DATA PROCESSING AGREEMENT

(hereinafter referred to as "DPA")

THIS AGREEMENT is entered into between:

PayU as described in the General Terms and Conditions of Use for PayU's Merchants, hereinafter "Merchant Agreement" or "Principal Agreement", acting for and on behalf of each relevant PayU Payment Provider; and the **Merchant** being a party of Principal Agreement.

This DPA sets out the details of the Processing of Personal Information by the PayU Payment Providers when rendering payment Services to the Merchant in the relevant jurisdictions as agreed by the Parties in the Merchant Agreement.

This DPA forms an integral part of theMerchant Agreement.

By signing the Merchant Agreement or by using the Services, the Merchant agrees to the following:

The General Terms and Conditions of Use for PayU's Merchants is hereinafter also referred to as the "Merchant Agreement" or "Principal Agreement". Each Party to this DPA is hereinafter collectively referred to as "**Parties**".

WHEREAS:

(a) The Parties have entered into a Merchant Agreement that involves the Processing of Personal Information of Data Subjects for or in the context of the Services provided under the API integration model in which the Merchant acts as Controller of the Personal Information and PayU acts as Processor. PayU affiliates render Services within various jurisdictions in accordance with Applicable Data Protection Law.

(b) The Parties have agreed to enter into a data processing agreement which shall govern the Processing of Personal Information of Data Subjects subject to Applicable Data Protection Law in the context of the Services provided in the Merchant Agreement.

(c) The validity of DPA is dependent on the full execution of Principal Agreement.

1. GENERAL PROVISIONS

1.1. This Data Processing Agreement (the"**DPA"**) sets out the basis for the Processing of Personal Information by Affiliates of PayU (the **"PayU Payment Providers"**) and constitutes integral part of the Principal Agreement.

1.2. In each case, unless expressly stated to the contrary, each PayU Payment Provider is bound as a principal to this DPA and to relevant references herein:

a) to "PayU" will be to PayU acting on behalf of each relevant PayU Payment Provider;

b) to a "party" or "parties" will be to the relevant PayU Payment Provider and the Merchant.

1.3. This document evidences a separate agreement between each Merchant and each PayU Payment Provider as though separate DPAs had been documented and executed between the Merchant and each PayU Payment Provider.

1.4. The obligations of each PayU Payment Provider under this DPA shall be several but not joint in respect of the obligations ofany other PayU Payment Provider and no PayU Payment Provider shall be liable to the Merchant/ for the actions of any other PayU Payment Provider.

1.5. Each PayU Payment Provider may sub-contract or delegate the performance of its obligations under this DPA to third parties including any of its Affiliates subject to any additional restrictions as per indicated in this DPA; however, the delegating PayU Payment Provider shall remain responsible for the performance of such duties.

1.6. In the event of a conflict between the DPA and the Principal Agreement, this DPA shall prevail in respect of the Processing of Personal Information

1.7. The DPA constitutes the entire agreement between the Parties in respect of the Processing of Personal Information and supersedes any such previous agreement, whether express or implied.

1.8. Any terms not otherwise defined in this DPA shall have the meaning that the Principal Agreement gives to them.

1.9. Terms used in this DPA that have meanings ascribed to them in Applicable Data Protection Laws, including 'data subject', 'processing', 'personal data', 'controller' and 'processor', carry the meanings set out under those laws to the extent that this DPA does not define them.

2. DEFINED TERMS

In this DPA:

2.1 **Affiliate** shall mean, in relation to any Party,any entity in the same group as that Party, including but not limited to a subsidiary or a holding company of that Party and any direct or indirect subsidiaries of such holding company. Also mentioned in this DPA as "**PayU Payment Providers".**

2.2 **Applicable Data Protection Law** shall mean: (i) the applicable national data protection and information privacy laws implemented in the country of incorporation of the relevant PayU contracting entity; (ii) to the extent applicable to this DPA, related data protection and privacy laws of other jurisdictions agreed between the Parties in writing in the Principal Agreement.

2.3 **Controller** shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes ('why') and means('how') of the processing of Personal Information.

2.4 **Data Security Breach** shall mean a breach ofsecurity leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise processed.

2.5 **Data Subject** shall mean an identifiable living natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, or as otherwise identified under Applicable Data Protection Law.

