Datenschutz und Sicherheit bei PayPal

Stand 9.10.2020

1. Was ist PayPal?

PayPal ermöglicht Privatpersonen und Unternehmen das Senden und Empfangen von elektronischem Geld (E-Geld) online. Zudem werden auch andere Finanzdienstleistungen und nicht finanzspezifische Dienstleistungen angeboten, die im Zusammenhang mit Online-Zahlungen stehen.
Es können einzelne bzw. einmalige Zahlungen vorgenommen oder auch regelmäßige Zahlungen abgewickelt werden.

2. Was ist E-Geld?

Gemäß Art. 1 der Richtlinie 2000/46 EG bezeichnet E-Geld einen Geldwert in Form einer Forderung gegen die ausgebende Stelle, der erstens, auf einem Datenträger gespeichert ist, zweitens, gegen Entgegennahme eines Geldbetrages ausgegeben wird, dessen Wert nicht geringer ist als der ausgegebene monetäre Wert und drittens, von anderen Unternehmen als der ausgebenden Stelle als Zahlungsmittel akzeptiert wird. E-Geld muss also einen monetären Wert darstellen, mithin einen Geldwert. Ähnlich wie ein gesetzliches Zahlungsmittel soll daher das E-Geld einen Nominalwert aufweisen, damit es als Zahlungsmittel fungieren kann.

3. Wie funktioniert das Bezahlen mit einem PayPal-Konto?

Seit 2007 besitzt PayPal in Europa eine Banklizenz und unterliegt der Regulierung durch die luxemburgische Bankaufsicht CSSF und damit dem Europäischen Recht.
Der Zahlungsvorgang bei PayPal-Konten erfordert das Einloggen in das PayPal-Konto und die Angabe der E-Mail Adresse des Zahlungsempfängers, sowie den Betrag und Verwendungszweck. Das PayPal-Netzwerk stellt damit eine Echtzeit-Zahlungslösung bereit.

4. Überwachung und Schutz der Nutzer durch die E-Geld-Richtlinie

Zahlungsdienstleister, die E-Geld in Europa anbieten unterliegen der Zahlungsdienste-Richtlinie 2007/64/EG.
Hauptziel dieser Richtlinie ist es, einen funktionierenden und EU-weiten Binnenmarkt für Zahlungsdienste zu schaffen. Auf Gemeinschaftsebene soll deshalb ein moderner und kohärenter rechtlicher Rahmen für Zahlungsdienste geschaffen werden. Dieser soll zum einen gewährleisten, dass einheitliche Informationspflichten für Zahlungsdienstleister sowie die Rechte und Pflichten von Zahlungsnutzern und Zahlungsdienstleistern festgelegt werden. Zum anderen, dass die Mitgliedsstaaten ihre aufsichtsrechtlichen Anforderungen aufeinander abstimmen.
Alle E-Geld-Institute nach Luxemburger Recht unterliegen der Zulassung und der prudentiellen Aufsicht durch die Bankenaufsicht Commission de Surveillance du Secteur Financier (CSSF). Eine Aufstellung der Organisation und Befugnisse der CSSF sind unter http://www.cssf.lu/nc/de/die-cssf/organisation/ abrufbar.

5. Höchste Priorität beim Datenschutz: Verschlüsselung und Sicherheitszertifikate

Der Schutz von persönlichen Angaben und Finanzinformationen gehört zu PayPals höchsten Prioritäten.

PayPal wendet bei der Verwaltung der Kundeninformationen höchste Standards für Informationssicherheit an. So werden beispielsweise Schutzmechanismen für Computer, wie Firewalls und Datenverschlüsselung verwendet. Der Zugriff auf persönliche Angaben der Kunden ist nur jenen Mitarbeitern möglich, die diese zur Erledigung ihrer Tätigkeiten benötigen. Um die Sicherheit der Daten zu gewährleisten unterliegen alle Mitarbeiter den strengen internen Compliance-Standards von PayPal. So müssen sie z.B. in regelmäßigen Abständen (jährlich) Schulungen und Trainings zum Thema Compliance absolvieren.

Die persönlichen Angaben werden auf Servern gespeichert und schwer bewacht, sowohl physisch als auch elektronisch. Um Kreditkarten- und Kontonummer geheim zu halten, werden die Firewall-geschützten Server nicht direkt mit dem Internet verbunden.

PayPal bietet durch die sogenannte Zwei-Faktor-Authentifizierung die Möglichkeit, den Zugriff auf das Konto zusätzlich zum Passwort über einen per SMS erzeugten Zahlencode abzusichern. Durch getrennten Zugriff auf Passwort und Zahlencode kann sichergestellt werden, dass Transaktionen im PayPal-Geschäftskonto nur bei Autorisierung durch zwei Mitarbeiter durchgeführt werden können. Diese zusätzliche Autorisierung steht auch für das PayPal-Konto des Käufers zur Verfügung und bietet somit auch auf Nutzerseite einen zusätzlichen Schutz.

6. Zertifikate und Überwachung

6.1. *PCI Zertifizierung* (Payment Card Industry Data Security Standard): Dies ist ein weltweit vorgeschriebenes Regelwerk im Zahlungsverkehr zur Sicherung der Identität des Kreditkarteninhabers und der Transaktionsinformationen.

6.2. *SAS70 Zertifizierung* (Statement on Auditing Standards): Dabei handelt es sich um einen weltweit anerkannten Auditierungsstandard für Service-Organisationen.

6.3. *Auditierung*: Der PayPal-Datenschutzbeauftragte in Luxemburg ist verpflichtet, alle vier Monate einen Bericht an die Nationale Kommission für den Datenschutz in Luxemburg (CNPD) einzureichen. Die CNPD (http://www.cnpd.public.lu/de/index.html) wertet diesen aus und stellt ggf. Nachfragen. Zudem erstellen die von PayPal beauftragten Wirtschaftsprüfer einen Bericht über Sicherheitsmaßnahmen (u.a. Datenschutz), der einmal jährlich an die Luxemburger Bankaufsicht übermittelt wird. Diese prüft daher auch anhand des Berichts und auf Basis von Nachfragen und Gesprächen die Einhaltung des Bankgeheimnisses und der Datensicherheit.

7. Binding Corporate Rules

PayPal hat sich mittels sogenannter Binding Corporate Rules (BCR) dazu verpflichtet, personenbezogene Daten unternehmensintern nach geltendem europäischem Recht zu transferieren - unabhängig vom Speicherort. PayPals BCR wurden von der Luxemburger Datenschutzaufsicht nach dem europäischen “mutual recognition process” genehmigt. Die Liste der Unternehmen, die diesen Genehmigungsprozess durchlaufen haben, ist auf der Seite der EU-Kommission verfügbar: https://ec.europa.eu/commission/index_de
PayPals Binding Corporate Rules sind hier zu finden:
https://www.paypal.com/de/webapps/mpp/ua/bcr