

## **Section 2 — 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.

### **BRAINTREE PAYMENT SERVICES 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 15 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 23 of the Addendum and Merchant to have signed as Merchant on page 22 and as data exporter on pages 31 and 33 of the Addendum); and

for Merchants who entered into a Payments Services Agreement before 15 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 23 of the Addendum and Merchant to have signed as Merchant on page 22 and as data exporter on pages 31 and 33 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 22 and 23;
- (ii) Merchant to complete and execute the signature pages at pages 31 and 33; and
- (iii) Merchant to submit the completed and fully executed Addendum to Braintree at [dataprivacy@braintreepayments.com](mailto: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

**Customer Data** means the Personal Data that Merchant's Customer provides to Braintree through the use of the Braintree Payment Services

**Data Controller** means the entity which determines the purposes and means of the Processing of Personal Data

**Data Exporter** means Merchant

**Data Importer** means PayPal

**Data Processor** means the entity which processes Personal Data on behalf of the Data Controller

**Data Protection Requirements** means all laws and regulation, including laws and regulations of the European Union, the European Economic Area and their member states, applicable to the Processing of Personal Data

**Data Subject** means the individual to whom Personal Data relates

**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 Merchant or its employees, officers or contractors provided to or obtained by Braintree in the provision of the Braintree Payment Services

**Personal Data** means any information relating to an identified or identifiable person

**Processing** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

**Sub-processor** means any Data 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 BRAINTREE PAYMENT SERVICES**

2.1 Braintree is the Data 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 Requirements.
- 2.2 Braintree is Merchant's Data Processor in respect of Customer Data. Braintree shall only Process Customer Data on behalf of and in accordance with Merchant's instructions. Merchant hereby instructs Braintree to Process Customer Data for the following purposes:
  - 2.2.1 as reasonably necessary to provide the services Merchant and its Customer;
  - 2.2.2 after anonymising the Customer Data, to use that anonymised Customer Data for any purpose whatsoever; and
  - 2.2.3 as required to comply with applicable binding legal requirements by 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 Data Controller).
- 2.3 **Scope and Purpose; Categories of Personal Data and Data Subjects.** The objective of Processing Customer Data by Braintree is the performance of the Services pursuant to the Agreement. The types of Customer Data and categories of Data Subjects Processed under this Addendum are further specified in Attachment 1, Appendix 1 (Details of the Processing) to this Addendum.
- 2.4 Merchant undertakes to provide all notices and obtain all consents necessary for Braintree's use of Merchant Data and Customer Data set out above.
- 2.5 The Parties will at all times comply with Data Protection Requirements.

### 3 DATA PROCESSOR TERMS

This section 3 applies only to the extent that Braintree acts as Data Processor or Sub-processor to Merchant. It does not apply where Braintree acts as Data Controller.

## Data subject rights

- 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 Requirements, 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 Data Subject for access to, correction, amendment or deletion of that person'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 Data Subject'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.

## Braintree personnel

- 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 **Reliability.** Braintree shall take commercially reasonable steps to ensure the reliability of any Braintree personnel engaged in the Processing of Customer Data.
- 3.5 **Limitation of Access.** Braintree shall ensure that Braintree's access 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 Requirements. The appointed person may be reached at [dataprivacy@braintreepayments.com](mailto:dataprivacy@braintreepayments.com).
- 3.7 **Sub-processors.** Merchant acknowledges and expressly agrees that PayPal's affiliates may be retained as Sub-processors; and (b) Braintree, PayPal and PayPal's affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.
- 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 2 months' 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 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 Braintree Payment Services which cannot be provided by Braintree without the use of the objected-to new Sub-processor, by providing 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 Braintree Payment 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 PayPal) 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. Since Braintree provides the Braintree Payment Service to all customers 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 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 Braintree shall promptly inform Merchant as soon as it becomes aware of serious disruptions of the processing operations, reasonable suspected or actual data protection violations or any security breach in connection with the processing of Customer

Personal Data which, in each case, may significantly harm the interest of the Data Subjects concerned.

#### 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 Braintree.
- 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 Braintree Payment 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.....  
*Victoria Reaney*  
6A3563798E9B4B1...

Name of signatory.....  
Victoria Reaney

Title of signatory.....  
Victoria Reaney

Date.....  
4/13/2016

DocuSigned by:  
*David Ferri*  
6A7A72A1D1C3458...

David Ferri

Authorised Manager

4/13/2016



**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

E-mail: [dataprivacy@braintreepayments.com](mailto:dataprivacy@braintreepayments.com)

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): Peggy Abkemeier

Position: CFO Americas & Global Credit

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

Signature.....

DocuSigned by:  
*Peggy Abkemeier*

9C2DD4F208FD4A1...

(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**

Peggy Abkemeier

Name:.....

DocuSigned by:  
*Peggy Abkemeier*  
9C2DD4F2Q8FD4A1...

