Relevant Body**":

(i) in the context of the UK GDPR, means the UK Information Commissioner's Office; and/or

(ii) in the context of the EU GDPR, means the European Commission.

(o) "**Restricted Country**":

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

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

that the Relevant Body has not deemed to provide an 'adequate' level of protection for Personal Data pursuant to a decision made in accordance Article 45(1) of the GDPR.

(p) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Personal Data to any person in a Restricted Country, which would be prohibited without a legal basis therefor under Chapter V of the GDPR.

(q) "**Security Requirements**" means FIS' information security policies and procedures for its suppliers attached hereto as Annex 3 (*Security Standards*), as may be updated from time to time by mutual agreement of the Parties.

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

(s) "**Standard Contractual Clauses**":

(i) in the context of a Restricted Transfer originating in the UK, means the standard contractual clauses approved by the European Commission pursuant to Commission Implementing Decision (EU) 2010/87, as set out in full in Annex 4 (*Standard Contractual Clauses For Restricted Transfers Originating in the UK*); and

(ii) in the context of a Restricted Transfer originating in the EEA, 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 in Annex 5 (*Standard Contractual Clauses For Restricted Transfers Originating in the EEA*);

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

(u) "**Supervisory Authority**":

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

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

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

(w) "**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).

1.2. In this Data Processing Addendum:

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

(b) unless otherwise defined in this Data Processing Addendum, all capitalised terms in this Data Processing Addendum shall have the meaning given to them in the Agreement; and

(c) any reference to any statute, regulation or other legislation in this Data Processing Addendum 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 CLIENT PERSONAL DATA

2.1. The parties acknowledge and agree that FIS supplies a service to Clients, and that FIS has appointed Vendor in connection with such services pursuant to the Agreement.

2.2. In the course of Vendor providing the Services under the Agreement, Vendor may from time-to-time Process Client Personal Data supplied to it by or on behalf of FIS or an FIS Affiliate. The parties acknowledge and agree that, in relation to any Client Personal Data provided or made available to Vendor for Processing in connection with the Services, the **Client is the Controller**, **FIS is a Processor**, and **Vendor is an additional Processor** for the purposes of the GDPR.

2.3. Vendor shall:

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

(b) not Process Client Personal Data other than:

(i) on Client's written instructions as relayed by FIS (including the instruction set out in Section 2.5); or

(ii) as otherwise strictly required by applicable laws.

2.4. To the extent permitted by applicable laws, Vendor shall inform FIS of:

(a) any Processing to be carried out under Section 2.3(b)(ii); and

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

before the relevant Processing of that Client Personal Data.

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

2.6. Annex 1 (*Data Processing Details*) sets out certain information regarding Vendor's Processing of Client Personal Data as required by Article 28(3) of the GDPR. The parties may from time to time amend Annex 1 (*Data Processing Details*) by mutual agreement.

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

3. VENDOR PERSONNEL

Vendor shall take reasonable steps to ensure the reliability of any Vendor's Personnel who may Process Client Personal Data, including ensuring:

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

(b) that all such individuals have been vetted by Vendor 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, Vendor shall implement appropriate technical and organisational measures in relation to Client Personal Data to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2. In assessing the appropriate level of security, Vendor shall take 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 4.1 and 4.2, Vendor shall, and shall cause each Subprocessor to, comply with the Security Requirements.

4.4. On FIS' request, Vendor shall (promptly following such request) provide to FIS written information describing in reasonable detail the technical and organisational measures taken by Vendor in relation to Client Personal Data pursuant to Section 4.1.

5. SUBPROCESSING

5.1. Vendor may continue to use those Subprocessors already engaged by Vendor as at the date of this Data Processing Addendum which are listed in Annex 2 (*Subprocessors*), subject to Vendor meeting or having met the obligations set out in Section 5.3.

5.2. Subject to Section 5.1, Vendor shall not appoint any new Subprocessors without obtaining FIS' prior approval in writing (such approval not to be unreasonably withheld or delayed).

5.3. With respect to each Subprocessor appointed by Vendor, Vendor shall:

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

(b) ensure that the arrangement between Vendor and the Subprocessor is governed by a written contract including terms which offer at least the same level of protection for Client Personal Data as those set out in this Data Processing Addendum.

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

(a) a list of the then-current Subprocessors engaged by Vendor, together with all relevant information relating to each such Subprocessor as shown in Annex 2 (*Subprocessors*); and

(b) written certification that the arrangements between Vendor and such Subprocessors meet the requirements set out in Section 5.3.

5.5. Vendor shall be liable for the acts and omissions of all Subprocessors under or in connection with this Data Processing Addendum.

6. DATA SUBJECT RIGHTS

6.1. Taking into account the nature of the Processing, Vendor shall assist FIS by implementing appropriate technical and organisational measures to enable FIS 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).

6.2. Vendor shall:

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

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

7. PERSONAL DATA BREACH

7.1. Vendor shall notify FIS without undue delay (and in any event within forty-eight (48) hours) upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Client Personal Data, providing FIS with sufficient information to allow it 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 Vendor to FIS pursuant to Section 7.1 shall include (to the extent available to Vendor 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. Vendor shall provide regular updates to FIS in respect of the resolution of any Personal Data Breach.

7.4. Vendor 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 each such Personal Data Breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Vendor shall provide reasonable assistance to FIS with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which FIS 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 Client Personal Data by, and taking into account the nature of the Processing by, and information available to, Vendor.

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 Client Personal Data (the "**Cessation Date**"), Vendor shall immediately cease all Processing of the Client Personal Data for any purpose other than for storage in accordance with this Section 9.

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

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

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

9.3. Vendor 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 Client Personal Data returned pursuant to Section 9.2(a), Vendor shall delete, and procure the deletion of, all other copies of Client Personal Data Processed by Vendor and/or any Subprocessor.

9.5. Vendor and any Subprocessor may retain certain Client 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 Vendor shall:

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

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

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

(d) ensure that such Client 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, Vendor 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, Vendor shall make available to FIS and Client all information reasonably necessary to demonstrate Vendor's compliance with the obligations laid down in this Data Processing Addendum and applicable Data Protection Laws. This could be in the form of mutually agreed third party certifications of industry standard. Vendor acknowledges and agrees that FIS may share such information with any Client.

