Paymetric Data Processing Addendum

PAYMETRIC ACTING AS PROCESSOR

This Data Processing Addendum (this "DPA"), forms part of the Paymetric Services Agreement between Paymetric, Inc, a Worldpay, LLC company, located at 8500 Governors Hill Drive, Symmes Township, Ohio 45249 ("Paymetric") acting on its own and as agent for the Paymetric Affiliates and Company (as amended from time to time, the "Agreement"). This DPA is effective as of the effective date of Agreement ("Effective Date"). For the purposes of this DPA, "Paymetric, Inc, Worldpay means the Worldpay contracting entity identified in the Agreement, and "Company" means the customer contracting entity identified in the Agreement. Worldpay and Company may be referred to herein collectively as the "Parties" or individually as a "Party".

Company enters into this DPA on behalf of itself and its Affiliates to the extent Paymetric Processes Personal Data in performance of the Services for such Affiliates. Where Worldpay Process Personal Data for both the Company and its Affiliates, the term "Company" shall apply to both.

1. **WHEN THIS DPA APPLIES**

1.1 This DPA is binding on the Parties only to the extent Data Protection Laws govern the Processing Personal Data and when Paymetric Processes Personal Data only on Company's instructions, or where Paymetric is classified as a "Processor," service provider, or equivalent entity in an applicable Data Protection Law for one or more Processing activities Paymetric performs for the Company.

This DPA is fully incorporated into the Agreement. This DPA replaces any existing terms, exhibits, schedules, appendices, addendums, or other attachments related to the Processing of Personal Data unless otherwise expressly stated in this DPA. In the event of any inconsistency between the terms of this DPA and any terms of the Agreement with respect to Personal Data, the terms of this DPA will govern and control.

2. **INTERPRETATION**

2.1 In this DPA:

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

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

2.2 In this DPA the following terms shall have the meanings set out in this Section 2, unless expressly stated otherwise:

(a) **"Addendum Effective Date**" means the first day of the calendar month following execution of the Agreement by both Paymetric and Company.

(b) "**Agreement**" means the Paymetric Services Agreement for the services received by Company from Paymetric entered into by and between the parties on or before the date of execution of this DPA.

(c) "**Cessation Date**" has the meaning given in Section 12.1.

(d) "**Affiliate**" of a Party means another Person that directly, or indirectly through one or more intermediaries, controls or owns, is controlled or owned by or is under common control or ownership with, such Person. As used in this definition, "control" means the power to direct the management or affairs of a Person; "ownership" means the beneficial ownership of more than fifty percent (50%) of the equity interests in the Person; and to "own" means to have ownership of a Person.

(e) "**Controller**" (or equivalent term under Data Protection Laws) means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(f) "**Data Protection Laws**" means any applicable laws or regulations that the Processing of Personal Data in one or more jurisdictions, in each case as amended and supplemented.

(g) "**Data Subject**" means an identified or identifiable natural person to whom Personal Data relates. An identifiable natural person is one who can be identified as a particular individual, directly or indirectly, whether by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(h) "**Data Subject Request**" means the exercise by a Data Subject of their rights under, and in accordance with Data Protection Laws in respect of Personal Data.

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

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

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

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

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

(n) "**Person**" means any association, corporation, individual, partnership, trust, joint venture, or other entity or organization.

(o) "**Personal Data**" means any information relating to a Data Subject that is subject to protection under Data Protection Laws.

(p) "**Personal Data Breach**" means an event leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Paymetric's possession, custody, or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

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

(r) "**Processing/Process/Processed**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collecting, recording, organizing, structuring, storing, adaption or altering, retrieving, consulting, retaining, using, disclosing by transmission, disseminating or otherwise making available, aligning or combing, restricting, erasing or destroying the Personal Data.

(s) "**Processor**" (or equivalent term under Data Protection Laws) means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

(t) "**Relevant Body**":

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

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

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

(u) "**Restricted Country**":

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

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

(iii) in the context of Switzerland, means a country or territory outside Switzerland,

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

(v) "**Restricted Transfer**" means the transfer or disclosure of Personal Data where the transfer or disclosure would be prohibited by one or more Data Protection Laws in the absence of appropriate safeguards, including the Standard Contractual Clauses or UK International Data Transfer Addendum (as applicable) and similar provisions provided under other Data Protection Laws. Such transfers could be either (a) a transfer or disclosure of Personal Data from Merchant to Worldpay; or (b) an onward transfer or disclosure of Personal Data from Worldpay to a Sub-Processor.

(w) "**Security Statement**" means the Worldpay Technical and Organization Measures (TOMs) found at Annex 4, as may be updated from time to time by mutual agreement of the parties.

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

(y) "**Sub-Processor**" means the relevant Sub-Processors on the Sub-Processor list. List available upon request.

