>> **Alle AGB anzeigen**

Standardvertragsklauseln für die Übermittlung von Verantwortlichen an Verantwortliche

PDF-Datei herunterladen

Letzte Aktualisierung: 17. Juni 2022

Diese Standardvertragsklauseln ("Standardvertragsklauseln") für die Übermittlung von Verantwortlichen an Verantwortliche sind Bestandteil der geltenden PayPal-Nutzungsbedingungen (die "Bedingungen") zwischen Ihnen als Verkäufer ("Sie" oder "Händler") und PayPal und durch Bezugnahme darin aufgenommen. Bei Widersprüchen zwischen den Bestimmungen dieser Standardvertragsklauseln und den Nutzungsbedingungen haben die Bestimmungen dieser Standardvertragsklauseln Vorrang. Zentrale Begriffe, die in diesen Standardvertragsklauseln verwendet, aber nicht definiert werden, haben die in den Nutzungsbedingungen festgelegte Bedeutung.

Soweit zutreffend: (i) Ihre Unterzeichnung der Nutzungsbedingungen gilt als Unterschrift und Annahme des Durchführungsbeschlusses der Europäischen Kommission (EU) 2021/914 vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 ("EU-Datenübermittlungsklauseln") durch den Händler als Datenexporteur und in der Rolle des für die Verarbeitung Verantwortlichen; (ii) die Unterzeichnung des Abkommens durch PayPal gilt als Unterschrift und Annahme der EU-Datenübermittlungsklauseln durch PayPal als Datenimporteur und als für die Verarbeitung Verantwortlicher; und (iii) die Parteien unterliegen den Bestimmungen von Modul 1 der EU-Datenübermittlungsklauseln.

Für den Fall, dass die Europäische Kommission die EU-Datenübermittlungsklauseln überarbeitet und danach neue Klauseln veröffentlicht (oder dies von der

Europäischen Kommission anderweitig vorgeschrieben oder umgesetzt wird), vereinbaren die Parteien, dass diese neuen EU-Datenübermittlungsklauseln die vorliegenden EU-Datenübermittlungsklauseln ersetzen werden und dass sie alle für die Durchführung der neuen EU-Datenübermittlungsklauseln erforderlichen Maßnahmen ergreifen werden.

Bei Übermittlungen personenbezogener Daten aus der Schweiz, die ausschließlich dem Schweizer Bundesgesetz über den Datenschutz und anderen Schweizer Datenschutzgesetzen ("Schweizer Datenschutzgesetze") unterliegen:

i. Gelten die EU-Datenübermittlungsklauseln auch für die Übermittlung von Informationen zu einer identifizierten oder identifizierbaren juristischen Person, wobei die Informationen ähnlich geschützt sind wie personenbezogene Daten gemäß den Schweizer Datenschutzgesetzen, bis diese Gesetze so geändert werden, dass sie nicht mehr für eine juristische Person gelten.
ii. Haben allgemeine und spezifische Verweise in den EU-Datenübermittlungsklauseln auf die Verordnung (EU) 2016/679 bzw. das EU-Recht oder das mitgliedstaatliche Recht die gleiche Bedeutung wie der entsprechende Verweis in den Schweizer Datenschutzgesetzen und Verweise auf "Mitgliedstaat" oder "EU-Mitgliedstaat" oder "EU" sind als Verweise auf die Schweiz zu lesen.

Die EU-Datenübermittlungsklauseln (Modul 1) werden durch Bezugnahme in die Nutzungsbedingungen aufgenommen und gelten bei Inkrafttreten der Nutzungsbedingungen zwischen den Parteien vorbehaltlich der folgenden Einzelheiten als ordnungsgemäß ausgeführt:

i. Für die Zwecke von Klausel 13 (Aufsicht) ist die zuständige Aufsichtsbehörde der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, sofern die jeweilige Datenübermittlung durch Schweizer Datenschutzgesetze geregelt wird;
ii. Option 1 von Klausel 17 (Anwendbares Recht) findet Anwendung, und die EU-Datenübermittlungsklauseln unterliegen dem Recht von Luxemburg;

iii. Gemäß Klausel 18 (Gerichtsstand und Zuständigkeit) werden alle Streitigkeiten im Zusammenhang mit den EU-Datenübermittlungsklauseln von den Gerichten Luxemburgs beigelegt; der betroffenen Person wird das Recht gewährt, bei Entsprechung mit dem Land des gewöhnlichen Aufenthalts Streitigkeiten den Gerichten der Schweiz zu unterbreiten; und

iv. die Parteien vereinbaren, dass die nach dem Anhang zu den EU-Datenübermittlungsklauseln erforderlichen Einzelheiten in Anlage 1 dargelegt sind.

