PayPal

>> Alle AGB anzeigen

PayPal-Datenschutzvorschriften für Nutzerdaten

Das Ziel der PayPal-Gruppe ist es, einheitliche, angemessene und globale Datenschutzstandards für den Umgang mit allen personenbezogenen Nutzerdaten in der gesamten PayPal-Gruppe anzuwenden. Diese Datenschutzvorschriften für Nutzerdaten gelten für alle personenbezogenen Nutzerdaten, die von Gruppenmitgliedern weltweit verarbeitet werden.

Nutzer geben ihre personenbezogenen Daten an die Gruppenmitglieder weltweit weiter, um die von der Gruppe angebotenen Dienste zu nutzen. Die meisten personenbezogenen Nutzerdaten werden in den USA erfasst und gespeichert. Das globale Geschäft von PayPal erfordert, dass personenbezogene Nutzerdaten an andere PayPal-Unternehmen in den USA und anderen Ländern weitergegeben werden, in denen PayPal derzeit präsent ist oder sein möchte.

Derzeit können Mitarbeiter in den folgenden EWR-Ländern auf personenbezogene Nutzerdaten zugreifen: Belgien, Deutschland, Frankreich, Irland, Italien, Luxemburg, Niederlande, Polen, Schweden und Spanien.

Auch Mitarbeiter, die derzeit in den folgenden Nicht-EU-Ländern ansässig sind, können auf personenbezogene Nutzerdaten zugreifen: Argentinien, Australien, Brasilien, Britische Jungferninseln, China, Großbritannien, Hongkong, Indien, Indonesien, Israel, Japan, Kanada, Malaysia, Mauritius, Mexiko, Philippinen, Republik Korea, Russland, Schweiz, Singapur, Taiwan, Türkei und USA.

PayPal verpflichtet sich, die Nutzerinformationen unabhängig davon, wo sich die personenbezogenen Daten befinden, angemessen zu schützen und die personenbezogenen Nutzerdaten, die außerhalb des EWR übermittelt werden, angemessen zu schützen.

Diese Länderliste kann sich ändern, wenn das Unternehmen expandiert.

1. Datenschutz-Führungsstruktur und Verantwortlichkeiten

Die Datenschutzvorschriften für Nutzerdaten werden durch eine Vereinbarung (die "IGA") zwischen PayPal (Europe) S.à r.l. & Cie, S.C.A. ("Führendes Gruppenmitglied") und anderen Unternehmen der PayPal-Gruppe rechtsverbindlich. Die IGA verlangt von den Gruppenmitgliedern die Einhaltung dieser Datenschutzvorschriften für Nutzerdaten.

Gruppenmitglieder fordern von ihren Mitarbeitern die Einhaltung dieser Datenschutzvorschriften für Nutzerdaten beim Umgang mit personenbezogenen Nutzerdaten.

Führungskräfte und die Geschäftsleitung der PayPal-Gruppe sind verantwortlich für die Einhaltung der Datenschutzvorschriften für Nutzerdaten; dies umfasst auch die Sicherstellung, dass Mitarbeiter die Datenschutzvorschriften für Nutzerdaten kennen und einhalten.

Der Leiter für Datenschutz-Compliance leitet das Datenschutzprogramm von PayPal. Er/sie hat eine leitende Position bei PayPal Holdings, Inc. inne und ist dem Chief Compliance Officer oder dem ranghöchsten Mitglied der Geschäftsleitung, das die Compliance-Abteilung bei PayPal leitet, direkt unterstellt. Der Leiter für Datenschutz-Compliance überwacht das PayPal Global Privacy Compliance-Team und arbeitet mit anderen internen Organisationen oder Teams zusammen, z.B. Geschäftsbetrieb, Informationssicherheit, Compliance, Risikomanagement und interne Prüfung, um konsistente Datenschutzkommunikationen, -praktiken und -richtlinien für die gesamte PayPal-Gruppe sicherzustellen. Das PayPal Global Privacy Compliance-Team erarbeitet eine Compliance-Strategie, koordiniert deren Implementierung in der gesamten PayPal-Gruppe und überprüft die Einhaltung der betrieblichen Vorschriften. Das PayPal Global Privacy Compliance-Team hat direkte und indirekte Vertreter in der gesamten PayPal-Gruppe, die unter anderem dazu beitragen, die Einhaltung der Datenschutzvorschriften für Nutzerdaten und der geltenden Datenschutzgesetze zu gewährleisten.

Der rechtliche Leiter für Datenschutz beaufsichtigt das PayPal Global Privacy Legal-Team und ist dem Chief Legal Officer oder dem ranghöchsten Mitglied der Geschäftsleitung, das die Rechtsabteilung bei PayPal leitet, direkt unterstellt. Der rechtliche Leiter für Datenschutz definiert die Verpflichtungen des Unternehmens gemäß den geltenden Datenschutzgesetzen und diesen Datenschutzvorschriften für Nutzerdaten. Der rechtliche Leiter für Datenschutz und das PayPal Global Privacy Legal-Team arbeiten eng mit dem Leiter für Datenschutz-Compliance und dem PayPal Global Compliance Privacy-Team zusammen und interagieren mit anderen internen Organisationen und Teams, z.B. Rechtsabteilung, Geschäftsbetrieb, Informationssicherheit und Risikomanagement, um Rechtsberatung bereitzustellen und weltweit die rechtlichen und regulatorischen Auswirkungen der sich weiterentwickelnden Datenschutzangelegenheiten für die gesamte PayPal-Gruppe zu interpretieren.

Das PayPal Global Privacy Compliance-Team und das PayPal Global Privacy Legal-Team bilden gemeinsam das PayPal Global Privacy-Team.