10.2. Where the information supplied by Vendor in accordance with Section 10.1 is deemed (in FIS' sole opinion, acting reasonably) insufficient to demonstrate Vendor's compliance, Vendor shall allow for and contribute to audits, including inspections, by any Client, FIS, or an auditor mandated by any Client or FIS in relation to the Processing of Client Personal Data by Vendor and any Subprocessors.

10.3. FIS shall give Vendor reasonable notice of any audit or inspection to be conducted under Section 10.1, and Vendor 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(b)(i) or (i) below), and FIS has given notice to Vendor 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 Vendor 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 Vendor's compliance with this Data Processing Addendum (including follow-up audits); or

(ii) FIS is required or requested to carry out 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 Vendor has failed to comply with its obligations under this Data Processing Addendum, FIS shall notify Vendor and Vendor 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 Vendor and/or any Subprocessor failed to comply in any material respect with the provisions of this Data Processing Addendum, in which case Vendor shall reimburse all reasonable and documented costs incurred by FIS in connection with such inspection or audit.

11. RESTRICTED TRANSFERS

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

11.2. Notwithstanding the generality of Section 11.1, the parties agree that to the extent any Processing of Client Personal Data by Vendor involves a Restricted Transfer, the relevant Standard Contractual Clauses shall be entered into by and between (as applicable):

(a) in respect of a Restricted Transfer from Client to Vendor, FIS as agent for Client as the "data exporter" and Vendor as the "data importer" with effect from the Addendum Effective Date; and

(b) in respect of a Restricted Transfer from FIS to Vendor, FIS as the "data exporter" and Vendor as the "data importer" with effect from the Addendum Effective Date.

12. CHANGE IN LAWS

12.1. FIS may propose any variations to this Data Processing Addendum which are necessary to address the changing requirements of any Data Protection Laws (including any updates to the Standard Contractual Clauses 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 that FIS considers (acting reasonably) that any failure to agree its proposed variations to this Data Processing Addendum may cause FIS or a Client to be in material breach of Data Protection Laws, FIS may terminate the Agreement in its entirety upon written notice to Vendor with immediate effect and without liability to Vendor.

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

13. INCORPORATION AND PRECEDENCE

13.1. This Data Processing Addendum 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 Data Processing Addendum and the Agreement, this Data Processing Addendum shall prevail; or

(b) any Standard Contractual Clauses entered into pursuant to Section 11 and this Data Processing Addendum and/or the Agreement, those Standard Contractual Clauses shall prevail.

Signed by _____	Signed by _____
for and on behalf of **[INSERT FIS ENTITY]**	for and on behalf of **[INSERT VENDOR ENTITY]**
Date: _____	**Date:** _____

Annex 1

Data Processing Details

Vendor's activities

[INSERT DESCRIPTION OF VENDOR'S ACTIVITIES RELEVANT TO THE SERVICES]

Subject matter and duration of the Processing of Client Personal Data

The subject matter and duration of the Processing of the Client Personal Data are set out in the Agreement and the Data Processing Addendum.

The nature and purpose of the Processing of Client Personal Data

Vendor will process the Client Personal Data to deliver the Services pursuant to the Agreement.

The types of Client Personal Data to be Processed

☐ Contact data (e.g. name, email address, postal address)

☐ Identification data (e.g. date of birth, nationality, social security number)

☐ Solution log in and usage data

☐ Bank account data

☐ Financial data

☐ Contract and deal data (e.g. contractual/legal/financial relationship information)

☐ Billing and payments data

☐ Disclosed information from third parties (e.g. credit reference agencies or from public directories)

☐ Other; please specify: _____

The categories of Data Subjects to whom the Client Personal Data relates

☐ Client's employees

☐ Client's customers

☐ Client's potential customers

☐ Client's suppliers

☐ Contact persons

☐ Other; please specify: _____

Authorised Subprocessors

FIS authorises Vendor to appoint the Subprocessors listed in Annex 2 (*Subprocessors*).

Data retention

Vendor will delete the Client Personal Data from its systems on expiry or termination of the Services in accordance with Section 9 of the Data Processing Addendum.

Annex 2

Subprocessors

Subprocessor (full legal entity name)	Processing activities	Categories of FIS Personal Data	Location (full address)
[INSERT]	[INSERT]	[INSERT]	[INSERT]

Annex 3

Security Standards

[If the Security Standards are already set out in the MSA, please delete the Security Standards below and insert "As described in Section [x] (Information Security Requirements) of the Master [Service] Agreement."]

1. **DEFINITIONS.**

An "**Affiliate**" of a party is an entity which, directly or indirectly, controls, is controlled by, or is under common control with that party, where "control" of the party or other entity means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the party or other entity, whether through record or beneficial ownership of voting securities, by contract, or otherwise.

"**Business Days**" means any day from Monday to Friday on which FIS is open for business at the applicable FIS location(s) under the Agreement.

A "**Change in Control**" of Vendor is any event or series of events by which (i) any person, entity or group of persons or entities acquires control of Vendor, where "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of Vendor, whether through record or beneficial ownership of voting securities, by contract, or otherwise, or (ii) if Vendor is a corporation, limited liability company or other entity having a board of directors or other group of individuals having similar functions, during any period of twelve (12) consecutive months commencing before or after the date hereof, individuals who at the beginning of such twelve-month period were members of Vendor's board of directors or other such group cease for any reason to constitute a majority of the members.

A "**Claim**" is any action, litigation, or claim for which a party is subject to an indemnification obligation under the Agreement.

A "**Client**" is any current or prospective client or customer of FIS or an FIS Affiliate.

The "**Confidential Information**" of a party is any information received from the party that is of a confidential nature or is designated as 'confidential' at or prior to disclosure.

A "**Contractor**" to a party is any individual (other than the party or an employee of the party), corporation or other entity providing services to or on behalf of the party, including any direct or indirect independent contractor or subcontractor to the party.

"**Control**" of a legal entity is the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity, whether through record or beneficial ownership of voting securities, by contract or otherwise.

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

The "**Deliverables**" are any tangible or intangible products or services and other outcomes and outputs of the Services provided by Vendor to FIS or a FIS Affiliate under and as more particularly described and identified in the Agreement.