Anlage 1

<u>Anhang zu den EU-Datenübermittlungsklauseln</u>

Anhang 1.A Folgendes gilt, soweit dies nach den EU-Datenübermittlungsklauseln erforderlich ist.

Datenexporteur

- Name und Anschrift: Der Datenexporteur ist der Händler und die Adresse entspricht der in den Nutzungsbedingungen angegebenen
- Name, Funktion und Kontaktdaten der Kontaktperson: entsprechen den in den Nutzungsbedingungen angegebenen
- Tätigkeiten, die für die gemäß den Standardvertragsklauseln übermittelten Daten von Belang sind: entsprechen den in den Nutzungsbedingungen angegebenen
- Unterschrift und Datum: sind den vorliegenden Standardvertragsklauseln zu entnehmen
- Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

Datenimporteur

- Name und Anschrift: Der Datenimporteur ist das Mitglied der PayPal-Gruppe, das die Dienstleistungen gemäß der Nutzungsbedingungen erbringt, und die Adresse entspricht der in den Nutzungsbedingungen angegebenen
- Name, Funktion und Kontaktdaten der Kontaktperson: entsprechen den in den Nutzungsbedingungen angegebenen
- Tätigkeiten, die für die gemäß den Standardvertragsklauseln übermittelten Daten von Belang sind: entsprechen den in den Nutzungsbedingungen angegebenen
- Unterschrift und Datum: sind den vorliegenden Standardvertragsklauseln zu entnehmen
- Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

Anhang 1.B Beschreibung der Übermittlung

Betroffene Personen, deren personenbezogene Daten übermittelt werden

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

- Kunden, Mitarbeiter und andere Geschäftskontakte des Datenexporteurs.

Kategorien der übermittelten personenbezogenen Daten

- Name, Rechnungsbetrag, Datum/Uhrzeit, Bankverbindung, Kreditkartendaten, CVC-Code, Postleitzahl, Ländercode, Anschrift, E-Mail-Adresse, Faxnummer, Telefonnummer, Website, Ablaufdaten, Versandangaben, Steuerstatus, eindeutige Kundenkennung, IP-Adresse, Ort und alle sonstigen Daten, die gemäß den Nutzungsbedingungen von PayPal erhalten werden.

Sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien sensibler Daten:

- Nicht zutreffend, es sei denn, der Händler konfiguriert den Dienst so, dass diese Daten erfasst werden.

Angewandte Beschränkungen und Garantien:

- Nicht zutreffend, es sei denn, der Händler konfiguriert den Dienst so, dass diese Daten erfasst werden.

Art der Verarbeitung

Wie in den Nutzungsbedingungen festgelegt.

Zweck(e) der Datenübermittlung(en)

Die Übermittlung findet zu folgenden Zwecken statt:

- Dienstleistungserbringung des Datenimporteurs gegenüber dem Datenexporteur gemäß den Nutzungsbedingungen.

- Erkennung von betrügerischen Aktivitäten und Risiken, die den Datenimporteur, den Datenexporteur oder andere Kunden des Datenimporteurs betreffen oder betreffen könnten.
- Einhaltung der für den Datenimporteur geltenden Gesetze und Strafverfolgungsersuchen.
- Wie in der Datenschutzerklärung des Datenimporteurs dargelegt.

Der Zeitraum, für den die personenbezogenen Daten gespeichert werden, oder, wenn dies nicht möglich ist, die Kriterien für die Bestimmung dieses Zeitraums

Der Datenimporteur bewahrt personenbezogene Daten nur so lange auf, wie es im Hinblick auf den jeweiligen Zweck, für den sie erhoben wurden, erforderlich ist (siehe oben genannte Zwecke). Um die angemessene Aufbewahrungsfrist für personenbezogene Daten zu ermitteln, berücksichtigt der Datenimporteur die Menge, Art und Sensibilität der personenbezogenen Daten, das potenzielle Schadenrisiko durch die unbefugte Nutzung oder Offenlegung der personenbezogenen Daten, die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, und ob solche Zwecke auf andere Weise erreicht werden können sowie anwendbare rechtliche, regulatorische, steuerliche, buchhalterische oder andere Anforderungen.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben

