PayPal

>> View all legal agreements

PayPal User Corporate rules

Last Update: March 28, 2022

The PayPal Group's goal is to apply uniform, adequate and global data protection and privacy standards for the handling of all User Personal Data throughout the PayPal Group. These User Corporate Rules apply to all User Personal Data Processed by Group Members worldwide.

Users globally provide their Personal Data to Group Members to utilize the services the Group offers. Most User Personal Data is collected and stored in the United States. PayPal's global business requires User Personal Data to be shared with other PayPal entities in the United States and globally where PayPal currently has or intends to have a presence.

Currently, Employees located in the following EEA countries may have access to User Personal Data: Luxembourg, Belgium, France, Germany, Ireland, Italy, the Netherlands, Poland, Spain, Sweden.

Employees currently located in the following non-EU countries may also have access to User Personal Data: the United States of America, Taiwan, Turkey, Virgin Islands (British), Australia, Canada, China, Hong Kong, India, Indonesia, Israel Japan, Republic of Korea, Malaysia, Mauritius, Philippines, Russia, Singapore, Switzerland, the United Kingdom, Argentina, Brazil and Mexico.

PayPal is committed to adequately protecting the User information regardless of where the Personal Data resides and to provide appropriate protection for the User Personal Data where it is transferred outside of the EEA.

This list of countries may change as the company's business expands.

1. Privacy Governance Structure and Responsibilities

The User Corporate Rules are made legally binding by an agreement (the "IGA") between PayPal (Europe) S.à r.l. & Cie, S.C.A. ("Lead Group Member") and other

PayPal Group entities. The IGA requires Group Members to comply with these User Corporate Rules. Group Members require their Employees to comply with these User Corporate Rules when handling User Personal Data.

Business leaders and senior management of the PayPal Group are responsible for enforcing compliance with these User Corporate Rules, including ensuring that Employees are aware of and abide by these User Corporate Rules.

The compliance privacy lead drives the PayPal privacy program. He/she holds a senior position within PayPal Holdings, Inc. and reports directly to the chief compliance officer or the highest senior executive leading the compliance function at PayPal. The compliance privacy lead oversees the PayPal Global Privacy Compliance Team and interacts with other internal organizations or teams, such as operations, information security, compliance, risk and internal audit to help ensure consistent privacy communications, practices and policies across the PayPal Group globally. The PayPal Global Privacy Compliance Team develops and coordinates implementation of its compliance strategy across the PayPal Group and verifies operational compliance. The PayPal Global Privacy Compliance Team has direct and indirect representatives throughout the PayPal Group who, among other things, help to ensure compliance with the User Corporate Rules and applicable data protection laws.

The legal privacy lead oversees the PayPal Global Privacy Legal Team and reports directly to the chief legal officer or the highest senior executive leading the legal function at PayPal. The legal privacy lead defines the company's obligations under applicable data protection laws and these User Corporate Rules. The legal privacy lead and the PayPal Global Privacy Legal Team works in close coordination with the compliance privacy lead and the PayPal Global Compliance Privacy Team, and interacts with other internal organizations and teams, such as legal, operations, information security, and risk to provide legal advice and interpret legal and regulatory implications on evolving privacy matters across the PayPal Group globally.

Collectively, The PayPal Global Privacy Compliance Team and the PayPal Global Privacy Legal Team from the PayPal Global Privacy Team.

The European Data Protection Officer located in Luxembourg, is appointed by and reports to the management of PayPal (Europe) S.à r.l. et Cie, S.C.A.. The European Data Protection Officer acts as the primary contact for the EEA data protection authorities and has, among others, the following duties: to inform and advise the Group Members and their employees, who are processing personal data, of their obligations under the privacy legislation to ensure compliance with these User Corporate Rules; to work with the PayPal Global Privacy Team to monitor compliance with privacy legislation and with related policies of the Group Members; and, to provide legal advice to the Group Members where requested as regards the data protection impact assessments and their implementation.

2. Principles For Processing User Personal Data

Group Members observe the following Processing principles for User Personal Data.