2.6 **Principal Agreement shall** mean the Merchant Agreement to which this DPA is appended.

2.7 **Personal Information** shall mean any information that identifies an individual or relates to an identifiable individual or as otherwise defined under Applicable Data Protection Law. Depending on the jurisdiction, Personal Information may include also information that identifies a juristic person. Also mentioned in this DPA as **"Personal Data"**

2.8 **Processing** shall mean the collection, recording, organization, alteration, use, access, disclosure, copying, transmission, transfer, deletion, storage, combination, destruction, elimination or other use of Personal Information in accordance with Applicable Laws.

2.9 **Transfer** means Processing of personal data that implies the communication of the same within or outside the territory, when its purpose is to carry out a Processing by the Processor on behalf of the Responsible.

2.10 **Processor** shall mean a natural or legal person, public authority, agency or other body which processes Personal Information on behalf of the Controller without coming under the direct authorityof the Controller.

2.11 **Services** shall mean the specific offering in scope for the relevant Principal Agreement.

3. PROCESSING PERSONAL INFORMATION-PARTIES' OBLIGATIONS

3.1. Each Party agrees to comply with the obligations that apply to it under ApplicableData Protection Law.

3.2. The Merchant shall abide by Applicable Data Protection Law, and its contractual and other obligations towards Data Subjects, in providing Personal Information to the PayU Payment Providers and Processing Personal Information through the use of the Services. Depending on the Services offered by the PayU Payment Provider in the relevant jurisdiction, additional data protection and privacy requirements may be applicable in accordance with Applicable Laws.

3.3. Each Party agrees to comply any current and enforceable payment card industry data security standards of the relevant Payment Schemes.

3.4. PayU is a global company with a global footprint. Personal Information may be processed by the relevant PayU Payment Provider either locally in the country wherethe Merchant provides its Services and/or in another country where the PayU Payment Provider or the PayU Payment Provider's approved third-party service providers operate to the extent this is deemed necessary and as permitted by and in accordance with Applicable Law. To this effect, PayU and its Affiliates have entered into an intracompany transfer agreement which ensures that the same level of data protection is applied as in the country where the Personal Information is initially processed.

3.5. The Merchant acknowledges that in some cases depending on the particular Services, thePayU Payment Providers may be required to contact Data Subjects to provide information and seek consents as necessary to allow the PayU Payment

Providers to use and disclose Personal Information in accordance with Applicable Data Protection Law. The Merchant shall take such steps, consistent with Applicable Data Protection Law, as the PayU Payment Providers reasonably request to facilitate these communications, including making available space in its web or mobile interfaces and/or providing Data Subject contact details.

3.6. The Merchant shall provide such information and offer such choices to ,and obtain such consents from Data Subjects as are required to enable the PayU Payment Providers to use and disclose the Personal Information as set out in in this DPA, in accordance with Applicable Data Protection Law. The Merchant shall (i) nonetheless use reasonable endeavours to facilitate Data Subjects' choices allowing such use and disclosure; and (ii) promptly notify the relevant PayU Payment Provider of any required consent which is withheld or subsequently withdrawn and any opt-out choice which is exercised.

3.7 The Parties will at all times comply with Applicable Data Protection Law and not, as far as is reasonable, do anything, or permit anything to be done, which might lead to a breach of Applicable Data Protection Law by the other Party. Further, upon each Party's request, the relevant Party will as soon as possible provide to the requesting Party in a manner and format requested by the requesting Party, any and all information that is required for the requesting Party to comply with Applicable Data Protection Law;

3.8 The Parties will at all times have in place, appropriate technical and organizational security measures so that Personal Information isprotected against unauthorized orunlawful processing and against accidental loss, destruction or damage.

4. PAYU AS A PROCESSOR

4.1. To the extent that PayU acts as Processor, it undertakes to treat the Personal Information in accordance with the following instructions provided by the Merchant under this DPA:

a) The Merchant hereby entrusts PayU with the Processing of the Personal Information on behalf of theMerchant made available to PayU in order to fulfill its obligations of Applicable Data Protection Law and for purposes of proper implementation and performance of the Services according to the provisions of the Principal Agreement and PayU's Privacy Policy.