Der Datenimporteur kann personenbezogene Daten an Drittanbieter weitergeben, die auf Anweisung und im Auftrag des Datenimporteurs Dienstleistungen und Funktionen erfüllen. Diese Drittanbieter können beispielsweise einen Teil der gemäß den Nutzungsbedingungen bereitgestellten Dienstleistungen erbringen, wie z.B. Kundenverifizierung, Transaktionsverarbeitung oder Kundenservice, oder für den Datenimporteur eine Dienstleistung erbringen, die die im Rahmen der Nutzungsbedingungen erbrachten Dienstleistungen, wie z.B. die Speicherung, unterstützt. Bei der Bestimmung der Dauer der Verarbeitung durch Drittanbieter wendet der Datenimporteur die oben in diesem Anhang 1.B genannten Kriterien an.

Anhang 1.C Aufsichtsbehörde

Gemäß Klausel 13 (a) der EU-Datenübermittlungsklauseln fungiert die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 für die Datenübermittlung einhält, als zuständige Aufsichtsbehörde.

B. Technische und organisatorische Maßnahmen, einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Daten

1. Pseudonymisierung, Verschlüsselung und Schutz der Daten während der Übermittlung

PayPal-Richtlinien gewährleisten die Einhaltung dieses Grundsatzes und erfordern die Verwendung technischer Kontrollen, um das Risiko der Offenlegung personenbezogener Daten zu vermeiden. PayPal setzt Verschlüsselung sowohl bei der Übermittlung als auch bei allen ruhenden personenbezogenen Daten ein. Dabei verwenden wir auch branchenübliche Pseudonymisierungstechniken, wie z.B. die Tokenisierung, um personenbezogene Daten gegebenenfalls zu schützen. PayPal verfügt über umfassende Richtlinien, die wichtige Pflichten und Verfahren zum Schutz von Daten enthalten, wenn diese innerhalb des Unternehmens und extern an Dritte übermittelt werden.

2. Änderungsverwaltung und Geschäftskontinuität

PayPals robustes Verfahren zur Änderungsverwaltung gewährleistet die kontinuierliche Verfügbarkeit und Resilienz von Daten und Systemen während ihres gesamten Lebenszyklus, indem sichergestellt wird, dass Änderungen angemessen geplant, genehmigt, ausgeführt und überprüft werden. Der Managementprozess für Geschäftskontinuität bietet einen Rahmen zum Aufbau von Resilienz im Unternehmen, um die Interessen der Hauptbeteiligten wirksam schützen zu können.

3. Notfallwiederherstellung

Das robuste PayPal-Programm zur Notfallwiederherstellung verfügt über Verfahren zur Wiederherstellung von Informations- oder Technologiesystemen nach einer erheblichen Störung, wobei der Fokus auf den IT-Systemen liegt, die kritische

Geschäftsprozesse und Kundenaktivitäten unterstützen. Die Technologieinfrastruktur von PayPal ist auf mehrere sichere Rechenzentren mit primärer und sekundärer Leistungsfähigkeit verteilt, die jeweils mit Netzwerk- und Sicherheitsinfrastruktur, dedizierten Anwendungs- und Datenbankservern sowie Speicher ausgestattet sind.

4. Regelmäßige Tests, Beurteilungen und Bewertungen der Wirksamkeit technischer und organisatorischer Maßnahmen

PayPal plant und führt regelmäßig eigene Testprogramme durch und berichtet über die Ergebnisse, um die Wirksamkeit seiner technischen und organisatorischen Maßnahmen zu beurteilen und einzuschätzen. Das Programm wird von unserem Team für Unternehmensrisiko und Compliance verwaltet, das mit den entscheidenden Interessengruppen zusammenarbeitet, um die Informationen zu erhalten und zu bewerten, die gegebenenfalls zum Testen, Melden und Einleiten von Gegenmaßnahmen erforderlich sind.

5. Nutzeridentifikation und -autorisierung

Die PayPal-Verfahren für die Zugriffsverwaltung erfordern, dass sich Benutzer mit einer eindeutigen Unternehmensnetzwerk-ID und einem Passwort für die Benutzeridentifikation und -authentifizierung im Unternehmensnetzwerk einloggen müssen, bevor sie auf andere Anwendungsbereiche zugreifen können. Es werden automatisch Richtlinien bezüglich Zusammensetzung, Länge, Änderung, Wiederverwendung und Sperrung des Passworts angewendet. Rollenbasierter Zugriff und vierteljährlich zertifizierte Genehmigungen werden in allen Systemen im Anwendungsbereich implementiert, um das Prinzip der "minimalen Privilegien" durchzusetzen.

