worldpay

Worldpay
Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered into as of the Addendum Effective Date by and between: (1) Worldpay; and (2) the Merchant.

1. INTERPRETATION

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

(a) **"Addendum Effective Date**" means the later of the effective date of the Agreement or the effective date of the amendment of the Agreement by which the terms and conditions of this Data Processing Addendum are first incorporated into the Agreement.

(b) "**Agreement**" means the Merchant Services Agreement or other agreement forming the framework agreement for the services received by the Merchant from Worldpay entered into by and between the Parties on around the date of execution of this Data Processing Addendum or amended to first incorporate the terms and conditions of this Data Processing Addendum.

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

(d) "**Client Portal**" means a self-service portal made available to the Merchant's designated representatives at Merchant's request at https://my.fisglobal.com/vendor-management offering specific Merchant resources to help better manage its relationship with Worldpay, including information about its information security practices.

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under the Agreement and this DPA, including without limitation European Data Protection Laws; in each case as amended, repealed, consolidated or replaced from time to time.

(f) "**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.

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

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

(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protection laws applicable in Europe, including the EU GDPR, the UK GDPR and the FADP, in each case, as may be amended, superseded or replaced.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 EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**").

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

(o) **"PIPL"** means the Personal Information Protection Law ("PIPL") in China and the relevant regulations as may be amended, superseded or replaced.

(p) "**Relevant Body**":

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

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

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

In the contact of the China PIPL, the Cyberspace Administration of China ("**CAC**").

(q) "**Restricted Country**":

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

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

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

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

in the context of China, means a country or territory outside of Mainland China.

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

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

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

in the context of Switzerland, a Restricted Country outside Switzerland (a "**Swiss Restricted Transfer**") and/or

in the context of China, a Restricted Country outside of Mainland China (a "**China Restricted Transfer**").

(s) "**Security Statement**" means the Worldpay Security Statement attached as Annex 2, as may be updated from time to time by mutual agreement of the parties.

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

(u) "**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.

(v) "**Subprocessors**" means the relevant sub-processors listed in the GDPR section of the Client Portal.

(w) "**Supervisory Authority**" means:

in the context of the EU GDPR, any authority within the meaning of Article 4(21) of the EU GDPR.

in the context of the UK GDPR, the UK Information Commissioner's Office; and

in the context of the FADP, the FDPIC.

(x) "**UK**" means the United Kingdom of Great Britain and Northern Ireland.

(y) "**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**").

1.2 In this DPA:

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

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

(c) 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).

1.3 If this DPA is incorporated into an Agreement in which the parties include Worldpay and a party which: (a) is referred to as either the "Payfac" or "Aggregator"; or (b) receives services from Worldpay under that Agreement for the purpose of the furtherance of that party's provision of its own payment aggregation services; (such party under (a) or (b) being an "**Aggregating Party**") this DPA shall apply to the Aggregating Party in all respects as if the Aggregating Party were the "Merchant". The Aggregating Party shall also procure that its own merchants/sellers/retailers are bound by and perform the same obligations that the Aggregating Party is bound by in this DPA.

2. PROCESSING OF SHARED PERSONAL DATA

2.1 In the course of Worldpay providing the Services under the Agreement, the Merchant may from time-to-time provide or make available Personal Data to Worldpay. The parties acknowledge and agree that each party is an independent Controller and shall independently determine the purposes and means of such Processing, except for Pazien Services, for which Worldpay will be a

Processor for the purposes of the Data Protection Laws. If Worldpay is processing Personal Data as a Processor, Section 11 of this DPA shall apply.

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

2.3 Each party shall (at its own cost):

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

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

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

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

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

2.5 The Merchant shall be responsible for:

(a) ensuring that the information referred to in Data Protection Laws (including Articles 13 and 14 of the GDPR) is made available to relevant Data Subjects in relation to the Processing carried out in connection with the Agreement, and that the information is in a concise, transparent, intelligible and easily accessible form, using clear and plain language as required by Data Protection Laws;

(b) providing Data Subjects with a link to the Worldpay Privacy Notice at www.fisglobal.com/privacy;

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

(d) informing Worldpay if a Data Subject withdraws his/her consent to the Processing of his/her Personal Data.