"**Designated End User**" shall mean the authorized employee(s) or agent(s) or Client(s) of FIS that are permitted to access and use the Software as contemplated under the Agreement.

A "**Destructive Element**" is any computer code or other technological device which (i) is intentionally designed to disrupt, disable, harm or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of a software, firmware, hardware, computer system or network (sometimes referred to as "viruses" or "worms"), (ii) would disable a Deliverable or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral (sometimes referred to as "time bombs," "time locks," or "drop dead" devices), (iii) would permit Vendor, any Vendor Personnel or any licensor or Contractor to Vendor to access a Deliverable to cause such disablement or impairment (sometimes referred to as "traps," "access codes" or "trap door" devices), or (iv) contains any other similar harmful, malicious or hidden procedures, routines or mechanisms which would cause a Deliverable or any other software, firmware, hardware, computer system or network to cease functioning or damage or corrupt data, storage media, programs, equipment or communications or otherwise interfere with the operations of FIS, Clients or their customers.

"**Documentation**" means the user manuals, training materials, specifications, release notes, and other written documentation, as applicable, made available by Vendor from time to time to FIS in connection with and/or related to the Software.

The "**Effective Date**" is the date of effectiveness specified in the Agreement. If no date of effectiveness is specified in the Agreement, the Effective Date is the date FIS signs the Agreement, as determined by the date indicated for its signature.

The "**Engagement**" is the engagement of Vendor by Fidelity Information Services, LLC or its Affiliate to provide Software or Services under the Agreement.

A "**Force Majeure Event**" is an event that prevents a party's performance of an obligation under the Agreement and is beyond the reasonable control of the party, such as a natural disaster, strike, riot, earthquake, epidemic, terrorist action, war, fire, flood, unavailability of communications or electrical service provided by a third party, or governmental regulations imposed after the fact.

"**FIS**" is Fidelity Information Services, LLC. However, if a FIS Affiliate enters into the Agreement with Vendor, "FIS" refers to that FIS Affiliate for purposes of the Agreement.

"**GDPR**" means the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

"**Good Industry Practice**" means the exercise of that degree of professionalism, skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same type of activity under the same or similar circumstances;

The "**Guidelines**" are the standards and guidelines established pursuant to (i) the Gramm-Leach-Bliley Act of 1999 or a state law equivalent, relating to the protection of NPI, (ii) the Health Insurance Portability and Accountability Act of 1996 or a state law equivalent, relating to the protection of PHI, (iii) other relevant privacy Laws, or (iv) PCI DSS, relating to Payment Card Data.

An "**Information Breach**" is any actual or attempted unauthorized intrusion or other breach to the network, systems, or security of or under the management or control of Vendor affecting FIS data, including any actual or attempted access to or use, possession or release of Personal Data, NPI, PHI, Payment Card Data or other FIS Confidential Information.

"**Inventions**" are any discoveries, improvements, copyrights, programs, trademarks, processes, and systems relating to the Deliverables and the business of FIS and applications thereof, that Vendor may conceive, discover or make solely or jointly at any time during the Engagement, whether or not patentable or eligible to be copyrighted, and whether or not using the time, facilities, equipment or personnel of FIS.

"**Law**" means applicable laws collectively, including statutes, codes, rules, regulations, ordinances and orders of governmental authorities.

"**Losses**" means liabilities, claims, proceedings, judgments, damages, demands, actions, costs, charges, expenses, penalties, fines, settlements and any other loss of whatever nature, including court costs, legal counsel costs and legal fees.

A "**Notice of Contract Breach**" is a notice by one party to the other to notify the other of a material breach of the Agreement by the other party, describing why the notifying party believes the other party has committed a breach, including the applicable provision(s) of the Agreement and the applicable date(s) of the other party's act(s) or omission(s), and the cure or other relief the notifying party is requesting.

"**NPI**" is "nonpublic personal information" protected under the Gramm-Leach-Bliley Act of 1999 or a state law equivalent.

"**Payment Card Data**" is cardholder data protected under the Payment Card Industry Data Security Standard (PCI DSS).

"**PHI**" is "protected health information" protected under the Health Insurance Portability and Accountability Act of 1996 or a state law equivalent.

The "**Privacy Regulations**" are the standards, guidelines and other regulations established by various federal or state regulatory agencies to protect the privacy and security of customer or patient information held by financial institutions, medical service providers and other entities.

A "**Service**" is a service provided under the Agreement for data processing, software hosting, software as a service, a knowledge or information service, provision of work or workers on an outsourced basis, production

management, customization or other custom development, training and support, and various other matters as requested by FIS and as more particularly described in the Agreement.

"**Software**" means the Vendor's software licensed to FIS under the Agreement including any subsequent modifications, enhancements, patches, versions, or updates thereto supplied by Vendor to FIS.

The "**Term**" is the term of the Agreement, including any extensions or renewals.

The phrase "**under the Agreement**" means under the Agreement directly or indirectly, such as through a statement of work or other contract made under the Agreement for the purchase of one or more Services or Software, and the phrase "with the Agreement" refers to the Agreement and any such other contract.

"**Use**" or "**use**" means FIS' and Designated End Users' right to (a) perform, display, copy, load into a computer's memory, and test the Software, (b) maintain copies of the Software and Documentation for back-up or archival purposes, (c) allow FIS' Contractors to utilize the Software exclusively for the purpose of processing FIS' or its Designated End User's data.

"**Vendor**" is the party identified as such in the Agreement.

"**Vendor Personnel**" are individuals who are assigned to perform a Service under the Agreement, including employees of Vendor or its Affiliates, employees of any Contractor to Vendor, and if an individual, Vendor or any Contractor to Vendor.

The terms, "**Controller**," "**Personal Data**," "**Processing**," and "**Processor**" shall have the same meaning as in the GDPR as it may be amended from time to time, and their related terms shall be construed accordingly for purposes of this Agreement.

2. **SAFETY AND SECURITY**.

2.1 ON PREMISES OF FIS AND ITS CLIENTS. All Vendor Personnel must comply with all FIS postings and notices regarding safety and security when on the premises of FIS, and with the postings and notices of Clients or their customers when on their premises. Without limitation of the foregoing, in all events Vendor Personnel must not carry weapons or ammunition onto the premises of FIS, Clients, or their customers and must not use or carry weapons or ammunition while attending FIS-sponsored events.

