von Rechtsanwalt **Nicolai Amereller**

Schreckgespenst „PSD2“ – Was kommt zum 14.09.2019 bei der Zahlungsabwicklung auf die Onlinehändler zu?

Die Umsetzungsfrist der „Payment Service Directive 2“-Richtlinie (kurz: PSD2) endet am 14.09.2019. Durch die Richtlinie sollen Zahlungsvorgänge EU-weit reguliert und insbesondere sicherer werden, vor allem durch den Einsatz einer starken Kundenauthentifizierung. Im Bereich des Onlinehandels herrscht aktuell einige Verunsicherung hinsichtlich der Begriffe PSD2, 2FA und SCA. Grund genug, dieses Thema einmal aus Sicht eines Onlinehändlers näher zu beleuchten.

Was ist der Hintergrund?

In den letzten Jahren haben sich – nicht nur im Bereich des Ecommerce – zahlreiche neue Zahlungsarten und Anbieter von Zahlungsdiensten auf dem Markt etabliert.

In der Regel werden solche innovativen Zahlungsdienste aber nicht von klassischen Banken (die bereits einer sehr weitgehenden staatlichen Regulierung unterliegen) angeboten, sondern eher von sog. FinTechs (Startups im Bereich Finanzen).

Damit auch die Anbieter solcher neuartiger Zahlungsdienste reguliert werden können, wurde auf EU-Ebene eine entsprechende Richtlinie geschaffen, die sog. „Payment Services Directive“ (kurz: PSD). Diese „erste Zahlungsdiensterichtline“ 2007/64/EG trat bereits am 25.12.2007 in Kraft und wurde die die „zweite Zahlungsdiensterichtlinie“ (EU) 2015/2366 (kurz: PSD2) ersetzt.

Mit der PSD2 rücken nun ein noch höherer Verbraucherschutz insbesondere hinsichtlich der Sicherheit von Zahlungen sowie die Schaffung innovativerer europäischer Zahlungsmethoden mit Zielrichtung eines digitalen Binnenmarktes in den Fokus des Richtliniengebers.

Der elektronische Zahlungsverkehr soll sicherer und transparenter werden und dadurch der faire Wettbewerb gestärkt sowie die Einstiegshürden für Zahlungsdiensteanbieter gesenkt werden.

Die PSD2 ist bereits seit dem 13.01.2018 gültig. Seitdem dürfen Onlinehändler in der EU für Zahlungen mittels Überweisung, Lastschrift und Debit- bzw. Kreditkarte keine Aufschläge mehr erheben. Dem aber nicht genug.

Starke Kundenauthentifizierung als Herzstück der PSD2

Mit der PSD2 wurden zudem neue technische Standards für eine verpflichtende starke Kundenauthentifizierung festgelegt.

Hierzu wurde am 13.03.2018 die Delegierte Verordnung (EU) 2018/389 zur starken Kundenauthentifizierung und für sichere offene Standards für die Kommunikation im Amtsblatt der Europäischen Union veröffentlicht. Diese Verordnung gilt ab dem 14.09.2019.

Die starke Kundenauthentifizierung muss folglich bis zum 14.09.2019 umgesetzt werden.

Was bedeutet starke Kundenauthentifizierung?

Mit der Einführung einer verpflichtenden starken Kundenauthentifizierung (englisch: Strong Customer Authentification, kurz SCA) sollen vor allem Betrugsfälle im elektronischen Zahlungsverkehr eingedämmt werden.

Dies soll dadurch erreicht werden, indem Zahlungen nur noch auf einem sicheren Weg autorisiert werden können. Bevor die Zahlung also ausgelöst werden kann, muss zunächst ein mehrstufiger Verifizierungsvorgang durchlaufen werden, um die Berechtigung der Zahlungsauslösung so gut wie möglich sicherzustellen.

Ziel ist es also, ab dem 14.09.2019 im Bereich elektronischer Zahlungen technisch sicherzustellen, dass die Person, die sich bei der Einleitung des Zahlungsvorgangs als autorisierte Person ausgibt auch tatsächlich diese autorisierte Person ist.

Während bislang häufig ein elektronischer Zahlungsvorgang meist „eindimensional“ angestoßen werden konnte, wird die Autorisierung künftig in vielen Fällen „zweidimensional“ erfolgen müssen.

