DATA PROCESSING ADDENDUM

DEFINITIONS

Capitalized words and phrases not otherwise defined in this Attachment have the meanings set forth in the Schedule or in the Master Agreement, as appropriate. The following additional definitions apply to this Attachment:

"WorkWave" means WorkWave LLC, and its Affiliates.

"WorkWave Privacy Notice" means the privacy notice to be found at **https://www.workwave.com/privacy-policy** or such other web link as may be provided by Workwave to Customer from time to time.

"APP" means the Australian Privacy Act of 1988.

"CCPA" means the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 to 1798.199) and its implementing regulations as amended or superseded from time to time.

"Controller" means the entity or entities which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

"Customer" means the party contracting for the Services.

"Customer Personal Data" means any Personal Data included in Customer Data or data derived from Customer Data that is in either case Personal Data.

"Data Exporter" means, in the case of an International Transfer, the Party from which the data originates.

"Data Importer" means, in the case of an International Transfer, the Party receiving the data.

"Data Protection Laws and Regulations" means (in respect of any Processing of Customer Personal Data under the Agreement) any law concerned with the protection of privacy or Personal Data that is binding on either Party and applies to that processing, including, where applicable (but not limited to) the GDPR, the UK Data Protection Act 2018, the Swiss Data Protection Law, the Australian Privacy Act of 1988 (APP), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the California Consumer Privacy Act (CCPA), and the U.S. State Privacy Laws as may be amended or superseded from time to time.

"Data Protection Officer" means anyone appointed as a "data protection officer" to comply with an obligation to appoint an officer with that title under the any of the Data Protection Laws and Regulations

"Data Subject" means any person to whom Customer Personal Data relates.

"Data Subject Request" means a request from a Data Subject to exercise any of the Data Subject's rights under the Data Protection Laws and Regulations relating to the Application Services Processing.

"Deidentified Data" means aggregate data relating to, derived, or generated from Customer Personal Data or derived from the Services, as defined by the CCPA.

"EEA International Transfer" means the transfer of Customer Personal Data that was at the time of transfer subject to processing by the transferor that fell within the scope of the GDPR, either:

(a) to a third country (as understood in the GDPR); or

(b) to an International Organization.

and which is not transferred on the basis of an adequacy decision in accordance with Article 45 of the GDPR.

"EU Data Protection Law" means all of the following, each as amended and replaced from time to time: the GDPR and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) and their respective national implementing legislations; the Swiss Federal Data Protection Act; the UK Data Protection Act 2018; each as applicable.

"GDPR" means the 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

"IDTA" means the International Data Transfer Addendum issued by the UK Information Commissioner under the Data Protection Act 2018.

"International Organization" shall have the same meaning as in the GDPR.

"International Transfer" shall mean an EEA International Transfer, Switzerland, Canada, Australia or a UK International Transfer.

"PIPEDA" shall mean the Canadian Personal Information Protection and Electronic Documents Act.

"Personal Data" means (i) anything that would constitute "personal data" as defined in the GDPR or "Personal Information" as that term is defined under the CCPA (or other analogous variations of such terms as defined under applicable Data Protection Laws and Regulations, together with (ii) any information relating to an identified or identifiable legal entity (but only where such information is protected in a similar way to Personal Data relating to a natural person under applicable Data Protection Laws and Regulations).

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and **"Process"** and **"Processes"** shall have a corresponding meaning.

"Processor" means an entity which Processes Personal Data on behalf of a Controller.

"**Public Authority Request**" means any request, legally binding on the recipient, from a public authority for disclosure of any Customer Personal Data.

"Representative" means, in the context of the European Union, the same as in the GDPR, and in the context of the UK, the same as in the UK Data Protection Act 2018.

"Services" means the Subscription Services, APIs, Software Products and other services as defined by the Master Services Agreement and the applicable Customer agreement.

"Standard Contractual Clauses" ("SCCs"), means the standard contractual clauses for the transfer of personal data from one country to another, under the GDPR.

"Swiss Data Protection Law" or **"FADP"** shall mean (i) Swiss Federal Data Protection Act (dated June 19, 1992, as of March 1, 2019) ("FDPA"); (ii) The Ordinance on the Federal Act on Data Protection ("FODP"); (iii) any national data protection laws made under, pursuant to, replacing or succeeding and any legislation replacing or updating any of the foregoing.

"Sub-processor" means any entity which Processes Customer Personal Data on behalf of WorkWave in the course of providing Payment Application Services.

"Supervisory Authority" means a public authority which has a responsibility for the regulation of the processing of Personal Data, whether established by a nation state, a part of a nation state, the European Union or otherwise under international law, including any "supervisory authority" within the meaning of the EU Data Protection Law.

"Third Party Providers", means any third parties indicated in the Master Agreement (including Schedules) that provide one or more services as part of the Application Services.

"UK GDPR" has the meaning give in the Data Protection, Privacy and Electronic Communications in force from time to time in the UK (Amendments etc.) (EU Exit) Regulations 2019.

"UK International Transfer" means any transfer of Customer Personal Data that was at the time of transfer subject to processing by the transferor that fell within the scope of the UK GDPR to a third country (as understood in the UK GDPR) which is not based on adequacy regulations (see Section 17A of the UK Data Protection Act 2018).

"U.S. State Privacy Laws" means, collectively, all U.S. state privacy laws and their implementing regulations, as amended or superseded from time to time, that apply to the processing of individuals' Personal Data. U.S. State Privacy Laws include but are not limited to the following: (i) California Consumer Privacy Act (California Civil Code §§ 1798.100 to 1798.199) ("CCPA"); (ii) Colorado Privacy Act (Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313) ("CPA"); (iii) Connecticut Personal Data Privacy and Online Monitoring Act (Public Act No. 22-15) ("CTDPA"); (iv) Iowa Consumer Data Protection Act ("ICDPA"); (v) Montana Consumer Data Privacy Act ("MTCDPA"); (vi) Tennessee Information Protection Act ("TIPA"); (vii) Texas Data Privacy and Security Act ("TDPSA"); (viii) Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 to 13-61-404) ("UCPA"); (iv) Virginia Consumer Data Protection Act (Virginia Code Ann. §§ 59.1-575 to 59.1-585) ("VCDPA").