2.2 ACCESS PRIVILEGES AND RESTRICTIONS. In the event Vendor Personnel will receive access credentials for FIS' facilities, applications, systems or servers, those of its Affiliates or those of any Clients or any of their customers, the following provisions will also apply:

2.2.1 Vendor will require all Vendor Personnel that will be issued access credentials to submit to FIS' then current access credentialing process.

2.2.2 Vendor will promptly, but in any event within twenty-four (24) hours, (i) confiscate each such access credential from Vendor Personnel when the Vendor Personnel's need to have such access in order for the Services to be performed is discontinued and (ii) notify FIS of any change in the status (including any such suspension, termination or discontinuation) of Vendor Personnel for whom such a device or access credential has been requested or to whom such a device or access credential has been provided.

2.2.3 Vendor will not request that such an access credential be provided, or provide such an access credential, to any individual who will not be directly engaged by or at the request of FIS to provide Services.

2.2.4 FIS reserves the right to deny any access credential request or terminate any access credential that has been provided. Vendor will notify FIS within twenty-four (24) hours of any changes to the Vendor Personnel for whom such an access credential has been requested or to whom such an access credential has been provided.

2.2.5 Vendor will not permit any such access credential to be used by more than one individual.

2.3 INFORMATION SECURITY AND INTERNAL CONTROLS. In the event Vendor (i) stores any data of FIS, its Clients or their customers, otherwise has any such data in its possession or control, (ii) has access to any such data from outside the premises of FIS, FIS Affiliates, Clients or customers of Clients, or (iii) has access to any networks of FIS, FIS Affiliates, Clients or customers of Clients, the following provisions will apply to Vendor. In the event an entity other than Vendor does so under a contract with Vendor or otherwise for or on behalf of Vendor, Vendor will ensure by contract or otherwise that the following provisions apply correspondingly to the other entity for the benefit of FIS.

2.3.1 Vendor will be responsible for establishing and maintaining an information security program to (i) ensure the security and confidentiality of such data, (ii) protect against any anticipated threats or hazards to the

security or integrity of such data, and (iii) protect against unauthorized access to or use of such data that could result in substantial harm or inconvenience to FIS, FIS Affiliates, Clients or customers of Clients.

2.3.2 The Vendor will implement and operate:

(a) Where technically possible, up to date anti-virus software upon all systems and networks used in the provision of the Services;

(b) The Services upon supported technologies which are kept up to date with the latest versions;

(c) A patch management process, which ensures patches are appropriately tested and deployed to rectify security vulnerabilities in a reasonable timeframe with critical or urgent patches deployed within thirty (30) days of release;

(d) A vulnerability management program that is undertaken on a frequent basis (at least quarterly) that includes (a) scanning the networks, infrastructure, applications and websites used in the provision of the Services, (b) validating any vulnerabilities found, and determining their criticality based upon industry recognized methods such as CVSS, and (c) creating and undertaking a plan to remediate the discovered vulnerabilities, based upon their criticality, at its own cost and in a timely manner;

(e) Standards to ensure that its systems are configured in a secure state, in line with industry recognized best practices, such as the National Institute of Standards and Technology ("**NIST**") or the Center of Internet Security;

(f) Robust processes to ensure that access to FIS data under its control is restricted to those individuals whom are explicitly authorized to access such data in the course of delivering the Services. Access shall be limited to those with a business need for such access and to those privileges needed to fulfil that need only. Access shall be assigned using unique logon credentials to ensure accountability is maintained;

(g) A robust and enforceable password policy in place that mandates the use of complex passwords and forces users to periodically change their password;

(h) Strong authentication methods (two-factor authentication) for those Vendor Personnel who work remotely and for those with administrative privileges upon systems used to provide the Deliverables or Services. Such access must be via encrypted communications;

(i) Multi-factor authentication for all internet facing systems storing and processing FIS data;

(j) Mechanisms to prevent the unauthorized removal of FIS data from the Vendor's networks via technologies such as removable media devices, the internet, email or instant messaging services;

(k) Strong encryption technologies (in line with industry standards such as NIST approved) to protect logon credentials, and FIS data during transmission and storage;

(l) The Vendor will implement and operate application level encryption ("**ALE**") technologies to protect sensitive data in-scope for FIS data at rest. ALE is defined as 1) the encryption of in-scope data by the application 2) encryption must occur before being written to a data store or being consumed by the application, 3) encryption must not be dependent on any underlying transport and/or other at-rest encryption including but not limited to the Vendor's use of native cloud encryption technologies and 4) ALE algorithms must meet strong encryption technologies (in line with industry standards such as NIST approved);

(m) Encryption technologies upon portable devices such as laptops, PDAs and smartphones, in order to protect any FIS information shared via, or stored upon, such technologies;

(n) Physical controls to mitigate the risk of unauthorized intrusion to Vendor's premises, networks and systems including, without limitation, (a) an auditable electronic access system that requires physical access tokens (such as swipe cards, biometric token, keys or fobs) to achieve access, (b) closed circuit television ("**CCTV**") coverage of all entry points, (c) intruder detection systems and burglar alarms, (d) processes to grant access only to authorized individuals, (e) processes to revoke physical access when no longer required, and (f) processes to manage visitors are authorized and supervised;

(o) Logical controls to mitigate the risk of unauthorized intrusion to Vendor's premises, networks and systems including, without limitation, (a) appropriately configured and maintained firewalls, (b) up to date intrusion detection systems, (c) centralized logging systems that records networks and systems activity and retains the ability to inspect these logs in the event of a suspected or realized security breach, (d) the monitoring and inspection of such logs by persons separate from those responsible for administration of networks and systems;

(p) Systems and software development processes to ensure that commonly known security flaws (such as those defined by the Open Web Application Security Project) are not introduced into systems used to supply the Services. Such controls must include: (i) sufficient training for its software developers to ensure that the probability of security flaws being introduced is minimalized, and (ii) the testing of application and website code to eliminate security flaws;

(q) Separate environments between test and production systems and will ensure that no production data of FIS is used in test systems;

(r) Robust processes to ensure that changes to the premises, networks, systems and software used to supply the Services are appropriately evaluated, tested and implemented to limit the potential of service degradation;

(s) Processes to continually monitor its networks and systems for potential or actual security breaches;