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

(aa) "**Third-Party User**" means any of Company's customers, or their customers, to the extent such persons are provided access to the Solution hereunder.

(bb) "**UK**" means the United Kingdom.

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

1.1 **CONTROLLER AND PROCESSOR.** In the course of Paymetric providing the Services under the Agreement, Company may from time-to-time provide or make available Personal Data to Paymetric. The parties acknowledge and agree that, in relation to any such Personal Data provided or made available by Company to Paymetric for Processing under the Agreement, Company may either act as a Controller or a Processor and Paymetric will be a (sub) Processor for the purposes of the Data Protection Laws.

1.2 **COMPANY AS CONTROLLER.** Company, as Controller, agrees that Company:

a) is solely responsible for the accuracy, quality, and legality of Personal Data, including the means by which Company acquires Personal Data;

b) is solely responsible for any registration, notice, or other authorization under applicable laws to engage Paymetric to perform the Services;

c) has the authority to transmit or disclose Personal Data to Paymetric (or permit Paymetric to access Personal Data); and

d) will provide Paymetric with lawful instructions with respect to the Processing of Personal Data.

3. **SUBJECT MATTER.** The Agreement determines the subject-matter and duration of Paymetric's Processing of Personal Data, and the obligations and rights of Company in relation to such Processing. The type of Personal Data, categories of Data Subjects and nature of Paymetric's Processing of Personal Data are set out in 0 (*Personal Data Attachment*).

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

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

6. **LAWFUL PROCESSING**

6.1 Company shall ensure that it is entitled to give access to the relevant Personal Data to Paymetric so that Paymetric may lawfully Process Personal Data in accordance with the Agreement on Company's behalf, which may include Paymetric Processing the relevant Personal Data outside the country where Company and/or the Data Subjects are located in order for Paymetric to provide the Services and perform its other obligations under the Agreement.

6.2 Company shall:

(a) comply with its obligations under the Data Protection Laws which arise in relation to this DPA, the Agreement and the receipt of the Services;

(b) inform Data Subjects that their Personal Data will be disclosed to Paymetric and, where applicable, request consent for the disclosure and/or cross-border transfer of their Personal Data; and

(c) not do or omit to do anything which causes Paymetric (or any sub-processor) to breach any of its obligations under the Data Protection Laws.

7. **RESTRICTED TRANSFERS**

7.1 The parties agree that, to the extent a) Company transfers Personal Data to Paymetric in a Restricted Country or b) Paymetric transfers Personal data to Company in a Restricted Country, it shall be effecting a Restricted Transfer. To allow such Restricted Transfer to take place without breach of applicable Data Protection Laws, the parties agree as follows:

(a) in the event of an EEA Restricted Transfer, the parties agree to incorporate the SCCs in this DPA, which SCCs are completed in accordance with Part 1 of Annex 2 (*Population of SCCs*);

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

(c) in the event of a Swiss Restricted Transfer, the parties agree to incorporate the SCCs in this DPA, which SCCs are completed in accordance with Part 1 of Annex 2 (*Population of SCCs*) and varied in accordance with Part 3 of Annex 2; and

(d) in the event of a Restricted Transfer, the parties agree to implement the "Supplementary Measures" set out in Annex 3, in addition to the SCCs.

Conflicts

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

Provision of full-form SCCs

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

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

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

10. **SUB-PROCESSORS**

10.1 Company hereby authorizes Paymetric to appoint the Sub-Processor as additional Processors of Personal Data under the Agreement, provided that Paymetric shall:

(a) impose upon such Sub-Processor data protection obligations that, in substance, provide for the same level of data protection as set out herein; and

(b) be responsible for the acts and omissions of such Sub-Processor under the Agreement.

10.2 Paymetric shall inform Company of any intended changes concerning the addition or replacement of other Sub-Processor not permitted hereunder, by making such information available to Company. Company may object to such changes in writing setting out its reasonable concerns in detail within ten (10) business days from such notice. If Company does not respond to such changes, Paymetric shall have the right to continue to Process the Personal Data in accordance with the terms of this DPA, including using the relevant Sub-Processor. If Company objects, Paymetric shall consult with Company, consider Company's concerns in good faith and inform Company of any measures taken to address Company's concerns. If Company upholds its objection and/or demands significant accommodation measures which would result in a material increase in cost to provide the Services, Paymetric shall be entitled to increase the fees for the Services or, at its option, terminate the Agreement.

11. **TECHNICAL AND ORGANIZATIONAL MEASURES**. Paymetric shall implement appropriate technical and organizational measures to protect Personal Data and ensure a level of security appropriate to the risk. Paymetric's measures comprise those documented in its Technical and Organizational Measures , attached as Annex 4, as may be updated from time to time by mutual agreement of the parties.

12. **DELETION**

12.1 Upon the date of termination or expiry of Services involving the Processing of Personal Data (the "**Cessation Date**"), Paymetric shall cease all Processing of Personal Data related to such Services except as set out in this Section.