1. INTRODUCTION

1.1. **Roles of the Parties**. The roles of the parties in relation to the Processing of Customer Personal Data are as follows:

1.1.1. In carrying out the Services, Customer is the Controller, WorkWave is a Processor under EU Data Protection Laws.

1.1.2 For the purpose of the US State Privacy Laws, Customer will act as a Controller (under the VCDPA, the CPA, the UCPA, and the CTDPA) and/or Business (under the CCPA) with respect to any Personal Data provided to WorkWave or made accessible by you under the Agreement. Further specifications about the roles of the Parties are further detailed in the US Addendum.

2. GENERAL PROVISIONS

2.1. **Compliance with Data Protection Laws.** Each Party shall Process Customer Personal Data in accordance with the Data Protection Laws and Regulations.

2.2. **Compliance with Biometric Privacy Law Requirements.** This paragraph 2.2 shall apply only if Processing Personal Data in accordance with the Master Agreement or the Schedule involves WorkWave Processing Biometrics (meaning "biometric data," "biometric information, "biometric identifiers," or similar terms as defined under Data Protection Laws and Regulations) to provide Services. If Customer provides or amends any notice or consent language to Data Subjects regarding Processing Biometrics, Customer shall ensure such language (1) is consistent with terms provided by WorkWave and with obligations for Biometrics under applicable Data Protection Laws and Regulations and (2) permits WorkWave to Process Biometrics and related Personal Data to deliver Services in accordance with the Master Agreement or the Schedule.

2.3. **Data Protection Impact Assessment.** Each party (the assisting party) shall provide, on request to the other party (the requesting party) reasonable cooperation and assistance needed to fulfil any obligation of the requesting party under the Data Protection Laws and Regulations to (a) carry out a data protection impact assessment related to the processing of Customer Personal Data; or (b) cooperate with or carry out a prior consultation of the Supervisory Authority. To the extent legally permitted, the requesting party shall be responsible for any costs arising from assisting party's provision of any assistance under this paragraph.

3. GENERAL PROVISIONS RELATING TO CUSTOMER

3.1. **Information on processing activities**. Each party shall, promptly upon the execution of the Agreement, inform the other Party of the name and contact details of: (1) its Data Protection Officer (if any) or, in the absence of a Data Protection Officer, a key contact responsible for data protection; and (2) any Representative it has appointed within the EU or the UK; and shall, thereafter, inform promptly the other if any of those details change. For the purposes of this paragraph, WorkWave shall be treated as having given the required information on the execution of this Agreement as follows: WorkWave's Data Protection Officer may be contacted at privacylead@workwave.com. WorkWave's Representative in the EU and the UK may be contacted at _____.

3.2. **Customer's Processing of Customer Personal Data**. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data and for ensuring that disclosure of Customer Personal Data and the Processing of Customer Personal Data in order to provide the Services in accordance with the Master Agreement by WorkWave is in accordance with the Data Protection Laws and Regulations.

3.3. **Use of Deidentified Data**. Customer acknowledges and agrees that WorkWave may Process Aggregate Consumer Information and De-identified data (together, "Deidentified Data") relating to, derived, or generated from Customer Personal Information or derived from the Services, for any lawful purpose. As between WorkWave and Customer, WorkWave exclusively will own rights, title, and interest in and to Deidentified Data. Customer further acknowledges and agrees that Deidentified Data does not constitute Customer Personal Information, and WorkWave may use, maintain, disclose, and otherwise Process such Deidentified Data for any lawful purpose.

4. INTERNATIONAL TRANSFERS OF DATA

4.1. **WorkWave Internal International transfers.** WorkWave may transfer Customer Data, internally or to Processors, from one jurisdiction to another, including outside the European Union or the United Kingdom, provided that, in doing so:

4.1.1. it ensures that such a transfer complies with any legal conditions imposed by the law of the jurisdiction from which Customer Data is being exported on such an export.

4.1.2. Where the transfer occurs in the course of performing the Services, it does so subject to the conditions of paragraph 6 of this Schedule, in particular as to the appointment of Sub-Processors.

4.2. **International transfers: general**. There may be circumstances where data is transferred from a Customer to WorkWave or vice versa. Both directions of transfer may need to be carried out under the protection of standard contractual clauses. Accordingly, suitable protective measures in relation to EEA International transfers and UK International transfers shall be taken as set out below.

4.3. **EEA International transfers**. Where an EEA International Transfer takes place between a Customer and WorkWave, then the EU-US DPF shall apply and, if inapplicable, then the SCCs shall apply and the SCCs are deemed to be incorporated into this Attachment as if the parties had executed one or more instances of Annex I to the SCCs. The parties' separate acts of signing this Schedule being deemed to be the act of signing one or more copies of Annex I.A to the SCCs. For purpose of Annex I.A to the SCCs shall be deemed to have been completed as follow:

4.3.1.1. where the EEA International Transfer of personal data is being made to Customer in the course of performance of the Services, then one copy of Exhibit A (part 1) of this Attachment shall be deemed to have been completed and signed by the parties selecting MODULE FOUR with the "Data Exporter" section identifying WorkWave's role as "Processor" and the "Data Importer" section identifying the Customer's role as "Controller";

4.3.1.2. where the EEA International Transfer of personal data is being made to WorkWave in the course of Payment Application Processing, then one copy of Exhibit A (part 1) of this Attachment shall be deemed to have been completed and signed by the parties selecting MODULE TWO with the "Data Exporter" section identifying Customer's role as "Controller" and the "Data Importer" section identifying WorkWave's role as "Processor";

4.3.2. In each case the remaining parts of the Annex I.A to the SCCs shall be deemed to have been completed as follows:

4.3.2.1. By entering the full names of the importer and exporter under "name" and followed by "Customer" or "WorkWave" (in order for the short names of the parties to be understandable in the context of Annex I).

