

Data Protection (Customer Data)

Data Protection Terms and EU Standard Contractual Clauses are set out in the EU Personal Data Standard Contractual Clauses Addendum and are hereby incorporated by reference into this Agreement.

EU PERSONAL DATA STANDARD CONTRACTUAL CLAUSES ADDENDUM

This EU Personal Data Standard Contractual Clauses Addendum (“**Addendum**”) is entered into between the entity identified as the “merchant” on the signature page to the Payment Services Agreement or whose details have been input as part of the online registration process (“**Merchant**”) and PayPal (Europe) S.á.r.l. et Cie, S.C.A. (“**Braintree**”) (collectively the “**Parties**”). This Addendum shall form part of the Payment Services Agreement between Merchant and PayPal (the “**Agreement**”) in accordance with the Execution of this Addendum section below.

PayPal, Inc., a Delaware corporation with offices located at 2211 North First Street, San Jose, CA 95131 (“**PayPal**”) is a party to the EU Standard Contractual Clauses as set out below.

Capitalized terms used but not defined in this Addendum shall have the meaning set out in the Agreement.

WHEREAS:

- (A) Braintree is established and located in the European Economic Area.
- (B) Braintree’s parent company PayPal and its subcontractors are located in the USA and certain other countries outside the European Economic Area.
- (C) The European Economic Area and Switzerland restrict the transfer of personal data to certain other jurisdictions, including the USA.
- (D) In order to assist Merchants established in the European Economic Area or Switzerland to transfer personal data to Braintree and Braintree’s parent company PayPal and its subcontractors in the provision of the Services, Braintree agrees to enter into this Addendum on the terms set out herein and PayPal agrees to enter into the EU Standard Contractual Clauses on the terms set out herein.

EXECUTION OF THIS ADDENDUM

This Addendum amends and forms part of your Payments Services Agreement. The Addendum has been electronically pre-executed for and on behalf of Braintree and the EU Standard Contractual Clauses at Attachment 1 has been electronically pre-executed for and on behalf of PayPal through the application of Braintree’s e-signature to the Addendum and PayPal’s e-signature to the EU Standard Contractual Clauses. Both documents will only come into effect as set out below.

Automatic execution option

Provided that Merchant is a party to an executed and effective Payment Services Agreement with Braintree, this Addendum shall take effect, as between Braintree and that Merchant only, and the EU Standard Contractual Clauses shall take effect, as between PayPal and that Merchant only:

for Merchants who have entered into a Payments Services Agreement on or after 18 April 2016,

automatically on execution of the Payment Services Agreement (and the name, address and contact details that Merchant provided when entering into the Payment Services Agreement shall be deemed to be inserted into the data exporter section on page 30 of the Addendum and Merchant to have signed as Merchant on page 29 and as data exporter on pages 36 and 38 of the Addendum); and for Merchants who entered into a Payments Services Agreement before 18 April 2016 in accordance with Section 9.05 (Amendments) of the Payments Services Agreement (and the name, address and contact details that Merchant provided when entering into the Payment Services Agreement shall be deemed to be inserted into the data exporter section on page 30 of the Addendum and Merchant to have signed as Merchant on page 29 and as data exporter on pages 36 and 38 of the Addendum), or (if earlier) on the date that Merchant completes the physical execution actions set out below:

Physical execution option (Merchant may require this option for the purposes of obtaining prior approval of transfers from Merchant's local data protection authority)

Notwithstanding the foregoing, provided Merchant is a party to an executed and effective Payment Services Agreement with Braintree, this Addendum shall take effect, as between Braintree and that Merchant only, and the EU Standard Contractual Clauses shall take effect, as between PayPal and that Merchant only upon completion of the following steps:

(i) Merchant to complete the information relating to the Data Exporter and execute the signature page at pages 29 and 30;

(ii) Merchant to complete and execute the signature pages at pages 36 and 38; and

(iii) Merchant to submit the completed and fully executed Addendum to Braintree and send it to our Data Protection Officer at **PayPal (Europe) S.à.r.l. et Cie, S.C.A., 22-24 Boulevard Royal L-2449, Luxembourg** with a copy via email to dataprivacy@braintreepayments.com

1 DEFINITIONS AND INTERPRETATION

- 1.1 The following terms have the following meanings when used in this Addendum:

“Customer” means a customer of Merchant who uses the Braintree Payment Services and for the purposes of this Agreement, is a data subject.

