>> **View all legal agreements**

Controller to Controller SCCs

Download PDF

Last update: June 17, 2022

These Controller-to-Controller Standard Contractual Clauses ("SCCs") form part of the applicable PayPal User Agreement (the "Agreement") between you, acting as a seller ("you" or "Merchant") and PayPal and are incorporated by reference therein. In the event there is any conflict between the terms of this SCCs and the Agreement, the terms of this SCCs will control. Capitalized terms used but not defined in this SCCs have the meaning set out in the Agreement.

To the extent applicable: (i) 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 Regulation (EU) 2016/679 ("EU Transfer Clauses") by Merchant, as the data exporter and in the role of controller; (ii) 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 (iii) the parties shall be subject to the Module 1 provisions of the EU Transfer Clauses.

In the event the European Commission revises and thereafter publishes new EU Transfer Clauses (or as otherwise required or implemented by the European Commission), the parties agree that such new EU Transfer Clauses will supersede the present EU Transfer Clauses, and that they will take all such actions required to effect the execution of the new EU Transfer Clauses.

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"):

i. the EU Transfer Clauses shall also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as personal data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity;
ii. general and specific references in the EU Transfer Clauses to Regulation (EU) 2016/679 or EU or Member State Law shall have the same meaning as the equivalent reference in the Swiss Data Protection Laws and references to "Member State" or "EU Member State" or "EU" shall be read as references to Switzerland.

The EU 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 the Agreement subject to the following details:

i. for the purposes of Clause 13 (Supervision) competent Supervisory Authority shall be the Swiss Federal Data Protection and Information Commissioner insofar as the relevant data transfer is governed by Swiss Data Protection Laws;
ii. option 1 of Clause 17 (Governing law) shall apply and the laws of Luxembourg shall govern the EU Transfer Clauses;

iii. in accordance with Clause 18 (Choice of forum and jurisdiction), the courts of Luxembourg will resolve any dispute arising out of the EU Transfer Clause; the data subject shall be granted the right to refer disputes to the courts of Switzerland, where corresponding to the country of his/her habitual residence; and

iv. the parties agree that the details required under the EU Transfer Clauses Appendix are as set forth on Attachment 1.

Attachment 1

<u>Appendix to the EU Transfer Clauses</u>

Annex 1.A. The following is applicable, to the extent required, under the EU 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 in these SCCs
- 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 in these SCCs
- 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 in these SCCs, 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.