(t) Processes to ensure that any FIS data is retained in accordance with a data retention policy which complies with FIS' requirements, and applicable legal or regulatory requirements;

(u) Processes to promptly return and/or erase all data in Vendor's possession or control, at the request and option of FIS, in a manner that maintains its confidentiality and integrity, as agreed between the parties;

(v) Processes to ensure that all information pertaining to, provided by, or owned by FIS is securely destroyed to beyond the point of recovery (once approved by FIS) as soon as it is outside the agreed retention policy or no longer required for a valid business purpose, including electronic and physical information assets. Certificates of destruction will be retained for audit purposes;

(w) Training in accordance good industry practice on secure software development at least annually for Vendor Personnel involved in the architecture and design, and development and testing of FIS software;

(x) Secure development lifecycle ("**SDLC**") processes based on Good Industry Practice; and

(y) Automated or manual analysis of the security of any code developed, remediation of any vulnerabilities prior to deployment to FIS, and the provision of reports of such analysis to FIS.

2.3.3 The Vendor will implement and operate regular penetration tests ("**Vendor Security Tests**") upon the networks, infrastructure, applications and websites used in the provision of the Services, no less than once per calendar year and share the results of the Vendor Security Tests with FIS on request. If after reviewing such test results, FIS believes that additional testing is warranted, FIS and Vendor will discuss such additional testing in good faith. Vendor shall also permit FIS or a security consultant selected and approved by FIS to carry out penetration tests ("**FIS Security Tests**") on the Vendor's systems. The Vendor shall provide FIS with all reasonable assistance to enable FIS to perform the FIS Security Tests. FIS agrees to share the results of any vulnerability scan or penetration test it performs on Vendor's environment to assist Vendor in correcting any information security vulnerabilities identified. Vendor will correct (at its own cost) any information security vulnerability identified in the Vendor Security Tests or the FIS Security Tests within the applicable time periods below, based on the severity level of the vulnerability:

- Critical (CVSS Score: 9 - 10) severity vulnerabilities will be corrected within fourteen (14) days.
- High (CVSS Score: 7 - 8.9) severity vulnerabilities will be corrected within forty-five (45) days.
- Medium (CVSS Score: 4 – 6.9) severity vulnerabilities will be corrected within ninety (90) days
- Low (CVSS Score: less than 4) severity vulnerabilities will be corrected within one hundred and twenty (120) days

2.3.4 Where all, or part of, the Services are provided using online services (i.e. accessible via the internet), the Vendor must ensure that adequate protection is in place to mitigate the risk of denial-of-service (DoS) threats.

2.3.5 Vendor shall ensure that processes employed in the provision of the Services are staffed in such manner as to prevent conflicts of interest, fraud or error by invoking appropriate separation of duties.

2.3.6 Vendor shall ensure that information security awareness and training programs are provided for those responsible for handling FIS data, upon hire and on at least an annual basis.

2.3.7 Vendor will promptly notify FIS of any and all breaches to Vendor's information security within twenty-four (24) hours of discovering the Information Breach and work with FIS management to identify the root cause of the incident and the potential impact to FIS, its Clients or their customers, as reasonably requested by FIS.

2.3.8 If and to the extent Vendor or any Service is subject to the Payment Card Industry Data Security Standard requirements (as amended from time to time) ("**PCI DSS**"), Vendor will comply with said requirements. In addition, if and to the extent Vendor or any Service is subject to PCI DSS requirements: (i) Vendor will submit their Attestation of Compliance ("**AOC**") and Vendor Responsibility Matrix within ten (10) days of the execution of this Agreement and will have an AOC and Vendor Responsibility Matrix prepared, and provide to FIS such updated AOC and Vendor Responsibility Matrix, annually thereafter; (ii) Vendor will publish to 'Visa' Global Service Vendor registry and maintain 'Green Status' in such registry throughout the duration of the Agreement; and (iii) if Vendor fails to maintain 'Green Status' in the Visa Global Service Vendor registry, the following provisions shall apply: (A) If Vendor in 'Yellow Status' in the Visa Global Service Vendor registry, Vendor will provide the Services free of charge until Vendor obtains 'Green Status'; and (B) If Vendor is in 'Red Status' or is not listed in the Visa Global Service Vendor registry: (a) Vendor will provide the Services free of charge free of charge until Vendor obtains 'Green Status' or the Agreement terminates, (b) Vendor will refund to FIS the six (6) then most recent months of fees paid by FIS under the Agreement (excluding any period in which Vendor was providing the Services free of charge due to Vendor being in 'Yellow Status' or 'Red Status' pursuant to this provision), and (c) FIS may, in addition to any other remedies FIS may have, terminate the Agreement with no financial obligation to Vendor arising from such termination.

2.4 BACKGROUND CHECKS. Vendor will perform the background check, as described herein, and also timely cooperate in good faith with FIS' performance of a background check, as described herein, for each individual who is performing any Services under the Agreement and has access to the facilities, records or data of FIS, any Affiliate, any Client or any customer of a Client. Where permitted by applicable Law, the background check will consist of, at a minimum, verification of the highest level of education completed, verification of employment for the past ten (10) years, social security number trace and validation, and a check of U.S. Government Specially Designated National (OFAC) and export denial lists. In addition, to the extent permitted by Law, the background check will include a 9-panel drug test and criminal record search. For the drug test, all specimens will be tested at a Department of Health and Human Services/Substance Abuse Mental Health Services Administration certified lab, and the screening service will include confirmation of all positive test results. The criminal record search will include, to the maximum extent permitted by Law, a federal, state and county check, and a National Criminal File check, for felony and misdemeanor convictions for the last ten (10) years in all locations where the individual has resided for the last ten (10) years. Vendor will comply with all applicable Laws related to the background check, including required notices and applicable consents. In addition, Vendor will require the individual to report any criminal convictions. Vendor will not assign anyone to perform Services for FIS who has tested positive for drugs or whose background check findings do not meet the standards established by Vendor in accordance with all applicable Laws, including without limitation if there is a conviction or referral to a pretrial diversion program for a crime that is related to his or her duties. Vendor acknowledges that under the banking Laws, an individual may not participate, directly or indirectly, in any manner in the conduct of the affairs of any insured depository institution without regulatory consent if he or she has a conviction, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution, of a crime involving dishonesty, breach of trust or money laundering, including any crime concerning the illegal manufacture, sale, distribution of or trafficking in controlled substances, unless the crime meets certain criteria for treating the crime as de minimis. The background check must be completed before assignment of an individual and periodically thereafter. FIS also reserves the right to request that Vendor provide an attestation confirming a background check as required by this provision has been completed and no disqualifying information has been identified on an annual basis during the Term of an Engagement. Upon five (5) Business Days' prior written notice, FIS may verify Vendor's compliance with this Section. Such verification will be conducted in a manner that minimizes disruption to Vendor's business. FIS may use an independent auditor to assist with such verification, provided that FIS has a written confidentiality agreement in place with such independent auditor. FIS will notify Vendor in writing if any such verification indicates that Vendor is not in compliance with this Section and Vendor will promptly remediate any issues of non-compliance discovered by FIS as part of such verification.