Der Europäische Datenschutzbeauftragte mit Sitz in Luxemburg wird von der Geschäftsführung von PayPal (Europe) S.à r.l. et Cie, S.C.A. ernannt und ist ihr direkt unterstellt. Der Europäische Datenschutzbeauftragte fungiert als Ansprechpartner für die EWR-Datenschutzbehörden und hat unter anderem folgende Aufgaben: Gruppenmitglieder und ihre Mitarbeiter, die personenbezogene Daten verarbeiten, über ihre Verpflichtungen gemäß den Datenschutzgesetzen zu informieren und zu beraten, um

die Einhaltung dieser Datenschutzvorschriften für Nutzerdaten zu gewährleisten; mit dem PayPal Global Privacy-Team zusammenarbeiten, um die Einhaltung der Datenschutzgesetze und der damit verbundenen Richtlinien der Gruppenmitglieder zu überwachen; und den Gruppenmitgliedern auf deren Anforderung hin Rechtsberatung bezüglich der Datenschutz-Folgenabschätzung und deren Durchführung zur Verfügung zu stellen.

2. Grundsätze für die Verarbeitung von personenbezogenen Nutzerdaten

Gruppenmitglieder beachten die folgenden Verarbeitungsgrundsätze für personenbezogene Nutzerdaten.

2.1 Zweckbindung

Die personenbezogenen Nutzerdaten dürfen nur für bestimmte, eindeutige und rechtmäßige Zwecke verarbeitet werden. Insbesondere können personenbezogenen Nutzerdaten zu folgenden Zwecken verarbeitet werden:

- Anbieten und Bereitstellen von Diensten auf Anfrage der Nutzer, einschließlich der Eröffnung eines Kontos;

- Verbessern der Dienste und Entwickeln neuer Dienste;

- Beilegen von Konflikten, Verwalten von Rechtsstreitigkeiten, Beheben von Problemen und Bereitstellen von Kundenservice;

- Durchführen des Risikomanagements;

- Verarbeiten von Transaktionen und Einziehen von fälligen Gebühren;

- Überprüfen der Kreditwürdigkeit und Zahlungsfähigkeit;

- Messen des Interesses der Nutzer an Diensten, Einholen von Nutzer-Feedback und -Meinungen in Bezug auf Dienste sowie Informieren von Nutzern über Online- und Offline-Angebote, Dienste und Neuerungen;

- Anpassen von Kundenerfahrungen;

- Erkennen von und Schützen vor Fehlern, Betrug und anderen kriminellen Aktivitäten;

- Erfüllen der rechtlichen, vertraglichen oder regulatorischen Verpflichtungen der PayPal-Gruppe;

- Durchsetzen der Nutzungsbedingungen für den Dienst und wie anderweitig für Nutzer zum Zeitpunkt der Erfassung und in den Datenschutzgrundsätzen für den Dienst beschrieben;

- Wahren der Sicherheit, Integrität und Verfügbarkeit der Dienste und des Netzwerks der PayPal-Gruppe; und

- Schutz der gesetzlichen Rechte und Interessen der PayPal-Gruppe, darin eingeschlossen, aber nicht beschränkt auf die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Die Verarbeitung personenbezogener Nutzerdaten für andere Zwecke erfolgt vorbehaltlich der vorherigen Zustimmung des PayPal Global Privacy Legal-Teams. Im Zweifelsfall holen die Gruppenmitglieder Rat beim PayPal Global Privacy Legal-Team ein.

Die personenbezogenen Nutzerdaten dürfen nicht in einer Weise verarbeitet werden, die mit den oben genannten Zwecken nicht vereinbar ist, es sei denn, es gibt nach dem geltenden Recht des Gruppenmitglieds im EWR-Raum, das für die Sammlung und/oder Übermittlung der personenbezogenen Nutzerdaten verantwortlich ist, eine Rechtsgrundlage dafür.

2.2 Datenqualität und Verhältnismäßigkeit

Personenbezogene Nutzerdaten müssen:

- sachlich richtig und, soweit erforderlich, auf dem neuesten Stand sein;
- angemessen, relevant und auf das für die Zwecke, für die sie verarbeitet werden, notwendige Maß beschränkt sein; und
- nur so lange gespeichert werden, wie dies für die Zwecke erforderlich ist, für die sie ursprünglich erfasst oder weiterverarbeitet wurden.

Personenbezogene Nutzerdaten, die für die Zwecke, für die sie verarbeitet wurden, nicht mehr benötigt werden, werden gelöscht, vernichtet oder anonymisiert, es sei denn, es besteht ein Rechtsgrund für die weitere Verarbeitung oder Aufbewahrung nach geltendem Recht.

2.3 Rechtsgrundlagen für die Verarbeitung

Die Gruppenmitglieder stellen sicher, dass personenbezogene Nutzerdaten fair und rechtmäßig und insbesondere auf der Grundlage von mindestens einem der folgenden Rechtsgründe verarbeitet werden:

- Eindeutige Zustimmung des Nutzers;

- die Verarbeitung ist erforderlich, um einen Vertrag zu erfüllen, an dem der Nutzer beteiligt ist, oder um auf Anfrage des Nutzers vor Abschluss eines Vertrags Maßnahmen zu ergreifen;
- die Verarbeitung ist erforderlich, um einer rechtlichen Verpflichtung nachzukommen, der die Gruppenmitglieder unterliegen;
- die Verarbeitung ist erforderlich, um die lebenswichtigen Interessen des Nutzers zu schützen;
- die Verarbeitung ist für die Durchführung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung von öffentlicher Gewalt erfolgt, die Gruppenmitgliedern oder einer dritten Partei, gegenüber der die Daten offengelegt werden, übertragen wurde; oder
- die Verarbeitung ist erforderlich, um die berechtigten Interessen des Gruppenmitglieds oder der dritten Partei oder Parteien, gegenüber denen die Daten offengelegt werden, zu wahren, es sei denn, die Grundrechte und Grundfreiheiten des Nutzers überwiegen.

Im Allgemeinen erfassen Gruppenmitglieder keine sensiblen personenbezogenen Nutzerdaten. Wenn eine solche Erfassung erforderlich ist oder wenn Nutzer Informationen freiwillig bereitstellen, verpflichten sich die Gruppenmitglieder sicherzustellen, dass eine Verarbeitung von sensiblen personenbezogenen Nutzerdaten nur aus mindestens einem der folgenden Gründe erfolgt:

- Ausdrückliche Zustimmung des Nutzers;
- die Verarbeitung ist erforderlich, um die lebenswichtigen Interessen des Nutzers oder einer anderen Person zu schützen und der Nutzer ist aus körperlichen oder rechtlichen Gründen außerstande, seine/ihre Zustimmung zu geben;
- die Verarbeitung bezieht sich auf personenbezogene Nutzerdaten, die der Nutzer offensichtlich öffentlich gemacht hat; oder
- die Verarbeitung ist erforderlich, um Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen.