4.3.2.2. By entering for each party under "Address", the address of that party for the purposes of this Schedule, and under "contact" either the party's DPO (provided pursuant to paragraph 3.1 of this Schedule) or, if no such DPO exists, for the purpose of this Schedule, the contact details of another individual who is an appropriate contact for that party in relation to data protection; in which case the latter shall be deemed to have been specified.

4.3.2.3. By excluding the optional docking clause (Clause 7 of the SCCs);

4.3.2.4. By selecting Option 2 for all instances of Clause 9(a) and selecting ten days as the relevant time period;

4.3.2.5. By removing the optional language in Clause 11(a);

4.3.2.6. Clause 17 (governing law) shall be deemed to be completed to specify (i) the governing law of the Master Agreement, if it is a law of a member state of the European Union or European Economic Area ("Member State"); (ii) failing that, the law applicable to Customer's domicile, if it is the law of a Member State; (iii) failing that, Ireland;

4.3.2.7. Clause 18 (Choice of forum and jurisdiction) shall be deemed to specify the jurisdiction of the Master Agreement, if it is the jurisdiction of a Member State; (ii) failing that, the jurisdiction applicable to Customer's centre of operations within Customer's domicile; if that is a jurisdiction of a Member State; (iii) failing that the courts of Ireland;

4.3.2.8. Annex I. B of the SCCs shall be deemed to be completed with the information contained in Exhibit A and Exhibit B (part 2) of this Attachment;

4.3.2.9. Annex I part C of the SCCs shall be deemed to specify either (i) where Customer is domiciled in a Member State, the supervisory authority of that state; or (ii) the Data Protection Commission of Ireland, otherwise;

4.3.2.10. Annex II to the SCCs shall be completed with the information contained in Exhibit C of this Attachment ; and

4.3.2.11. Where MODULE TWO has been selected, Annex III to the SCCs shall be completed with the information contained in Exhibit D of this Attachment.

4.3.3. Customers are responsible for completing their own records of processing activities, or similar records prescribed by applicable law, and determining any information necessary for that completion. Nothing in this Attachment shall be construed as giving any representation, warranty, or guidance as to the correct manner of completing any such records.

4.4. **UK International transfers.** Where a UK International transfer takes place between WorkWave and a Customer, then the UK-U.S. DPF shall apply and, if inapplicable, then IDTA shall apply and is deemed to be incorporated into this Attachment as if the parties had executed one or more instances of the IDTA.

4.4.1. Table 1 of the IDTA, shall be deemed to have been completed and signed by the parties as follows:

4.4.1.1. By entering the full name of the party under “Full legal name” as entered under paragraph 4.3.2.1 of this Attachment;

4.4.1.2. By entering for each party under “Main Address”, the address of that party for the purposes of this Schedule, and under “Official registration number” the official registration number (if any) contained in the Master Agreement;

4.4.1.3. By entering under “contact”, for the importer and exporter the same information as entered for “contact” under paragraph 4.3.2.2 of this Attachment;

4.4.2. In Table 2 of the IDTA, the second alternative will be selected.

4.4.3. The details of Table 2 and Table 3 of the IDTA will be completed to be consistent with the options and selections set out in Clause 4.3.2 of this Attachment.

4.4.4. In Table 4 of the IDTA, selecting “neither party”.

4.5. **Responsibility for transfers to third parties**. Where either party carries out an International Transfer to any third party, then the transferring party shall be responsible for ensuring that the transfer is lawful.

4.6. **Law and jurisdiction for the standard clauses.** Clause “Governing Law and Venue” of the Master Agreement shall not apply to the SCCs or IDTA notwithstanding the adoption by the SCCs or IDTA of the same governing law by the operation of paragraphs 4.3.2.6 and 4.3.2.7.

5. GENERAL PROVISIONS RELATING TO WORKWAVE

5.1. **Confidentiality.** WorkWave shall ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of Customer Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

5.2. **Reliability.** WorkWave shall take commercially reasonable steps to ensure the reliability of any WorkWave personnel engaged in the Processing of Customer Personal Data.

5.3. **Limitation of Access.** WorkWave shall ensure that, in carrying out the Services, its personnel’s access to Customer Personal Data is limited to those personnel performing Services in accordance with the Master Agreement or the Schedule.

5.4. **Customer Personal Information**. WorkWave does not receive Customer Personal Information as consideration for any of the Services. WorkWave will not Sell (as that term is defined by the CCPA) Customer Personal Information provided by Customer to WorkWave for the provision of the Services to Customer.

6. Instructions and Details of Processing

6.1. **WorkWave’s Processing of Customer Personal Data**. WorkWave shall carry out the Services only on Controller’s documented instructions unless required to do so by applicable law. Customer warrants that the Master Agreement, the Schedule (including all its contents), and any instructions it gives to WorkWave for the Processing of Customer Personal Data are Controller’s documented instructions and that any such instructions comply with Data Protection Laws and Regulations.

6.2. **Instructions as to International Transfers.** The provisions of this Attachment shall constitute the Controller's instructions with respect to International Transfers relating to the Services**.**

6.3. **Details of the Processing.** The duration of the Services, the nature and purpose of the Processing, the types of Customer Personal Data and categories of Data Subjects Processed are further specified in Exhibit A, part B (Description of Transfer) to this Attachment.