4.2 Below are the categories of data subjects and types of Personal Information that could be in scope depending on the particular Service and country that the Service is being provided:

Categories of data subjects:	Employees Merchants Customers Buyers Resellers End users/Consumers
Scope of Personal Information:	First and last name Business contact information Personal ID registration number Email address IP address Telephone numbers Series and number of the identification document Home address like street name and number, city name, postal code Date of birth Tax identification number Bank account number Credit card number

4.3 PayU and any person acting under the authority of the Processor shall process the Personal Information only on documented instructions from the Merchant to the extent thatproviding the Services related to the processing activities requires them to, unless otherwise required bythe Applicable Data Protection Law.

5. OBLIGATIONS OF THE MERCHANT

5.1 The Merchant confirms that the processing activities relating to the Personal Information, as specified in the Principal Agreement and in this DPA are lawful, fair and transparentin relation to the Data Subject. In particular, the Merchant undertakes to:

a) Comply with its obligations as Controller of Personal Information under the Applicable Data Protection Law .

b) Comply with its obligations towards the Data Subject, including but not limited to the collection of the consent of the Data Subject, where applicable; the implementation of appropriate measures to provide Data Subjects the information required to facilitate the exercise of their rights and respond the Data Subject's requests according to provisions of Applicable Data Protection Law;c) Implement precautionary measures required to protect Personal Information against loss, abuse and unlawful, fraudulent or non-authorized access, use, consultation or modification of any third party, according to the Applicable Data Protection Law.

c) remain responsible for the Processing of Personal Information according to its rol of Controller and obligations under the Principal Agreement;

5.2 The Merchant hereby confirms that the instructions for the Processing ofPersonal Information comply with the Applicable Data Protection Law and the technical and organizational measures of the Processor are appropriate andsufficient to protect the rights of the Data Subject.

6. INTERNATIONAL DATA TRANSFERS

6.1 The Merchant hereby authorizes PayU to transfer Personal Information to countries that at the time of signing the Merchant Agreement provide an adequate level of protection ofPersonal Information according to the Applicable Data Protection Law. In any other scenario, if the Applicable Data Protection Law considers that the recipient country does not offer an adequate level of protection, PayU will:

a) warrant that any such transfers will be executed in accordance with a lawful data transfer mechanism.

b) be responsible for the processing activities of Personal Information performed by third parties other than PayU; that provides an adequate level of protection under Applicable Data Protection Law, i.e.

c) comply any other obligation under Applicable Data Protection Law.

6.2 For Transfers of Personal Informationoutside the scope of the purposes of this agreement, the relevant rules under Applicable Data Protection Law shall apply and both Parties agree to enter into separate transfer agreements.

7. CONFIDENTIALTY

7.1 PayU ensures that persons authorized by PayU to processPersonal Information are suitably informed, trained and instructed and have

committed themselves in writing to confidentiality or are under an appropriate statutory obligation of confidentiality.

8. SECURITY

8.1 PayU undertakes, prior to the processing of Personal Information, to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Applicable Data Protection Law and to ensure the protection of the rights of the Data Subject. In particular and in addition toExhibit B (Data Security):

a) PayU implements precautionary measures required to protect Personal Information against loss, abuse and unlawful, fraudulent or non-authorized access, use, consultation or modification of any third party, according to the Applicable Data Protection Law; b) PayU takes all measures guaranteeing the security of Personal Information, as described below; c) PayU shall also implement appropriate technical and organizational measures to ensure a level of security appropriate tothe risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, including among others and as appropriate:

- The pseudonymization and encryption of Personal Information
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore theavailability and access to Personal Information in a timely manner in the event ofa physical or technical incident;
- a process for regularlytesting, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing; and/or
- in assessing the appropriate level of security, account shall be taken, in particular, of therisks that are presented byProcessing, from e.g., the accidental or unlawfuldestruction, loss, alteration, unauthorized disclosure of, oraccess to Personal Information transmitted, stored or otherwise Processed.

9. DATA SUBJECT RIGHTS

9.1 PayU will respond the requests from Data Subjects in the case that it is required by the Applicable Data Protection Law, otherwise PayU commits to taking reasonable steps to assist the Merchant by appropriate measures to fulfil its obligation to respond to requests from Data Subjects concerning the exercise of their rights under the corresponding Applicable Data Protection Law, insofar as this is possible, taking into account the nature of processing and the information available to PayU. In any event, Merchant shall first seek to obtain the information required to respond to Data Subjects request on its own and shall contact PayU only if it cannot reasonably obtain such information itself.