Beispiele:

Bei einer Kreditkartenzahlung im Onlineshop kann die Zahlung derzeit in der Regel durch bloßen Zugriff auf die Karte selbst (nämlich durch Angabe der Kartennummer und des auf dieser ebenfalls abgedruckten Sicherheitscodes der Kreditkarte) ausgelöst werden.

Bei einer Zahlung via Paypal im Onlineshop kann die Zahlung derzeit in der Regel durch bloße Eingabe der bei Paypal hinterlegten Email-Adresse und des Passworts für den Paypalaccount initiiert werden.

Die Gefahr eines Missbrauchs ist hierbei jeweils recht hoch, da die Zahlung durch bloßen Zugriff auf die Karte bzw. auf den Paypal-Datensatz (Email und Passwort) ausgelöst werden kann. Sind Karte bzw. Paypal-Zugangsdaten in falsche Hände gelangt, ist die Zahlung für diese Person trotz fehlender Berechtigung technisch meist problemlos möglich.

Schutzmechanismus Zwei-Faktor-Authentifizierung (2FA)

Das Ziel sicherer elektronischer Zahlungen soll durch eine verpflichtende Zwei-Faktor-Authentifizierung (kurz 2FA) erreicht werden.

Neu ist damit, dass eine verpflichtende zweite Stufe bei der Kundenauthentifizierung hinzutritt, wenn es um die Auslösung von Zahlungen durch den Kunden geht. Es sind mithin künftig zwei Faktoren des Kunden abzufragen, bevor eine Zahlung ausgelöst wird.

Der Richtliniengeber sieht drei Kategorien vor, aus denen die Faktoren stammen können:

- **Wissen** (z.B. Passwörter, PINs, persönliche Daten, Antworten auf Sicherheit – also etwas, dass nur der Kunde kennt)
- **Besitz** (z.B. Zahlungskarte, Smartphone, Chip-TAN-Generator – also etwas, was nur der Kunde in Besitz hat)
- **Inhärenz/ Biometrie** (z.B. Fingerabdruck-Scan, Iris-Scan, Gesichts- oder Stimmerkennung – also etwas, was nur dem Kunden anhaftet)

Eine starke Kundenauthentifizierung liegt nach Art. 4 Nr. 30 der PSD2 dann vor, sobald eine Authentifizierung unter Heranziehung von mindestens zwei verschiedenen Elementen erfolgt.

Ab dem 14.09.2019 werden für eine 2FA somit zwei verschiedene Faktoren, die aus zwei verschiedenen dieser drei vorgenannten Kategorien stammen müssen benötigt, damit von einer starken Kundenauthentifizierung gesprochen werden kann. Stammen beide Faktoren dagegen nur aus einer Kategorie (z.B. Passwort und PIN, beides aus der Kategorie Wissen), reicht dies nicht aus.

In den genannten Beispielen bedeutet dies, dass der Kreditkartenanbieter bzw. Paypal vom Kunden neben der Kartennummer und dem Sicherheitscode bzw. den Zugangsdaten künftig noch ein weiteres Merkmal abfragen müssen (etwa eine in eine Smartphone-App gepushte TAN), bevor die Zahlung autorisiert wird.

Durch die 2FA wird die Gefahr eines Missbrauchs erheblich reduziert, da Dritte für eine Autorisierung der Zahlung Zugriff auf zwei „Lebensbereiche“ des Opfers benötigen.

Bekannt aus dem stationären Handel oder Onlinebanking

Ein typisches Beispiel für eine 2FA ist der Einsatz einer EC-Karte im stationären Handel bei Zahlungsautorisierung mittels PIN: Zum einen benötigt der Kunde für die Auslösung der Zahlung etwas aus seinem Besitz (die Karte an sich), zum anderen benötigt er etwas aus dem Bereich Wissen (die PIN zur Karte).

Auch beim typischen Onlinebanking kommt bereits 2FA zur Anwendung. Für den Login muss der Kunde Nutzerkennung und Passwort eingeben (Wissen). Für die Autorisierung der gewünschten Zahlung dann eine bei ihm (auf seinem Smartphone via App) generierte TAN (Besitz) einsetzen.

Sache der Zahlungsanbieter

Zunächst die gute Nachricht für die Onlinehändler: Die Vorgaben der PSD2 richten sich an die Anbieter von Zahlungsdiensten (also z.B. Kreditkartenunternehmen, Banken, Paypal, Klarna) und nicht an Onlinehändler.