6.4. **Deletion of Data**. On termination or expiry of the Master Agreement, WorkWave shall return Customer Personal Data which has been, or is being, processed solely for the purposes of the Services to Customer or, to the extent allowed by applicable law, delete such data in accordance with the procedures and timeframes specified in the Master Agreement except where it is required by law to retain any data.

6.5. **Assistance to the Controller**. Taking into account the nature of Processing and the information available to WorkWave, WorkWave shall on request by Customer, assist in ensuring compliance with its obligations as to security and in relation to data breaches under the Data Protection Laws and Regulations.

6.6. **Appointment of Sub-processors.** WorkWave’s Affiliates may be retained as Sub-processors; and WorkWave and WorkWave’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services provided that WorkWave or the relevant Sub-processor has entered into a written agreement (a “Sub-Processing Agreement”) with each Workwave Affiliate containing data protection obligations no less protective than those in the Master Agreement with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Any such Sub-Processing Agreement shall be binding on the Sub-processor with regard to the Controller and shall specifically confer on

the Controller any rights given to a Controller under paragraphs 2.2, 2.3, 6.1, 6.2, 6.4 - 6,7, 6.9, 7.3, 7.5 and 8.3 of this Attachment.

6.7. **List of Current Sub-processors and Notification of New Sub-processors.** WorkWave is specifically authorized to engage any Sub-processor Affiliate as a Sub-processor. A list of WorkWave's sub-processors can be found **here**.

6.8. **Objection Right for New Sub-processors.** Customer may object to WorkWave's use of the initial list of Sub-processors or any new Sub-processor subsequently appointed by WorkWave by notifying WorkWave promptly in writing within ten (10) business days of being informed of the identity of the Sub-processor. In the event Customer objects to a Sub-processor as permitted in the preceding sentence WorkWave will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Customer Personal Data by such Sub-processor without unreasonably burdening Customer. If WorkWave is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the Master Agreement or the Schedule with respect only to those Services which cannot be provided by WorkWave without the use of the relevant Sub-processor by providing written notice to WorkWave. WorkWave will refund Customer any prepaid fees for such Services covering the remainder of the term of the Master Agreement or Schedule following the effective date of termination with respect to such terminated Services, without imposing a termination charge for such termination on Customer, but without prejudice to any right of WorkWave to charge any amount in respect of Services or assistance provided on termination.

6.9. **Liability for Sub-processors.** WorkWave shall be liable for the acts and omissions of its Sub-processors to the same extent WorkWave would be liable if performing the services of each Sub-processor directly under the terms of this Attachment, except as otherwise set forth in the Master Agreement.

6.10. **Use of Service Providers**. WorkWave may disclose Customer Personal Information to, and permit the Processing of Customer Personal Information by, its Service Providers who perform services on behalf of WorkWave. WorkWave will take steps to ensure that such Service Providers are subject to contractual requirements with respect to the processing of Customer Personal Information at least as protective as those to which WorkWave is subject pursuant to the Master Agreement. WorkWave may retain, use, or disclose Customer Personal Information to detect data security incidents or protect against fraudulent or illegal activity. Further, WorkWave may retain and use Deidentified Data (and combine it with Deidentified Data from other customers) to build or improve the quality of its Services.

7. RIGHTS OF DATA SUBJECTS

7.1. **Regulatory requests.** WorkWave shall notify Customer of any legally binding request for disclosure of Customer Personal Data relating to the Services by a law enforcement authority unless otherwise prohibited from doing so, such as by a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

7.2. **Data Subject Requests.** WorkWave shall, to the extent legally permitted, promptly notify Customer using Customer email address if WorkWave receives a Data Subject Request. Customer shall have the responsibility for responding, and for deciding how to respond, to any Data Subject Request.

7.3. **Assistance by WORKWAVE**. Taking into account the nature of the Processing, WorkWave shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of any Customer's obligation to respond to a Data Subject Request (whether made directly to Customer or notified by WorkWave under this Schedule or otherwise). In addition, to the extent Customer, by its use of the Services, does not have the ability to address a Data Subject Request, WorkWave shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent WorkWave is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from WorkWave's provision of such assistance.

7.4. **Notification by Customer.** Customer must make any Data Subject Request or request for assistance in relation to a Data Subject Request by contacting privacylead@workwave.com.

7.5. **Giving information to Data Subjects**. When acting as Controller, WorkWave is required by the GDPR, UK GDPR, PIPEDA and other Data Protection Laws and Regulations to give information to Data Subjects about its processing of personal data. Since WorkWave does not communicate directly with Data Subjects it requires Customer's assistance in order to meet its obligations. Accordingly, Customer shall, on WorkWave's behalf, provide to Data Subjects, at or before the time at which any Personal Data is collected from them, free of charge and in an easily accessible form, with the information that their Personal Data is being shared with WorkWave and with a hyperlink to the WorkWave Privacy Notice or some other indication that the relevant information may

be obtained from WorkWave. In addition, each party shall give, on request, all reasonable assistance to the other party in complying with its obligations under Applicable Data Protection Laws and Regulations to give information to Data Subjects.

8. SECURITY

8.1. **Controls for the Protection of Customer Personal Data.** WorkWave shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Personal Data), confidentiality and integrity of Customer Personal Data taking into account the state of the art, costs or implementation and the nature, scope, context and purpose of Processing. WorkWave regularly monitors compliance with these measures. WorkWave may update or modify such security measures but will not materially decrease the overall security of the Services during the term of the Schedule.