9.2 In case the Merchant has a direct relationship with the Data Subject, PayU will not reply to

any requests coming directly from the Data Subject, unless PayU is required to reply under the Applicable Data Protection Laws. In case a Data Subject makes a request to PayU about the processing of Personal Data by the Merchant, PayU will forward to the Merchant such request, without delay and in writing to define together with PayU the response that will be provided to the Data Subject or for the Merchant to provide a response directly, as required by the Applicable Data Protection Law.

10 DATA SECURITY BREACH

10.1 PayU shall notify the Merchant without undue delay and at least within 72 hours after PayU becomes aware of a Data Security Breach at PayU or at its sub-processors' premises which results in a risk to the rights and freedoms of the Data Subjects. In case of a Data Security Breach, PayU will use reasonable endeavours to co- operate and assist the Merchant in investigating and mitigating, wherepossible, the adverse effects of the Data Security Breach.

10.2 PayU agrees to provide sufficient information in order to meet any obligations to report to orinform Data Subjects of the Data Security Breach in case it is necessary under the Applicable Data Protection Law.

10.3 In the event of a Data Security Breach, PayU shall promptly take adequate remedial measures. PayUshall fully cooperate with the Merchant to develop and execute a response plan to address the Data Security Breach. PayU shall at the request of the Merchant cooperateadequately informing the Data Subjects involved or in adequately informing a competent public authority.

10.4 PayU will report any Data Security Breach to the competent data privacy authority in the event it is required by the Applicable Data Protection Law.

10.5 PayU reserves the right to conduct risk assessments to ensure regulatory compliance and identify appropriate controls to mitigate security risks or other incidents and its effects.

11. ASSISTANCE TO THE CONTROLLER

11.1 PayU shall provide reasonableassistance to the Merchant with any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, which the Merchant reasonably considers to be required by the Applicable Data Protection Law, in each case solely in relation to the Processing of Personal Information and taking into account the nature of the processing and information available to PayU.

11.2 Furthermore, PayU shall take reasonable steps to make available to the Merchant all information reasonably necessary to demonstrate compliance with the obligations laid down in this DPA.

12. AUDITS

12.1 PayU shall notify the Merchant without undue delay any legally binding request for disclosure of Personal Information by a supervisory authority or a law enforcement authority, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

12.2 Upon written request by the Merchant, PayU shall make available to the Merchant all information reasonablynecessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections in the Processor's premises, conducted by the Merchant or another auditor mandated by the Merchant. PayU shall be notified at least 30 days before any planned inspection or audit. Such audits shall be performed during normal business hours and in a way that does not interfere with normal business activities of PayU, which includes Personal Information Processing by PayU for itself or on behalf ofany other PayU's customers.

12.3 Any audits and inspections described above can relate to the Processing provided under this DPA and PayU may refuse to disclose the Merchant

confidential information which must be protected by PayU according to relevant and applicable legal obligations.

12.4 PayU shall be authorized toreceive from the Merchant reimbursements of reasonable and documented costs incurred in connection to the audit and/or inspection more than once a year unless theaudit has been initiated by a relevant supervisory authority or if it is in connectionwith a Data Security Breach.

13 DELETION or RETURN

13.1. PayU, at the choice of the Merchant, will delete or return all the Personal Information to the Merchant/PayU after the termination of this GDPA or the Principal Agreement and will delete or return existing copies within 30 days, unless Applicable Data Protection Law requires the retention of the Personal Information by PayU in which case, PayU orthe applicable PayU Provider (as the case may be) will preserve it for the time required under Applicable Law.

14 SUB-PROCESSING

14.1 The Merchant gives a general authorization to PayU to engage sub-processors for the provision of the services. PayU guarantees that it has contracted subprocessors in accordance with the Applicable Law and that at the time of signing the Merchant Agreement they are located in a country that offers an adequate level of protection. In any other scenario, PayUwill ensure that:

a) each sub-processor is contractually bound by substantially the same provisions with respect to the Processing as those which PayU is bound to under this DPA,

b) PayU will remain fully liable for all obligations subcontracted to, and allacts and omissions of the sub- processor.

