PayPal

PayPal Direct Checkout Agreement

Last Update: May 10, 2022

Print

1. Introduction and Important Information.

PayPal Direct Checkout is an optimized checkout for Receiving Users that enables individuals who do not hold a PayPal Account to process payments ("PayPal Direct Checkout").

PayPal Direct Checkout is only available to eligible Receiving Users and upon prior application. Eligibility to PayPal Direct Checkout is at PayPal's sole discretion, as set forth in Section 2 ("PayPal Direct Checkout Integration and Requirements") below.

This PayPal Direct Checkout Agreement ("PayPal Direct Checkout Agreement") is a contract entered into by and between you, Receiving User, and Operadora PayPal de México, S. de R.L. de C.V. ("PayPal"), a company organized and existing under the laws of Mexico, and applies to your use of the PayPal Services to accept online payments using PayPal Direct Checkout.

All capitalized words and expressions used herein shall have the meanings ascribed to them in this PayPal Direct Checkout Agreement or in PayPal User Agreement. The headings and subheadings below are for reference only and do not limit the scope of each section.

You must read, agree with and accept all of the terms and conditions contained in this PayPal Direct Checkout Agreement in order to use PayPal Direct Checkout to accept

online payments. By using PayPal Direct Checkout, you acknowledge that you have agreed to this PayPal Direct Checkout Agreement.

This PayPal Direct Checkout Agreement, with the PayPal User Agreement and any other agreement in which you have entered into with PayPal (collectively " PayPal Agreements"), apply to your use of PayPal Direct Checkout. If any inconsistency exists between the terms of the PayPal User Agreement and this PayPal Direct Checkout Agreement, PayPal Direct Checkout Agreement shall control your use of PayPal Direct Checkout.

PayPal Agreements are electronic agreements available on **PayPal Legal Agreements Page**, as well as the policies that are part of PayPal Agreements and that are available on the same page.

PayPal reserves the right to amend the terms of PayPal Direct Checkout Agreement at any time, without prior notice, by posting a revised version on its website, through the **PayPal Direct Checkout Agreement's link.** Any new revised version will be effective at the time it is posted on the aforesaid link. If such version includes a Substantial Change, we will provide you with a, at least, 30-day prior notice of any Substantial Change by email or by posting a notice on the "Agreement Updates" page of our website, through the **Policy Update link**.

This PayPal Direct Checkout Agreement amends and restates any other agreement entered by You and PayPal in the past in connection with the PayPal Direct Checkout service.

The continuous use of PayPal Direct Checkout after this, or a new revised version of this PayPal Direct Checkout Agreement becomes effective shall automatically imply Receiving User's full knowledge and acceptance of all terms and conditions thereof.

PayPal reserves the right to suspend or limit your access to PayPal Direct Checkout and/or PayPal Services immediately if you violate any terms of this PayPal Direct Checkout Agreement, PayPal User Agreement and any other PayPal policy. Please note the following risks of using the PayPal Services, as set forth on PayPal User Agreement:

i. If you qualify as a Receiving User, the payments received in your Account may be reversed at a later time, for example, if a payment is subject to a Chargeback, Reversal, Claim, or is otherwise invalidated. This means that a payment may be reversed from your Account after you, as a Receiving User, have provided the products or services that were purchased by a Paying User.

ii. Receiving Users may lower the risk of a payment being reversed from their Account by following the criteria set out in Section 10 of PayPal User Agreement (Protection for PayPal Sellers) and by following the other security guidelines provided in the "**Security Center**" page of the PayPal website; and

iii. PayPal reserves the right to close, suspend, or limit your access to your Account or to the PayPal Services, and/or limit access to the funds held in your Account if you violate the PayPal User Agreement, the PayPal Acceptable Use Policy, or any other agreement you may have entered into with PayPal.

Back to top

2. PayPal Direct Checkout Integration and Requirements.

At PayPal's exclusive criteria, PayPal Direct Checkout may be integrated on your website in two different formats: i) in context screen or ii) mini browser.

You may request PayPal Direct Checkout integration on your website by calling 01-800-925-0304 or your PayPal account manager. If your website is hosted in a Platform that offers PayPal Direct Checkout as a checkout option, you may request PayPal Direct Checkout integration by sending your request through the Platform.

To be eligible to use PayPal Direct Checkout, you must have a PayPal Account in good standing and provide certain business, operations and/or financial information as requested by PayPal, in order to PayPal to proceed with a review of your business and website. You also need to be compliant with Payment Card Industry Data Security Standards (PCI DSS) and Payment Application Data Security Standards (PA DSS) if you integrate PayPal Direct Checkout with in context screen, as set forth in Section 3 ("Data Protection; Data Security; Data Portability") below.