“Customer Data” means the personal data that the Customer provides to Merchant and Merchant passes on to Braintree through the use by the Customer of the Braintree Payment Services

“data controller” (or simply **“controller”** and **“data processor”** (or simply **“processor”**) and **“data subject”** have the meanings given to those terms under the Data Protection Laws.

“Data Exporter” means Merchant

“Data Importer” means PayPal

"Data Protection Laws" means:

- (i) prior to 25 May 2018, EU Directive 95/46/EC;
- (ii) from 25 May 2018, the General Data Protection Regulation (EU 2016/679) (GDPR) and any other applicable law; and
- (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003, together with any other applicable legislation.

"EU Standard Contractual Clauses" means the agreement executed by and between Merchant and PayPal and attached hereto as Attachment 1 pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

"Merchant Data" means any personal data relating to business contact details of Merchant or its employees, officers or contractors provided to or obtained by Braintree in the provision of the Braintree Payment Services

"PayPal Group" means PayPal and all companies in which PayPal or its successor directly or indirectly from time to time owns or controls.

"personal data" has the meaning given to it in the Data Protection Laws.

"processing" has the meaning given to it in the Data Protection Laws and **"process"**, **"processes"** and **"processed"** will be interpreted accordingly.

"Security Incident" means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Braintree.

"Services" means the "Braintree Payment Services" as defined in the Agreement.

"Sub-processor" means any processor engaged by PayPal and/or its affiliates in the processing of personal data

1.2 Addendum. This Addendum comprises: (i) paragraphs 1 to 5, being the main body of the Addendum; and (ii) Attachment 1 (EU Standard Contractual Clauses).

1.3 Conflict. If and to the extent that there is any inconsistency between this Addendum and the EU Standard Contractual Clauses in Attachment 1, the EU Standard Contractual Clauses shall prevail.

2 PROCESSING OF PERSONAL DATA IN CONNECTION WITH THE SERVICES

2.1 Braintree is the controller in respect of Merchant Data and may use it for the following purposes:

2.1.1 as reasonably necessary to provide the Services to Merchant and its Customer;

2.1.2 to conduct anti-money laundering, know your customer and fraud checks on the Merchant;

2.1.3 to market to the employees and contractors of Merchant; and

2.1.4 any other purpose that it notifies (or Merchant agrees to notify on its behalf) to the employees and contractors of Merchant in accordance with Data Protection Laws.

2.2 Braintree shall comply with the requirements of the Data Protection Laws applicable to controllers in respect of the use of Merchant Data under this Agreement (including without limitation, by implementing and maintaining at all times all appropriate security measures in relation to the processing of Merchant Data and by maintaining a record of all processing activities carried out in respect of Merchant Data) and shall not knowingly do anything or permit anything to be done with respect to the Merchant Data which might lead to a breach by the Merchant of the Data Protection Laws.

2.3 With regard to any Customer Data to be processed by Braintree in connection with this Agreement, Merchant will be a controller and Braintree will be a processor in respect of such processing. Merchant will be solely responsible for determining the purposes for which and the manner in which Customer Data are, or are to be, processed.

2.4. Braintree shall only process Customer Data on behalf of and in accordance with Merchant's written instructions. The Parties agree that this Addendum is Merchant's complete and final written instruction to Braintree in relation to Customer Data. Additional instructions outside the scope of this Addendum (if any) require prior written agreement between Braintree and Merchant, including agreement of any additional fees payable by Merchant to Braintree for carrying out such additional instructions. Merchant shall ensure that its instructions comply with all applicable laws, including Data Protection Laws, and that the processing of Customer Data in accordance with Merchant's instructions will not cause Braintree to be in breach of Data Protection Laws. Merchant hereby instructs Braintree to process Customer Data for the following purposes:

2.4.1 as reasonably necessary to provide the Services to Merchant and its Customer;

2.4.2 after anonymising the Customer Data, to use that anonymised Customer Data directly or indirectly, which is no longer identifiable personal data, for any purpose whatsoever.