2.6 If the Merchant receives any complaint, notice or communication from a Supervisory Authority which relates directly to:

a. Worldpay's Processing of the Shared Personal Data; or

b. a potential failure by Worldpay to comply with Data Protection Laws in respect of the activities of the Parties under or in connection with this Agreement,

the Merchant shall, to the extent permitted by Law, promptly notify Worldpay and provide such information as it shall reasonably request in that regard.

3. PERSONNEL

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

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

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

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

4. SECURITY

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk (which may be of varying likelihood and severity) for the rights and freedoms of natural persons, each party shall implement appropriate technical and organisational measures in relation to Shared Personal Data to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

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

5. DATA SUBJECT RIGHTS

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

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

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

6. PERSONAL DATA BREACH

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

6.2 At a minimum, any notification made by a party pursuant to Section 6.1 shall include (to the extent available at the relevant time):

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

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

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

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

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

7. RESTRICTED TRANSFERS

7.1 The parties agree that, to the extent either party transfers Shared Personal Data to the other party in a Restricted Country, it shall be effecting a Restricted Transfer. To allow such Restricted Transfer to take place without breach of applicable Data Protection Laws, the parties agree as follows:

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

(d) in the event of a China Restricted Transfer, the parties agree to incorporate the SCCs in this DPA, which SCCs are varied to address the requirements of the PIPL in accordance with Part 4 of Annex 3, until such time as the Relevant Body issues a final version of the Chinese specific standard contractual clauses, in which case parties shall cooperate to incorporate such Chinese specific standard contractual clauses in this DPA; and

(e) in the event of a Restricted Transfer, the parties agree to implement the "Supplementary Measures" set out in Annex 4, 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 Shared Personal Data in such manner as may be required.

Introduction of Binding Corporate Rules

7.4 Notwithstanding Section 7.1, to the extent Worldpay implements, at any time during the term of this DPA, Binding Corporate Rules which may be relied on to legitimatise Restricted Transfers from Merchant to Worldpay made in connection with the Agreement:

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

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

8. **CHANGE IN LAWS**

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

8.2 If Worldpay gives notice under Section 8.18.1, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in the notice as soon as is reasonably practicable.

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

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

9. **REIMBURSEMENT**. Merchant shall reimburse Worldpay for time spent and any costs reasonably incurred by Worldpay at rates agreed between Merchant and Worldpay (or if none have been agreed, at Worldpay's standard professional services rate) in performing its obligations under Sections 2, 5 , 6 and (if applicable) 11.4 to 11.8, in each case except to the extent that such costs were incurred as a result of any breach by Worldpay of its obligations under this DPA.

10. **INCORPORATION AND PRECEDENCE**

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

In the event of any conflict or inconsistency between:

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

(b) any SCCs entered into pursuant to Section 7 and this DPA and/or the Agreement, those SCCs shall prevail.

11. **WORLDPAY AS A PROCESSOR**

The following provisions only apply if Worldpay is Processing Personal Data under the Agreement in a capacity as Processor. The Sections 1 – 10 also apply, except to the extent this Section 11 deviates from Section 1 – 10.

11.1 **INSTRUCTIONS**. Worldpay shall Process Personal Data on behalf of Merchant and only in accordance with the instructions given by Merchant 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 Worldpay shall to the extent not prohibited by such laws inform Merchant of that legal requirement before the relevant Processing of that Personal Data. Worldpay shall promptly inform Merchant if, in its opinion, an instruction infringes against applicable Data Protection Laws.