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 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: 917 South Lusk, 3rd Floor, Boise, ID 83706**
- 2. Kount Inc: 100 CenturyTel Drive, Monroe, LA 71203**

## Certificate Of Completion

Envelope Id: F1D64FF38E7442509BC721320A35B4D4	Status: Completed
Subject: CRF-2016-000096-P-2016-01875-Safe Harbour - Braintree Payment Service	
Source Envelope:	
Document Pages: 20	Signatures: 4
Certificate Pages: 5	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	PayPal EMEA CMS
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	2211 North First Street
	San Jose, CA 95131
	emeacms@paypal.com
	IP Address: 173.224.161.81

## Record Tracking

Status: Original 4/13/2016 4:48:44 AM	Holder: PayPal EMEA CMS emeacms@paypal.com	Location: DocuSign
--	---	--------------------

## Signer Events

Victoria Reaney  
vreaney@paypal.com  
Victoria Reaney  
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:  
Accepted: 4/13/2016 6:58:55 AM  
ID: 8b931c75-6e6a-401c-840d-97e86d0d36d8

## Signature

DocuSigned by:  
  
6A3563798E9B4B1...  
Using IP Address: 185.97.81.96

## Timestamp

Sent: 4/13/2016 5:00:00 AM  
Viewed: 4/13/2016 6:58:55 AM  
Signed: 4/13/2016 6:59:18 AM

David Ferri  
dferri@paypal.com  
Authorised Manager  
PayPal, Inc.  
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:  
Not Offered via DocuSign  
ID:

DocuSigned by:  
  
6A7A72A1D1C3458...  
Using IP Address: 173.224.162.99

Sent: 4/13/2016 6:59:20 AM  
Viewed: 4/13/2016 8:36:20 AM  
Signed: 4/13/2016 8:36:32 AM

Peggy Abkemeier  
pabkemei@paypal.com  
CFO Americas & Global Credit  
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:  
Accepted: 9/28/2015 12:22:22 PM  
ID: 120fb8ec-f651-402b-a12b-e659b8a7674a

DocuSigned by:  
  
9C2DD4F208FD4A1...  
Using IP Address: 173.224.162.69

Sent: 4/13/2016 12:43:53 PM  
Viewed: 4/13/2016 1:14:13 PM  
Signed: 4/13/2016 1:14:27 PM

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Amerjit Bria abriah@paypal.com PayPal Salesforce Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign ID:	<b>COPIED</b>	Sent: 4/13/2016 5:00:00 AM Viewed: 4/13/2016 12:34:55 PM
--	---------------	---

Lupe Sampedro gsampedro@paypal.com Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign ID:	<b>COPIED</b>	Sent: 4/13/2016 5:00:00 AM
---	---------------	----------------------------

Notary Events	Timestamp
---------------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	4/13/2016 12:43:53 PM
Certified Delivered	Security Checked	4/13/2016 1:14:13 PM
Signing Complete	Security Checked	4/13/2016 1:14:27 PM
Completed	Security Checked	4/13/2016 1:14:27 PM

Electronic Record and Signature Disclosure
--

## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, PayPal, Inc. (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through your DocuSign, Inc. (DocuSign) Express user account. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the "I agree" button at the bottom of this document.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. For such copies, as long as you are an authorized user of the DocuSign system you will have the ability to download and print any documents we send to you through your DocuSign user account for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign "Withdraw Consent" form on the signing page of your DocuSign account. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use your DocuSign Express user account to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through your DocuSign user account all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

**How to contact PayPal, Inc.:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: kaagarwal@paypal.com

**To advise PayPal, Inc. of your new e-mail address**

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at kaagarwal@paypal.com and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in DocuSign.

**To request paper copies from PayPal, Inc.**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to kaagarwal@paypal.com and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

**To withdraw your consent with PayPal, Inc.**

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign account, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to kaagarwal@paypal.com and in the body of such request you must state your e-mail, full name, IS Postal Address, telephone number, and account number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

**Required hardware and software**

Operating Systems:	Windows2000 or WindowsXP
Browsers (for SENDERS):	Internet Explorer 6.0 or above
Browsers (for SIGNERS):	Internet Explorer 6.0, Mozilla FireFox 1.0, NetScape 7.2 (or above)
Email:	Access to a valid email account
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	<ul style="list-style-type: none"> <li>• Allow per session cookies</li> <li>• Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection</li> </ul>

\*\* These minimum requirements are subject to change. If these requirements change, we will provide you with an email message at the email address we have on file for you at that time providing you with the revised hardware and software requirements, at which time you will have the right to withdraw your consent.

**Acknowledging your access and consent to receive materials electronically**

To confirm to us that you can access this information electronically, which will be similar to



other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the "I agree" button below.

By checking the "I Agree" box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC RECORD AND SIGNATURE DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify PayPal, Inc. as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by PayPal, Inc. during the course of my relationship with you.