2.5 All FIS' audit rights of the Agreement including without limitation to examine Vendor's records (which must include auditable records of all financial and non-financial transactions relating to Products and Services) may, to the extent required by the regulators of FIS and/or its Clients, be exercised by FIS, FIS' Clients, and its and their regulators.

2.6 DESTRUCTIVE ELEMENTS. Vendor represents, warrants and covenants that it will not introduce or allow any Destructive Elements into the Services, any Products or Deliverables, or into the systems of FIS or any of FIS Clients or their customers. Without limitation of the foregoing, Vendor warrants and covenants that it will use best efforts to avoid the coding or introduction of Destructive Elements into any systems used to provide Services, Products or Deliverables. Vendor will assist FIS with mitigation of any loss of operational efficiency or loss of data

caused by such Destructive Elements. Upon learning of or discovering a cyber or information-security threat or vulnerability to FIS systems or to FIS Clients or their customers (including without limitation notifications received from security researchers, industry resources, or bug bounty programs), Vendor will promptly notify and cooperate with FIS and take all reasonable and necessary steps to isolate, mitigate, and remediate such known or suspected threat or vulnerability.

3. **SAFEGUARDING INFORMATION**

3.1 CONSUMER INFORMATION AND PRIVACY. If, in connection with the Agreement, Vendor receives, stores or accesses any Personal Data, NPI, PHI, Payment Card Data, or other information or materials that are subject to the Privacy Regulations and Guidelines, Vendor will comply with the applicable requirements of the Privacy Regulations and Guidelines. Vendor acknowledges that the Guidelines include provisions regarding the safeguarding of consumer information, response programs and notice in the event of unauthorized access to consumer information, that FIS provides information processing services to Clients subject to the Guidelines, and that FIS may be required to notify Clients, their customers or other third parties of security incidents that result, or are likely to result, in misuse or unauthorized possession or disclosure of Personal Data, NPI, PHI, Payment Card Data or other Confidential Information. Without limiting the foregoing, and in addition to its confidentiality and security obligations as otherwise set forth in the Agreement, Vendor will (i) ensure the security and confidentiality of such information or materials, (ii) protect against any anticipated threats or hazards to the security or integrity of such records, (iii) detect unauthorized access to or use of such records or information, and (iv) protect against unauthorized access to or use of such records or information that would result in harm or inconvenience to any Client or any customer of a Client. Vendor represents and warrants that it has and will maintain in place commercially reasonable precautions to safeguard the confidentiality, security and integrity of FIS Confidential Information in a manner designed to meet the requirements of this Section. These precautions will include but will not be limited to (i) contractual restrictions on access to the information by Contractors and Vendor's other vendors, (ii) intrusion detection systems on all information systems of FIS maintained or controlled by Vendor, and (iii) notification procedures for notifying FIS promptly in the event a security breach is detected or suspected, as well as other response programs when there is a suspected or detected Breach involving Personal Data, NPI, PHI or Payment Card Data. These precautions will also include, as appropriate, (A) access controls to FIS information systems, including controls to identify and permit access only to authorized individuals and controls to prevent access to FIS Confidential Information through improper means, (B) Vendor Personnel controls and training, (C) physical access restrictions at locations where FIS Confidential Information is located, (D) encryption of electronic FIS Confidential Information when appropriate or legally required, and (E) a disaster recovery plan as appropriate to protect against loss or damage to FIS Confidential Information due to potential hazards such as fire or water damage or technological failures. Vendor will (1) monitor the foregoing measures with periodic audits or testing and (2) provide copies of the same sufficient to assure FIS or its regulatory authorities that Vendor is implementing these precautions, and (3) notify FIS immediately in the event there is any suspected or actual unauthorized access, use, disclosure or alteration to FIS Confidential Information. Vendor will indemnify FIS from, defend FIS against, and pay any final judgments awarded against FIS, resulting from any claim brought by a third party, including but not limited to a customer of FIS, against FIS based on any breach of such privacy Laws, rules or regulations by Vendor, including Vendor Personnel.

3.1.1 Vendor will also use the information security safeguards described in Section 3.1 to protect any Confidential Information of FIS and FIS Clients comprising technical data, technical schematics, and any infrastructure, hardware, and/or software and systems information of FIS and FIS Clients that, if disclosed publicly, could enable or facilitate unauthorized access to such Confidential Information.

3.2 PROTECTION OF CONFIDENTIAL INFORMATION. Each party must protect the other's Confidential Information with the same degree of care used to protect its own Confidential Information, but in no event may either party use less than a reasonable standard of care be in connection with the preservation of the other's Confidential Information. FIS designates as its Confidential Information (i) the Agreement, (ii) any information obtained from or related to any Client of FIS including FIS Client business strategy, direction and contract information, (iii) any Personal Data, NPI, PHI, or Payment Card Data (iv) FIS' employee records (name, address, phone number, salary, taxpayer or government identification number, date of birth, health records, bank account information, labor party), (v) any business strategies and directions, operating or marketing plans, intellectual capital or trade secrets, (vi) memos or other documents or communications pertaining to pending FIS litigation or contracts (including the Agreement), (vii) any information disclosed by FIS that is designated as "confidential" at or prior to disclosure, (viii) other FIS data or information which is not generally known, including business information, specifications, research, software, trade secrets, discoveries, ideas, know-how, designs, drawings, flow charts, data, computer programs, marketing plans, budget figures, and other financial and business information, and (ix)