2.5 In relation to Customer Data processed by Braintree under this Agreement, Braintree shall co-operate with Merchant to the extent reasonably necessary to enable Merchant to adequately discharge its responsibility as a controller under Data Protection Laws, including without limitation that Braintree shall cooperate and provide Merchant with such reasonable assistance as Merchant requires in relation to:

2.5.1. assisting Merchant in the preparation of data protection impact assessments to the extent required of Merchant under Data Protection Laws; and

2.5.2 responding to binding requests for the disclosure of information as required by local laws, provided always that where the request is from a non-EEA law enforcement agency Braintree will (a) inform Merchant of the request, the data concerned, response time, the identity of the requesting body and the legal basis for the request; (b) wait for Merchant's instructions provided the instruction and the opinion are received within a reasonable period of time, which shall be assessed in light of the time period afforded by the law enforcement agency to Braintree; (c) where Braintree is prohibited from informing Merchant about the law enforcement agency's request, take reasonable steps to have this prohibition waived and to make available relevant information about the request as soon as possible to Merchant (these efforts will be documented); and (d) where the prohibition cannot be waived, compile a list, in compliance with its national law and on an annual basis, of the number of such requests received, the type of Customer Data requested and the identity of the law enforcement agency concerned and make it available to the Customer's data protection authority annually on request (in which circumstances Braintree will be acting as a controller).

2.6 Scope and Details of Customer Data processed by Braintree. The objective of processing Customer Data by Braintree is the performance of the Services pursuant to the Agreement. Braintree shall process Customer Data in accordance with the specific duration, purpose, type and categories of data subjects as set out in Attachment 3 (*Data Processing of Customer Data*).

2.7 Merchant undertakes to provide all notices and obtain all consents necessary for Braintree's use of Merchant Data and Customer Data set out above.

2.8 The Parties will at all times comply with Data Protection Laws.

3 DATA PROCESSOR TERMS

This paragraph 3 applies only to the extent that Braintree acts as a processor or Sub-processor to Merchant. It does not apply where Braintree acts as a controller.**3.1 Correction, Blocking and Deletion.** To the extent Merchant, in its use of the Services, does not have the ability to correct, amend, block or delete Customer Data, as required by Data Protection Laws, Braintree shall comply with any commercially reasonable request by Merchant to facilitate such actions to the extent Braintree is legally permitted to do so. To the extent legally permitted, Merchant shall be responsible for any costs arising from Braintree's provision of such assistance.

3.2 Data Subject Requests. Braintree shall, to the extent legally permitted, promptly notify Merchant if it receives a request from a Customer for access to, correction, amendment or deletion of that Customer's personal data. Braintree shall not respond to any such Customer Data Subject request without Merchant's prior written consent except to confirm that the request relates to Merchant to which Merchant hereby agrees. Braintree shall provide Merchant with commercially reasonable cooperation and assistance in relation to handling of a Customer's request for access to that person's personal data, to the extent legally permitted and to the extent Merchant does not have access to such Customer Data through its use of the Services. If legally permitted, Merchant shall be responsible for any costs arising from Braintree's provision of such assistance.

3.3 Confidentiality. Braintree shall ensure that its personnel engaged in the processing of Customer Data are informed of the confidential nature of the Customer Data, have received

appropriate training on their responsibilities and have executed written confidentiality agreements. Braintree shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

3.4 Training. Braintree undertakes to provide training as necessary from time to time to the Braintree personnel with respect to Braintree's obligations in this Addendum to ensure that the Braintree personnel are aware of and comply with such obligations.

3.5 Limitation of Access. Braintree shall ensure that access by Braintree's personnel to Customer Data is limited to those personnel performing Services in accordance with the Agreement.

3.6 Data Protection Officer. Members of the PayPal Group have appointed a data protection officer where such appointment is required by Data Protection Laws. The appointed person may be reached at **PayPal (Europe) S.à.r.l. et Cie, S.C.A., 22-24 Boulevard Royal L-2449, Luxembourg.**

3.7 Sub-processors. Merchant specifically authorizes the engagement of members of the PayPal Group as Sub-processors in connection with the provision of the Services. In addition, Merchant generally authorises the engagement of any other third parties as Sub-processors in connection with the provision of the Services. When engaging any Sub-processor, Braintree will execute a written contract with the Sub-processor which contains terms for the protection of Customer Data which are no less protective than the terms set out in this Addendum.