11.2 **LAWFUL PROCESSING** Merchant shall ensure that it is entitled to give access to the relevant Personal Data to Worldpay so that Worldpay may lawfully Process Personal Data in accordance with the Agreement on Merchant's behalf, which may include Worldpay Processing the relevant Personal Data outside the country where Merchant and/or the Data Subjects are located in order for Worldpay to provide the Services and perform its other obligations under the Agreement. Merchant 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 Worldpay and, where applicable, request consent for the disclosure and/or cross-border transfer of their Personal Data;

(c) provide Data Subjects with a link to the Worldpay Privacy Notice at www.fisglobal.com/privacy;

(d) inform Worldpay if a Data Subject withdraws his/her consent to the Processing of his/her Personal Data; and

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

11.3 **SUB-PROCESSORS**

11.3.1 Merchant hereby authorizes Worldpay to appoint the Subprocessors as additional Processors of Personal Data under the Agreement, provided that Worldpay shall:

(a) impose upon such Subprocessors 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 Subprocessors under the Agreement.

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

11.3.3 Where necessary to legalize the use of any such other Subprocessors, Merchant hereby authorizes Worldpay to conclude the SCCs in accordance with Section 7 with such Subprocessors as agent on behalf of Merchant and (if required) Merchant's Affiliates. Each such conclusion of SCCs shall be considered a supplement to the Agreement and shall be subject to the terms and conditions set out therein.

11.4 **DELETION**

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

11.4.2 Merchant hereby acknowledges and agrees that, due to the nature of Personal Data Processed by Worldpay, return (as opposed to deletion) of Personal Data may require exceptional effort by Worldpay in some circumstances. Having regard to the foregoing, Merchant 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, Worldpay shall delete all relevant Personal Data Processed on behalf of Merchant within thirty (30) days of the Cessation Date, subject to Worldpay retaining any copies required by applicable laws (and in that case, for such period as may be required by such applicable laws).

11.5 **ASSISTANCE AND COOPERATION**. Worldpay shall, upon Merchant's reasonable written request, provide reasonable assistance to Merchant with its legal obligations under Data Protection Laws, including any data protection impact assessments and prior consultations with Supervisory Authorities which Merchant 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, Worldpay.

11.6 **DATA SUBJECT REQUESTS**

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

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

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

11.7 **PERSONAL DATA BREACHES**

11.7.1 If Worldpay confirms any actual Personal Data Breach affecting Personal Data that Worldpay Processes for Merchant, Worldpay shall: (i) notify Merchant 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 Worldpay 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 Worldpay to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

11.7.2 Merchant is solely responsible for complying with data breach notification laws applicable to Merchant and fulfilling any third-party notification obligations related to any Personal Data Breach. Worldpay's notification of, or response to, a Personal Data Breach under this Section is not an acknowledgement by Worldpay of any fault or liability with respect to the Personal Data Breach.

11.8 **DEMONSTRATION OF COMPLIANCE**

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

11.8.2 If Merchant (acting reasonably and in good faith) considers that the information provided in accordance with Section 11.8.1 is not sufficient to demonstrate Worldpay's compliance with the obligations set out in this DPA, or where otherwise required by Data Protection Laws, Merchant may (at its cost) perform on-site audits at the Worldpay processing facility (or facilities) that provides the Services to Merchant, subject to the following:

(a) on-site audits may only be carried out once per calendar year, unless a Supervisory Authority having jurisdiction over Merchant 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 Merchant, 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 Merchant 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 Merchant 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 Worldpay's compliance with this DPA;

(d) on-site audits shall be conducted during normal business hours for the facility and shall be coordinated with Worldpay so as to cause minimal disruption to Worldpay'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 Merchant's employees and/or a reputable third-party auditor agreed to by both parties, it being understood that Merchant (and its representatives) shall at all times be bound by the confidentiality provisions of the Agreement and shall be accompanied by a representative of Worldpay;

(g) Worldpay 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, Worldpay shall receive and be entitled to comment on any report prepared by or on behalf of Merchant prior to that report being published or disseminated (such report to be Worldpay Confidential Information except to the extent it relates to the business or affairs of Merchant, which information will be Merchant 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-Merchant environments, care should be taken to ensure that risks to another Merchant's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.