2.1 Purpose Limitation

User Personal Data shall be Processed for specific, explicit and legitimate purposes only. In particular, User Personal Data may be Processed to:

- Offer and facilitate the provision of Services at Users' requests, including opening an account;

- Improve the Services and develop new Services;

- Resolve disputes, manage litigation, troubleshoot problems, and provide customer service;

- Perform risk management;

- Process transactions and collect fees owed;

- Check creditworthiness and solvency;

- Measure Users' interest in and feedback and opinion concerning Services, and inform Users about online and offline offers, Services, and updates;

- Customize Users' experiences;

- Detect and protect against error, fraud and other criminal activity;

- Fulfill PayPal Group's legal, contractual or regulatory obligations;

- Enforce the Service's terms and conditions and as otherwise described to Users at the time of collection and in the Service's privacy policy;

- Protect the security, integrity and availability of the Services and the PayPal Group network; and

- Protect the PayPal Group's legal rights and interests, including, but not limited to, establishing, exercising, or defending against legal claims.

Processing of User Personal Data for other purposes is subject to prior approval from the PayPal Global Privacy Legal Team. When in doubt, Group Members will consult the PayPal Global Privacy Legal Team.

User Personal Data shall not be further Processed in a way that is incompatible with the above listed purposes, unless there is a legal basis for doing so under the applicable law of the Group Member in the EEA responsible for the collection and/or transfer of the User Personal Data.

2.2 Data Quality and Proportionality

User Personal Data shall be:

- Accurate and, where necessary, kept up-to-date;
- Adequate, relevant and not excessive in relation to the purposes for which it is Processed; and
- Retained for no longer than necessary to achieve the purposes for which it was originally collected or further Processed.

User Personal Data which is no longer required for the purposes for which it was Processed shall be erased, deleted, destroyed or anonymized, unless there is a legal ground for further Processing or retention is required by applicable law.

2.3 Legal Grounds for Processing

Group Members shall ensure that User Personal Data is Processed fairly and lawfully and in particular on the basis of at least one of the following legal grounds:

- Unambiguous consent of the User;
- Processing necessary for the performance of a contract to which the User is party or in order to take steps at the request of the User prior to entering into a contract;
- Processing necessary for compliance with a legal obligation to which Group Members are subject;
- Processing necessary in order to protect the vital interests of the User;
- Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Group Members or in a Third Party to whom the data are disclosed; or
- Processing necessary for the purposes of the legitimate interests pursued by the Group Member or by the Third Party or Parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the User.

As a general practice, Group Members do not collect Sensitive User Personal Data. Where such collection is required or where Users voluntarily provide such information, Group Members shall ensure that the Sensitive User Personal Data is only Processed on the basis of at least one of the following grounds:

- Express consent of the User;
- Processing necessary to protect the vital interests of the User or of another person where the User is physically or legally incapable of giving his/her consent;

- Processing relates to User Personal Data manifestly made public by the User; or
- Processing necessary for the establishment, exercise or defense of legal claims.

Where the Processing involves automatic decision-making ("Automated Decisions"), Group Members shall provide suitable measures to safeguard the User's legitimate interests, such as providing the User an opportunity to have a customer support representative review the decision individually and permit the User to provide their point of view. The customer support representative shall escalate the matter to the EU Data Protection Officer in case the User continues to disagree with an Automated Decision. When appropriate, the Legal Privacy Lead will be consulted and the Compliance Privacy Lead will be apprised.

2.4 Transparency

When collecting User Personal Data, Group Members shall inform Users of:

- The name and address of the Group Member responsible for the original collection and Processing;
- The categories of User Personal Data concerned;
- The intended purposes of the Processing;
- The categories of recipient Processors and Third Parties of the User Personal Data;
- Whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
- The existence of User rights; and
- In case of automated decision-making, the logic involved.

Group Members may provide the information in a Service privacy policy which shall be accessible via a link and/or displayed in a prominent location of each Service website or application and during registration. The obligation to inform Users does not apply if Users already are aware of the information.

Where the provision of information proves impossible or would involve a disproportionate effort, Group Members may refrain from providing the information. This would only be the case for User Personal Data that has not been obtained from the User directly.

In exceptional circumstances, the provision of specific information may be postponed or omitted, for example, in the context of investigations into wrongful conduct or to comply with applicable laws or where provision of the information could jeopardize the integrity of the investigation.

2.5 Confidentiality and Security

Group Members use physical, technical and organizational security controls commensurate with the amount and sensitivity of the User Personal Data to prevent

unauthorized Processing, including but not limited to, unauthorized access to, acquisition and use of, loss, destruction, or damage to User Personal Data. Group Members use encryption, firewalls, access controls, standards and other procedures to protect User Information from unauthorized access. Physical and logical access to electronic and hard copy files is further restricted based upon job responsibilities and business needs.