3.7.1 List of Current Sub-processors and Notification of New Sub-processors. Braintree shall make available to Merchant a current list of Sub-processors for the respective Services with the identities of those Sub-processors ("**Sub-processor List**"). The Sub-processor List is included in Attachment 2 to this Addendum. Where a Sub-processor is proposed to be changed Braintree shall provide prior notice by email to Merchant before implementing such change

3.7.2 Objection Right for new Sub-processors. If Merchant has a reasonable basis to object to Braintree's use of a new Sub-processor, Merchant shall notify Braintree promptly in writing within two (2) months after receipt of Braintree's notice. In the event Merchant objects to a new Sub-processor(s) and that objection is not unreasonable Braintree will use reasonable efforts to make available to Merchant a change in the affected Services or recommend a commercially reasonable change to Merchant's configuration or use of the affected Services to avoid processing of personal data by the objected-to new Sub-processor without unreasonably burdening Merchant. If Braintree is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Merchant may terminate the Agreement in respect only of those Services which cannot be provided by Braintree without the use of the objected-to new Sub-processor, by providing no less than sixty (60) days' written notice to Braintree. Merchant shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

3.8 Audits and Certifications. Where requested by Merchant, subject to the confidentiality obligations set forth in the Agreement, Braintree shall make available to Merchant (or Merchant's independent, third-party auditor that is not a competitor of Braintree or any member of PayPal or the Paypal Group) information regarding Braintree's compliance with the obligations set forth in this Addendum in the form of the third-party certifications and audits (if any) set forth in the Privacy Policy set out on our website. Merchant may contact Braintree in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of personal data. Merchant shall reimburse Braintree for any time expended for any such on-site audit at Braintree's then-current professional services rates, which shall be made available to Merchant upon request. Before the commencement of any such on-site audit, Merchant and Braintree shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Merchant shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Braintree. Merchant shall promptly notify Braintree with information regarding any non-compliance discovered during the course of an audit.

3.9 Security. Braintree shall, as a minimum, implement and maintain appropriate technical and organizational measures as described in Attachment 1, Appendix 2 of the Addendum to keep Customer Data secure and protect it against unauthorised or unlawful processing and accidental loss, destruction or damage in relations to the provision of the Services. Since Braintree provides the Services to all Merchants uniformly via a hosted, web-based application, all appropriate and then-current technical and organisational measures apply to Braintree's entire customer base hosted out of the same data centre and subscribed to the same service. Merchant understands and agrees that the technical and organizational measures are subject to technical progress and development. In that regard, Braintree is expressly permitted to implement adequate alternative measures as long as the security level of the measures is maintained in relation to the provision of the Services. In the event of any detrimental change Braintree shall provide a notification together with any necessary documentation to Merchant by email or publication on a website easily accessible by Merchant.

3.10 Data Transfers. Merchant agrees that Braintree may, subject to paragraph 4 (EU Standard Contractual Clauses Related Terms), store and process Customer Data in the United States of America and any other country in which Braintree or any of its Sub-processors maintains facilities.

3.11 Security Incident Notification. If Braintree becomes aware of a Security Incident in connection with the processing of Customer Data, Braintree will: (a) notify Merchant of the Security Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimise harm and secure Customer Data.

3.12 Details of Security Incident. Notifications made under paragraph 3.11 (Security Incident Notification) will describe, to the extent possible, reasonable details of the Security Incident, including steps taken to mitigate the potential risks.

3.13 Communication. Braintree will deliver its notification of any Security Incident to one or more of Merchant's administrators by any means Braintree selects, including via email.

Merchant is solely responsible for maintaining accurate contact information and ensuring that any contact information is current and valid.

3.14 Deletion. Upon termination or expiry of the Agreement, Braintree will delete or return to Merchant all Customer Data processed on behalf of the Merchant, and Braintree shall delete existing copies of such Customer Data except where necessary to retain such Customer Data strictly for the purposes of compliance with applicable law.

3.14 Data Portability. Upon any termination or expiry of this Agreement, Braintree agrees, upon written request from Merchant, to provide Merchant's new acquirer or payment service provider ("Data Recipient"), as applicable, with any available credit card information (including personal data) relating to Merchant's Customers, subject to the following conditions: (i) Merchant must provide Braintree with proof that the Data Recipient is in compliance with the Association PCI-DSS Requirements (level 1 PCI compliant) by giving Braintree a certificate or report on compliance with the Association PCI-DSS Requirements from a qualified provider and any other information reasonably requested by Braintree; (ii) the transfer of such information is compliant with the latest version of the Association PCI-DSS Requirements; and (iii) the transfer of such information is allowed under the applicable card association rules, and any applicable laws, rules or regulations (including Data Protection Laws).