[Merchant]	WORLDPAY, LLC
Signature: _____	**Signature:** _____
Name: _____	**Name:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____

Annex 1
Data Processing Details

Data exporter: Merchant

- Address: as identified in the Agreement
- Contact person's details: as identified in the Agreement
- Activities relevant to the data transferred under the SCCs: Merchant shall be providing Personal Data as necessary to receive the Services pursuant to the Agreement.
- Role: Controller

Data importer: Worldpay

- Address: as identified in the Agreement
- Contact person's details: data.protection@fisglobal.com
- Activities relevant to the data transferred under the SCCs: Worldpay shall Process Personal Data as necessary to perform the Services pursuant to the Agreement.
- Role: Controller or Processor, depending on the type of Services provided under the Agreement: Worldpay is acting as an independent Controller, except where it provides Pazien Services. For these Services, Worldpay acts as a Processor.

Subject matter and duration of the Processing of Shared Personal Data

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

Data retention

Data importer will delete the Shared Personal Data from its systems on expiry or termination of the Services in accordance with its usual data retention practices. If Data Importer acts as a Processor, the deletion of the Personal Data is set out in Section 11.4 of the DPA.

The nature and purpose of the Processing of Shared Personal Data

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

The types of Shared Personal Data to be Processed

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

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

☒ Solution log in and usage data

☒ Bank account data

☒ Financial data

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

☒ Billing and payments data

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

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

☒ Merchant and its affiliates' employees

☒ Merchant and its affiliates' customers

☒ Merchant and its affiliates' potential customers

☒ Merchant and its affiliates' suppliers

- ☒ Users of the Solution
- ☒ Contact persons

Special categories of Personal Data (if appropriate):

None

Frequency of the Transfer

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

Annex 2
Security Statement

1. Introduction

This Security Statement ("**Statement**") summarizes Worldpay's information security policies, procedures and standards including its technical and organizational measures for the security of data ("**Worldpay's Information Security Practices**") and forms an integral part of the agreement between Merchant and Worldpay which incorporates this Statement by reference ("**Agreement**"). 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 27001:2013, are aligned to the NIST and CIS frameworks, and are designed to protect the security, confidentiality and integrity of Merchant Data, including Merchant Personal Data. Worldpay's ISO 27001:2013 certification is available on the Vendor Management Resource Center on the Client Portal (as defined below) or upon request.

Additional information on Worldpay's Information Security Practices is made available to Merchant under the Vendor Management Resource Center on the Client Portal or upon request. Such information is Worldpay's Confidential Information.

2. Organizational Practices

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

Worldpay maintains Worldpay's Information Security Practices that are designed to comply with (1) all applicable laws relating to the privacy, confidentiality and security of Worldpay's Confidential Information and Merchant Data, including Merchant 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 Worldpay's Information Security Policy.

Worldpay's internal and external auditors regularly review Worldpay's Information Security Practices. Worldpay performs security assessment reviews to determine whether identified vulnerabilities, in particular as related to web and network environments, have been remediated. Security assessment reviews include: diagnostic reviews of devices, internal and external penetration testing, assessments of applications that can access sensitive data and assessments of Worldpay's Information Security Practices.

Worldpay updates Worldpay's Information Security Practices from time to time in response to evolving information security threats. Such updates provide at least an equivalent or increased level of security compared to what is described in this Statement, and Worldpay will provide Merchant with a summary of material updates upon request. In no event shall Worldpay make any material changes to its Information Security Practices that reduce, limit, or adversely affect the rights and obligations under this Statement without the prior written consent of Merchant.