12.2 Company hereby acknowledges and agrees that, due to the nature of Personal Data Processed by Paymetric, return (as opposed to deletion) of Personal Data may require exceptional effort by Paymetric in some circumstances. Having regard to the foregoing, Company agrees that it is hereby deemed (at the Cessation Date) to have irrevocably selected deletion, in preference of return, of such Personal Data. As such, Paymetric shall delete all relevant Personal Data Processed on behalf of Company within thirty (30) days of the Cessation Date, subject to Paymetric retaining any copies required by applicable laws (and in that case, for such period as may be required by such applicable laws).

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

14. **DATA SUBJECT REQUESTS**

14.1 Paymetric shall, upon Company's reasonable written request, provide Company with such assistance as may be reasonably necessary and technically possible in the circumstances to assist Company in fulfilling its obligation to respond to Data Subject Requests.

14.2 Upon receipt of any Data Subject Request that relates to Personal Data that Paymetric Processes for Company, Paymetric shall promptly notify Company and not respond to such Data Subject Request except on the written instructions of Company.

14.3 Company is solely responsible for responding to Data Subject Requests. Paymetric's notification of or response to a Data Subject Request under this Section is not an acknowledgement by Paymetric of any fault or liability with respect to the Data Subject Requests.

15. **PERSONAL DATA BREACHES**

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

(a) describe the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point at Paymetric where more information can be obtained;

(c) describe the likely consequences of the Personal Data Breach; and

(d) describe the measures taken or proposed to be taken by Paymetric to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

16. **DEMONSTRATION OF COMPLIANCE**

16.1 Paymetric shall, upon Company's reasonable written request, make available to Company all information reasonably necessary to demonstrate Paymetric's compliance with the obligations set out in this DPA in relation to Personal Data that Paymetric Processes for Company. Paymetric and Company will use current certifications or other existing audit reports to minimize repetitive audits.

16.2 If Company (acting reasonably and in good faith) considers that the information provided in accordance with Section 16.1 is not sufficient to demonstrate Paymetric's compliance with the obligations set out in this DPA, or where otherwise required by Data Protection Laws, Company may (at its cost) perform on-site audits at the Paymetric processing facility (or facilities) that provides the Services to Company, subject to the following:

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

(b) requests for on-site audit visits shall be made in writing by Company at least sixty (60) days in advance (unless shorter notice is given by the Supervisory Authority or specifically required by the relevant regulatory obligation, in which case Company 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;

(c) on-site audits will be limited to a review of Paymetric's compliance with this DPA;

(d) on-site audits shall be conducted during normal business hours for the facility and shall be coordinated with Paymetric so as to cause minimal disruption to Paymetric's business operations;

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

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

(g) Paymetric may require on-site audits to be conducted remotely if necessary for health and safety reasons;

(h) except as prohibited by applicable laws or the relevant Supervisory Authority, Paymetric shall receive and be entitled to comment on any report prepared by or on behalf of Company prior to that report being published or disseminated (such report to be Paymetric Confidential Information except to the extent it relates to the business or affairs of Company, which information will be

Company Confidential Information), which publication or dissemination shall be done only pursuant to the confidentiality provisions of the Agreement; and

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

17. **REIMBURSEMENT**. Company shall reimburse Paymetric for time spent and any costs reasonably incurred by Paymetric at rates agreed between Company and Paymetric (or if none have been agreed, at Paymetric's standard professional services rate) in performing its obligations under Sections 11 to 16, in each case except to the extent that such costs were incurred as a result of any breach by Paymetric of its obligations under this DPA.

Annex 1
Personal Data Attachment

The purpose of this Personal Data Attachment is to set out the details of any Personal Data of Company that Paymetric processes (including, but not limited to, has access to) as a result of the Agreement.

Company transferring Personal Data from Europe to Paymetric in a Restricted Country:

Data exporter: Company

- Address: as identified in the Agreement
- Contact person's details: as identified in the Agreement
- Activities relevant to the data transferred under the SCCs: Company shall be providing Personal Data as necessary to receive the Services pursuant to the Agreement.
- Role: Controller or Processor (when Company processes Personal Data on behalf of, and under the instruction, of its Third-Party Users).