Wenn die Verarbeitung eine automatische Entscheidungsfindung beinhaltet ("Automatisierte Entscheidungen"), treffen die Gruppenmitglieder angemessene Maßnahmen zum Schutz der berechtigten Interessen des Nutzers treffen, wie zum Beispiel die Möglichkeit, dass ein Kundenservice-Mitarbeiter die Entscheidung individuell überprüft und dem Nutzer erlaubt, seinen eigenen Standpunkt darzulegen. Wenn der Nutzer der automatisierten Entscheidung weiterhin widerspricht, eskaliert der Kundenservice-Mitarbeiter die Angelegenheit an den EU-Datenschutzbeauftragten. Gegebenenfalls wird der rechtliche Leiter für Datenschutz konsultiert und der Leiter für Datenschutz-Compliance benachrichtigt.

2.4 Transparenz

Wenn Gruppenmitglieder personenbezogene Nutzerdaten erfassen, müssen sie die Nutzer über Folgendes informieren:

- Name und Anschrift des Gruppenmitglieds, das für die ursprüngliche Erfassung und Verarbeitung verantwortlich ist;
- die Kategorien der betroffenen personenbezogenen Nutzerdaten;
- die beabsichtigten Verarbeitungszwecke;
- die Kategorien der die personenbezogenen Nutzerdaten empfangenden Auftragsverarbeiter und Dritten;
- ob die Beantwortung von Fragen verpflichtend oder freiwillig ist sowie über die möglichen Konsequenzen bei Nichtbeantwortung;
- das Bestehen von Rechten des Nutzers; und
- im Falle von automatisierten Entscheidungen die entsprechende Logik.

Gruppenmitglieder können die Informationen in einer Datenschutzrichtlinie für den Dienst bereitstellen, auf die über einen Link zugegriffen werden kann und/oder die an prominenter Stelle auf jeder Dienst-Website oder -Anwendung sowie während der Registrierung angezeigt wird. Die Informationspflicht besteht nicht, wenn Nutzer die Informationen bereits kennen.

Wenn sich die Bereitstellung von Informationen als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden wäre, können die Gruppenmitglieder die Bereitstellung der Information unterlassen. Dies wäre nur der Fall bei personenbezogenen Nutzerdaten, die nicht direkt beim Nutzer eingeholt wurden.

In Ausnahmefällen kann die Bereitstellung der Informationen ausgesetzt oder ganz weggelassen werden, z.B. im Rahmen von Untersuchungen fehlerhaften Verhaltens, zwecks Einhaltung der geltenden Gesetze oder wenn die Bereitstellung von Informationen die Integrität der Untersuchung gefährden könnte.

2.5 Vertraulichkeit und Sicherheit

Gruppenmitglieder setzen entsprechend der Menge und Vertraulichkeit der personenbezogenen Nutzerdaten physische, technische und organisatorische Sicherheitskontrollen ein, um eine unbefugte Verarbeitung zu verhindern, darin eingeschlossen, jedoch nicht beschränkt auf unbefugten Zugriff, Erwerb und Verwendung, Verlust, Zerstörung oder Beschädigung von personenbezogenen Nutzerdaten. Die Gruppenmitglieder setzen Verschlüsselungen, Firewalls, Zugangsbeschränkungen, Standards und andere Maßnahmen ein, um die Informationen des Nutzers vor unbefugtem Zugriff zu schützen. Der physische und logische Zugriff auf elektronische und gedruckte Dateien wird basierend auf beruflichen Verantwortlichkeiten und geschäftlichen Anforderungen weiter eingeschränkt.

2.6 Entscheidungen und Rechte der Nutzer

Nutzer können auf die meisten personenbezogenen Nutzerdaten, die sie betreffen und die von den Gruppenmitgliedern mithilfe des entsprechenden Online-Tools oder Self-Service-Prozesses über die Website oder Anwendung des Diensts verwaltet werden, zugreifen und diese berichtigen.

In allen Fällen haben Nutzer das Recht, einen Anforderung auf Zugriff der Daten einer betroffenen Person zu stellen, um eine Kopie der personenbezogenen Nutzerdaten anzuzeigen oder zu erhalten, die nicht über die Website oder Anwendung des Diensts zugänglich sind. Nutzer sollten sich an den Kundenservice wenden, indem sie den Anweisungen auf der Website oder in der Anwendung des Diensts folgen. Gruppenmitglieder werden die Anträge innerhalb der nach geltendem Recht vorgeschriebenen Fristen bearbeiten, es sei denn, das geltende Recht sieht eine Ausnahme von dieser Verpflichtung vor. Nutzer können aufgefordert werden, ihre Identität nachzuweisen, und wenn es das geltende Recht erlaubt, kann auch eine Servicegebühr erhoben werden.

Nutzer können auch eine Berichtigung ihrer Daten verlangen, wenn diese unvollständig oder fehlerhaft sind. Die Gruppenmitglieder werden dieser Anforderung nachkommen und die Nutzer benachrichtigen, sobald ihre Daten berichtigt worden sind. Die Gruppenmitglieder werden Dritte, denen gegenüber die Daten des Nutzers offengelegt wurden, über die Berichtigung dieser Daten informieren, sofern sich dies nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert.

Aus zwingenden legitimen Gründen können Nutzer der Verarbeitung ihrer personenbezogenen Nutzerdaten widersprechen. Die Gruppenmitglieder kommen solchen Anforderungen nach, es sei denn, die Aufbewahrung personenbezogener Nutzerdaten ist gesetzlich vorgeschrieben oder für die Verteidigung der PayPal-Gruppe gegen Rechtsansprüche erforderlich. Die Nutzer werden über das Ergebnis ihrer Anforderung und die von den Gruppenmitgliedern getroffenen Maßnahmen informiert.