Worldpay implements reasonable administrative, technical, and physical safeguards designed to: (i) provide for the security and confidentiality of Client Data, including Client Personal Data; (ii) protect against any anticipated threats or hazards to the security or integrity of Client Data, including Client Personal Data; and (iii) protect against unauthorized access to or use of Client Data, including Client 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 each site to confirm appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which data is processed and continually monitors any changes to the physical infrastructure, business, and known threats.

Access to Worldpay facilities is restricted and monitored using controls such as badge access, camera coverage, door alarms and guards. Badges and keys are only distributed in accordance with documented organizational procedures. Visitors are screened prior to admittance, are provided a visitor badge, and in sensitive areas require an escort in accordance with Worldpay's Information Security Policy. 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 offices are designed to protect employees, 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. Security is staffed 24 hours a day, seven days a week, at Worldpay data center facilities. Secure shred bins or shredders are provided for the proper disposal of hard copy documentation and other small media at Worldpay offices.

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 the facility 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 acknowledgement 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.

For data centers, Worldpay maintains automatic early-warning sensors (e.g., fire, water, temperature and humidity), independent air conditioning systems and fire suppression systems. Mission-critical hardware is protected by an emergency power supply system with batteries and backup generators. Hazardous or combustible materials are kept at a safe distance from information assets.

3.1.2 Merchant Location Policies and Merchant Location Access

While Worldpay personnel are performing Services at Merchant's site, Worldpay will ensure that such personnel comply with Merchant's security policies and procedures that are generally applicable to Merchant's other suppliers providing similar services and that have been provided to Worldpay in writing in advance. If Worldpay personnel receive access cards or keys that provide them with access to Merchant's premises, Worldpay shall take reasonable measures designed to ensure that (a) such access cards and/or keys are only used for their intended purpose; (b) are protected from access by unauthorized third parties; (c) are promptly returned to Merchant once the Services have been completed; and (d) any loss is reported to Merchant without undue delay.

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 (collectively, "**Logical Controls and Security**"). 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, as described herein, for each Worldpay employee who is performing the Services. Currently, the background check in the United States of America consists of, at a minimum, verification of the highest level of education completed, verification of employment (as allowed by applicable law), social security number trace and validation, and a check of U.S. Government Specially Designated National (OFAC) and other export denial lists. Background checks outside of the United States consist of similar reviews to the extent allowed by local laws of each country. Worldpay complies with all applicable laws related to the background check, including required notices and applicable consents. Worldpay will not assign any employee

to perform the Services if his/her background check findings do not meet the standards established by Worldpay. Worldpay assigns all employees mandatory security 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 Merchant Data, including Merchant Personal Data is suspended upon termination.

3.2.2 Network Security

Worldpay employs a defensive 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 perform the Services.

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's systems and networks, Worldpay requires the use of multi-factor authentication. Privileged access to the internal Worldpay technology environment requires network access control (NAC) which evaluates the security posture of the connecting device.

Worldpay does not intentionally create back doors or similar programming that could be used to access the Merchant Data, including Merchant Personal Data, without Merchant's permission.

Except as required by applicable law, Worldpay shall not create or change its business processes with the intention to facilitate access to Merchant Data, including Merchant Personal Data, by any government without Merchant'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 merchants (such technology, "**Suspicious Technology**"). Due to the unknown timing of cyber threats, Worldpay may not be able to provide Merchant prior notice of blocking the Suspicious Technology, and it may impact the availability of the Solution. If Merchant is adversely affected, Worldpay will make reasonable efforts to resolve any impacts to Merchant as long as Worldpay can reasonably prevent any ongoing threats to the Solution, systems and merchants. Worldpay will make information regarding this practice available to Merchant on the Client Portal or upon request.

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 and Services 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 0-14 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 score >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

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

3.2.10 Merchant Security Testing

Worldpay permits and encourages Merchants to evaluate, test, and monitor the security of the Solution at Merchant's expense, as set out below. Any testing not explicitly allowed by this Section is not permitted.