2.6 Users Choices and Rights

Users may access and rectify most of the User Personal Data relating to them that Group Members maintain using the appropriate online tool or self-service process made available to them through the Service website or application.

In all cases, Users have the right to submit a data subject access request to view or receive a copy of their User Personal Data not accessible via the Service's website or application. Users should contact customer support via directions provided via the Service's website or application. Group Members will comply with requests in the timeframes prescribed by applicable law, except where applicable law provides for an exception to such obligation. Users may be required to provide proof of their identity and may be subject to a servicing fee as permitted by applicable law.

Users also may request the rectification of their data if they are incomplete or inaccurate. Group Members will comply with such request and will inform Users when their data have been rectified. Group Members will notify third parties whom the User's data have been disclosed of any rectification, unless this proves impossible or involves a disproportionate effort.

On compelling legitimate grounds, Users may object to the Processing of their User Personal Data. Group Members will comply with such requests, unless retention of User Personal Data is required by applicable law or to defend the PayPal Group against legal claims. Users will be informed about the outcome of their request and the measures taken by the Group Members.

Furthermore, Users may request to have their accounts closed by following the instructions provided via the Service's website or application. Group Members will remove or render anonymous a User's information from a Service as soon as reasonably possible based upon account activity. In some instances, Group Members may delay the closure of an account or retain User Personal Data to conduct an investigation or where required by applicable law. Group Members also may retain User Information from closed accounts to detect and prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with any investigations, manage risk, enforce a Service's terms and conditions, comply with legal or regulatory requirements and take other actions otherwise permitted by applicable law. The data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed and will be deleted once the underlying reason for retaining it has been addressed or resolved.

With the exception of those Users who have selected not to receive certain communications, Group Members may use User Personal Data to target communications to Users based on their interests according to applicable law. Users that do not wish to receive marketing communications from the PayPal Group will be offered easily accessible means to oppose further advertising, for example, in their account settings or by following the directions provided in an email or from a link on the communication.

Users can exercise the above rights by contacting customer support. Where a User's identity is difficult to verify, Group Members may require the User to provide additional proof of identification.

2.7 Disclosures of Personal Data

Group Members may share User Personal Data in the normal course and scope of business with other Group Members worldwide for the purposes identified in Section 2.1.

In accordance with applicable law, treaties or applicable international conventions, Group Members may share Personal Data with law enforcement and regulatory authorities when necessary in a democratic society to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences, and, in particular to comply with sanctions as laid down in international and/or national instruments, tax-reporting requirements or anti-money-laundering reporting requirements.

Group Members do not sell or rent User Personal Data to Third Parties for their own marketing purposes without the User's explicit unambiguous informed consent. Group Members may disclose User Information to other Third Parties in accordance with the User's instructions or consent (where permissible under applicable law).

When transferring User Personal Data to Processors, the Processors will be subject to a privacy, data protection and information security risk assessment prior to the initiation of work and prior to any transfer of User Personal Data. The scope of the assessment will vary based upon the sensitivity of the User Personal Data processed. Processors, including a Group Member intervening as a Processor, must enter into an agreement with the relevant Group Members to provide adequate privacy, data protection and information security measures. Such an agreement includes clauses ensuring the appropriate use of User Personal Data and security measures commensurate with the amount, nature and sensitivity of the User Personal Data involved. At a minimum, the contractual safeguards must cover the following matters:

- Requirements to comply with the law and to Process User Personal Data only in accordance with the terms of the agreement and only on the instructions of the Group Members concerned;
- Appropriate technical and organizational measures adapted to the sensitivity of the User Personal Data and Processing concerned;
- A right to audit Processors' compliance with the contractual guarantees;
- Security breach notification obligations; and

- Provisions on remediation in the event of non-compliance by the Processor with its legal or contractual obligations.

The agreements must contain provisions ensuring that failure to comply with the terms of the agreement may result in the suspension or termination of the agreement among other remedies identified in the agreement.

The privacy, data protection and information security assessment is not mandatory for Processors that already have been subject to such an assessment, unless the Processing activities involve high risk activities taking into account the nature and amount of Personal Data and the type of Processing activities concerned.