Darüber hinaus können Nutzer die Schließung ihrer Konten beantragen, indem sie den Anweisungen auf der Website oder in der Anwendung des Diensts folgen. Die Gruppenmitglieder werden die Informationen eines Nutzers aus einem Dienst entfernen oder anonymisieren, sobald dies unter Berücksichtigung der Kontoaktivitäten möglich ist. In einigen Fällen können Gruppenmitglieder die Schließung eines Kontos verzögern oder personenbezogene Nutzerdaten speichern, um eine Untersuchung durchzuführen oder wenn dies gesetzlich erforderlich ist. Gruppenmitglieder können auch Nutzerinformationen von geschlossenen Konten aufbewahren, um Betrug zu erkennen und zu verhindern, zur Zahlung fällige Gebühren einzutreiben, Rechtsstreitigkeiten beizulegen, Probleme zu beheben, bei Untersuchungen behilflich zu sein, Risiken zu verwalten, die Nutzungsbedingungen eines Diensts durchzusetzen, gesetzliche oder regulatorische Anforderungen zu erfüllen und andere nach geltendem Recht zulässige Maßnahmen zu ergreifen. Die Daten werden so aufbewahrt, dass eine Identifizierung der betroffenen Personen nur so lange möglich ist, wie dies für die Zwecke, für welche die Daten erhoben wurden oder für die sie weiterverarbeitet werden, erforderlich ist; die Daten werden gelöscht, sobald der zugrunde liegende Grund für ihre Aufbewahrung bearbeitet oder gelöst wurde.

Die Gruppenmitglieder können personenbezogene Nutzerdaten verwenden, um Nutzern gemäß geltendem Recht Kommunikationen basierend auf ihren Interessen zukommen zu lassen; hiervon ausgenommen sind diejenigen Nutzer, die sich gegen den Erhalt

bestimmter Mitteilungen entschieden haben. Nutzern, die keine Marketing-Kommunikationen von der PayPal-Gruppe erhalten möchten, werden leicht zugängliche Mittel angeboten, um dem Erhalt weiterer Werbung zu widersprechen, beispielsweise in ihren Kontoeinstellungen oder indem sie den Anweisungen in einer E-Mail oder einem Link in der Kommunikation folgen.

Nutzer können die oben genannten Rechte ausüben, indem sie den Kundenservice kontaktieren. Wenn die Identität eines Nutzers schwer zu bestätigen ist, können die Gruppenmitglieder vom Nutzer einen zusätzlichen Identitätsnachweis verlangen.

2.7 Offenlegung personenbezogener Daten

Gruppenmitglieder können personenbezogene Nutzerdaten im Rahmen der üblichen Geschäftstätigkeit an andere Gruppenmitglieder weltweit zu den in Abschnitt 2.1 genannten Zwecke weitergeben.

In Übereinstimmung mit geltenden Gesetzen, Abkommen oder geltenden internationalen Übereinkünften können Gruppenmitglieder personenbezogene Daten an Strafverfolgungs- und Aufsichtsbehörden weitergeben, wenn dies in einer demokratischen Gesellschaft erforderlich ist, um die nationale Sicherheit, Verteidigung, öffentliche Sicherheit, Prävention, Untersuchung, Erkennung und Verfolgung von Straftaten sicherzustellen und insbesondere um auf internationaler und/oder nationaler Ebene festgesetzte Sanktionen sowie Vorschriften zur Steuermeldung und zur Bekämpfung von Geldwäsche einzuhalten.

Gruppenmitglieder dürfen personenbezogene Nutzerdaten nur mit der ausdrücklichen und unmissverständlichen Einverständniserklärung des Nutzers an Dritte für deren eigenen Marketingzwecke verkaufen oder vermieten. Gruppenmitglieder können personenbezogene Nutzerdaten gemäß den Anweisungen oder der Zustimmung des Nutzers an Dritte weitergeben (soweit dies nach geltendem Recht zulässig ist).

Bei der Übermittlung von personenbezogenen Nutzerdaten an Auftragsverarbeiter unterliegen die Auftragsverarbeiter vor Beginn der Arbeit und vor der Übermittlung personenbezogener Nutzerdaten einer Risikobewertung in Bezug auf Datenschutz und Informationssicherheit. Der Umfang der Bewertung hängt davon ab, wie sensibel die verarbeiteten personenbezogenen Nutzerdaten sind. Auftragsverarbeiter, darunter auch Gruppenmitglieder, die als Auftragsverarbeiter intervenieren, müssen eine Vereinbarung mit relevanten Gruppenmitgliedern treffen, um angemessene Sicherheitsmaßnahmen in Bezug auf Datenschutz und Informationssicherheit zu gewährleisten. Eine solche Vereinbarung enthält Klauseln, die eine angemessene Verwendung der personenbezogenen Nutzerdaten sowie Sicherheitsmaßnahmen, die der Menge, Art und Sensibilität der betreffenden personenbezogenen Nutzerdaten entsprechen, gewährleisten. Die vertraglich festgelegten Sicherheitsmaßnahmen müssen mindestens die folgenden Punkte abdecken:

- Anforderungen zur Einhaltung der Gesetze und zur Verarbeitung personenbezogener Nutzerdaten nur in Übereinstimmung mit den Bedingungen der Vereinbarung und nur auf Anweisung der betreffenden Gruppenmitglieder;
- angemessene technische und organisatorische Maßnahmen, die an die Sensibilität der betroffenen personenbezogenen Nutzerdaten angepasst sind;
- ein Recht auf Überprüfung der Einhaltung der vertraglichen Garantien seitens der Auftragsverarbeiter;
- Benachrichtigungspflicht bei Sicherheitsverletzungen; und
- Bestimmungen zur Sanierung, falls der Auftragsverarbeiter seinen gesetzlichen oder vertraglichen Verpflichtungen nicht nachkommt.

Die Vereinbarungen müssen Bestimmungen enthalten, die sicherstellen, dass die Nichteinhaltung von Bedingungen der Vereinbarung neben anderen vertraglich genannten Rechtsmitteln die Aussetzung oder Kündigung der Vereinbarung zur Folge haben kann.