information of the kind described by any of the foregoing categories that is of or disclosed by a Client, an FIS Affiliate, or a customer of a Client. Vendor will (A) restrict the use and disclosure of the FIS' Confidential Information to its Vendor Personnel and do so solely on a "need to know" basis in connection with Vendor's obligations to provide Software or to perform Services in accordance with the Agreement, (B) ensure Vendor Personnel who receive or have access to FIS Confidential Information are bound by confidentiality obligations at least as restrictive and as protective of the FIS Confidential Information as the provisions of this Section, (C) require its Vendor Personnel to protect and restrict the use of the FIS' Confidential Information, (D) establish procedural, physical and electronic safeguards, designed to prevent the compromise or unauthorized disclosure of FIS Confidential Information and to achieve the objectives of the Guidelines (if applicable), (E) promptly investigate any security breach to determine whether such incident has resulted or is likely to result in misuse or unauthorized possession or disclosure of FIS Confidential Information and (F) not use or disclose FIS' Confidential Information except in accordance with the Agreement.

3.3 In providing any notice of an Information Breach, Vendor will use commercially reasonable efforts to (i) provide notice to one or more FIS managers generally responsible for security matters relating to the FIS Confidential Information affected by the Information Breach, within twenty-four (24) hours of discovering the Information Breach, and (ii) keep FIS informed as to the actual and anticipated effects of the Information Breach and the corrective actions taken or to be taken in response to the Information Breach. In addition, if the Information Breach results or is likely to result in misuse of Personal Data, NPI, PHI or Payment Card Data, Vendor will (A) notify FIS as soon as possible and reasonably cooperate with FIS in its efforts to notify affected Clients and their customers and to mitigate the actual or potential harm resulting from the Information Breach and (B) reimburse FIS for its reasonable costs in notifying Clients or their customers of the Information Breach and making available to them any credit monitoring services and for any other costs FIS reasonably incurs with respect to the Information Breach.

3.4 Confidential Information will remain the property of the party from or through whom it was provided. Except for NPI, PHI, Payment Card Data, or other information protected by the Guidelines, the parties' respective confidentiality obligations under the Agreement do not apply to any information that: (i) was previously known by the party; (ii) is a matter of public knowledge; (iii) was or is independently developed by the party; (iv) is released for disclosure with written consent of the party; or (v) is received from a third party to whom it was disclosed without restriction.

3.5 Each party may disclose information notwithstanding its confidentiality obligations under the Agreement to the extent required (i) by Law, (ii) in connection with the tax treatment or tax structure of the Agreement; or (iii) in response to a valid order of a U.S. court or other governmental body, provided that the party provides the other party with written notice and the other party is afforded a reasonable opportunity to obtain a protective order with respect to the disclosure.

3.6 Upon termination of the Agreement, Vendor will destroy all FIS Confidential Information in a manner designed to preserve its confidentiality, or, at the other party's written request and expense, return it to FIS. Upon FIS' written request, Vendor shall, at FIS' choice, delete or return all Personal Data Processed on behalf of FIS to FIS after the end of the provision of Services relating to Processing, subject to Vendor retaining any copies required by applicable EU member state law.

3.7 FIS will have and retain all right, title and interest in all of FIS' Confidential Information, whether possessed by FIS prior to, or acquired or refined by FIS (either independently or in concert with Vendor) during the Term.

3.8 Vendor will not, without the prior written consent of FIS, (i) provide the Software or Services or access, store or process any of FIS' Confidential Information outside the United States or (ii) export any of FIS' Confidential Information to anywhere outside the United States. The provisions of the Agreement apply without regard to where the Software or Services are provided or FIS Confidential Information is accessed, stored or processed.

3.9 EU GDPR Compliance. If Vendor shall process any Personal Data from FIS or a Client as part of the Services under the Agreement regarding individuals domiciled in countries outside of the United States (or to which the GDPR is otherwise applicable), such processing shall be in compliance with the Data Protection Addendum attached hereto as Appendix A and incorporated herein by this reference.

4. **SUBCONTRACTORS.**

4.1 Vendor will not utilize any Contractor to perform Services or provide any part of a Deliverable, without the prior written consent of FIS. Vendor will notify FIS of its intention to so engage another party not less than thirty (30) days prior to the entity commencing performance of any Services or to provide any part of the Deliverable. Vendor will provide such information and documentation concerning any such proposed party as FIS requests.

Vendor will ensure that any such Contractor complies with all obligations of Vendor under the Agreement. Vendor is responsible for all of its obligations under the Agreement regardless of where performed or whether performed by any Contractor, and Vendor will be liable for the acts and omissions of any Contractor that Vendor uses to perform Services or provide any part of any Deliverable.

4.2 SERVICES PERFORMED BY PROVIDER PERSONNEL IN UK. If Vendor shall assign Vendor Personnel that are located in the United Kingdom to perform any part of the Services under the Agreement, then such performance shall be in compliance with the UK Services Terms attached hereto as **Appendix B** and incorporated herein by this reference.

5. Vendor may not engage sub-Processors under the Agreement or give access to or transfer any Personal Data to any third party (including any affiliates, group companies or sub-contractors) without the prior written consent of FIS and the relevant FIS Affiliates. If FIS consents to the use of third parties as sub-Processors Vendor shall (i) impose in writing upon such sub-Processors the same data protection obligations as set out herein and as are required by applicable Data Protection Legislation and (ii) be responsible for the acts and omissions of such sub-Processors under the Agreement. Where prior written consent given by FIS pursuant to this clause authorizes a class of third party to Process Personal Data, the Vendor shall notify FIS of any intended changes concerning the addition or replacement of any sub-Processors within such class, and FIS shall have the right to object to, and prevent, any such addition or replacement of sub-Processors within such class.

