PayPal

>> View all legal agreements

PayPal Data Protection Addendum for Card Processing Products

Print

Last update: December 1, 2021

This PayPal Data Protection Addendum for Card Processing Products (this "Addendum") applies to any product, service or other offering where a member of the PayPal Group ("PayPal") is providing card processing, gateway and/or fraud protection services (the "Payment Services") to you, the Merchant (the "Merchant" or "You"). This Addendum does not apply to PayPal wallet services such as pay with PayPal or PayPal's pay later offers. This Addendum shall form part of the relevant agreement between Merchant and PayPal that governs PayPal's provision of the Payment Services to you (the "Agreement") and is incorporated by reference therein. In the event there is any conflict between the terms of this Addendum and the Agreement, the terms of this Addendum shall control. Capitalized terms used but not defined in this Addendum shall have the meaning set out in the Agreement.

This Addendum is effective as of the later of (i) the effective date specified in the Agreement or (ii) the effective date stated in the notice posted or provided to you in connection with this Addendum. We may amend this Addendum from time to time. The revised version will be effective at the time we post it on our website, unless otherwise noted. If our changes reduce your rights or increase your responsibilities, we will post a notice on the "Policy Updates" page of our website within the timeframe required by the Agreement. If you do not agree with any change to this Addendum, you may discontinue your use of the Payment Services.

Definitions

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

"**Controller**" means an entity that *determines the purposes and means of the processing of Personal Data, or, if such term (or terms addressing similar functions) in defined in Data Protection Law, "Controller" shall have the meaning as defined in the applicable Data Protection Law*.

"**Customer**" means your customers who use the Payment Services and for the purposes of this Addendum, are data subjects.

"**Customer Data**" means the Personal Data that (i) the Customer provides to Merchant and Merchant passes on to PayPal through the use by Merchant of the Payment Services and (ii) PayPal may collect from the Customer's device and browser through use by Merchant of the Payment Services.

"**Data Protection Laws**" means any applicable data protection laws, regulations, directives, regulatory requirements and codes of practice applicable to the provision of the Payment Services including any amendments thereto and any associated regulations or instruments (e.g., the California Consumer Privacy Act 2018, Cal. Civ. Code § 1798.100 et seq, the General Data Protection Regulation (EU) 2016/679 (GDPR), the Australian Privacy Act 1988 (Cth) the Personal Information Protection and Electronic Documents Act (Canada), the Personal Data (Privacy) Ordinance (Cap.486) (Hong Kong), the Brazilian General Data Protection Law, Federal Law no. 13,709/2018 and the Personal Data Protection Act 2012 (Singapore)).

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

"**Personal Data**" means any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Process**" or terms addressing similar functions when used in this Addendum shall have the meaning as defined in the applicable Data Protection Laws.

PayPal As a Controller

PayPal shall comply with the requirements of the Data Protection Laws applicable to Controllers in respect of the Processing of Customer Data under this Addendum (including without limitation, by implementing and maintaining at all times all appropriate security measures in relation to the Processing of Customer Data) and shall not knowingly do anything or permit anything to be done with respect to the Customer Data that likely would lead to a breach by Merchant of the Data Protection Laws. Customer Data. PayPal shall only transfer Customer Data to third parties, sub-processors or members of the PayPal Group who shall sign written agreements which contain terms for the protection of Customer Data, which are no less protective than the terms set out in this Addendum.

Processing of Customer Data in Connection with the Payment Services

The parties acknowledge and agree that Merchant and PayPal are each independent Controllers in respect of all Customer Data Processed in connection with the Payment Services. As such, PayPal independently determines the purpose and the means of the Processing of such Customer Data and is not a joint Controller with Merchant with respect to such Customer Data.

The parties acknowledge and agree that PayPal is permitted to use, reproduce and Process Customer Data and payment transaction data for the following limited purposes:

- as reasonably necessary to provide and improve the Payment Services to Merchant and its Customers, including fraud protection tools;
- to monitor, prevent and detect fraudulent payment transactions and to prevent harm to Merchant, PayPal and to third parties,
- to comply with legal or regulatory obligations applicable to the Processing and retention of payment data to which PayPal is subject, including applicable anti-money laundering and identity verification obligations;
- to analyze, develop and improve PayPal's products and services;
- internal usage, including but not limited to, data analytics and metrics;
- to compile and disclose Customer Data and payment transaction data in the aggregate where your individual or user Customer Data is not identifiable, including calculating your averages by region or industry;
- complying with applicable legal requirements and assisting law enforcement agencies by responding to requests for the disclosure of information in accordance with laws; and
- any other purpose that it notifies Merchant so long as such purpose is in accordance with Data Protection Laws.

Merchant Notice to Customers

Merchant shall use commercially reasonable efforts to (i) notify Customers in their privacy policy that PayPal is an independent Controller for the purpose of Processing Customer Data as described in this Addendum and (ii) include a link to the PayPal privacy statement available at www.paypal.com in Merchant's privacy policy.