Die Bewertung hinsichtlich Datenschutz und Informationssicherheit ist für die Auftragsverarbeiter, die bereits einer solchen Bewertung unterzogen wurden, nicht verpflichtend, es sei denn, die Verarbeitungstätigkeiten umfassen Tätigkeiten mit hohem Risiko unter Berücksichtigung der Art und Menge der personenbezogenen Daten und der Art der betreffenden Verarbeitungstätigkeiten.

Ungeachtet des Vorstehenden muss ein Gruppenmitglied Folgendes sicherstellen, wenn Gruppenmitglieder personenbezogene Nutzerdaten aus dem EWR an Dritte oder an Auftragsverarbeiter übermitteln, die keine Gruppenmitglieder sind und (i) die sich in Ländern befinden, die kein angemessenes Schutzniveau bieten (im Sinne der Richtlinie 95/46/EG), (ii) die nicht durch genehmigte verbindliche interne Datenschutzvorschriften abgedeckt sind oder (iii) die keine anderen Vorkehrungen getroffen haben, welche die Angemessenheitsanforderungen der EU erfüllen würden:

- in Zusammenhang mit Dritten, dass diese angemessene vertragliche Kontrollen, wie z.B. von der Europäischen Kommission genehmigte Standardvertragsklauseln umsetzen, mit denen für ein Schutzniveau entsprechend diesen Datenschutzvorschriften für Nutzerdaten gesorgt wird, oder alternativ, dass die Übermittlung (i) mit der eindeutigen Zustimmung des Nutzers erfolgt, (ii) zum Abschluss oder zur Erfüllung eines mit dem Nutzer geschlossenen Vertrags erforderlich ist, (iii) aus wichtigen Gründen des öffentlichen Interesses notwendig oder gesetzlich erforderlich ist oder (iv) zum Schutz der lebenswichtigen Interessen des Nutzers erforderlich ist;
- Auftragsverarbeiter setzen vertragliche Kontrollen, wie z.B. von der Europäischen Kommission genehmigte Standardvertragsklauseln, um, mit denen für ein Schutzniveau entsprechend diesen Datenschutzvorschriften für Nutzerdaten gesorgt wird.

3. Beschwerdeverfahren

Wenn Nutzer glauben, dass die Verarbeitung ihrer personenbezogenen Nutzerdaten gegen die Datenschutzvorschriften für Nutzerdaten verstößt, können sie ihre Bedenken dem Kundenservice des jeweiligen Gruppenmitglieds über die entsprechende Website des Diensts, E-Mail oder wie anderweitig in den jeweiligen Nutzungsbedingungen angegeben melden. In der Regel finden Nutzer Antworten auf die häufigsten Fragen und Bedenken, indem sie das Wort "Datenschutz" in den Hilfe-Bereich des jeweiligen Diensts eingeben. Von dort gelangen sie in der Regel zu bestimmten Datenschutzseiten oder -richtlinien. Der "Hilfe"-Abschnitt des jeweiligen Diensts ist der zentrale Einstiegspunkt für alle Nutzerfragen in Bezug auf Datenschutz oder die Verarbeitung ihrer Nutzerdaten und bietet Nutzern die Möglichkeit, Kontakt zum Kundenservice aufzunehmen.

Im Zweifelsfall können sich Nutzer online mit dem Europäischen Datenschutzbeauftragten in Verbindung setzen, um die Bedenken bezüglich des Datenschutzes zu melden.

Der Kundenservice untersucht die Anliegen von Kunden und versucht, diese zu lösen. Mitarbeiter, die für die Bearbeitung von datenschutzbezogenen Anliegen verantwortlich sind, arbeiten eng mit dem PayPal Global Privacy-Team zusammen und antworten auf Nutzeranfragen in Übereinstimmung mit den Richtlinien, Verfahren und Anweisungen von PayPal. Wenn Kunden glauben, dass ihr Anliegen nicht zufriedenstellend gelöst wurde, oder wenn sie keine Antwort erhalten, können sie darum bitten, dass es an den Europäischen Datenschutzbeauftragten weitergeleitet wird. Der rechtliche Leiter für Datenschutz wird hinzugezogen, und der Leiter für Datenschutz-Compliance wird benachrichtigt. Die Eskalationswege werden auf Grundlage von Art und Umfang des Anliegens festgelegt und unverzüglich an das zuständige Team weitergeleitet. Der Nutzer erhält innerhalb einer angemessenen Frist eine Antwort auf seine Beschwerde, in jedem Fall jedoch innerhalb von drei (3) Monaten nach dem Tag der Anfrage, es sei denn, es liegen ungewöhnliche Umstände oder komplexe Fragen vor; in diesem Fall wird der Nutzer darüber informiert, dass die Antwort länger als drei (3) Monate in Anspruch nehmen wird.

Das Recht des Nutzers, Beschwerden bei der zuständigen Datenschutzbehörde oder vor Gericht einzureichen, bleibt vom Beschwerdebearbeitungsverfahren unberührt.

4. Rechte und Verbindlichkeiten von Dritten

EWR-Nutzer, die einen Verstoß gegen die Datenschutzvorschriften für Nutzerdaten außerhalb des EWR vermuten, haben Anspruch auf Durchsetzung der Datenschutzvorschriften für Nutzerdaten als Drittbegünstigte für die Abschnitte 2, 3, 4, 7 und 8 der Datenschutzvorschriften für Nutzerdaten, entweder vor den zuständigen Datenschutzbehörden, vor den Gerichten des führenden Gruppenmitglieds oder vor den Gerichten des Gruppenmitglieds, das als Datenexporteur agiert. Diese Durchsetzungsrechte gelten zusätzlich zu anderen von PayPal eingeräumten oder gesetzlich geltenden Rechtsmitteln und Rechten.

EWR-Nutzern wird empfohlen (sie sind jedoch nicht dazu verpflichtet), ihre Anliegen zunächst direkt an das betreffende Gruppenmitglied anstatt an die Datenschutzbehörden oder Gerichte heranzutragen. Dies ermöglicht eine effiziente und schnelle Reaktion seitens der PayPal-Gruppe und beschränkt etwaige Verzögerungen aufseiten der Datenschutzbehörden oder Gerichte auf ein Minimum.