14.2 PayU shall notify the Merchant regarding engaging any new sub-processor, in case that notification is required by the Applicable Law. If the Merchant has a reasonable objection to any new sub-processor, it shall notify PayU of such objection in writing. Within thirty (30) days after receipt of such notification by PayU, the parties will seek to resolve the matter in good faith. If PayUrequires the use of the sub-processor and isunable to satisfy the Merchant as to: (a) the suitability of the sub-processor according to the requirements established by the competent data privacy authority related to the services or the location of a relevant sub-processor or (b) the documentation and protections in place between PayU and the sub-processor, within sixty (60) days from the date of the Merchant's written objection, the Parties may terminate the Services under the Principal Agreement requiring the use of the relevant sub-processor.

14.3 Notwithstanding the above, the Merchant authorizes PayU to use the sub- processors listed in Exhibit A of this DPA, which can be modified from time to time depending on the service requirements.

15 LIABILITY

15.1 The liability of PayU for any breach of this DPA shall be subject to the limitations of liability provisions included in the Principal Agreement.

16 APPLICABLE LAW

16.1 This DPA and any non-contractual obligations arising out of or in connection with it are governed by the applicable Law set forth in the Principal Agreement.

16.2 The courts established in the Principal Agreementhave exclusive jurisdiction to settle any dispute arising out of or in connection with this Agreement (including a dispute relating to the existence, validity or termination of this Agreement or the consequences of its nullity or any non-contractual obligations arising out of or in connection with this Agreement) (a "**Dispute**")

17 MODIFICATION OF THIS AGREEMENT

17.1 This DPA may only be modified by a written amendment signed by each of the Parties.

18 TERM AND TERMINATION

18.1 The Parties agree that this DPA is terminated upon the termination of the Principal Agreement. This DPA shall remain valid for the duration of the Principal Agreement, starting from the date of signing of bothParties (Effective Date) and may be terminated by either Party giving notice pursuant to the Principal Agreement.

19 INVALIDITY AND SEVERABILITY

19.1 If any provision of this DPA is found by any court or administrativebody of a competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full forceand effect.

EXHIBIT A

AUTHORIZED THIRD PARTY SUB-PROCESSORS

Name of Sub-processor	Full address of the Sub-processor	Processing activities	Location of processing of Personal Information
Rackspace International GmbH	Rackspace Technology. 1 Fanatical Pl. City of Windcrest San Antonio, TX 78218	PayU Latam use Rackspace as Data center provider. Hosted all infrastructure, networking and storage devices.	Infrastructure operator for processing payments databases on physical servers. Operating system and data managed by PayU
Amazon	400 9th Ave N, Seattle, WA 98109	Amazon web services (AWS) is a Cloud computing provider. PayU Latam has accounts for transactional and non transactional activities.	Infrastructure operator for processing payments databases on physical servers. Operating system and data managed by PayU.
Feedzai, Inc.	registered offices at 1875 S. Grant St. #950, San Mateo, CA 94402, USA.	Feedzai's Risk Management Cloud Platform. Monitor all payment request in real time. Prevent even the most complex fraud situations with precision and adaptability.	Location of processing hosted in EU (use of data centres in the Ireland)
Salesforce	village 9, floor 26 Salesforce Tower, 110 Bishopsgate, London, UK, EC2N 4AY.	PayU Latam cloud tool for C.R.M processing merchant requests and payers requirements. Salesforce provides C.RM.	Processing in the United Kingdom, UK

Aldeamo	-	PayU Latam main merchant and payer notification tool. Aldeamo enhances PayU Latam notification and communication solutions,	EE.UU.
Mandrill by Mailchimp	Atlanta, Georgia, United States	Transacctional mail provider, used in PayU as a Backup from Sparkpost. PayU Latam backup merchant and payer notification tool. SendGrid is an email delivery with HTTP rest integration for notification in real time.	EE.UU
Snowflake, Inc	450 Concar Drive San Mateo, CA 94402, USA, utilising AWS servers located in Germany	PayU Global stora service. Snowflake is a cloud computing-based data storage.	E.U. Processing is in AWS servers located in EU
Tableau	1621 N 34th St. Seattle, WA	PayU Global main data visualisation Tool. Tableau Software is an interactive data visualization software company focused on business intelligence	EE.UU
Akamai Technologics, inc.	145 Broadway Cambridge, Massachusetts (MA) 02142	PayU Global tool for protection and cloud storage services. Akamai is a corporation that provides distributed computing platform for global Internet content delivery and application delivery.	Akamai has multiple location, they have point of presence in every country that PayU has operation, it's part of it key advantages
Sparkpost, Inc	9160 Guilford Road in Columbia, Md	Transacctional mail provider. SparkPost is an email sender service. It is PayU Latam main merchant and payer notification tool.	They use the Amazon cloud in the USA