Data importer: Paymetric

- Address: as identified in the Agreement
- Contact person's details: dpo@worldpay.com
- Activities relevant to the data transferred under the SCCs: Paymetric shall Process Personal Data as necessary to perform the Services pursuant to the Agreement.
- Role: (Sub) Processor

Paymetric transferring Personal Data from Europe to Company in a Restricted Country:

Data exporter: Paymetric

- Address: as identified in the Agreement
- Contact person's details: dpo@worldpay.com
- Activities relevant to the data transferred under the SCCs: Paymetric shall Process Personal Data as necessary to perform the Services pursuant to the Agreement.
- Role: Processor

Data importer: Company

- Address: as identified in the Agreement
- Contact person's details: as identified in the Agreement
- Activities relevant to the data transferred under the SCCs: to receive the Services pursuant to the Agreement.
- Role: Controller

Categories of Personal Data:

The processing of Personal Data by Paymetric as processor on behalf of Company comprises the following data types/categories:

☐ 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: _____

Special categories of Personal Data: None

Categories of Data Subjects: The Personal Data processed by Paymetric on behalf of Company may relate to the following categories of natural persons:

☐ Company and its Affiliates' employees

- ☐ Company and its Affiliates' customers
- ☐ Company and its Affiliates' potential customers
- ☐ Company and its Affiliates' suppliers
- ☐ Users of the Solution
- ☐ Contact persons
- ☐ Other; please specify: _____

Frequency of the Transfer: The Personal Data will be transferred on a continuous basis for the duration of the Agreement.

Nature and purpose of the processing of Personal Data: Paymetric will process the Personal Data to deliver the Services pursuant to the Agreement.

Data retention: Paymetric will delete the Personal Data from its systems on expiry or termination of the Services in accordance with Section 12 of the DPA.

Technical and organizational data security measures: Paymetric will protect the Personal Data in accordance with the security measures set out in the Security Statement.

Authorized Sub-Processor: Company authorizes Paymetric to appoint the Sub-Processor.

Annex 2
Population of SCCs

Notes:

- In the context of any EEA / Swiss Restricted Transfer, the SCCs completed in accordance with Part 1 of this Annex 2 are incorporated by reference into and form an effective part of the DPA.
- In the context of any UK Restricted Transfer, the SCCs as varied by the UK Transfer Addendum and completed in accordance with Part 2 of this Annex 2 are incorporated by reference into and form an effective part of the DPA.
- In the context of any Swiss Restricted Transfer, the SCCs as amended in accordance with Part 3 of this Annex 2 are incorporated by reference into and form an effective part of the DPA.

PART 1: EEA AND SWISS RESTRICTED TRANSFERS

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

2. **APPLICABLE MODULE**

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

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

3.1 The SCCs shall be completed as follows:

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

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

(c) Parties agree that the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 16 of this DPA.

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

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

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

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

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

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

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

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

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

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

4. **POPULATION OF ANNEXES TO THE SCCs**

4.1 Annex I to the Appendix to the SCCs is completed with the corresponding information detailed in Annex 1 (*Personal Data Attachment*) to this DPA, with – for module 2 and 3 - Company being 'data exporter' and Paymetric being 'data importer' and – for module 4 – Paymetric being 'data exporter' and Company being 'data importer'.

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

The competent Supervisory Authority shall be determined as follows:

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

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

PART 2: UK RESTRICTED TRANSFERS

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

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

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

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

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

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

PART 3: SWISS RESTRICTED TRANSFERS

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

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

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

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

Annex 3
Supplementary Measures

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

Technical measures

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

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

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

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

Further details of Paymetric's security program are summarized in the Security Statement found at Annex 4.

Contractual measures

1. Paymetric provides regular information – by publishing Transparency Reports - on government requests received by Paymetric from law enforcement and public authorities based in a third country outside Europe to access data relating to individuals in Europe. These Transparency Reports are available request.

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

Organizational measures

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

Annex 4

WORLDPAY TECHNICAL AND ORGANIZATIONAL MEASURES

1. INTRODUCTION

This Security Statement summarizes Worldpay's information security policies, procedures, processes and standards including its technical and organizational measures for the security of data and forms an integral part of the agreement between Merchant and Worldpay which incorporates this Statement by reference. The Statement sets out Worldpay's obligations with respect to information security and data protection in relation to the Agreement. To the extent of any conflict or inconsistency between the provisions of this Statement and any provision of the Agreement, the provisions of this Statement prevail and take precedence over such conflicting or inconsistent provisions.

Worldpay's Information Security Practices are compliant with International Organization for Standardization ISO 27001:2022, are aligned to industry standard frameworks, and are designed to protect the security, confidentiality and integrity of Merchant Data, including Personal Data. Worldpay's ISO 27001:2022 certification is available on upon request.

2. ORGANIZATIONAL PRACTICES

Worldpay's Information Security Department is responsible for developing and implementing Information Security Practices. Worldpay maintains safeguards designed to prevent the compromise or unauthorized disclosure of, or access to Company's Confidential Information, Company data including Company Personal Data, including loss, corruption, destruction or mis-transmission of Company's cConfidential Information, Company data, including Company Personal Data.