Mutual Assistance

The parties agree to co-operate with each other to the extent reasonably necessary to enable the other party to adequately discharge their responsibility as an independent Controller under Data Protection Laws. The parties agree that to the extent Merchant receives a subject access request or any exercise by a Customer of its rights under Data Protection Laws, Merchant shall respond to such Customer's access request directly. Merchant also shall inform the Customer that they may exercise their data subject rights in connection with the Payment Services with PayPal according to the instructions described in the Privacy Statement available at **www.paypal.com**. In addition, if in connection with any security incident, PayPal determines in its sole decision that it must notify affected Customers and PayPal does not have the necessary contact information

about an affected Customer to make such communication, then Merchant shall use commercially reasonable efforts to provide PayPal with information about Customer that Merchant may possess for the limited purpose of PayPal's compliance with applicable notification obligations regarding affected Customers under Data Protection Laws.

Cross Border Data Transfers

The parties agree that PayPal may transfer Customer Data Processed under this Agreement outside the country where it was collected as necessary to provide the Payment Services. If PayPal transfers Customer Data protected under this Addendum to a jurisdiction for which the applicable regulatory authority for the country in which the data was collected has not issued an adequacy decision, PayPal will ensure that appropriate safeguards have been implemented for the transfer of Customer Data in accordance with applicable Data Protection Laws. For example, and for purposes of compliance with the GDPR, we rely on Binding Corporate Rules approved by competent supervisory authorities and other data transfer mechanisms for transfers of Customer Data to other members of the PayPal Group.

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 or the United Kingdom, we each agree that (i) to the extent applicable, your signing of the Agreement will be deemed to be signature and acceptance of the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR ("EU Transfer Clauses") by Merchant, as the data exporter and in the role of controller, and will be deemed to be signature and acceptance of the standard data protection clauses specified in regulations made by the Secretary of State under section 17C(b) of the 2018 Data Protection Act and for the time being, in force in the United Kingdom (the "UK Transfer Clauses"), as the data exporter (ii) to the extent applicable, PayPal's signature of the Agreement will be deemed to be signature and acceptance of the EU Transfer Clauses by PayPal, as the data importer and in the role of controller, and will be deemed to be signature and acceptance of the UK Transfer Clauses, as the data importer; and (iii) the parties shall be subject to the Module 1 provisions of the EU Transfer Clauses. In the event the European Commission or the UK Secretary of State (or other applicable UK authorized body) revises and thereafter publishes new EU Transfer Clauses or UK Transfer Clauses, respectively (or as otherwise required or implemented by the European Commission or the UK Secretary of State (or other applicable UK authorized body)), the Parties agree that such new EU Transfer Clauses or UK Transfer Clauses, as applicable, will supersede the present EU Transfer Clauses or UK Transfer Clauses, as applicable, and that the parties agree to take all such actions required to effect the execution of the new EU Transfer Clauses or UK Transfer Clauses, as applicable. The EU Transfer Clauses (Module 1) and the UK Transfer Clauses 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:

A) EU Transfer Clauses

1. option 1 of Clause 17 (Governing law) shall apply and the laws of Luxembourg shall govern the EU Clauses;
2. in accordance with Clause 18 (Choice of forum and jurisdiction), the courts of Luxembourg will resolve any dispute arising out of the EU Clauses; and
3. The parties agree that the details required under the EU Transfer Clauses Appendix are as set forth on Attachment 1.

B) UK Transfer Clauses

1. Clause II(h)(iii) is incorporated and signature of the Agreement by PayPal will be deemed the requisite initials from PayPal as the data importer;
2. The parties agree that the details required under Annex B of the UK Transfer Clauses are as set forth on Attachment 1 (to the extent applicable).

Attachment 1

Appendix to the EU Transfer Clauses and Annex B of the UK Transfer Clauses

A. The following is applicable, to the extent required, under the EU Transfer Clauses and the UK Transfer Clauses

Annex 1.A. List of Parties

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 see the "Cross Border Transfers" section of this Addendum
- 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 see the "Cross Border Transfers" section of this Addendum
- Role (controller/processor): controller

Annex 1.B. Description of Transfer

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

- The data exporter and its Customers, employees and other business contacts.

Categories of Personal Data Transferred

The personal data transferred may include the following categories of data:

- 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.

Purposes 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 applicable to the data importer.
- As set forth in the Data Protection Addendum.

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.

Annex II. 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.

B. The following is applicable to UK Transfer Clauses only

Recipients
The personal data transferred may be disclosed only to the following recipients:

- The importer's service providers, affiliates, and personnel performing services in accordance with the Agreement.

Data protection registration information of data exporter (where applicable)

Not applicable**.**

Additional useful information (storage limits and other relevant information)

As set forth in the Agreement and above in this Attachment 1.