Notwithstanding the above, where Group Members transfer EEA User Personal Data to Third Parties or to Processors that are not Group Members: (i) located in countries that do not provide adequate levels of protection (within the meaning of the Directive 95/46/EC), (ii) not covered by approved binding corporate rules, or (iii) who do not have other arrangements that would satisfy EU adequacy requirements, the Group Member shall ensure in relation to:

- Third Parties, that they shall implement appropriate contractual controls, such as model contractual clauses approved by the European Commission, providing levels of protection commensurate with these User Corporate Rules or, alternatively, ensure that the transfer (i) takes place with the unambiguous consent of the User, (ii) is necessary to conclude or perform a contract concluded with the User, (iii) is necessary or legally required on important public interest grounds, or (iv) is necessary to protect the vital interests of the User;
- Processors, that they shall implement contractual controls, such as model contractual clauses approved by the European Commission, providing levels of protection commensurate with these User Corporate Rules.

3. Complaint Mechanism

If Users believe that their User Personal Data has been processed in violation of the User Corporate Rules, they may report concerns to the customer service function of the relevant Group Member via the relevant service's website, email or as otherwise indicated in the applicable terms and conditions. Users generally can find answers to the most common privacy questions and concerns by typing the word "privacy" into the relevant service's help section, which will usually direct the User to a privacy specific page or policy. The "help" section of the relevant service is the unique entry point for all Users' queries relating to their privacy or the processing of their User Information and provides User's the opportunity to contact customer support.

In case of doubt as to which channel to use to report privacy related concerns, Users can contact the European Data Protection Officer Online.

Customer support investigates and attempts to resolve concerns raised by Users. Employees responsible for addressing privacy related concerns work closely with the PayPal Global Privacy Team and reply to Users in accordance with PayPal's policies, procedures and guidance. If Users believe their concerns have not been addressed adequately, or if they did not get a response, they can request that their concern be escalated to the European Data Protection Officer. The legal privacy lead will be consulted and the compliance privacy lead will be apprised. Escalation paths shall be determined based upon the nature and scope of the concern and shall be forwarded to the appropriate team without delays. A response to the complaint shall be provided to the User within a reasonable timeframe, and in any case within a period of three (3) months after the date of inquiry, except in unusual circumstances or complex questions in which case the User will be informed that the reply will take longer than three (3) months.

The complaint handing mechanism does not prejudice Users' right to bring complaints before competent Data Protection Authorities or courts.

4. Third-Party Beneficiary Rights and Liability

EEA Users who suspect a breach of the User Corporate Rules outside the EEA have the right to claim enforcement of the User Corporate Rules as third party beneficiaries for Sections 2, 3, 4, 7 and 8 of the User Corporate Rules before the competent data protection authorities, before the courts of the Lead Group Member or before the courts of the Group Member acting as data exporter. These enforcement rights are in addition to other remedies or rights provided by PayPal or available under applicable law.

While it is not required, EEA Users are encouraged to first report their concern directly to the Group Member rather than the Data Protection Authorities or the courts. This enables an efficient and prompt response from the PayPal Group and minimizes possible delays from Data Protection Authorities or court procedures.

PayPal Europe S.à r.l. et Cie, S.C.A., a Luxembourg private limited liability company accepts responsibility for and agrees to oversee the Group Member's adherence to the User Corporate Rules. The Lead Group Member undertakes (i) to take the necessary action to remedy a breach committed by Group Members outside of the EEA; and (ii) to pay the compensation to EEA Users awarded by the Lead Data Protection Authority or Luxembourg courts for any damages directly resulting from the breach of the User Corporate Rules by Group Members outside the EEA, should the relevant Group Member be unable or unwilling to pay the compensation or comply with the order.

The Lead Group Member acknowledges and accepts that it carries the burden of proof with regard to an alleged breach of the User Corporate Rules.

The Lead Group (or any other Group Member) shall not be liable if it reasonably demonstrates, based on the available facts and taking into account the comments of the

User, that the non-EEA Group Member has not violated the User Corporate Rules or is not responsible for any damage alleged by the User.

5. Training

Group Members will ensure that all Employees Processing User Personal Data as well as those Employees that are involved in the design of tools that will be used to collect or process User Personal Data receive privacy and information security awareness training to emphasize and inform Employees of the need to protect and secure User Personal Data consistent with these User Corporate Rules.

Employees are required to complete online compliance training centered around the Code of Business Conduct & Ethics, which includes a section on data protection, on an annual basis. New Employees are required to complete the online compliance training upon starting their employment.