Worldpay maintains Worldpay's Information Security Practices that are designed to comply with (1) all applicable laws and industry best practices relating to the privacy, confidentiality and security of client data, including Company's confidential information and Company Personal Data, to the extent applicable to Worldpay as a third-party service provider; (2) the requirements set forth in this Statement; and (3) all applicable provisions of Worldpay's related policies, including but not limited to the Worldpay Information Security Policy.

Worldpay internal and external auditors regularly review Worldpay Information Security Practices. Additionally, Worldpay performs regular security assessments to determine whether identified vulnerabilities, in particular as related to web and network environments, have been remediated. Security assessments include: reviews of device configuration, internal and external penetration testing, assessments of applications processing sensitive data, assessments of Worldpay various systems, and reviews of Worldpay Information Security Practices.

Periodic updates are made to Worldpay Information Security Practices in response to evolving information security threats. Such updates provide an equivalent or increased level of security compared to what is described in this Statement. In no event shall Worldpay make any material changes to its Information Security Practices that reduce, limit, or adversely affect Company's rights and/or Worldpay's obligations under this Statement without the prior written consent of Company.

Worldpay implements reasonable administrative, technical, organizational and physical safeguards designed to: (i) provide for the security and confidentiality of Company data, including Company Personal Data; (ii) protect against any anticipated threats or hazards to the security or integrity of client data, including Company Confidential Information and Company Personal Data; and (iii) protect against unauthorized access to or use of Company data, including Company Confidential Information and Company Personal Data. Worldpay will review and test such safeguards on no less than an annual basis. Worldpay has processes for regularly testing, assessing and evaluating the effectiveness of its technical and organizational measures in order to verify the security of its processing. The measures are described throughout this Statement.

3. SECURITY CONTROLS

3.1 Access Control to Facilities

3.1.1 Worldpay Facility Restrictions

Worldpay uses a number of technological and operational approaches in its physical security program to mitigate security risks to the extent reasonably practicable. Worldpay's security team works closely with Worldpay facilities teams at each Worldpay facility to confirm appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which data is processed. Worldpay's security team also continually monitors any changes to the physical infrastructure, business, and known threats which may impact the physical security of Worldpay work sites.

Access to Worldpay facilities is restricted and monitored using controls such as badge access, camera coverage, door alarms and security guards. Badges and keys are only distributed in accordance with documented organizational procedures. Visitors are registered prior to admittance, are provided a visitor badge, and in sensitive areas require an escort in accordance with Worldpay's Corporate Security Policy. Where appropriate, alarm systems are in place to notify appropriate individuals of potential threats. Worldpay regularly tests its emergency procedure protocols.

Physical security measures implemented at Worldpay facilities are designed to protect employees, contractors, visitors, and assets. Physical security consists of a combination of physical barriers, electronic access and monitoring systems, security officers and procedures for controlling access to buildings and sensitive or restricted areas. Secure shred bins or shredders are provided for the proper disposal of hard copy documentation and other small media at Worldpay facilities.

An access control system utilizing individual badge identification, doors protected by an electronic badge reader or locked with limited access to the physical key, closed circuit camera monitoring, and onsite physical security guards stationed in strategic locations are utilized to provide facility physical security and protection. Physical access to Worldpay buildings, office spaces and certain secured areas within Worldpay facilities are controlled by an electronic access control system. The system provides for real-time monitoring of all electronic badge accesses across the monitored facility, requires physical security officer acknowledgment of system identified error codes or issues, and is tied to centralized servers communicating the exact date and time stamp for each entry (utilizing network time protocol). Automated database backups are performed daily and are replicated on the secondary server.

3.2 Logical Controls and Security

Worldpay has a dedicated group that is responsible for overseeing operational security, network security, host and server security, applications and system development, patch and vulnerability management, authentication and remote passwords, encryption, passwords and monitoring systems. Worldpay has documented protocols for all Logical Controls and Security including the following:

3.2.1 Employees

Worldpay conducts (at the time of hire) a background check for each Worldpay employee who is involved in the provision of the Solution and/or performing Professional Services. Background checks consist of reviews to the extent allowed by local laws of each country in which Worldpay operates. Worldpay complies with all applicable laws related to the background check, including required notices and applicable consents. Worldpay will not assign any employee to the provision of the Solution if their background check findings do not meet the standards established by Worldpay. Worldpay assigns all employees mandatory security and privacy awareness training on an annual basis. Worldpay requires all employees with access to sensitive information to follow a clean desk and clear screen standard such that the information is controlled and/or protected at all times. Worldpay has formal disciplinary procedures in place to address policy violations. A terminated employee's access to Worldpay facilities and Worldpay systems containing Client Data, including Client Personal Data is suspended upon termination.

3.2.2 Network Security

Worldpay employs a defense in-depth model when building networks in a multi-tiered approach and uses separate layers of presentation, business logic and data when considered necessary. Connection between networks is limited to those ports, protocols and services required for Worldpay to support, secure, monitor and provide the Solution.