8.2. **Confidentiality of Processing.** WorkWave shall ensure that any person that it authorizes to process Customer Personal Data (including its staff, agents and subcontractors) shall be subject to a duty of confidentiality (whether a contractual or a statutory duty) ensuring appropriate security for the Personal Data in question.

8.3. **Third-Party Certifications and Audits.** WorkWave has obtained the third-party certifications and audits applicable to the processing of Customer Personal Data. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Master Agreement, WorkWave shall make available to any Customer that is not a competitor of WorkWave (or Customer's independent, third-party auditor that is not a competitor of WorkWave) a copy of WorkWave's then most recent third-party audits or certifications, as applicable.

8.4. **Customer Data Incidents.** WorkWave maintains security incident management policies and procedures and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored or otherwise Processed by WorkWave or its Sub-processors of which WorkWave becomes aware (a "**Customer Data Incident**"). Where a Customer Data Incident is not caused by Customer, WorkWave shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as WorkWave deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within WorkWave's reasonable control.

8.5. **Breach notification.** Upon becoming aware of any Customer Data Incident, WorkWave shall notify Customer without undue delay and pursuant to the terms of the Master Agreement, but within no more than seventy-two (72) hours and shall provide such timely information as Customer may reasonably require to enable Customer to fulfil any data breach reporting obligations under Data Protection Laws and Regulations. WorkWave will take steps to immediately identify and remediate the cause of such incident. WorkWave's obligation to report or respond to a Customer Data Incident shall not be construed as an acknowledgment by WorkWave of any fault or liability of any kind.

9. RELATIONSHIP WITH THIRD PARTY PROVIDERS

9.1 If, in order to carry out its obligations under the Master Agreement and its schedules, it is necessary for WorkWave to share the Customer Personal Data with Third Party Providers, Customer:

a) consents to WorkWave sharing the Data with Third Party Provider;

b) warrants that it is lawful for it to share the Customer Personal Data with WorkWave for the purpose of carrying out WorkWave's obligations under this Agreement, including any consequential sharing of Data with Third Party Provider;

c) shall have the sole responsibility for the accuracy, quality, legality and reliability of Data provided by it to WorkWave for processing and of the means by which it acquires such Customer Personal Data;

9.2 Where WorkWave is under a duty to assist Third Party Provider with their compliance with obligations imposed on them by any applicable Data Protection Laws and Regulations relating to the processing of the Customer Personal Data in the course of the provision of Services to Customer under the Agreement, Customer shall give (and where

they exist, procure that Merchants give) WorkWave all reasonable assistance required by WorkWave for the carrying out of such a duty.

10. LIMITATION OF LIABILITY

10.1. Each party's liability and the liability of its Affiliates, taken together in the aggregate, arising out of or related to this Attachment and whether in contract, tort (including without limitation negligence) or under any other theory of liability is, to the extent permitted by law, subject to the limitation provision in the Master Agreement (including any provision titled 'Limitation of Liability') and shall be treated as liability under the Master Agreement, and any reference in any such limitation to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Master Agreement including this Attachment. Notwithstanding the foregoing, nothing in this clause shall affect any Party's liability to Data Subjects as require by applicable law nor any liability that might arise to the other under Article 82 of the GDPR or UK GDPR.

10.2. For the avoidance of doubt, WorkWave's and its Affiliates' total liability for all claims from Customer and all of its Affiliates arising out of or related to the Master Agreement shall apply in the aggregate for all claims under the Master Agreement including the Schedule and this Attachment.

11. TRANSPARENCY

Customer shall, on WorkWave's behalf, provide (or where Customer has an indirect relationship with Data Subjects ensure that the appropriate party provides) to Data Subjects, free of charge and in accessible form (as required by Article 14 of the GDPR and UK GDPR and any Data Protection Laws and Regulations applicable) with the information that their Personal Data is being shared with WorkWave and with a hyperlink to the WorkWave Privacy Policy.

12. OTHER RELATIONSHIPS WITH DATA SUBJECTS

Customer shall be responsible for (whether directly, or by contract with one or more third parties) managing the relationship with Data Subjects arising out of the Processing of Customer Personal Data under this Schedule. Where the Data Protection Laws and Regulations give Data Subjects any right which may be exercised against a Controller, then Customer shall be responsible for managing the response to any attempt, or purported attempt, to exercise that right by a Data Subject.

US ADDENDUM

In addition to the requirements set forth under this Attachment, the obligations set forth under this addendum ("US Addendum") shall further apply and regulates the Processing of Customer Personal Information of Consumers subject to the U.S. State Privacy Laws (as defined above). Capitalized terms used in this US Addendum but not otherwise defined herein have the meaning ascribed to them in this Addendum or the Agreement

Section A: California.

This Section A of the US Addendum applies to WorkWave's provision of and Customer's use of the Services to the extent that in carrying out the Services, Customer is a Business and WorkWave is a Service Provider.

1. Definitions.

The terms "Business", "Service Provider", "Contractor", "Third Party Business", shall have the same meaning as ascribed to them in the CCPA. "Data Subject" as intended by the EU Data Protection Law shall also mean and refer to "Consumer", as such term is defined in the CCPA. "Personal Data" shall include "Personal Information" under this DPA. The terms "Controller", "Processor", "Business purpose", "Sell" and "Share" shall have the same meaning as in the applicable U.S. State Privacy Laws.

2. Obligations in carrying out the Processing. With respect to Customer Personal Information, the Parties acknowledge and agree that: (i) WorkWave does not receive Customer Personal Information as consideration for any of the Services; (ii) Customer represents and warrants that it has provided notice that the Consumer Personal Information is being used or disclosed as required by the U.S. State Privacy Laws.

2.1. Provisions relating to WorkWave. WorkWave will comply with obligations applicable to it as a Service Provider under the CCPA and as Processor under applicable U.S. State Privacy Laws.