PayPal will review the information provided by you and answer, in a timely manner, if you are approved or not to use PayPal Direct Checkout. You must be previously approved by PayPal to use PayPal Direct Checkout.

After your request to use PayPal Direct Checkout is approved, you may integrate PayPal Direct Checkout, according to PayPal Direct Checkout's integration guidelines that will be informed to you by PayPal.

PayPal reserves the right to reassess your eligibility for PayPal Direct Checkout at any time if your business and/or website become different from the information you provided when you requested PayPal Direct Checkout integration.

Back to top

3. Data Protection; Data Security; Data Portability

You agree to comply with all applicable laws and rules in connection with the collection, security and sharing of any personal or transaction information ("Data") on your website. You are fully responsible for the security of any Data on your website or otherwise in your possession or control. With regard to any personal data processed by either you or PayPal in connection with this PayPal Plus Agreement, you and PayPal will respectively each be a data controller in respect of such processing. You and PayPal each agrees to comply with the requirements of the data protection laws applicable to data controllers in respect of the provision of the services provided under this PayPal Plus Agreement and otherwise in connection with this agreement, including with respect to the information provided by PayPal to you pursuant to the PayPal Privacy Statement. For the avoidance of doubt, you and PayPal each have their own, independently determined privacy policies, notices and procedures for the personal data they hold and are each a data controller (and not joint data controllers). In complying with the data protection laws, you and PayPal each shall, without limitation:

i. implement and maintain at all times all appropriate security measures in relation to the processing of personal data;
ii. maintain a record of all processing activities carried out under this PayPal Plus Agreement; and
iii. not knowingly do anything or permit anything to be done which might lead to a breach by the other party of the applicable data protection laws.

With respect to your data transfers to PayPal of your customers located in the European Union, Switzerland, the Europeans Economic Area, and/or their member states and the United Kingdom, we each agree that (i) your signing of the Agreement will be deemed to be signature and acceptance of Module 1 (Controller-to-Controller) provisions of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 approved by European Commission Decision 2021/914 of 4 June 2021 (“C2C Transfer Clauses”) by Merchant, as the data exporter and (ii) PayPal’s signature of this Agreement will be deemed to be signature and acceptance of the C2C Transfer Clauses by PayPal, as the data importer. In the event the European Commission revises and thereafter publishes new C2C Transfer Clauses (or as otherwise required or implemented by the European Commission) or the UK Secretary of State (or other applicable UK authorized body) approves and issues UK standard contractual clauses or other similar contractual mechanism (“UK Clauses”) to be used instead of C2C Transfer Clauses to legitimize personal data transfer outside the United Kingdom, the parties agree that, respectively, such new C2C Transfer Clauses or UK Clauses will supersede the present C2C Transfer Clauses or UK Clauses, as applicable, and that they will take all such actions required to effect the execution of the new C2C Transfer Clauses or UK Clauses, as applicable. The C2C Transfer Clauses (Module 1) will be incorporated into the Agreement by reference and will be considered duly executed between the parties upon entering into force of this Agreement subject to the following details:

1. in case of any transfers of personal data from Switzerland, subject exclusively to the Swiss Federal Act on Data Protection and other data protection laws of Switzerland (“Swiss Data Protection Laws”); or the United Kingdom, general and

specific references in the C2C Transfer Clauses to: (a) Regulation (EU) 2016/679 or EU or Member State Law, shall have the same meaning as the equivalent reference in, respectively, the UK GDPR, the Data Protection Act 2018 and other data protection laws of United Kingdom ("UK Data Protection Laws"), or the Swiss Data Protection Laws; and (b) "Member State" or "EU Member State" or "EU" shall be read as references to, respectively, Switzerland, United Kingdom;