Worldpay uses Network Intrusion Detection and/or Prevention Systems to monitor threats to the Worldpay environment. Where all, or part of, the Solution is provided using online services (i.e., accessible via the internet), Worldpay deploys a web application firewall (WAF) and controls designed to protect against distributed denial of service (DDoS) attacks. For remote access to Worldpay systems and networks, Worldpay requires the use of multi- factor authentication. Access to the internal Worldpay technology environment requires network access control (NAC) which evaluates the security posture of the connecting device.

Except as required by applicable law, Worldpay shall not create or change its business processes with the intention to facilitate access to Company data, including Company Confidential Information and Company Personal Data, by any government without Company's permission.

Worldpay may from time to time in its reasonable discretion block attempted access to the Solution from technology of individuals, entities, or governments which Worldpay reasonably believes may pose a threat to the Solution, systems or clients.

3.2.3 Host and Server Security

Worldpay hardens its operating systems in accordance with industry security standards and procedures. Worldpay's hardening standards are based on the Center for Internet Security (CIS) standards. For example, Worldpay requires that all default passwords are changed, unneeded functionality is disabled or removed, the concept of "least-privileged" access is adhered to, file permissions do not include world writeable ability, administrative or "root" access is limited to the console only, and only those network ports that are necessary to provide the Solution are opened. For database installations, Worldpay uses security at a table and row level, based upon the placement of a system and its role in the environment.

Access to Worldpay's operating systems is limited to those individuals required to support the system including where privileged access is restricted and controlled. Worldpay has implemented appropriate change management processes. Servers and workstations are enabled with auto-locking (password-protected) screensavers that activate after a period of inactivity. Installation of personal software is not allowed. Local administrative rights are not permitted on Worldpay's end user computing devices.

3.2.4 Anti-virus, anti-malware, anti-spyware, PC controls

Worldpay requires that anti-virus, anti-malware, anti-spyware, and event detection and response (EDR) software is enabled on its operating systems when they are available and supported by a commercially available solution. Worldpay PCs and laptops have industry standard controls including disk encryption, access management, whitelisting, anti-virus/anti-malware, and administrative controls.

3.2.5 Applications and Systems Development

Worldpay uses System Development Lifecycle and system change procedures, which include requirements for code review and secure coding practices. Development and testing environments are segregated and firewalled from Worldpay's production environment. Version control software is utilized for the management and deployment of code through appropriate support groups. Worldpay applies measures for verifying system configuration, including default configuration. Worldpay considers data protection issues as part of the design and implementation of systems, services, products and business practices (Privacy by Design).

3.2.6 Electronic Mail

Worldpay scans incoming emails, embedded links and attachments prior to allowing them into the Worldpay environment. Worldpay also uses industry standard software to control what files are allowed or blocked as attachments to protect against malicious executable files

being delivered and/or opened. Worldpay configures email domains with industry standard anti-phishing technologies such as Sender Policy Framework (SPF) and Domain-based Message Authentication Reporting and Compliance (DMARC).

3.2.7 Vulnerability & Patch Management

Worldpay employs reasonable efforts to identify and remediate or mitigate vulnerabilities in the Solution in accordance with Worldpay's Vulnerability Management Policy. This includes weekly network scanning of Worldpay's public internet facing infrastructure and monthly network scanning of Worldpay's non-public internet facing infrastructure. Worldpay, in its sole discretion, may pause or otherwise modify the scanning schedule to accommodate peak volume periods or resolve performance issues associated with scanning. Worldpay will perform scanning of Worldpay developed source code and related libraries for the presence of vulnerabilities in currently supported versions of the Solution. Worldpay undertakes reasonable efforts to remediate or mitigate critical vulnerabilities within 14 days of Worldpay becoming aware of the vulnerability. A critical vulnerability is defined as a public internet exposed vulnerability which has been validated as remotely exploitable and has a CVSS >9. Worldpay will make reasonable efforts to meet the vulnerability remediation targets defined within Worldpay's vulnerability management policy. Such policy conforms to industry standards and generally applied best practices.

3.2.8 Bug Bounty Program

Worldpay maintains a public bug bounty program to encourage responsible disclosure of discovered vulnerabilities in the Solution, which is the "Worldpay Bug Bounty Program"; participating in the Worldpay Bug Bounty Program shall be subject to conditions set forth by Worldpay at its discretion, to be updated from time to time. Subject to Company's participation in the Worldpay's Bug Bounty Program as described at the following link: https://bugcrowd.com/Worldpay will pay financial "bounties" to clients who identify and report vulnerabilities in accordance with the Worldpay's Bug Bounty Program requirements.

3.2.9 Authentication

The level of authentication required to access a particular Worldpay environment is based on the type of data protected within that environment. Worldpay permits only authorized persons to access any Worldpay systems in accordance with Worldpay's Information Security Policy. User authentications (i.e., username and password) are bound to the respective user and may not be shared. The use of an emergency user account must be documented and logged. Remote access to Worldpay's systems requires the use of multi-factor authentication.