EXHIBIT B

DATA SECURITY

1. Organizational Security Measures.

1.1 **Point of Contact**. PayU shall appoint a representative to act as a point of contact for Merchant with respect to this Data Security exhibit. The representative shall be responsible for ensuring PayU's compliance with this Data Security exhibit.

1.2 **Security Program**. PayU has developed and implemented, and will consistently update and maintain as needed a written and comprehensive information security program in compliance with applicable laws, rules, regulations and industry standards and reasonable policies and procedures designed to detect, prevent, and mitigate the risk of data security breaches or identify theft ("Security Program"). Specifically, such Security Program shall include, at a minimum and in addition to the items contained below:

(a) a data loss prevention program, with appropriate policies and/or technological controls designed to prevent loss of Personal Information;

(b) a disaster recovery/business continuity plan that addresses ongoing access, maintenance and storage of Personal Information as well as security needs for back-up sites and alternate communication networks;

(c) secure transmission and storage of Personal Information;

(d) personnel security and integrity, including background checks where consistent with Applicable Data Protection Laws and other Applicable Law;

(e) annual training to PayU's employees involved in the processing of Personal Information on how to comply with PayU's physical, technical, and administrative information security safeguards and confidentiality obligations under applicable laws, rules, regulations and guidelines;

(f) authentication and access control mechanisms over Personal Information, media, applications, operating systems and equipment; and

(g) data retention and destruction procedures in accordance with Applicable Law.

1.3 **Training**. PayU shall provide appropriate training to its personnel to ensure theirtreatment of the Personal Information is in accordance with the Agreement, including this DPA. Such training shall be consistent with industry best practices.

1.4 **Access**. PayU shall limit disclosure of and access to Personal Information to

only those personnel who have a business need to access such Personal Information in order to provide the Services to Merchant and/or to fulfil the purposes of the Agreement. PayU shall establish, maintain, and enforce the security principles of "segregation of duties" and "least privileged access" with respect to all Personal Information. PayU shall reasonably update all access rights based on personnel or computer systemchanges, and shall periodically review all access rights at an appropriate frequency to ensure current access rights to Personal Information are appropriate and no greater than are required for an individual to perform hisor her functions necessary to deliver the Services to Merchant and/or to fulfil the purposes of the Agreement. PayU shall verify all access rights through effective authentication methods.

2. Physical and Technical Security Measures.

2.1 **Data Segregation**. PayU shall not merge or combine Personal Information with any other data set. PayU shall maintain Personal Information in Merchant segregated logical access restricted folders or systems throughout the processing of such data.

2.2 **Network Configuration, Access Control and Limiting Remote Access.** PayU shall secure its computer networks by using and maintaining appropriate firewall and security screening technology that is designed to prevent unauthorized access. PayU ensures that the following network security controls are in place: (a) firewall platforms are hardened and have real time logging and alerting capabilities, (b) intrusion detection and prevention systems are in place and maintained at the perimeter and critical server systems, (c) access lists are implemented on network routers to restrict access to sensitive internal networks or servers, (d) remote access requires two factor authentication and occurs over an encrypted tunnel e.g. IPSec, SSL-VPN, and (e) systems servicing Merchant are segregated from other network zones logically and physically including DMZ, production databases, back office, and software development areas. PayU shall secure access to and from its systems by disabling remote communications at the operating system level if no business need exists and/or by tightly controlling access through management approvals, robust controls, logging, and monitoring access events and subsequent audits. PayU shall identify computer systems and applications that warrant security event monitoring and logging, and reasonably maintain and analyse log files. PayU ensures that privileged accounts (administrator, super user, etc.) will be controlled and reviewed on at least an annual basis. PayU enforces a process to control and manage user accounts upon termination of employment or change in role within 24 hours or as soon as practicable possible from such termination or change.