6. Physische Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Die globalen Sicherheitsrichtlinien und -verfahren von PayPal legen die Anforderungen fest, die gemäß den geltenden Gesetzen, Vorschriften und Partneranforderungen für eine ordnungsgemäße Durchführung von Sicherheitsverfahren, einschließlich der physischen Sicherheit, erforderlich sind. Bei der Einrichtung von besonderen oder sensiblen Bereichen, wie Poststellen, Gerätelagerräumen, Posteingang und Versand, Computer-/Serverräumen,

Kommunikationstresoren oder Lagerbereichen für Verschlusssachen, wird gemäß dem Standard für die Informationssicherheit des Unternehmens besonderes Gewicht auf Sicherheitssysteme und Garantien gelegt.

7. Protokollierung von Ereignissen und Konfiguration

PayPal hat die Protokollierung von Ereignissen sowie die Überwachungsarten und -attribute beschrieben und definiert. Das Unternehmen erfasst und aggregiert verschiedene Arten von Protokollen im zentralisierten Sicherheitsüberwachungssystem. Eine standardmäßige Kontrolle für die Konfigurationsverwaltung stellt sicher, dass Protokolle von den Systemen erfasst und an unser zentralisiertes Sicherheitsüberwachungssystem weitergeleitet werden. PayPal-Richtlinien und unterstützende Prozesse legen fest, dass die Grundlinien für Systemkonfiguration und -härtung über alle Systeme hinweg implementiert werden müssen.

8. Governance und Verwaltung der IT; Zertifizierung und Qualitätssicherung von Prozessen und Produkten

PayPal setzt sich für eine starke Sicherheitsphilosophie im gesamten Unternehmen ein. Unser Chief Information Security Officer ist für die Informationssicherheit in unserem globalen Unternehmen verantwortlich. Im Rahmen unseres Enterprise Risk and Compliance Management Program ist unser Technology Oversight and Information Security Program darauf ausgerichtet, das Unternehmen bei der Verwaltung von Technologie- und Informationssicherheitsrisiken zu unterstützen und Informationen zu identifizieren und zu schützen sowie Bedrohungen der Informationssicherheit zu erkennen, darauf zu reagieren und die Wiederherstellung abzuschließen. PayPal zertifiziert und sichert seine Prozesse und Produkte durch eine Vielzahl von Unternehmensprogrammen, zu denen die folgenden zählen: (i) Prüfungen und Beurteilungen der Verpflichtungen von PayPal hinsichtlich der technischen Industriestandards, zu denen unter anderem ISO 27001, die anwendbaren Standards der Payment Card Industry (PCI) (DSS, PIN, P2PE usw.) und SOC-1 und SOC-2 des American Institute of Certified Public Accountants (AICPA) gehören, (ii) ein Risikosteuerungsprüfungsverfahren (RCIP), was ein frühzeitiges Engagement und einen Standardansatz für Messung, Management und Überwachung von Risiken im Zusammenhang mit der Entwicklung und Freigabe von Produktlösungen gewährleistet, (iii) Datenschutzfolgenabschätzungen, die in

den frühen Phasen der Produkt- und Softwareentwicklungsprozesse integriert sind, und (iv) ein umfassendes Programm zum Management von Dritten, das durch kontinuierliches Risikomanagement während des gesamten Lebenszyklus einer Interaktion mit einem Dritten für Qualitätssicherung sorgt.

9. Datenminimierung

Unsere Richtlinien sorgen mithilfe technischer Kontrollen dafür, dass nur die Datenelemente erfasst und generiert werden, die im Hinblick auf die Verarbeitungszwecke angemessen, relevant und notwendig sind. Die PayPal-Verfahren zur Datenschutzfolgenabschätzung gewährleisten die Einhaltung dieser Richtlinien.

10. Qualität und Speicherung von Daten

Die Zugangs- und Qualitätsrichtlinie von PayPal gewährleistet, dass alle personenbezogenen Daten korrekt, vollständig und aktuell sind, sodass einzelne Benutzer auf das System zugreifen können, um ihre Angaben (z.B. Adresse, Kontaktdaten usw.) zu berichtigen und zu ändern, und dass, wenn eine Berichtigungsanforderung von einer betroffenen Person eingeht, eine Dienstleistung bereitgestellt wird, um ihr Recht auf Berichtigung umzusetzen. Unser Data Governance-Programm überwacht, soweit erforderlich, die Datenqualität, Probleme und sowie Problembehandlungen. Alle Daten müssen aufgrund ihres Geschäftswertes klassifiziert und es muss eine Aufbewahrungsfrist zugewiesen werden, die auf den gesetzlichen, regulatorischen und geschäftlichen Aufzeichnungsvorschriften von PayPal beruht. Nach Ablauf der Aufbewahrungsfrist werden Daten und Informationen entsorgt, gelöscht oder vernichtet.