4 EU STANDARD CONTRACTUAL CLAUSES RELATED TERMS

4.1 Application. The EU Standard Contractual Clauses are set out in Attachment 1 (the "EU Standard Contractual Clauses"). The EU Standard Contractual Clauses apply only to Customer Data that is transferred by Merchants established in the European Economic Area ("EEA") or Switzerland to any country outside the EEA that is not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR) in which Braintree may store and process Customer Data..

4.2 Instructions. This Addendum and the Agreement are Data Exporter's complete and final instructions to Data Importer for the processing of Customer Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the EU Standard Contractual Clauses, the Data Exporter gives the following instructions: (a) to process Customer Data in accordance with the Agreement; and (b) to process Customer Data initiated by Merchants in their use of the Services during the Term. These instructions also describe the duration, object, scope and purpose of the processing.

4.3 Sub-processors. Pursuant to Clause 5(h) of the EU Standard Contractual Clauses, the Data Exporter acknowledges and expressly agrees that the provisions of paragraph 3.7 of this Addendum shall also apply to the Data Importer as if it were Braintree.

4.3.1 The Parties agree that the copies of the sub-processor agreements that must be sent by the Data Importer to the Data Exporter pursuant to Clause 5(j) of the EU Standard Contractual Clauses may have all commercial information, or clauses unrelated to the EU Standard Contractual Clauses or their equivalent, removed by the Data Importer beforehand;

and, that such copies will be provided by Data Importer only upon reasonable request by Data Exporter.

4.4 Audits and Certifications. The Parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the EU Standard Contractual Clauses shall be fulfilled in the following manner: the provisions of paragraph 3.8 of this Addendum shall also apply to the Data Importer as if it were Braintree.

4.5 Certification of Deletion. The Parties agree that the certification of deletion of personal data that is described in Clause 12(1) shall be provided by the Data Importer to the Data Exporter only upon Data Exporter’s request.

4.6 Liability. The Parties agree that all liabilities between them (and in respect of PayPal, such liabilities shall be aggregated with those of Braintree so that collectively their cumulative joint liability is capped at the level set out in the Agreement) under this Addendum and the EU Standard Contractual Clauses will be subject to the terms of the Agreement (including as to limitation of liability), except that such limitations of liability will not apply to any liability that PayPal may have to data subjects under the third party rights provisions of the EU Standard Contractual Clauses.

4.7 Exclusion of third party rights. Subject to paragraph 4.6, PayPal shall be granted third party rights in relation to obligations expressed to be for the benefit of the Data Importer or PayPal in this Addendum and Data Subjects are granted third party rights under the EU Standard Clauses. All other third party rights are excluded.

5 LEGAL EFFECT

This Addendum shall take effect between, and become legally binding on the Parties and the EU Standard Contractual Clauses shall take effect between, and become legally binding between PayPal and Merchant, on the date determined by “Execution of this Addendum” section above.

Merchant

For and on behalf of (insert Merchant legal name).....

Signature.....

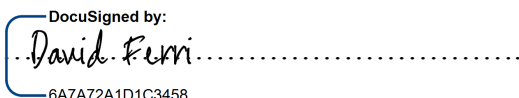
Name of signatory.....

Title of signatory.....

Date.....

Braintree

For and on behalf of PayPal (Europe) S.á.r.l. et Cie, S.C.A.

Signature... .....
6A7A72A1D1C3458...

Name of signatory..... David Ferri

Title of signatory..... Authorised Manager

Date..... March 8, 2018

ATTACHMENT 1

STANDARD CONTRACTUAL CLAUSES

Controller to Processor export of personal data (from EEA countries)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.:

fax:

e-mail:

Other information needed to identify the organisation: (the data exporter)

And

Name of the data importing organisation: Paypal, Inc

Address: 2211 North First Street, San Jose, CA 95131

Other information needed to identify the organisation: (the data importer)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.



Clause 1

Definitions

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) 'the data exporter' means the controller who transfers the personal data;
- (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by

- operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
 4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in

accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the

security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):


Signature.....(stamp of organisation)

On behalf of the data importer (Paypal, Inc):

Name (written out in full): Juan Benetiz

Position: GM Braintree

Address: 2211 North First Street, San Jose, CA 95131

Signature.....(stamp of organisation)


APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is: Merchant

An entity that uses the Data importer's services in respect of its Customers

Data importer

The data importer is: Paypal, Inc

A payment services provider which in relation to the Braintree services provides a payment gateway so that Merchant can provide Customer credit card and other details to banks and other payment service providers to process payments from Customers

Data subjects

The personal data transferred concern the following categories of data subjects:

The data exporter's Customers

Categories of data

The personal data transferred concern the following categories of data:

Customer name, amount to be charged, card number, CSV, post code, country code, address, email address, fax, phone, website, expiry date, shipping details, tax status

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Not applicable, unless Merchant configures the service to capture such data.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

The receipt and storage of Personal Data in the performance of the Services during the Term of the Agreement.