2.3 **Labeling**. PayU shall, to the extent possible, limit the appearance of Personal Information on physical media, including paper documents. PayU shall control and protect access to such media to avoid loss or damage. PayU shall ensure safe and secure storage, transfer, exchange, and disposal of such media. If Personal Information is stored on media off-site for back-up purposes, such media shall not include any visible label identifying or listing Merchant's name (or the name of any Merchant affiliate).

2.4 **Encryption**. PayU shall encrypt all Personal Information in its possession, custody or control while in transit or at rest. For the avoidance of doubt, "encryption" shall be deployed using PGP or other industry best practice for key based encryption protocol. PayU shall have in place appropriate technology to receive, store, and transmit the sensitive Personal Information in an encrypted format in order to provide the Services.

2.5 **Third-Party Data Centers**. Where applicable, PayU using a third party data center to host the Services shall ensure that (a) all application and database servers are physically isolated within the data center and secured from unauthorized physical access; (b) physical and network access is limited to PayU's personnel or approved subcontractor; (c) Personal Information remains logically segregated from other data stored in any shared environment at all times and that use of any shared environment does not compromise the security, integrity, or confidentiality of Personal Information.

2.6 **Security Patches**. PayU shall deploy all applicable and necessary system security patches to all software and systems that process, store, or otherwise support the Services, including operating system, application software, database software, web server software within industry best practices and in accordance with its information security policies.

2.7 **Virus/Malware Scanning.** PayU shall use commercial virus/malware scanning software on systems used by PayU to collect, use, disclose, store, retain or otherwise process Personal Information. For purposes of this agreement, "virus/malware" refers to any programming routines intended to damage, surreptitiously intercept or expropriate any system data or personal information. PayU shall run up-to-date industry standard anti-virus software and software that identifies malicious code on all PayU systems that contain Personal Information, including scanning all email attachments for malicious code. PayU shall use commercially reasonable efforts to protect its own information technology against malicious code and ensure that its connection to the Internet and for any other platform or network running the Services is secure, and shall in accordance with industry standards and its own information security practices, acquire and implement new technology, including monitoring hardware and software, as the technology becomes available and is proven stable, in PayU's reasonable discretion, to ensure a secure and stable environment.

2.8 **Vulnerability Testing**. Prior to providing any code, hosting services, or network connectivity to Merchant, PayU must perform and be able to show proof that external penetration testing has been completed and that any reported vulnerabilities have been remediated. For software, this includes tests for security vulnerabilities that are a part of the OWASP Top 10 or SANs Top 25. PayU will promptly address and correct all security vulnerabilities identified in a vulnerability test or report.

2.9 **Life Cycle Development**. PayU shall implement and maintain a secure software development life cycle for all applications which integrate with Merchant's environment or are developed on Merchant's behalf. PayU will observe all industry standard application security guidelines, such as

the Open Web Application Security Project (OWASP). PayU will ensure that:

(a) regular reviews of application source code occur;

(b) developers receive detailed coding and design training in application security;

(c) development, testing, production and operational facilities are separated to reduce the risk of unauthorized access or changes to the production and operational systems and Personal Information;

(d) software developers are restricted from accessing production environment; and

(e) data masking functionality is implemented in relation to software processing any financial-related Personal Information (including payment card and banking information).

2.10 **System Change Control**. PayU ensures that change control procedures are documented and maintained and detail why the change was required, how and why changes were executed andinclude an emergency change process. The change control process includes considering security control requirements, implementing them where necessary and testing these changes prior to implementation. PayU will notify Merchant of any upgrades or configuration changes which may impact the security of Personal Information.

2.11 **PCI DSS Compliance**. Where PayU provides financial transactional functionality as part of the Services to Merchant, PayU confirms it, and any third party that may perform such functions on its behalf, complies with the latest version of the PCI DSS requirements and will provide such evidence of compliance as required by Merchant upon Merchant's request and that it will maintain such certification until termination of this agreement.

2.12 **Non-Compliance**. PayU will not materially lessen the security of any system used to collect, use, disclose, store, retain or otherwise process Personal Information during the term of the Agreement. In the event that PayU determines it is unable to comply with the obligations stated in the Agreement or this Data Security exhibit, PayU shall promptly notify Merchant, and the Merchant shall be entitled to take such action as is stated in the DPA.