Denn der typische Onlinehändler ist selbst gerade kein Zahlungsdiensteanbieter, sondern bedient sich im Rahmen seines Onlineshops oder seines Marktplatzauftritts bei der Zahlung gerade eines solchen Zahlungsdiensteanbieters (z.B. durch die Verwendung von Paypal).

Onlinehändler sollten aber darauf achten, dass diese spätestens ab dem 14.09.2019 nur noch „PSD2-kompatible“ Paymentanbieter einsetzen (sofern die von Ihnen angebotene(n) Zahlungsart(en) überhaupt von den neuen Vorgaben nach PSD2 erfasst wird).

Änderungen bei Zahlung per Kreditkarte und Paypal

Die SCA muss ab dem 14.09.2019 insbesondere bei den Zahlungsarten Kreditkarte und Paypal zur Anwendung kommen. Hier teilen viele Kreditkartenanbieter und auch Paypal auf Anfrage mit, dass an einer Umsetzung der SCA bereits mit Hochdruck gearbeitet wird.

Vorkasseüberweisung, Kauf auf Rechnung und Zahlung via Lastschrift nicht von SCA erfasst

Eine Vorkasseüberweisung nimmt der Kunde nicht im Shop des Händlers vor, sondern veranlasst diese direkt gegenüber seiner Bank (z.B. im Wege des Onlinebankings oder durch einen klassischen Überweisungsauftrag vor Ort). Dies trifft ebenso auf die Zahlung auf Rechnung zu. Der Händler selbst kommt bei diesen Zahlungsarten mit den PSD2-Vorgaben also nicht einmal in Kontakt.

Die Zahlungsart Lastschrift ist als sog. „Pull-Verfahren“ nicht unmittelbar von dem SCA-Erfordernis der PSD2 betroffen. Denn hier veranlasst nicht der Kunde die Zahlung, sondern der Händler bzw. sein Zahlungsabwickler fordern das Geld bei der Bank des Kunden an. SCA ist von der PSD2 aber nur für sog. „Push-Verfahren“ vorgeschrieben, bei denen der Kunde selbst die Zahlung veranlasst.

Was haben Onlinehändler nun also zu tun?

Händler sollten die verbleibende Zeit bis zum 14.09.2019 nutzen, um zu prüfen, ob betroffene Zahlungsarten in ihrem Shop „PSD2-kompatibel“ sind.

Dies bedeutet: Es muss eine starke Kundenauthentifizierung im Wege technisch (mindestens) der Zwei-Faktor-Authentifizierung gegeben sein. Gewährleisten kann dies in aller Regel nur der jeweilige Paymentanbieter durch Schaffung eines entsprechenden Authentifizierungsprozesses, welchen der jeweilige Onlinehändler dann jeweils nur technisch im Rahmen seines Onlineshops abbilden kann (z.B. durch Einbindung entsprechender, an die PSD2 angepasster, aktualisierter Plugins der

Paymentanbieter).

In erster Linie technische Änderungen – Umsetzung der SCA muss durch den Paymentanbieter erfolgen

Wie dargestellt, sind in aller Regel nicht die Händler selbst Zahlungsanbieter im Sinne der PSD2, sondern machen sich vielmehr solche Zahlungsanbieter als Dritte zu Nutze bei der Abwicklung ihrer Zahlungen im eigenen Shop. Die Vorgaben einer SCA müssen vom Zahlungsanbieter selbst umgesetzt werden, nicht vom Händler.

Dementsprechend trifft den Händler selbst keine originäre Pflicht zur Umsetzung von Vorgaben der PSD2. Im Interesse einer reibungslosen Zahlungsabwicklung und Vermeidung möglicher Rückforderungen sollten Händler jedoch darauf achten, dass von der PSD2 erfasste Zahlungsarten spätestens vom 14.09.2019 an „PSD2-konform“ abgewickelt werden.

Dies bedeutet meist technische Anpassungen. Das „Material“ hierfür muss der jeweilige Paymentanbieter zur Verfügung stellen.

In aller Regel wird der jeweilige Onlinehändler auch gar keinen konkreten Einfluss auf den Ablauf der SCA nehmen können. Wie diese abläuft, ist ebenfalls Sache des jeweiligen Zahlungsdiensteanbieters.

Diese läuft technisch dann auch auf der Seite des Zahlungsdiensteanbieters ab, welche in den Shop des Händlers mittels eines Plugins / iframe eingebunden wird.

Welche Ausnahmen gibt es?

Nicht jede elektronische Zahlung im Bereich des Onlinehandels wird von dem SCA-Erfordernis der PSD2 erfasst.