PayPal Europe S.à r.l. et Cie, S.C.A., eine luxemburgische Gesellschaft mit beschränkter Haftung, trägt die Verantwortung für die Einhaltung der Datenschutzvorschriften für Nutzerdaten und verpflichtet sich, diese Einhaltung zu überwachen. Das führende Gruppenmitglied verpflichtet sich, (i) erforderliche Maßnahmen zur Heilung eines von Gruppenmitgliedern außerhalb des EWR begangenen Verstoßes zu ergreifen und (ii) die von der leitenden Datenschutzbehörde oder den luxemburgischen Gerichten gewährten Entschädigungen an EWR-Nutzer für Schäden zu zahlen, die sich direkt aus dem Verstoß gegen die Datenschutzvorschriften für Nutzerdaten durch Gruppenmitglieder außerhalb des EWR ergeben, sollte das betreffende Gruppenmitglied nicht in der Lage oder willens sein, die Entschädigung zu zahlen oder der Anordnung Folge zu leisten.

Das leitende Gruppenmitglied erkennt an und akzeptiert, dass es die Beweislast in Bezug auf mutmaßliche Verstöße gegen die Datenschutzvorschriften für Nutzerdaten trägt.

Das leitende Gruppenmitglied (oder ein anderes Gruppenmitglied) kann nicht haftbar gemacht werden, wenn es auf Grundlage der verfügbaren Fakten und unter Berücksichtigung der Aussagen des Nutzers nachweisen kann, dass das Nicht-EWR-Gruppenmitglied nicht gegen die Datenschutzvorschriften für Nutzerdaten verstoßen hat oder nicht für die vom Nutzer behaupteten Schäden verantwortlich ist.

5. Schulung

Die Gruppenmitglieder tragen dafür Sorge, dass alle Mitarbeiter, die personenbezogene Nutzerdaten verarbeiten, sowie diejenigen Mitarbeiter, die an der Entwicklung von Tools zur Erfassung oder Verarbeitung personenbezogener Nutzerdaten beteiligt sind, Schulungen zu Datenschutz und Informationssicherheit erhalten, in denen sie auf die Notwendigkeit des Schutzes personenbezogener Nutzerdaten in Einklang mit diesen Datenschutzvorschriften für Nutzerdaten aufmerksam gemacht werden.

Mitarbeiter sind verpflichtet, jedes Jahr eine Online-Compliance-Schulung zum Verhaltens- und Ethikkodex des Unternehmens, die unter anderem einen Abschnitt zum Thema Datenschutz umfasst, zu absolvieren. Neue Mitarbeiter sind verpflichtet, die Online-Compliance-Schulung zu Beginn ihrer Beschäftigung abzuschließen.

Neben dieser Online-Schulung führen das PayPal Global Privacy-Team und der Europäische Datenschutzbeauftragte auch andere Schulungen zu Datenschutz und Informationssicherheit durch, um Mitarbeiter auf die Notwendigkeit des Schutzes

personenbezogener Daten aufmerksam zu machen. Diese Schulungen werden jährlich durchgeführt oder häufiger, sollten die Umstände dies erfordern.

Die Schulungen, die Mitarbeiter erhalten, werden an deren jeweiligen Zugriffsrechte für personenbezogene Nutzerdaten angepasst; Mitarbeiter mit höheren Zugriffsrechten erhalten zusätzliche Schulungen.

Die Gruppenmitglieder setzen ihre Mitarbeiter darüber in Kenntnis, dass Verstöße gegen die Datenschutzvorschriften für Nutzerdaten Disziplinarmaßnahmen und andere nach geltendem Recht zulässige Maßnahmen nach sich ziehen können. Eine Kopie dieser Datenschutzvorschriften für Nutzerdaten und andere relevante Datenschutz- und Sicherheitsrichtlinien und -verfahren stehen Mitarbeitern jederzeit im Intranet des Unternehmens zur Verfügung. Die Datenschutzvorschriften für Nutzerdaten sind auch im Verhaltens- und Ethikkodex des Unternehmens enthalten; alle Mitarbeiter sind verpflichtet, diesen Verhaltens- und Ethikkodex zu lesen und sich zu dessen Einhaltung zu verpflichten.

6. Überprüfungen und Überwachung

Zur Gewährleistung der Einhaltung der Datenschutzvorschriften für Nutzerdaten prüft das PayPal Global Privacy Compliance-Team laufend die Aktivitäten und Praktiken zur Verarbeitung personenbezogener Daten. Diese Aktivitäten werden in enger Abstimmung mit dem Europäischen Datenschutzbeauftragten koordiniert.

Das interne Prüfungsteam ist ein unabhängiger und objektiver Berater der Geschäftsführung und des Verwaltungsrats und übermittelt über den Prüfungsausschuss die Prüfungsergebnisse an den Verwaltungsrat, die Leiter für Datenschutz und den Europäischen Datenschutzbeauftragten.

Das interne Prüfungsteam kann regelmäßig eine Überprüfung der vom Global Privacy-Team genannten Aktivitäten oder Praktiken vornehmen. Das interne Prüfungsteam, die Leiter für Datenschutz und der Europäische Datenschutzbeauftragte verlangen, falls erforderlich, die Durchführung eines Aktionsplans zur Einhaltung der Binding Corporate Rules. Soweit interne Teams eine jeweilige Angelegenheit nicht angemessen beheben, kann die Gruppe unabhängige, externe Prüfer für weitere Lösungsbemühungen bestellen.

Der Europäische Datenschutzbeauftragte, das PayPal Global Privacy Compliance-Team oder das interne Prüfungsteam und externe Prüfer stellen detaillierte Prüfungs- und Zeitpläne basierend auf dem Risiko der Verarbeitung auf.

Die Ergebnisse der Datenschutzprüfung werden den zuständigen Datenschutzbehörden zur Verfügung gestellt. PayPal behält sich das Recht vor, Teile der Prüfungsberichte zu redigieren, um die Vertraulichkeit firmeneigener oder anderer vertraulicher Unternehmensinformationen zu wahren.