3.2.10 Passwords

Worldpay requires the use of complex passwords. Worldpay's password controls do not allow the previous ten (10) passwords to be used, and current passwords expire at regular intervals. Remote access to Worldpay's systems requires the use of multi-factor authentication. User accounts are locked after a defined number of abortive or unsuccessful logon attempts. If a password is possibly disclosed, it is changed without undue delay. Using a documented procedure, Worldpay employs processes to minimize the risk of unauthorized or no longer needed user accounts in the systems and audits user accounts to determine that access that is no longer required is revoked.

3.2.11 Data Classification, Retention, and Controls

Worldpay's Information Classification Policy addresses the confidentiality, integrity, security, and availability of Company data. Company data retention and disposal are to be stipulated in the contract to meet business requirements. All Worldpay employees and vendors with access to Company data including Company Confidential Information and Company Personal Data are required to comply with secure deletion standards in alignment with the latest NIST *Guidelines for Media Sanitization*. Worldpay will store Company data, including Company Confidential Information and Company Personal Data, only for as long as necessary to achieve the purposes for which it was collected, for a contractually committed time period as set forth in the Agreement or in accordance with applicable laws and thereafter delete it in accordance with the secure deletion standards.

Worldpay takes reasonable steps to determine access to Company Personal Data. Worldpay's Enterprise Identity and Access Management Policy is based on the "principle of least privilege," which calls for authorized users to access only the minimum level of Company Personal Data required to satisfy the user's job responsibilities. Where required, Worldpay will take adequate steps to keep Company Personal Data relating to different clients or purposes separate.

3.2.12 Encryption

Worldpay's Encryption Policy aligns with industry standards. Worldpay encrypts data at rest that is Company data including Company Confidential Information and Company Personal Data where technically feasible with reasonable effort. Data is encrypted based on data classification policies and standards. Worldpay will use encryption key lengths that meet current NIST FIPS 140-2 standards where possible. Worldpay policies require that Worldpay shall not transmit any unencrypted Company data including Company Confidential Information and Company Personal Data over the internet. Specific algorithm and other minimum key lengths are specified within Worldpay's policy.

3.2.13 Monitoring Systems and Procedures / Logging

Worldpay uses a real-time event management system to monitor its networks and servers via system logs, intrusion detection/prevention systems, data loss prevention, file integrity monitoring and firewall logs on a 24-hour per day, 7 days a week, 365 days a year basis. Worldpay will perform reasonable logging, monitoring, or record keeping of user activity, including but not limited to where applicable administrator access, login attempts, hostnames/ IP addresses of connections, date and time of connections where legally permissible and in accordance with Worldpay's applicable information retention standards.

Worldpay utilizes a 24/7/365 security operations center which monitors and responds to security threats.

Worldpay shall securely collect, monitor and retain event logs so access to Confidential information and systems can be traced. Worldpay shall provide mutually agreed upon logs to Company upon request. The summary will advise root cause of the incident and the mitigating actions taken to bring the incident to a satisfactory conclusion.

3.2.14 Security Incident Response

The Worldpay Security Incident Response Team is responsible for investigating and responding to confirmed security incidents impacting Worldpay technology. Company may review Worldpay's Security Incident Response Plan, which is available upon request. The Security Incident Response Plan documents the processes and procedures of the incident response team. If Company becomes aware of a security incident impacting Worldpay's technology, Solutions, Company should contact the Worldpay Helpdesk as detailed in the contract and service handbook.

Should Worldpay confirm a security incident or privacy incident that results in the loss of or unauthorized access to, use or disclosure of Client Confidential Information in Worldpay's possession or control (such an incident a "data breach"), Worldpay shall provide Company with notification without undue delay, making all reasonable efforts to provide such notification within 24 hours of Worldpay's confirmation of the described impact to Client's Confidential Information. The notification shall summarize, in reasonable detail, to the extent possible and to the extent known, the nature and scope of the data breach and if known, the corrective action already taken or planned by Worldpay shall promptly take all reasonable and necessary actions to end the data breach, mitigate its impact, and prevent recurrence.

Worldpay shall cooperate with Company in the investigation of the data breach and shall promptly respond to Company's reasonable inquiries about the data breach. Worldpay shall provide to Company regular updates regarding such data breach, and at the conclusion of the investigation, Worldpay shall provide to Company, to the extent possible and to the extent known, a report detailing the data breach, its impact, and the mitigation and/or remediation steps taken by Worldpay. Based on the nature of the incident, Worldpay will perform this investigation internally or with a third- party response or forensic firm of Worldpay's choosing.