2.2.1 Except as otherwise permitted by law, WorkWave will not: (i) retain, use, or disclose Customer Personal Information for any purpose other than for the specific purpose of performing the Services specified in the Agreement for Customer; (ii) Sell or share Customer Personal Information; (iii) combine the Customer Personal Information with other Personal Information except as expressly permitted under the law, such as to detect data security incidents or protect against fraudulent or illegal activity.

2.2.2 WorkWave shall provide commercially reasonable assistance, where required, to Customer for the fulfillment of Customer's obligations to respond to Consumer Requests.

2.2.3 WorkWave shall ensure that all persons authorized to Process Customer Personal Information are made aware of the confidential nature of Customer Personal Information and are subject to a duty of confidentiality with respect to the data.

2.2.4 Taking into account the context of Processing, WorkWave shall maintain appropriate technical and organizational measures with regard to Customer Personal Information to ensure a level of security appropriate to the risk in accordance with this Addendum and as otherwise expressly stated in the Agreement.

2.2.5 WorkWave will notify Customer if it makes a determination that it can no longer meet its obligations as a Service Provider under the CCPA.

2.2.6 For any sub-service provider or processor used by WorkWave to process personal information subject to U.S. State Privacy Laws, WorkWave will ensure that WorkWave's agreement with such sub-service provider or processor complies with the law.

2.2.7 Customer acknowledges and agrees that WorkWave may Process Aggregate Customer Personal Data and De-identified data (together, "Deidentified Data") relating to, derived, or generated from Customer Personal Data or derived from the Services, for any lawful purpose. As between WorkWave and Customer, WorkWave exclusively will own rights, title, and interest in and to Deidentified Data. Customer further acknowledges and agrees that Deidentified Data does not constitute Customer Personal Data, and WorkWave may use, maintain, disclose, and otherwise Process such Deidentified Data for any lawful purpose.

2.2 **Provisions relating to the Customer.** Customer will comply with obligations applicable to it as a Business under U.S. State Privacy Laws.

2.2.1 Customer acknowledges and agrees that it is responsible for compliance with all notice, consent, opt out, and privacy policy requirements under applicable law, as well as for complying with all requests from individuals with respect to Customer Personal Information (including but not limited to requests to know, requests to delete, and requests to opt out), as may be required by applicable law. If WorkWave receives any request directly from Customer's consumer, then WorkWave may either (i) advise the Consumer to contact Customer directly or (ii) contact Customer to respond directly to the consumer.

2.2.2 Upon notice, Customer will have the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of personal data.

2.2.3 Customer will conduct audits, reviews and assessments in accordance with the Master Agreement and this Addendum.

.

EXHIBIT A (part 1) of this Attachment

PAYMENT APPLICATION PROCESSING

The following includes the information required by Annex I.A of the EU SCCs and Table 2 and 3 of the UK IDTA.

LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

EXHIBIT A (part 2) of this Attachment

The following includes the information required by Annex I.B of the EU SCCs and Table 2 and 3 of the UK IDTA.

DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

[insert nature of services offered]

Categories of personal data transferred

Any subset of the data points about any transaction that WorkWave is able to accept, as agreed with Customer. These data points include (but are not limited to):

- Name, Address, Telephone numbers, Email addresses
- Transaction amount
- Account numbers, Cardholder account number, Cardholder name, Card expiration date
- Device identifiers
- [include any other categories of data collected/transferred]

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Data is transferred on a continuous basis.

Nature of the processing.

[insert description]

Purpose(s) of the data transfer and further processing

To provide the Services offered to the Customer.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

[Insert period or criteria].

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.

WorkWave may transfer personal data to Affiliates of WorkWavefor further sub-processing. Any such sub-processing would be of the same type as described under this part of Annex I – WorkWave is simply delegating the carrying out of its duties.

EXHIBIT B (part 1) of this Attachment

FRAUD APPLICATION PROCESSING

The following includes the information required by Annex I.A of the EU SCCs and Table 2 and 3 of the UK IDTA.

LIST OF PARTIES

MODULE ONE: Transfer controller to controller

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

EXHIBIT B (part 2) of this Attachment

The following includes the information required by Annex I.B of the EU SCCs and Table 2 and 3 of the UK IDTA.

DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

Categories of data subjects whose personal data is transferred

[insert nature of services offered]

Categories of personal data transferred

Any subset of the data points about any transaction that WorkWave is able to accept, as agreed with Customer. These data points include (but are not limited to:

- Name, Address, Telephone numbers, Email addresses

- Account numbers, Cardholder account number, Cardholder name, Card expiration date

- Device identifiers

- [include any other categories of data collected/transferred]

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Data is transferred on a continuous basis.

Nature of the processing

[include description]

Purpose(s) of the data transfer and further processing

To provide the Services offer to the Customer.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

[insert period]

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

WorkWave may transfer personal data to Affiliates of WorkWave for further sub-processing. Any such sub-processing would be of the same type as described under this part of Annex I – WorkWave is simply delegating the carrying out of its duties.

WorkWave may also transfer to one or more processors that have been explicitly identified by WorkWave's Customer to add value to its risk management services.

– EXHIBIT C of this Attachment
TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The following includes the information required by Annex II of the EU SCCs and Table 3 of the UK IDTA.

[WHERE WORKWAVE IS THE IMPORTER]

WorkWave

At WorkWave, the security of storing, transmitting, and processing of personal data is important to us. We have implemented commercially reasonable precautions consistent with applicable regulatory requirements and industry recognized security standards to protect any personal data submitted to WorkWave. The overview of WorkWave's information security program establishes our commitment to safeguarding Personal Data which is stored, processed, and transmitted by WorkWave.