7. Beziehung zwischen den Datenschutzvorschriften für Nutzerdaten und nationalem Recht

Angesichts der weltweit unterschiedlichen gesetzlichen Anforderungen in Bezug auf Datenschutz wurden mit den Datenschutzvorschriften für Nutzerdaten einheitliche Anforderungen aufgestellt, mit denen eine angemessene Verarbeitung von personenbezogenen Nutzerdaten sichergestellt werden soll. Die Datenschutzvorschriften für Nutzerdaten enthalten grundlegende Anforderungen, die von den Gruppenmitgliedern einzuhalten sind; die Gruppenmitglieder sind darüber hinaus jedoch auch verpflichtet, geltende Gesetze zu befolgen, mit denen unter Umständen strengere Standards als die in diesen Datenschutzvorschriften für Nutzerdaten festgelegten verlangt werden.

Nichts in diesen Datenschutzvorschriften für Nutzerdaten berührt die Verpflichtungen eines Gruppenmitglieds unter den geltenden Bankgesetzen, insbesondere in Bezug auf das Bankgeheimnis. Wenn geltendes Recht mit diesen Datenschutzvorschriften für Nutzerdaten auf eine Weise in Konflikt steht, dass ein Gruppenmitglied daran gehindert werden könnte, seinen Verpflichtungen gemäß den Datenschutzvorschriften für Nutzerdaten nachzukommen, und wenn dies erhebliche Auswirkungen auf die darin enthaltenen Zusicherungen hat, muss das Gruppenmitglied den Europäischen Datenschutzbeauftragten unverzüglich darüber informieren, es sei denn, die Bereitstellung solcher Informationen wird von einer Strafverfolgungsbehörde oder durch ein Gesetz untersagt. Der Europäische Datenschutzbeauftragte, die Leiter für Datenschutz und das leitende Gruppenmitglied legen in diesem Fall die geeignete Vorgehensweise fest und beraten sich im Zweifelsfall mit der zuständigen Datenschutzbehörde.

8. Gegenseitige Unterstützung und Kooperation mit Datenschutzbehörden

Die Gruppenmitglieder werden zusammenarbeiten und sich gegenseitig dabei unterstützen, Anfragen oder Beschwerden von Nutzern in Bezug auf diese Datenschutzvorschriften für Nutzerdaten zu bearbeiten.

Die Gruppenmitglieder werden sorgfältig und angemessen auf Anfragen von Datenschutzbehörden zu den Datenschutzvorschriften für Nutzerdaten reagieren. Wenn ein Mitarbeiter eine solche Anfrage von einer Datenschutzbehörde erhält, sollte er dies unverzüglich dem Europäischen Datenschutzbeauftragten mitteilen.

Die Gruppenmitglieder werden bei Anfragen von zuständigen Datenschutzbehörden im EWR bezüglich der Einhaltung dieser Datenschutzvorschriften für Nutzerdaten kooperieren und Prüfungen akzeptieren sowie deren Entscheidungen in Einklang mit dem geltenden Recht und den entsprechenden Verfahrensrechten respektieren.

9. Änderungen am Inhalt dieser Datenschutzvorschriften für Nutzerdaten und an der Liste der daran gebundenen Mitglieder

PayPal behält sich das Recht vor, diese Datenschutzvorschriften für Nutzerdaten nach Bedarf zu ändern, zum Beispiel im Falle von Änderungen bei den geltenden Gesetzen, Regeln, Vorschriften, PayPal-Praktiken, -Verfahren und -Organisationsstrukturen oder Anforderungen, die von relevanten Datenschutzbehörden auferlegt werden.

Das PayPal Global Privacy Legal-Team (unter der Führung des rechtlichen Leiters für Datenschutz) wird ggf. erforderliche Änderungen an diesen Datenschutzvorschriften für Nutzerdaten vorschlagen. Das PayPal Global Privacy Compliance-Team (unter der Führung des Leiters für Datenschutz-Compliance) und der Europäische Datenschutzbeauftragte müssen alle Änderungen an den Datenschutzvorschriften für Nutzerdaten genehmigen sowie alle Änderungen an den Datenschutzvorschriften für Nutzerdaten sowie Änderungen an der Liste der Gruppenmitglieder festhalten. Gemäß dem geltenden Recht melden die Gruppenmitglieder den zuständigen Datenschutzbehörden Änderungen an den Datenschutzvorschriften für Nutzerdaten, damit diese offiziell genehmigt werden können.

Das leitende Gruppenmitglied berät sich mit der leitenden Datenschutzbehörde über wesentliche Änderungen der Datenschutzvorschriften für Nutzerdaten, die sich auf die Einhaltung der Datenschutzbestimmungen oder die Umsetzung der Datenschutzvorschriften für Nutzerdaten auswirken würden. Das leitende Gruppenmitglied wird der leitenden Datenschutzbehörde mindestens einmal jährlich wesentliche Änderungen an den Datenschutzvorschriften für Nutzerdaten und Änderungen an der Liste der Gruppenmitglieder mitteilen. Das PayPal Global Privacy-Team wird zusammenarbeiten, um den Europäischen Datenschutzbeauftragten zu unterstützen, der insbesondere die Antworten koordiniert und umgehend auf Kommentare, Vorschläge oder Einwände zu den von der leitenden Datenschutzbehörde im Auftrag von PayPal vorgenommenen Änderungen reagiert. Etwaige Kommentare, Vorschläge oder Einwände anderer Datenschutzbehörden werden dem Europäischen Datenschutzbeauftragten von der leitenden Datenschutzbehörde mitgeteilt, die im Auftrag der anderen Datenschutzbehörden handelt.