2. in accordance with Clause 13 (Supervision) the competent Supervisory Authority shall be the (i) the National Commission for Data Protection (CNDP) in Luxembourg, or (ii) where the data exporter is established in the United Kingdom or falls within the territorial scope of application of the UK Data Protection Laws, the Information Commissioner's Office, or (iii) where the data exporter is established in Switzerland or falls within the territorial scope of application of the Swiss Data Protection Laws, Swiss Federal Data Protection and Information Commissioner insofar as the relevant data transfer is governed by Swiss Data Protection Laws;
3. option 1 of Clause 17 (Governing law) shall apply and the laws of Luxembourg (or where the data exporter is established in the United Kingdom, of the United Kingdom) shall govern the C2C Transfer Clauses;
4. in accordance with Clause 18 (Choice of forum and jurisdiction), the courts of Luxembourg (or where the data exporter is established in the United Kingdom, of the United Kingdom) will resolve any dispute arising out of the C2C Transfer Clauses. Without prejudice to the other rights of a data subject under the C2C Transfer Clauses, a data subject shall be granted the right to refer disputes under the C2C Transfer Clauses to the courts of the Member State in which such data subject resides (including the United Kingdom or Switzerland, where corresponding to the country of data subject's habitual residence);
5. the parties agree that the details required under the C2C transfer Clauses Appendix are as set forth on Annex 1.

You agree that you shall be compliant with the PCI DSS and the PA DSS at all times while using PayPal Plus with in context screen, to the extent required for integrating and maintaining PayPal Plus on your website.

In order to integrate and maintain PayPal Plus with in context screen, you shall fill in and/or provide any and all documentation required to be compliant with PCI DSS and PA DSS. You agree to promptly provide PayPal with any documentation evidencing compliance with PCI DSS and/or PA DSS upon request by PayPal. Failure to comply with such requirement shall be deemed a Restricted Activity, pursuant of PayPal User Agreement, and may result in the adoption of the measures described PayPal User Agreement, including, but not limited to placing Reserves on funds held in your PayPal Account and immediate suspension of PayPal Plus processing capabilities, without incurring in any penalty to PayPal.

If PayPal believes that a security breach and/or compromise of Data on your website has occurred and/or that you are not compliant with PCI DSS and/or PA DSS when using PayPal Plus with in context screen, you may be required to hire a forensic examiner or

specialist, at your own cost, to certify that you can keep using PayPal Plus, without limiting the ability of PayPal to adopt the measures described in PayPal User Agreement. You agree to indemnify PayPal for any and all damages and/or losses, including but not limited to fines and/or penalties related to potential security breach and/or compromise of Data on your website.

You agree that PayPal may hire third parties services to periodically review the security of your website ("Inspectors"), with the purpose of verifying potential vulnerabilities that may put the Data and/or PayPal and/or PayPal customers' information at risk. You agree to cooperate with the Inspectors so that they may perform the verifications on your website, giving to the Inspectors and/or to PayPal access to your systems and all documentation related to the security of the Data.

You expressly waive to any act against PayPal and/or PayPal Affiliates originated from the verifications mentioned above and/or damages caused by the Inspectors. You accept that the Inspectors are solely responsible for the verifications performed.

Upon any termination or expiry of this Agreement, PayPal agrees, upon written request from you, to provide your new acquiring bank or payment service provider ("Data Recipient") with any available credit card information including personal data relating to your customers ("Card Information"). In order to do so, you must provide PayPal with all requested information including proof that the Data Recipient is in compliance with the Association PCI-DSS Requirements and is level 1 PCI compliant. PayPal agrees to transfer the Card Information to the Data Recipient so long as the following applies: (a) you provide PayPal with proof that the Data Recipient is in compliance with the Association PCI-DSS Requirements (Level 1 PCI compliant) by providing PayPal a certificate or report on compliance with the Association PCI-DSS Requirements from a qualified provider and any other information reasonably requested by PayPal; (b) the transfer of such Card Information is compliant with the latest version of the Association PCI-DSS Requirements; and (c) the transfer of such Card Information is allowed under the applicable Association Rules, and any applicable laws, rules or regulations (including data protection laws).

Back to top

4. PayPal Seller Protection

You, Receiving User, approved to use PayPal Direct Checkout may be eligible to PayPal Seller Protection for transactions with PayPal Direct Checkout if, besides fulfilling all the requirements set forth in Section 10 ("Protection for PayPal Sellers") of PayPal User Agreement, you also share with PayPal the shipping address, email and phone number from your customers who paid their purchases using PayPal Direct Checkout. This data sharing is necessary to verify fulfillment of PayPal Seller Protection requirements, pursuant to Section 10 of PayPal User Agreement.