A.1 Information Security Program

WorkWave has implemented and maintains a comprehensive security program designed to protect the security, confidentiality, and integrity of Personal Data. This program maintains an appropriate level of information security and data privacy and includes policies and standards for security management, risk management, personnel security, physical security, operations management, security monitoring and response, communications management, access control, network security, third party services, application management, business continuity, compliance, IT management, IT incident management, and privacy. These policies and standards are approved by WorkWave Executive Management and are reviewed and updated as needed and at least annually.

A.2 Organizational Security

WorkWave Board of Directors and Executive Management charges [include third party compliance provider] with the responsibility for developing, maintaining, and communicating the above information security program to all employees, subcontractors, and/or third-party entities providing services, processing, storing, or transmitting Personal Data. It is the responsibility of all personnel involved in the processing of Personal Data to comply with these policies and standards. [include third party compliance provider] has responsibility to:

- Communicate with appropriate business units to ensure systems and applications are built with strong security foundations and ensure all security compliance and regulatory requirements are met.
- Ensure WorkWave employees is continually educated on their responsibilities to protect assets used to process Personal Data.
- Development of initiatives to continually enhance WorkWave's security posture
- Create and publish reports to Executive Management demonstrating the security posture of WorkWave along with identification of gaps to allow focus on those areas
- Ensure the deployment and maintenance of tools and processes to continually assess the security posture of WorkWave
- Rapidly respond and collaborate with business units to address security issues

A.3 Human Resources Security

All potential WorkWave users are screened prior to access to WorkWave Information assets and are only provided the minimum access commensurate with their assigned job responsibilities for handling Personal Data. Once annually, WorkWave requires all users to complete online data protection and information security awareness training. This training covers how to properly handle and protect Personal Data and includes updating employees on changes to WorkWave security policies, standards, and security controls. All users are legally bound to maintain and protect the confidentiality of any Personal Data they are granted access to.

A.4 Asset Management

WorkWave documents and manages all assets used during the performance of services which involves any Personal Data. These assets include:

- Physical Assets – tangible items such as equipment, property, devices, servers, desktops/laptops, printers, communication devices, etc.
- Information Assets – body of information such as personally identifiable information (PII), databases, intellectual property, strategies and plans, and trade secrets.
- Software Assets – any application or software used to support the processing, transmission, and/or storage of personal data

All assets are identified, evaluated, and classified based on the criticality and value to WorkWave. The appropriate level of security controls is assigned depending on the classification of each asset. These security controls help facilitate protecting and safeguarding of Personal Data throughout the lifecycle of each asset, from Planning and Acquisition to Monitoring and Disposal. Industry accepted standards are applied to determine which security controls are required for asset discovery and monitoring, access management, backup and recovery, and archival, retention, disposal, and destruction.

A.5 Access Control

Access to WorkWave's assets are restricted to authorized users who are required to support the performance of services involving Personal Data. Formalized processes and procedures have been implemented and govern how access is granted to authorized users, to include the level of access required for that user to perform their job responsibilities. User entitlement reviews are performed on a designated cadence to ensure users only retain the level of access required to perform their job responsibilities. Personal Data is not permitted to be read, copied, modified, or removed without prior authorization and all activities are monitored and logged.

A.6 Encryption and Pseudonymization

WorkWave implements industry-standard encryption practices during the transmission of Personal Data in all transfer cases. These practices include the use of Transport Layer Security (TLS), Internet Protocol Security (IPSec), and secure shell protocol (SSH). Furthermore, AES (128-bit or stronger) encryption is used for both Personal Data at rest and in transit.

In addition to encryption, WorkWave adopts several pseudonymization methods to decouple personal data from individuals during the processing, transmission, and storage of Personal Data. They include: scrambling, masking, data blurring, and tokenization.

A.7 Physical and Environmental Security

WorkWave ensures that systems used to process, transmit, and/or store Personal Data are hosted within a physical environment designed to protect the security and integrity of those physical assets. WorkWave staff is located on-site who can identify, categorize, and respond to a physical security incident, restrict access to only authorized individuals, and actively monitor security controls for all locations (buildings, computer facilities, and record storage facilities) where Personal Data is hosted.

WorkWave has taken measures to ensure only those personnel with the appropriate authorization have access to any facility processing, storing, and/or transmitting Personal Data. WorkWave has deployed an access control system for entering all facilities. Surveillance equipment is deployed in all security-relevant areas and is recorded using CCTV (Closed Circuit Television) cameras, entrance doors are secured using alarms and mantraps where appropriate, and access is controlled via ID card or similar authentication system. All access to any physical environment is monitored and logged.

A.8 Operations Security

WorkWave has created and maintains a comprehensive suite of documented operating procedures to cover all systems storing, processing, and/or transmitting Personal Data. These operating procedures are followed by both the Global Information Security and Technology and Operations teams and cover required security related activities to identify assets, analyze threats, analyze vulnerabilities, and deploy appropriate countermeasures. These activities include:

- Security Assessments and Testing – WorkWave Security Assessment and Testing program has been established to verify the appropriate level of security controls that are in place to protect Personal Data and the assets it resides on. It also tests these security controls for any vulnerabilities while taking account of all known threats which could compromise a security control. These assessments and testing include: security assessments, vulnerability testing, penetration testing, and auditing activities (by both external and internal entities). All testing is conducted on a designated frequency and any vulnerabilities or issues found are remediated according to industry accepted standards, regulations, and WorkWave policies and procedures.