Änderungen an den Datenschutzvorschriften für Nutzerdaten gelten für alle Gruppenmitglieder zum Zeitpunkt ihres Inkrafttretens. Die Gruppenmitglieder werden den Nutzern gemäß deren jeweiligen Einstellungen wesentliche Änderungen an den Datenschutzvorschriften für Nutzerdaten vorab entweder per Rund-E-Mail oder mit einer Nachricht auf der Website mit einem klarem Hinweis zu den Änderungen mitteilen. Die Gruppenmitglieder veröffentlichen die überarbeiteten Datenschutzvorschriften für Nutzerdaten auf ausgewählten externen Websites oder Anwendungen, auf die Nutzer zugreifen können. Änderungen an den Datenschutzvorschriften für Nutzerdaten treten innerhalb von zwei Monaten in Kraft, nachdem die Gruppenmitglieder die Nutzer

benachrichtigt und die überarbeiteten Datenschutzvorschriften für Nutzerdaten veröffentlicht haben.

10. Veröffentlichung

Die Datenschutzvorschriften für Nutzerdaten werden veröffentlicht, und auf der Website oder in den Anwendungen des Diensts wird ein Link zur Verfügung gestellt. Nutzer können beim Europäischen Datenschutzbeauftragten unter der Adresse PayPal (Europe) S.à r.l et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxemburg oder online ein Exemplar anfordern.

11. Schlussbestimmungen

Datum des Inkrafttretens: 25. Mai 2018

Kontakt: Nutzer können Fragen oder Bedenken in Bezug auf die Datenschutzvorschriften für Nutzerdaten an folgende Stelle richten:

An den Europäischen Datenschutzbeauftragten (DSB)

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

12. Definitionen

Gruppenmitglieder interpretieren die Datenschutzvorschriften für Nutzerdaten in einer Weise, die mit den Grundsätzen der EU-Richtlinie 95/46/EG oder einer diese Grundsätze ersetzenden Richtlinie oder Verordnung soweit wie möglich übereinstimmt.

Für die Zwecke dieser Datenschutzvorschriften für Nutzerdaten gelten folgende Definitionen:

Verwaltungsrat bezeichnet den Verwaltungsrat des leitenden Gruppenmitglieds.

Datenschutzbehörden bezeichnet die Behörden, die für die Überwachung und Durchsetzung der von den EWR-Mitgliedstaaten erlassenen nationalen Rechtsvorschriften in ihrem jeweiligen Hoheitsgebiet gemäß der EU-Datenschutzrichtlinie (95/46/EG) verantwortlich sind.

EWR bezeichnet den Europäischen Wirtschaftsraum, der derzeit die EU-Mitgliedstaaten, Island, Liechtenstein und Norwegen umfasst.

„Mitarbeiter“ bezeichnet Mitarbeiter, Arbeitnehmer, Auszubildende und sonstige Beschäftigte oder Angestellte, einschließlich Leiharbeitnehmer, Aushilfskräfte oder Vertragspartner eines Gruppenmitglieds, unabhängig davon, ob es sich um Vollzeit- oder Teilzeitbeschäftigungen handelt und unabhängig von der Art der jeweiligen Beschäftigung oder des Arbeitsverhältnisses.

Europäischer Datenschutzbeauftragter (DSB) bezeichnet den Mitarbeiter, der von der Geschäftsleitung des leitenden Gruppenmitglieds ernannt wird und dieser unterstellt ist und darüber hinaus Mitglied des PayPal Global Privacy Legal-Teams ist. Der Europäische DSB hat seinen Sitz in Luxemburg.

Gruppenmitglied bezeichnet ein Unternehmen der PayPal-Gruppe, das die IGA unterzeichnet hat.

IGA bezeichnet die gruppeninterne Vereinbarung (Intra-Group Agreement)

Leitende Datenschutzbehörde bezeichnet die "Commission nationale pour la protection des données" ("CNPD") in Luxemburg.

Leitendes Gruppenmitglied bezeichnet PayPal (Europe) S. à r.l. & Cie, S.C.A., eine Gesellschaft mit beschränkter Haftung in Luxemburg.

PayPal Global Privacy-Team bezeichnet das koordinierte PayPal Global Privacy Compliance-Team und das PayPal Global Privacy Legal-Team.

PayPal Global Privacy Compliance-Team bezeichnet die Mitglieder der Compliance-Organisation, die sich mit der Einhaltung und der Umsetzung des PayPal-Datenschutzprogramms beschäftigt.

PayPal Global Privacy Legal-Team bezeichnet die Mitglieder der Rechtsabteilung, die konkret mit dem Datenschutz betraut wurden.

PayPal-Gruppe bezeichnet die PayPal Holdings, Inc. ("PayPal") und jedes direkt oder indirekt von PayPal kontrollierte Unternehmen, das Nutzerdaten verarbeitet, wobei Kontrolle den Besitz von mehr als fünfzig Prozent (50%) der Stimmrechte zur Wahl der Direktoren des Unternehmens bedeutet oder mehr als fünfzig Prozent (50%) der Eigentumsanteile am Unternehmen.

Personenbezogene Daten bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; eine identifizierbare Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere anhand einer Identifikationsnummer oder eines oder mehrerer Merkmale, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Verarbeitung bezeichnet einen mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder eine Vorgangsreihe in Zusammenhang mit personenbezogenen Daten,; dies umfasst unter anderem das Erheben, das Erfassen, die Organisation, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Sperrung, das Löschen oder die Vernichtung.

Auftragsverarbeiter bezeichnet jede natürliche oder juristische Person, die personenbezogene Daten im Auftrag eines Gruppenmitglieds verarbeitet.

Sensible personenbezogene Daten bezeichnet personenbezogene Daten, die Aufschluss über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftsmitgliedschaft, Straftaten oder Gesundheit oder Sexualleben geben.

Dienst bezieht sich auf eine Website, Anwendung oder andere Produkte oder Dienstleistungen, die von einer PayPal-Gruppe für die Verwendung durch einen Nutzer angeboten werden.

Dritter bezeichnet jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle außer dem Nutzer, dem Gruppenmitglied, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Weisungsbefugnis des Gruppenmitglieds oder des Auftragsverarbeiters berechtigt sind, personenbezogene Daten zu verarbeiten (z.B. Mitarbeiter).

Nutzer bezeichnet ehemalige und bestehende Kunden, potenzielle Kunden, Investoren, Geschäftspartner und Händler.

Personenbezogene Nutzerdaten bezeichnet personenbezogene Daten in Bezug auf Nutzer.