In addition to this online compliance training, the PayPal Global Privacy Team and the European Data Protection Officer conduct privacy and information security awareness trainings to emphasize and inform Employees of the need to protect and secure Personal Data. Such trainings are conducted on an annual basis or more frequent if circumstances require it.

The training Employees receive shall be adapted to their levels of access to User Personal Data, and additional training shall be provided to Employees with greater levels of access.

Group Members shall inform Employees that failure to comply with these User Corporate Rules may result in disciplinary actions and other actions permitted by applicable law. A copy of these User Corporate Rules and other relevant privacy and security related policies and procedures is available to Employees at any time via the company's Intranet. The User Corporate Rules are also included in the Code of Business Conduct & Ethics which all Employees are required to review and agree to abide by.

6. Audits and Monitoring

To help ensure compliance with these User Corporate Rules, the PayPal Global Privacy Compliance Team reviews, on an ongoing basis, Personal Data processing activities and practices. These activities are coordinated in close consultation with the European Data Protection Officer.

The Internal Audit team is an independent and objective advisor to management and the Board of Directors, which, through the audit committee, communicates audit findings to the Board of Directors, the privacy leads and to the European Data Protection Officer.

The Internal Audit team may conduct a review of activities or practices identified by the Global Privacy Team on a regular basis. The Internal Audit team, the privacy leads and the European Data Protection Officer, shall, if necessary, require that an action plan be executed to ensure compliance with the BCRs. To the extent that internal groups do not resolve matters adequately, the Group may appoint independent external auditors for further resolution.

The European Data Protection Officer, the PayPal Global Privacy Compliance Team or internal audit teams and external auditors develop detailed audit plans and schedules based upon the risk of the Processing.

Privacy audit findings will be available to competent DPAs. PayPal reserves the right to redact portions of the audit reports to ensure confidentiality of proprietary or other company confidential information.

7. Relationship between User Corporate Rules and National Law

With varying legal requirements throughout the world relating to data protection, the User Corporate Rules establish a consistent set of requirements to help ensure the appropriate Processing of User Personal Data. While the User Corporate Rules create a baseline requirement for Group Members to comply with, Group Members will comply with applicable laws that may impose a stricter standard than those set forth in these Corporate Rules.

Nothing in these User Corporate Rules affects a Group Members' obligations under applicable banking laws, in particular in relation to bank secrecy. If applicable law conflicts with these User Corporate Rules in that it might prevent a Group Member from fulfilling its obligations under the User Corporate Rules and has a substantial effect on the guarantees provided therein, the Group Member shall promptly notify the European Data Protection Officer, except where providing such information is prohibited by a law enforcement authority or law. The European Data Protection Officer, the privacy leads and the Lead Group Member shall determine the appropriate course of action and, in case of doubt, consult with the competent Data Protection Authority.

8. Mutual Assistance and Cooperation with Data Protection Authorities

Group Members will cooperate and assist each other to handle requests or complaints from Users with regard to these User Corporate Rules.

Group Members will respond diligently and appropriately to requests from Data Protection Authorities about the User Corporate Rules. If an Employee receives such a request from a Data Protection Authority, he or she should immediately inform the European Data Protection Officer.

Group Members will cooperate with inquiries and accept audits from competent Data Protection Authorities in the EEA in respect of compliance with these User Corporate Rules and will respect their decisions, consistent with applicable law and due process rights.

9. Updates of the Content of these User Corporate Rules and List of Bound Members

PayPal reserves the right to modify these User Corporate Rules as necessary, for example, to comply with changes in applicable laws, rules, regulations, PayPal practices, procedures and organizational structure or requirements imposed by relevant data protection authorities.

The PayPal Global Privacy Legal Team (under the leadership of the legal privacy lead), will propose any necessary changes to these User Corporate Rules. The PayPal Global Privacy Compliance Team (under the leadership of the compliance privacy lead) and the European Data Protection Officer must approve all changes to the User Corporate Rules and shall track all modifications to the User Corporate Rules as well as any change in the list of Group Members. Group Members shall report to the relevant Data Protection Authorities changes to the User Corporate Rules for formal approval and as required by applicable law.