- Change Management – A process by which changes are identified, planned, approved, and recorded. Rollback procedures are identified for each change prior to implementation. All changes are tested prior to implementation in a lower (e.g., test) environment. At all times, security implications are evaluated, and any associated risk is assessed.
- Malware Protection – All assets hosting Personal Data are subject to malware protection using industry standard practices to cover the prevention, detection, and recovery against known malware. This includes anti-malware software updates applied on a frequent basis and ensure systems are scanned regularly for all known malware.
- System Logging– All assets hosting Personal Data are configured to create logs recording user activities, exceptions, and security events. These logs include specific activities such as: authentication attempts and their results, end of user sessions, creation/modification/deletion of user accounts and system level objects, modification of user privilege levels, access to audit logs, and all activities conducted by any user with elevated privileges.
- Backup and Recovery – A process of ensuring a regular backup copy of all Personal Data is available in the event of a security incident involving recovery activities. Backups are taken on a regular basis and are tested for usability. Backup files are appropriately protected based on the information they contain, and those containing Personal Data are encrypted.

A.9 Communication Security

WorkWave has implemented measures to ensure that Personal Data cannot be read, copied, modified, or removed during electronic transmission and/or transmission while stored on data media. Security measures ensure that only permissive traffic is allowed to traverse to any asset processing, storing, and/or transmitting personal data. All networks used to support and deliver services are managed and controlled to protect Personal Data. Network segregation is used to protect Personal Data. All data traversing any public network will be encrypted as defined in A.6 Encryption and Pseudonymization.

A.10 System Acquisition, Development, and Maintenance

All systems have specific and relevant security requirements documented and are created using the appropriate baseline “gold” image. These images represent the approved baseline security configuration of all systems provisioned within the WorkWave environment. All images are continually scanned for compliance with WorkWave system hardening and configuration policies and are updated as needed.

WorkWave has established and maintains a Secure Software Development policy which covers all development activities used to support services. Development concepts include the requirement for ensuring data protection by developing security by design and by default. A formal change control process is followed during the software development lifecycle.

All software developed is subjected to security assessment testing to identify and remediate vulnerabilities. All vulnerabilities are remediated in accordance with WorkWave policies and procedures.

A.11 Supplier Relationship

WorkWave has an established Third-Party Risk Management (TPRM) Program that ensures WorkWave’s Vendors operate in a well-controlled environment including a review of sound security controls. WorkWave's third party vendors are subject to pre-engagement due diligence including a review of all industry and regulatory standards for the services they provide. Vendors are subject to ongoing assessments. WorkWave is responsible for ensuring that the third-party vendor’s security program includes all commercially reasonable security precautions designed to protect the security, confidentiality, and integrity of Personal Data.

A.12 Information Security Incident Management

WorkWave has an established Information Security Incident Management program. This program is a formalized process to detect, respond, mitigate, report, recover, and remediate from all security and privacy related incidents involving a ‘breach of security’ to Personal Data.

- Detection – Intrusion detection and prevention systems, are in place to help detect events of interest. Anti-malware software (covered in A.8 Operations Security), is deployed across the environment to detect the presence of malware. All personnel are trained to promptly report any suspected or actual security event through the appropriate channels. The Security Incident Event Management (SIEM) correlates and centralizes events of interest to assist in rapid detection of a potential security event.

- Response – Upon confirmation of a security incident, the incident response team is mobilized depending on the severity of the incident. The Incident response team roles and responsibilities are clearly defined, and each member receives annual training on their respective roles. A formalized incident response plan is followed which clearly outlines when the response team is mobilized, when to notify, and what steps are to be taken to help mitigate, report, recover, and remediate the security incident. Additionally, tabletop incident response exercises are conducted annually and are facilitated by a third party.
- Mitigation – All necessary steps are taken to contain the security incident and any related erroneous activity.
- Reporting – WorkWave will escalate and notify senior leadership of a security incident in accordance with the incident response plan. Furthermore, WorkWave has a legal obligation to notify based on applicable laws and regulations depending on the extent of the security incident and the potential impact to the data subject if Personal Data is exposed. In all cases, the standard for notification is no longer than twenty-four (24) hours upon becoming aware of a security incident.
- Recovery – The incident response team will take all necessary steps to recover the system to the previous state prior to the breach. This may include rebooting necessary devices, rebuilding affected assets, and/or restoring systems from previous backup versions.
- Remediation – A root cause analysis is performed on all security incidents detailing the cause of the incident and any factors which attributed to the security incident. A remediation plan is developed and provided to any customer affected by the security incident. All remediation activity is performed in accordance with the remediation plan. An investigation is performed to document what systems, data and information were affected by the event, and the result of that investigation is provided to all customers affected by the incident. WorkWave will cooperate with all Customers and any law enforcement or regulatory officials and investigating such incident.

A.13 Business Continuity Management

WorkWave has implemented a Business Continuity Plan (BCP) and Disaster Recovery (DR) to plan, and in preparation for, an adverse event which may affect delivery of services while maintaining adequate protection of Personal Data. The implementation of the BCP/DR plan ensures that all information security controls remain in place during the response and recovery from an adverse event. The BCP/DR plan is regularly reviewed and updated as needed to improve the delivery of services. These plans ensure the resiliency of all Personal Data managed and hosted at WorkWave facilities.

A.14 Compliance

WorkWave complies with all applicable laws, statutes, ordinances, and regulations with regards to the processing, storing, and transmission of Personal Data. Global Information Security, legal, and compliance departments work together to identify all applicable laws and regulations to WorkWave. Specific areas of consideration are intellectual property of WorkWave and its customers, protection of personal information, handling of personal data, financial and operational procedures, and trans-border data transmission.

WorkWave 's established policies and programs, such as the information security program, contract management, security awareness program, internal and external audits/assessments, internal and external legal counsel consultation, internal security controls assessment, external and internal penetration testing, vulnerability assessments, exception program, and risk management help WorkWave drive towards compliance with these areas of consideration.

EXHIBIT D of this Attachment

LIST OF SUB-PROCESSORS

The following includes the information required by Annex III of the EU SCCs and Table 3 of the UK IDTA.