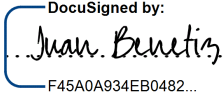
DATA EXPORTER

Name:

Authorised Signature

DATA IMPORTER

Name: Juan Benetiz

Authorised Signature 

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The following technical and organizational measures will be implemented:

1. Measures taken to prevent any unauthorised person from accessing the facilities used for data processing (e.g. secured access, badges);
2. Measures taken to prevent data media from being read, copied, amended or moved by any unauthorised persons(e.g. data kept in locked premises);
3. Measures taken to prevent the unauthorised introduction of any data into the information system, as well as any unauthorised knowledge, amendment or deletion of the recorded data (e.g. restricted access to the IT infrastructure);
4. Measures taken to prevent data processing systems from being used by unauthorised person using data transmission facilities (e.g. firewalls);
5. Measures taken to guarantee that authorised persons when using an automated data processing system may access only data that are within their competence (e.g. specific users accounts);
6. Measures taken to guarantee the checking and recording of the identity of third parties to whom the data can be transmitted by transmission facilities (e.g. VPN, encryption of data);

7. Measures taken to guarantee that the identity of the persons having had access to the information system and the data introduced into the system can be checked and recorded ex post facto at any time and by any authorised person ;
8. Measures taken to prevent data from being read, copied, amended or deleted in an unauthorised manner when data are disclosed and data media transported;
9. Measures taken to safeguard data by creating backup copies (encryption of data back-ups).

ATTACHMENT 2

Sub-processor List

1. **Century Link: 100 CenturyTel Drive, Monroe, LA 71203**
2. **Kount Inc: 71203917 South Lusk, 3rd Floor, Boise, ID 83706**
3. **Amazon Web Services, Inc.: 410 Terry Avenue North Seattle, WA 98109-5210**

ATTACHMENT 3

Data Processing of Customer Data

Subject-matter of the processing

The payment processing services offered by Braintree which provides Merchant with the ability to accept credit cards, debit cards, and other payment methods on a website or mobile application from Customers.

Nature and purpose of the processing

Braintree processes Customer Data that is sent by the Merchant to Braintree for purposes of obtaining verification or authorization of the Customer's payment method as payment to the Merchant for the sale goods or services.

Type of personal data

Merchant shall inform Braintree of the type of Customer Data Braintree is required to process under this Agreement. Should there be any changes to the type of Customer Data Braintree is required to process then Merchant shall notify Braintree immediately.

Braintree processes the following Customer Data, as may be provided by the Merchant to Braintree from time to time:

| | |
|--|--------------------------|
| Full name | <input type="checkbox"/> |
| Date of birth | <input type="checkbox"/> |
| Home address | <input type="checkbox"/> |
| Shipping address | <input type="checkbox"/> |
| Work address | <input type="checkbox"/> |
| Billing address | <input type="checkbox"/> |
| Email address | <input type="checkbox"/> |
| Telephone number | <input type="checkbox"/> |
| Fax number | <input type="checkbox"/> |
| Government ID | <input type="checkbox"/> |
| Bank account number and bank routing number | <input type="checkbox"/> |
| Financial account number | <input type="checkbox"/> |
| Card or payment instrument type | <input type="checkbox"/> |
| Card Primary Account Number (PAN) or Device-specific Primary Account Number (DPAN) | <input type="checkbox"/> |
| Card Verification Value (CVV) | <input type="checkbox"/> |

| | |
|----------------------|--------------------------|
| Card expiration date | <input type="checkbox"/> |
| Username | <input type="checkbox"/> |
| IP address | <input type="checkbox"/> |
| Device ID | <input type="checkbox"/> |
| Browser data | <input type="checkbox"/> |
| Business TAX ID | <input type="checkbox"/> |

Special categories of data (if relevant)

The transfer of special categories of data is not anticipated.

Duration of Processing

The term of the Agreement.