11. Rechenschaftspflicht

PayPal hat eine Reihe von Grundsätzen und Richtlinien zu Informationssicherheit, Technologie, Data Governance, Management von Dritten und Datenschutz entwickelt, die an den Branchenstandards ausgerichtet sind und die Zusammenarbeit mit Interessengruppen und Partnerschaften im Hinblick auf die Sensibilisierung und Compliance mit solchen Richtlinien und Kontrollen im gesamten Unternehmen fördern sollen, um ausgehend von der Geschäftsleitung die Umsetzung und die Rechenschaftspflicht im gesamten Unternehmen zu

gewährleisten. Jedes Programm definiert Verantwortlichkeiten für funktionsübergreifende datenbezogene Entscheidungen, Prozesse und Kontrollen. Als Datenverantwortlicher ist PayPal für die Einhaltung der entsprechenden Artikel verantwortlich, die in der DSGVO und anderen anwendbaren Datenschutzgesetzen eine Rechenschaftspflicht beinhalten, indem eine Datenschutzerklärung und eine zugrundeliegende, mehrschichtige Organisations- und technische Kontrollstruktur umgesetzt werden, um die unternehmensweite Einhaltung des Datenschutzrechts, der Vorschriften, Richtlinien und Verfahren zu gewährleisten. Dazu gehört der Nachweis der Einhaltung der Datenschutzgesetze durch: 1) eine starke Compliance-Kultur, 2) eine Unternehmensrisiko- und Compliance-Governance-Struktur, die Verwaltungsausschüsse, Aufsichtsfunktionen, Datenschutzberichte umfasst, 3) die Verantwortung für die Einhaltung des Datenschutzprogramms, einschließlich der Einrichtung, Dokumentation und Wartung von Geschäftsprozessen und -kontrollen, 4) eine globale Datenschutzabteilung innerhalb der Enterprise Compliance Organisation, die die Einhaltung des Datenschutzprogramms durch das Unternehmen überwacht und Richtlinien, Standards, Verfahren und Tools definiert, die durch Unternehmensfunktionen operationalisiert werden, 5) Kommunikation mit dem Unternehmen im Rahmen der globalen Datenschutzfunktion, um die Sensibilisierung und ein Verständnis des Datenschutzes zu fördern, 6) einen Rahmen für Unternehmensrisiko- und Compliance-Management, um die Verwendung einheitlicher Prozesse, einschließlich Datenschutzfolgenabschätzungen, Datenschutzüberwachung und -tests, Issue Management im Datenschutz, Datenschutztraining, jährlicher Datenschutzpläne zu gewährleisten und 7) eine Berichterstattung und Analyse an die Adresse der Verwaltungsausschüsse, die das Datenschutzprogramm überwachen.

12. Rechte betroffener Personen

PayPal verfügt über ein Programm, um sicherzustellen, dass die Rechte betroffener Personen, einschließlich Zugang, Berichtigung und Löschung, erfüllt werden. Die Anträge auf Löschung von Daten werden erfüllt, es sei denn, dass PayPal eine rechtliche, regulatorische Verpflichtung oder einen anderen rechtmäßigen Geschäftsgrund zur Speicherung der Daten hat. Die Richtlinien von PayPal gewährleisten, dass die Löschung über den gesamten Kundenlebenszyklus hinweg erfolgt.

13. Auftragsverarbeiter

PayPal verfügt über ein umfassendes Programm zum Management von Dritten, das durch kontinuierliches Risikomanagement während des gesamten Lebenszyklus einer Interaktion mit Dritten Sicherheit gewährleistet. Wir verfügen über vertragliche Kontrollen, die von unseren Auftragsverarbeitern und deren Unterauftragsverarbeitern verlangen, dass sie in der gesamten Verarbeitungskette umfassende Datenschutz- und Datensicherheitsstandards einführen müssen. Alle Unterauftragsverarbeiter müssen vor ihrer Beauftragung vorab von uns genehmigt werden.