5.1 **COMPLIANCE WITH LAWS.** In all circumstances, Vendor will comply with, and will ensure that all Software, Services and Deliverables comply with all Law, including Law relating to export and import, privacy, use, disclosure or transfer of personal information, or security, and Law relating to the employment, health, safety and payment of Vendor Personnel. Vendor will perform an on-going review of Law applicable to Vendor's performance under the Agreement, including Law enacted or amended after the effective date of the Agreement. Vendor will identify and procure all permits, certificates, approvals, licenses, and inspections necessary for Vendor's performance under the Agreement other than such permits, certificates, approvals, licenses and inspections that FIS is directly responsible for obtaining under the Agreement. Without limiting any other obligation of Vendor under the Agreement, Vendor will at all times comply with all Law relating to trade sanctions, export controls, the U.S. Foreign Assets Control Regulations, the U.S. Export Administration Regulations, and the U.S. International Traffic in Arms Regulations.

6. **DATA PROTECTION TECHNICAL AND ORGANISATIONAL MEASURES**

6.1 In the course of Vendor providing Services under the Agreement(s), FIS may from time-to-time provide or make available Data to Vendor. The Agreement(s) determines the subject matter and the duration of Vendor's Processing of Personal Data, as well as the nature and purpose of any collection, use, and other Processing of Personal Data and the rights and obligations of FIS.

6.2 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 of varying likelihood and severity for the rights and freedoms of natural persons, Vendor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. As a minimum, these should include the requirements required under applicable Data Protection Legislation and the requirements set out in the Agreement. Upon request, Vendor shall provide a written description of the technical and organizational measures the Vendor employs for Processing Personal Data.

6.3 Vendor must cooperate upon FIS' reasonable request in order to assist FIS with its compliance with applicable privacy laws, including FIS' handling of Data Subject rights requests.

6.4 Where Vendor is acting as a Processor under the Agreement, at FIS' written request, Vendor shall make available to FIS all information reasonably necessary to demonstrate Vendor's compliance with the obligations agreed to in the Agreement(s), applicable privacy laws, and any data protection addenda.

6.5 Unless Vendor needs identifiable information in order to provide the product or service, Vendor will deidentify or pseudonymize FIS' data unless there is a need for the data to be identifiable.

6.6 Vendor must consider data protection issues as part of the default configuration of its systems, services, products, and business practices. Vendor's default configuration will follow privacy by default principles, including data quality, minimization, and accountability. Vendor will Process FIS data in accordance with FIS instructions and only when relevant, minimal, and not excessive.

6.7 Vendor will provide certification and assurance of its processes and products pursuant to the GDPR.

7. **BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY**. To the extent applicable to the Services, Vendor will establish and maintain disaster recovery and business continuity plans designed to minimize the risks associated with a disaster affecting Vendor's ability to provide the Services, which includes off-site data storage and recovery infrastructure. Vendor's recovery time objective for the Services ("**RTO**") under such plan is [INSERT TIMEFRAME] hours/minutes. Vendor will maintain adequate backup procedures in order to recover FIS' or if applicable any Client's data to the point of the last available good backup. Vendor's recovery point objective ("**RPO**") is [INSERT TIMEFRAME] hours/minutes. Vendor will test its disaster recovery and business continuity plans, including call trees, not less frequently than annually, will annually provide to FIS disaster recovery and business continuity plans test results. If Vendor fails to meet the RTO and RPO in any annual test, Vendor shall perform a root cause analysis of the cause of the failure to meet the RTO or RPO and will remediate the cause of such failure and retest within six (6) months of the failed test. If Vendor fails to meet the RTO or RPO in the retest, Vendor will have a second six (6) month period to remediate and retest. If provider fails a second time, FIS may request that the parties attempt to reach a mutually agreeable resolution, and if the parties are unable to agree upon a resolution within thirty (30) days of FIS' request, FIS may terminate the Agreement with no further financial obligation to Vendor. Vendor will provide its disaster recovery plan and test results to FIS and FIS may share such disaster recovery plan and test results with Clients who have contracted for the Services, if any, FIS' auditors, and FIS' regulators. Vendor will implement the applicable disaster recovery or business continuity plan upon the occurrence of a disaster, and shall notify FIS promptly following such event. In the event of a disaster (as defined in the plan), Vendor will not charge fees higher than or in addition to the agreed fees under the Agreement. Vendor will notify of, and invite FIS to participate in (at no additional charge to FIS), Vendor's disaster recovery and business continuity plan test.

Annex 4

Standard Contractual Clauses for Restricted Transfers Originating in the UK

Clause 1

Definitions

For the purposes of the Clauses:

(a) *"personal data", "special categories of data", "process/processing", "controller", "processor", "data subject"* and *"supervisory authority"* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) "*the data exporter"* means the controller who transfers the personal data;

(c) *"the data importer"* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *"the subprocessor"* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) "*the applicable data protection law"* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *"technical and organisational security measures"* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result

of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions

received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue

a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the laws of the jurisdiction in which the data exporter is established (being either a jurisdiction within the United Kingdom or a Member State of the EEA).

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the laws of the jurisdiction in which the data exporter is established (being either a jurisdiction within the United Kingdom or a Member State of the EEA).

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1
Particulars of the Transfer

Data exporter	FIS.
Data importer	Vendor.
Categories of Data Subjects	As set out in Annex 1 (*Data Processing Details*).
Categories of Data	As set out in Annex 1 (*Data Processing Details*).
Special categories of data	As set out in Annex 1 (*Data Processing Details*).
Processing Operations	Storing, copying, accessing, sharing, modifying.

Appendix 2
Data Security

The technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are those set out in Annex 3 (*Security Standards*).

Annex 5

Standard Contractual Clauses for Restricted Transfers Originating in the EEA

SECTION 1

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Unused (Optional)

SECTION II – O BLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and

purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex I

Particulars Of The Transfer

A. LIST OF PARTIES

Data exporter	FIS.
Data importer	Vendor.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects	As set out in Annex 1 (*Data Processing Details*).
Categories of Data	As set out in Annex 1 (*Data Processing Details*).
Sensitive Data	As set out in Annex 1 (*Data Processing Details*).
Frequency of Transfer	Continuous for the term of the Agreement.
Nature of Processing	Storing, copying, accessing, sharing, modifying.
Purposes of the Transfer	The provision of the Services by data importer to data exporter.
Data Retention	Data importer will delete the personal data from its systems on expiry or termination of the services in accordance with its usual data retention practices.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority should be the authority in the country where the Client as data exporter is established.

Annex II

Technical And Organisational Measures Including Technical And Organisational Measures To Ensure The Security Of The Data

As set out in Annex 3 (*Security Standards*).