Scanning

Merchant may perform automated scanning of Worldpay's public internet exposed Solutions. Worldpay may block or otherwise interfere with Merchant's scanning activity, as deemed appropriate and necessary by Worldpay in its sole discretion. Worldpay will not provide a response to Merchant's scan results although confirmed exploitable vulnerabilities identified via Merchant's scanning activity may be submitted to FIS' Bug Bounty Program as outlined in the paragraph 3.2.8.

"Ethical Hacking"

Merchant may conduct ethical hacking of Worldpay's public internet exposed Solutions subject to the terms of FIS' Bug Bounty Program. Vulnerabilities identified through such tests must be promptly submitted to Worldpay as documented in FIS' Bug Bounty Program. Worldpay may block or otherwise interfere with merchant/customer ethical hacking, as deemed appropriate and necessary by Worldpay in its sole discretion. Worldpay will not be liable for Merchant's inability to access its product or service as a result of Merchant's performance of security testing.

3.2.11 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.

3.2.12 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.

3.2.13 Data Classification, Retention, and Controls

Worldpay's Information Classification Policy addresses the confidentiality, integrity, security, and availability of Merchant Data. Merchant data retention and disposal are to be stipulated in the contract to meet business requirements All Worldpay employees and vendors with access to Merchant Data including Merchant Personal Data are required to comply with secure deletion standards in alignment with the latest NIST *Guidelines for Media Sanitization*. Worldpay will store Merchant Data, including Merchant 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 Merchant 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 Merchant Personal Data required to satisfy the user's job responsibilities. Where required, Worldpay will take adequate steps to keep Merchant Personal Data relating to different merchants or purposes separate.

3.2.14 Encryption

Worldpay's Encryption Policy aligns with industry standards. Worldpay encrypts data at rest that is Merchant Data including Merchant 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 Merchant Data including Merchant Personal Data over the internet. Specific algorithm and other minimum key lengths are specified within Worldpay's policy.

3.2.15 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 operates 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 Merchant upon request. The summary will advise root cause of the incident and the mitigating actions taken to bring the incident to a satisfactory conclusion.

3.2.16 Security and Privacy Incident Response

The FIS Security Incident Response Team (FSIRT) is responsible for investigating and responding to confirmed security incidents impacting Worldpay technology. FSIRT is staffed 24/7/365 with cyber security response experts and is authorized to take the necessary actions to contain and respond to a cyber security incident. Merchant may review Worldpay's Security Incident Response Plan, which is available on the Client Portal or upon request. The FSIRT Security Incident Response Plan documents the processes and procedures of FSIRT. If Merchant becomes

aware of a security incident impacting Worldpay's technology, Solutions or Services, Merchant should contact FSIRT at FSIRT@fisglobal.com.

The Worldpay Privacy Incident Response Team (PIRT) employs a coordinated incident response approach, leading a specialized form of privacy compliance protocols that respond to and investigate privacy incidents. Merchant may review Worldpay's Privacy Incident Response Plan, which is available on the Merchant Portal or upon request. By utilizing a coordinated approach, Worldpay mitigates, contains, and reduces the potential of any negative impact or risk associated with these incidents. PIRT is responsible for triaging and leading all investigations, as well as verifying documentation and facilitating communication amongst all stakeholders when potential and confirmed privacy incidents are identified. PIRT confirms Worldpay is timely in its identification, containment, and mitigation of privacy incidents as well as maintaining compliance with all applicable legal requirements. If Merchant becomes aware of a privacy incident impacting Worldpay's technology, Solutions or Services, Merchant should contact PIRT at PIRT@fisglobal.com.