Annex 1

C2C Transfer Clauses Appendix

A. The following is applicable, to the extent required, under the C2C Transfer Clauses

Data Exporter

- Name and Address: The data exporter is the Merchant and the address is as provided in the Agreement
- Contact person's name, position and contact details: as provided in the Agreement
- Activities relevant to the data transferred under the Standard Contractual Clause: as provided in the Agreement
- Signature and date: please refer to what provided under Section 3 ("Data Protection; Data Security; Data Portability")
- Role (controller/processor): controller

Data Importer

- Name and Address: The data importer is the member of the PayPal Group providing the services pursuant to the Agreement and the address is as provided in the Agreement
- Contact person's name, position and contact details: as provided in the Agreement
- Activities relevant to the data transferred under the Standard Contractual Clause: as provided in the Agreement

- Signature and date: please refer to what provided under Section 3 ("Data Protection; Data Security; Data Portability")

- Role (controller/processor): controller

Annex 1.B. Description of Transfer

Data subjects Whose Personal Data is Transferred
The personal data transferred concern the following categories of data subjects:

- The data exporter's customers, employees and other business contacts.

Categories of Personal Data Transferred

- Name, amount to be charged, date/time, bank account details, payment card details, CVC code, post code, country code, address, email address, fax, phone, website, expiry data, shipping details, tax status, unique customer identifier, IP Address, location, and any other data received by PayPal under the Agreement.

Sensitive data (if appropriate) and Applied Restrictions or Safeguards
The personal data transferred concern the following categories of sensitive data:

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

Applies restrictions and safeguards:

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

Nature of the Processing

As set forth in the Agreement.

Purpose(s) of the Transfer(s)

The transfer is made for the following purposes:

- Performance of the services provided by data importer to data exporter in accordance with the Agreement.
- To identify fraudulent activity and risk that is, or may, affect the data importer, the data exporter or other customers of the data importer.
- To comply with laws and law enforcement requests applicable to the data importer.
- As set forth in the Privacy Statement of the data importer.

The Period for which the Personal Data will be Retained, or, if that is not Possible, the Criteria Used to Determine that Period

The data importer only retains the personal data for as long as is necessary with regards the relevant purpose(s) it was collected for (please see purposes above). To determine the appropriate retention period for personal data, the data importer considers the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of the personal data, the purposes for which the personal data is processed and whether such purposes can be achieved through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

For transfers to (Sub-) Processors, also Specify Subject Matter, Nature and Duration of the Processing

The data importer may share personal data with third-party service providers that perform services and functions at the data importer’s direction and on its behalf. These third-party

service providers may, for example, provide an element of the services provided under the Agreement such as customer verification, transaction processing or customer support, or provide a service to the data importer that supports the services provided under the agreement such as storage. When determining the duration of the processing undertaken by the third-party service providers, the data importer applies the criteria provided above in this Annex1.B.

Annex 1.C. Supervisory Authority

In accordance with Clause 13(a) of the EU Transfer Clauses, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated shall act as competent supervisory authority.

B. Technical and Organisations Measures Including Technical and Organisational Measures to Ensure the Security of the Data

1. Pseudonymization, Encryption and the Protection of Data During Transmission.

PayPal's policies ensure compliance with this principle and require the use of technical controls to prevent the risk of disclosure of personal data. PayPal employs encryption in transit and at rest for all personal data. We also employ industry standard pseudonymization techniques, such as tokenization to protect personal data where applicable. PayPal has comprehensive policies that provide key obligations and processes to protect data when it is transferred within the enterprise and externally with third parties.

2. Change Management and Business Continuity.

PayPal's robust change management process protects the ongoing availability and resiliency of data and systems throughout their lifecycle by ensuring that changes are planned, approved, executed, and reviewed appropriately. The Company's business continuity management process provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders.

3. Disaster Recovery.

PayPal's robust disaster recovery program has processes for recovering information or technology systems in the event of any significant disruption, focusing on the IT systems that support critical business processes and customer activities. PayPal's technology infrastructure is housed in multiple secure data centers, with primary and secondary capability, each equipped with network and security infrastructure, dedicated application and database servers and storage.

4. Regular Testing, Assessment and Evaluating Effectiveness of Technical and Organizational measures.

PayPal regularly plans, executes and reports on the results of the Company's testing program to assess and evaluate the effectiveness of its technological and organizational measures. The program is managed through our enterprise risk and compliance team who work with relevant stakeholders to obtain and evaluate information required for testing, reporting and remediating as necessary.

5. User Identification and Authorization.

PayPal's access management processes require users to log into the corporate network using a unique corporate network account ID and password for user identification and authentication before accessing any other in-scope applications. Automated policies regarding password composition, length, change, reuse, and lockout are applied. Role-based access and approvals, which are certified quarterly, are implemented across all in-scope systems to enforce least privileged principle.