The parties acknowledge and agree that this Section does not require notice of unsuccessful security incidents, as described below. "**Unsuccessful security incidents**" means, without limitation, pings and other broadcast attacks on Worldpay's firewall, port scans, unsuccessful log-on attempts, unsuccessful denial of service attacks, unsuccessful exploit attempts, and any mix of the above, so long as no such incident results in unauthorized access, use or disclosure of Company Confidential Information. Worldpay and Company shall mutually agree upon any external communications that specifically name Company in response to a data breach impacting Company systems or Company Confidential Information including Company Confidential Information and Company Personal Data. Nothing in this Section shall prevent Worldpay from making any notifications or notifying third parties and/or regulators of any incident, cyber-attack, or data breach, which may be required under applicable laws, regulations, by such regulator, or in accordance with any client contracts. Worldpay will not inform any third party of a data breach naming Company without first obtaining Company's prior written consent, unless and to the extent Worldpay is otherwise required to provide notice by law and/or regulator.

Worldpay shall conduct forensic investigation following a data breach when Worldpay and Company mutually agree it is necessary and conduct any investigations in accordance with legal requirements for preserving evidence. Any forensic investigation will be conducted in a timely manner and will maintain the appropriate chain of custody**.**

3.2.15 Ransomware

Worldpay has robust controls in place to protect against ransomware. These controls are regularly tested and validated, providing Worldpay confidence that we have minimized the risk of a ransomware attack. Worldpay also regularly tests its ability and processes to respond to a ransomware attack. In the event of a ransomware attack, Worldpay will recover (rebuild) from trusted backups.

3.2.16 Work from Home

Employees will have only the access rights required for their role. All logical controls remain in place, including the following:

- Working remote means working from a private, reasonably secure location, such as a home, apartment or flat. Working in a public location such as an internet café is not allowed.
- Workers must use Worldpay-owned and managed laptops that are imaged by Worldpay and have all of the standard controls including disk encryption, access management, whitelisting, anti-virus/anti- malware, and administrative controls.
- Workers must access Worldpay networks using multi-factor authentication, network access control, and VPN.
- Navigation of Worldpay networks must have the same or more stringent controls as from the office, such as the use of hardened intermediary devices to access highly sensitive environments.

In the case where workers are accessing client networks and assets, they must do so based on client connection requirements (for example, virtual desktop infrastructure) and strictly follow client protocols.

4. BUSINESS CONTINUITY AND DISASTER RECOVERY

Worldpay has a Global Business Resilience ("**GBR**") program and maintains recovery and response plans ("**Plans**") designed to minimize the risks associated with crisis events affecting Worldpay's ability to provide the Solution. Plans are designed to maintain a consistent provision of the Service(s) in the event of a crisis incident affecting Worldpay's operations. Worldpay's GBR program meets the ISO 22301 business continuity international standards or similar equivalent standard.

Worldpay's collection of comprehensive and coordinated Plans are designed to address the agreed crisis response, continuity, and recovery needs for the Service(s), including recovery time objective ("**RTO**") and recovery point objective ("**RPO**").

Worldpay provides a summary of the GBR program upon request. Worldpay's RTO and RPO for the Solution are as set forth in such summary (or as set forth in the Agreement, with any RTO and RPO in the Agreement prevailing over such summary). Worldpay maintains adequate backup procedures in order to recover Company data to such RPO and within the RTO. Worldpay validates the efficacy

and viability of its Plans at least annually to confirm viability and provide assurance of resilience capabilities as well as the readiness of Plans' participants. Recovery exercise results are provided upon request.

5. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

For Worldpay's products that require compliance with the then current version of the Payment Card Industry Data Security Standard ("**PCI DSS**"), Worldpay will maintain compliance with the then current version of the PCI DSS throughout the term of the Agreement and shall make available upon request, evidence of certification of compliance to Company.

6. VENDOR MANAGEMENT

Worldpay has an established Third- Party Risk Program that uses subject matter experts from across the enterprise to determine Worldpay's suppliers' criticality and ability to meet business and control requirements throughout the lifecycle of the relationship.

Worldpay conducts a risk assessment for all third-party suppliers engaged in the provision of the Solution to validate compliance with Worldpay standards. Worldpay's risk assessment requires suppliers to confirm if they have appropriate contracts in place with their vendors that store, process, transmit, manage or access Company data, including Company Confidential Information and/or Company Personal Data. Worldpay only allows such third-party suppliers to access, store, transmit, manage, or process Client Data, including Client Confidential Information and Company Personal Data, to the extent permissible under the Agreement and applicable laws.

Worldpay requires its suppliers who process Company data to agree to data protection agreements to oblige such suppliers to comply with applicable data protection laws. Such suppliers shall, at a minimum, implement appropriate technical and organizational measures to verify a level of security appropriate to the risk. Worldpay's suppliers must cooperate upon reasonable request in order to assist Worldpay with its compliance with applicable privacy laws.