Should Worldpay confirm a security incident or privacy incident that results in the loss of or unauthorized access to, use or disclosure of Merchant Confidential Information in Worldpay's possession or control (such an incident a "data breach"), Worldpay shall provide Merchant 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 Merchant'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. Worldpay shall promptly take all reasonable and necessary actions to end the data breach, mitigate its impact, and prevent recurrence. Worldpay shall cooperate with Merchant in the investigation of the data breach and shall promptly respond to Merchant's reasonable inquiries about the data breach. Worldpay shall provide to Merchant regular updates regarding such data breach, and at the conclusion of the investigation, Worldpay shall provide to Merchant, 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 using the FSIRT/PIRT team or with a third-party forensic firm of Worldpay's choosing. Merchant may request that a third-party forensic firm performs a review, at Merchant's sole expense, and Worldpay will negotiate in good faith with Merchant to select a mutually agreeable third party firm and perform the related review.

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 combination of the above, so long as no such incident results in unauthorized access, use or disclosure of Merchant Confidential Information.

Worldpay and Merchant shall mutually agree upon any external communications that specifically name Merchant in response to a data breach impacting Merchant systems or Merchant Confidential Information including Merchant 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 merchant contracts. Worldpay will not inform any third party of a data breach naming Merchant without first obtaining Merchant'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 Merchant 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.

3.2.17 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.

3.2.18 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 merchant networks and assets, they must do so based on merchant connection requirements (for example, VDI) and strictly follow merchant protocols.

3.2.19 Industry Hot Topics

Industry Hot Topics are published on the Vendor Resource Management Center within the Worldpay Client Portal. Keeping Worldpay's merchants informed of high-profile potential issues or new security and risk developments is a key tenet of Worldpay's partnership with its merchants. To help educate merchants on these high-profile industry hot topics, Worldpay has developed a downloadable document that provides:

- A definition of each issue,
- Worldpay's response to the issue,
- Worldpay's recommendations for merchant action.

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 Services. 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 FFIEC business continuity guidelines and the PS-Prep / 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 in the Client Portal or upon request. Worldpay's RTO and RPO for the Services 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 Merchant 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 via the Client Portal or upon request.

Further details of the GBR program, applicable when Worldpay hosts the Solution or provides it as a Service, is set out in the Business Continuity and Disaster Recovery Attachment below.

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, via the Client Portal or upon request, evidence of certification of compliance to Merchant.

6. Vendor Management

Worldpay has an established Vendor Risk Management 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's 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 Merchant Data and/or Merchant Personal Data. Worldpay only allows such third-party suppliers to access, store, transmit, manage, or process Merchant Data, including Merchant Personal Data, to the extent permissible under the Agreement and applicable laws.

Worldpay requires its suppliers who process Merchant 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.

Worldpay maintains a list of all third-party suppliers with access to Merchant Personal Data on the Client Portal.

7. Data Minimization

Merchant is responsible for verifying Merchant Data, including Merchant Personal Data, provided to Worldpay for processing or other purposes under the Agreement is accurate, current, adequate, of appropriate quality, relevant, minimal, and not excessive.

8. Defined Terms

As used in this Statement, the following terms have the following meanings and all other capitalized terms shall have the meaning as defined in the Agreement:

"**Merchant Data**" means data introduced into the Solution by or on behalf of Merchant or Merchant's customers that is stored in or processed by the Solution.
"**Merchant Personal Data"** means any personal Personal Data provided by Merchant to Worldpay, or on Merchant's behalf, for the purpose of Worldpay providing the Solution(s) to Merchant pursuant to the Agreement.
"**Personal Data**" is any information relating to an identified or identifiable natural person.
"**Client Portal**" means a self-service portal made available to Merchant's designated representatives at Merchant's request at https://my.fisglobal.com/vendor-management offering specific Merchant resources to help better manage its relationship with Worldpay, including information about Worldpay's Information Security Practices.
"**Confidential Information**" is all business or technical information disclosed by Merchant to Worldpay or by Worldpay to Merchant in connection with the Agreement. Confidential Information includes without limitation: (i) Merchant Data, including Merchant Personal Data, and the details of Merchant's computer operations; and (ii) details of the Solution(s).

"**Services**" means services (including SaaS and hosting services) provided by Worldpay to Merchant.