So sind etwa Kleinbeträge unter 30 Euro vom Erfordernis der SCA ausgenommen.

Ferner besteht auch die Möglichkeit, dass der Kunde einen Zahlungsempfänger (z.B. seinen Stamm-Onlineshop) auf eine Whitelist setzen lässt, so dass bei der Autorisierung von Zahlungen an diesen Empfänger dann keine SCA erforderlich ist.

Zu beachten ist ferner, dass die PSD2 ausschließlich Zahlungen innerhalb der EU reguliert.

Wenn etwa ein Schweizer oder Amerikaner bei einem deutschen Onlineshop bezahlt, sind diese Zahlungen nicht von den Vorgaben der PSD2 erfasst. Auch bei Zahlungen aus Großbritannien könnte hier in Zukunft also ein anderer Rechtsrahmen gelten.

Aber auch hier gilt: Umgesetzt werden muss eine solche Ausnahme vom jeweiligen Paymentanbieter, nicht vom Onlinehändler.

Kein 2FA für Login in Kundenkonto erforderlich

Die IT-Recht Kanzlei erreichen derzeit viele Fragen, ob die Anmeldung des Kunden im Onlineshop des Händlers ebenfalls ab dem 14.09.2019 zwingend via 2FA erfolgen muss. Die klare Antwort lautet: Nein!

Selbst wenn der Kunde nach dem Einloggen in sein Kundenkonto ggf. ohne weitere Legitimation „händlereigene" Zahlungsmittel wie Vorkasseüberweisung, Kauf auf Rechnung oder Zahlung per Lastschrift (erneut) nutzen kann (die er evtl. bereits zuvor einmal genutzt hatte), macht dies keine 2FA für den Login erforderlich. Für diese Zahlungsarten sieht die PSD2 keine 2FA vor.

Eine (erneute) Zahlungsauslösung im Rahmen eines Zahlungsmittels, für das ab dem 14.09.2019 eine SCA Voraussetzung ist (z.B. Kreditkarte oder Paypal) darf in diesem Fall aber nicht alleine durch einen Login in das Kundenkonto möglich sein (was jedenfalls bei Paypal aber bereits jetzt technisch ausgeschlossen sein dürfte).

Fazit

Die PSD2-Richtlinie dürfte an den Onlinehändlern juristisch „vorbeirauschen".

Verpflichtet werden durch diese Richtlinie grundsätzlich die Zahlungsanbieter wie z.B. Paypal oder VISA selbst. Nur die wenigsten Onlinehändler treten selbst als Zahlungsdiensteanbieter auf. Das Gros der Händler bedient sich zur Abwicklungen von Zahlungen gerade solcher Anbieter und kann sich daher zurücklehnen.

Bei Zahlungen per Lastschrift oder Rechnung bzw. Vorkasseüberweisung, welche die Händler ggf. selbst durchführen, brauchen sich diese in Sachen PSD2 keine Gedanken machen. Auch die Zahlung via Nachnahme ist nicht erfasst.

Wer als Händler aber andere Zahlungsarten, wie die Zahlung per Kreditkarte oder Paypal anbietet, sollte den verbleibenden Monat nutzen, um zu prüfen, ob sein Paymentanbieter bereits eine 2FA unterstützt bzw. welche Schritte hierfür technisch noch implementiert werden müssen.

Oftmals muss dazu auch nur das vom Paymentdienstleister zur Verfügung gestellte Plugin geupdatet werden. Auskünfte und Hilfestellung erteilen hierzu die Paymentanbieter.

Das „Problem" PSD2 stellt sich für Onlinehändler also als ein technisches und nicht rechtliches dar.

Zu befürchten bleibt aber, dass die „Verkomplizierung" der Zahlungsabwicklung im Rahmen des Checkouts zu vermehrten Kaufabbrüchen führen dürfte.

Hat der Kunde den zusätzlichen Faktor für eine erfolgreiche 2FA nicht zur Hand, kommt er mit dem Checkout nicht weiter und wird diesen daher abbrechen. Gerade beim Bestellen von der Couch aus oder via Mobilgerät dürfte es dann schnell vorbei sein mit der gewohnte Bequemlichkeit.

Sie möchten Ihren Onlinehandel rechtssicher gestalten? Verlassen Sie sich auf die Schutzpakete der IT-Recht Kanzlei.

Autor:
RA Nicolai Amereller
Rechtsanwalt