The Lead Group Member will consult with the Lead Data Protection Authority regarding material changes to the User Corporate Rules that would affect data protection compliance or the operation of the User Corporate Rules. The Lead Group Member will communicate material changes to the User Corporate Rules and changes to the list of Group Members at least once a year to the Lead Data Protection Authority. The PayPal Global Privacy Team will work together to support the European Data Protection Officer who, in particular, will coordinate responses and promptly address comments, suggestions or objections to the changes raised by the Lead Data Protection Authority on behalf of PayPal. Any comments, suggestions or objections raised by other Data Protection Authorities will be communicated to the European Data Protection Officer by the Lead Data Protection Authority who will act on behalf of the other Data Protection Authorities.

Changes to the User Corporate Rules shall be applicable to all Group Members on the effective date of implementation. Group Members will provide notice of material changes to the User Corporate Rules to Users in accordance with the User's Service preferences either by mass email or by website posting with a clear warning to Users,

ahead of time, that the User Rules have changed. The Group Members shall post the revised User Corporate Rules on selected external websites or applications accessible by Users. Revisions to the User Corporate Rules are effective within a two month period after Group Members notify Users and posts the revised User Corporate Rules.

10. Publication

The User Corporate Rules shall be published and a link shall be made available on the Service's website or applications. Users may request a copy from The European Data Protection Officer (DPO), PayPal (Europe) S.à r.l et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg or Online.

11. Final provisions

Effective date: 25 May 2018

Contact: Users can raise any questions or concerns in relation to these User Corporate Rules by contacting:

The European Data Protection Officer (DPO)

PayPal (Europe) S.à r.l et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg

12. Definitions

Group Members shall interpret the User Corporate Rules in a way that is most consistent with the basic concepts of the principles of EU Directive 95/46/EC or any superseding directive or regulation.

For the purpose of these User Corporate Rules, the following definitions apply:

Board of Directors means the board of directors of the Lead Group Member.

Data Protection Authorities means the public authorities that are responsible for monitoring and enforcing the application within their respective territory of the national laws adopted by the EEA Member States - pursuant to the EU Data Protection Directive (95/46/EC).

EEA means the European Economic Area, currently comprising the EU Member States, Iceland, Liechtenstein and Norway.

Employee means employees, workers, trainees and other personnel or staff members, including contingent or temporary workers, alternate work force, or contractors of a Group Member, whether employed or engaged on a full or part-time basis and irrespective of the type of employment or engagement.

European Data Protection Officer (DPO) means the employee who is appointed by and reports to the management of the Lead Group Member and also serves as a member of the PayPal Global Privacy Legal Team. The European DPO is located in Luxembourg.

Group Member means a PayPal Group entity that has executed a copy of the IGA.

IGA means Intra-Group Agreement

Lead Data Protection Authority means the "Commission nationale pour la protection des données" ("CNPD") in Luxembourg.

Lead Group Member means PayPal (Europe) S.à r.l. & Cie, S.C.A., a Luxembourg private limited liability company.

PayPal Global Privacy Team means the coordinated PayPal Global Privacy Compliance Team and the PayPal Global Privacy Legal Team.

PayPal Global Privacy Compliance Team means members of the Compliance Organization dealing specifically with the compliance and operation of the PayPal privacy program.

PayPal Global Privacy Legal Team means members of the Legal Department dealing specifically with privacy and data protection.

PayPal Group means PayPal Holdings, Inc. ("PayPal") and any entity directly or indirectly Controlled by PayPal that processes User Information, where Control means the ownership of greater than fifty percent (50%) of the voting power to elect the directors of the company, or greater than fifty percent (50%) of the ownership interest in the company.

Personal Data means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

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

Processor means any natural or legal person that Processes Personal Data on behalf of a Group Member.

Sensitive Personal Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, information relating to criminal offences, or information concerning health or sex life.

Service means a website, application, or other product or service offered by a PayPal Group for use by a User.

Third Party shall mean any natural or legal person, public authority, agency or any other body other than the User, the Group Member, the Processor and the individuals who, under the direct authority of the Group Member or the Processor, such as Employees, are authorized to Process Personal Data.

User means past and existing customers, prospects, investors, business partners, and merchants.

User Personal Data means Personal Data relating to Users.

Status disclosure

PayPal is deemed authorised and regulated by the Financial Conduct Authority. The nature and extent of consumer protections may differ from those for firms based in the UK. Details of the Temporary Permissions Regime, which allows EEA-based firms to operate in the UK for a limited period while seeking full authorisation, are available on the Financial Conduct Authority's website.