"**Solution(s)**" means the software and/or services (as applicable) being provided by Worldpay to Merchant under the terms of the Agreement.

worldpay

Annex 3
Population of SCCs

Notes:

- In the context of any EEA/Swiss Restricted Transfer, the SCCs completed in accordance with Part 1 of this Annex 3 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 3 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 3 are incorporated by reference into and form an effective part of the DPA.
- In the contect of any China Restricted Transfer, the SCCs as varied by Part 4 of this Annex 3 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 the 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. **MODULE**

- For Services that Worldpay provides as a Controller: Module One of the SCCs shall apply to any EEA and Swiss Restricted Transfer.
- For Services that Worldpay provides as a Processor: Module Two of the SCCs shall apply to any EEA and Swiss Restricted Transfer.

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

Module One

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) Clause 9 shall be deemed inapplicable.

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

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

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

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

Module Two

3.2 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 11.8 of this DPA.

(d) In Clause 9, OPTION 2: GENERAL WRITTEN AUTHORISATION applies, and the minimum time period for advance notice of the addition or replacement of Subprocessors shall be the advance notice period set out in Section 11.3 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.

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 to this DPA (*Data Processing Details*), with the sending party being 'data exporter' and the receiving party 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 the data exporter is established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of that EU Member State in which the data exporter is established.
- Where the data exporter is not established in an EU Member State, Article 3(2) of the GDPR applies and the data exporter 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 the data exporter's EU representative relevant to the processing hereunder is based (from time-to-time).
- Where the data exporter is not established in an EU Member State, Article 3(2) of the GDPR applies, but the data exporter 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 the data importer'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 Standards in Annex 2 of the DPA.

PART 2: UK RESTRICTED TRANSFERS

Where relevant in accordance with Section 7 of the 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:

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 to this DPA (*Data Processing Details*) and the foregoing provisions of Part 1 of Annex 2 (subject to the variations effected by the Mandatory Clauses described in (b) below); and

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.

PART 4: CHINA RESTRICTED TRANSFERS

Where relevant in accordance with Section 7 of this DPA, if Client acts as a Controller and transfers Personal Data from Mainland of China to FIS, acting as Processor, the SCCs – as varied below – shall apply until such time as the Cyberspace Administration of China issues a final version of the Chinese specific standard contractual clauses, in which case parties shall cooperate in good faith to incorporate such Chinese specific contractual clauses.

(d) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by references to the PIPL;

(e) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with "People's Republic of China";

(f) The "competent supervisory authority" and "supervisory authority" are both replaced with the Cyberspace Administration of China and China Banking and Insurance Regulatory Commission;

(g) Clause 17 is replaced with: "These Clauses are governed by the laws of People's Republic of China";

(h) Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the competent courts of People's Republic of China.

Annex 4
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 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: Both parties use industry standard encryption protocols for both in-transit and at-rest critical data.

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

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

Contractual measures

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

6. Both parties declare 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 such party to create or maintain back doors or to facilitate access to personal data or systems or for either party to be in possession or to hand over the encryption key.

Organizational measures

7. Training: all 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 policies and standards affiliated with privacy.

China additional measures

The parties have agreed to implement the additional measures when China's Measures on cross border data transfer security assessment are applicable to the China Restricted Data Transfer, Merchant acts as a Controller (and data exporter) and transfers Personal Data from Mainland of China to Worldpay acting as Processor (and data importer):

Worldpay shall provide the Merchant a reasonable prior notice under the following circumstances:

8. Substantial changes in the ownership or in the scope of business of Worldpay, that may result in material data security risks;

9. Changes to the network security environment or the data protection and privacy laws and regulations in the country or region where Worldpay is located that may result in material data security risks;

10. Force majeure events that impose material data security risks.

Upon occurrence of any of the above situations, Worldpay may choose either to (i) stop providing service to the Merchant without any penalty, or (ii) continue the cooperation with the Merchant if Worldpay is able to take effective security measures agreed by both parties to mitigate the risks and ensure the security of the Personal Data.