6. Physical Security of Locations Where Personal Data is Processed.

PayPal global safety and security policies and processes set forth the requirements necessary to facilitate sounds safety and security processes, including physical security, in accordance with applicable laws, regulations and partner requirements. Special emphasis is placed on security systems and safeguards when constructing special or sensitive areas such as mail rooms, equipment storage, shipping and receiving areas, computer/server rooms, communications vaults or classified document/information storage areas in accordance with the Company's information security handling standard.

7. Events Logging and Configuration.

PayPal has outlined and defined event logging and monitoring types and attributes. The Company collects and aggregates several types of logs to the centralized security monitoring system. Standard configuration management control is in place to ensure logs are collected from the systems, and then forwarded to our centralized security monitoring system. PayPal policies and supporting processes set forth that system configuration and hardening baselines must be implemented across all systems.

8. IT Governance and Management; Certification and Assurance of Processes and Products.

PayPal promotes a strong security philosophy across the Company. Our Chief Information Security Officer oversees information security across our global enterprise. As part of our Enterprise Risk and Compliance Management Program, our Technology Oversight and Information Security Program is designed to support the Company in managing technology and information security risks and identifying, protecting, detecting, responding to and recovering from information security threats. PayPal

certifies and assures its processes and products through a variety of enterprise programs, including (i) audits and assessments of PayPal's technical industry standard obligations including but not limited to, ISO 27001, Payment Card Industry's (PCI) applicable standards (DSS, PIN, P2PE, etc.) and the American Institute of Certified Public Accountants (AICPA) SOC-1 and SOC-2, (ii) Risk Control Identification Process (RCIP) which ensures early engagement and a standard approach to the measurement, management, and monitoring of risk associated with the development and release of product solutions, (iii) privacy impact assessments which are integrated into the early stages of the product and software development processes, and (iv) a comprehensive third party management program, which provides assurance through continuous management of risks throughout the lifecycle of an engagement with a third party.

9. Data Minimization.

Our policies require, through technical controls, that data elements collected and generated are those which are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. PayPal's privacy impact assessment processes ensure compliance with these policies.

10. Data Quality and Retention.

PayPal's access and quality policy ensures that all personal data is correct, complete, and up to date, enabling individual users to access the system to correct and modify their particulars (e.g., address, contact details etc.), and, where a request for correction is received from a data subject, to provide a service which delivers their right to correction. Our data governance program monitors data quality, issues and remediations, as necessary. We require that all data be classified according to its business value with assigned retention periods, which is based upon PayPal's legal, regulatory, and business recordkeeping requirements. Upon expiration of the retention period, data and information is disposed, deleted, or destroyed.

11. Accountability.

PayPal has developed a set of information security, technology, data governance, third party management and privacy policies and principles that are aligned to industry standards and designed to engage stakeholder collaboration and partnership in awareness and compliance with such policies and controls across the organization to ensure participation and accountability from the top down across the organization. Each program defines accountabilities for cross-functional data related decisions, processes and controls. As a data controller, PayPal is responsible for and demonstrates compliance with the relevant articles carrying an accountability obligation in the GDPR and other applicable data protection laws through the implementation of a privacy program policy and an underlying layered organizational and technical control structure to ensure enterprise-wide compliance with privacy law, regulation, policy, and procedures. These include being able to demonstrate compliance with the data protection laws through: 1) a strong culture of compliance, 2) an enterprise risk and compliance governance structure

which includes management committees, oversight roles, privacy reporting, 3) business function accountability for compliance with the privacy program including establishment, documentation and maintenance of business processes and controls, 4) a global privacy department within the Enterprise Compliance Organization to oversee business compliance with the privacy program and define policies, standards, procedures, and tools which are operationalized by business functions, 5) communications to the enterprise by the global privacy function to promote awareness and understanding of privacy, 6) Enterprise Risk and Compliance Management Framework to ensure the use of consistent processes including privacy impact assessments, privacy monitoring and testing, privacy issue management, privacy training, annual privacy plan, and 7) reporting and analysis to management committees which oversee the Privacy Program.

12. Data Subject Rights.

PayPal has a program in place to ensure data subject rights are fulfilled, including access, correction and erasure. Data erasure requests are fulfilled unless PayPal has a legal, regulatory obligation or other legitimate business reason to retain it. PayPal's policies ensures that erasure occurs throughout the customer lifecycle.

13. Processors.

PayPal has a comprehensive third-party management program, which provides assurance through continuous management of risks throughout the lifecycle of an engagement with a third party. We have contractual controls in place to require our processors and their subprocessors to put in place comprehensive data security and privacy standards throughout the processing chain. All subprocessors must require our advance approval before being engaged.

Back to top