Zahlungsdiensterichtlinie bis 14. September 2019 umsetzen

Die gar nicht mehr so neue Zahlungsdiensterichtlinie schlägt momentan Wellen und verunsichert Händler. Wer ist verpflichtet? Was ist zu tun? ECC-Clubmitglied Rechtsanwalt Rolf Becker, Partner bei WIENKE & BECKER – KÖLN, bringt Licht ins Dunkel.

Open Banking, „Aus" der SMS-TAN und starke Kundenauthentifizierung: Die EU-Zahlungsdiensterichtlinie PSD2 (Payment Services Directive 2) hält einige Neuerungen bereit, die im bereits seit 13.01.2018 gültigen Gesetz zur Umsetzung der 2. Zahlungsdiensterichtlinie verankert sind. Die Neuerungen sollen mit der Öffnung zu Datenzugängen Wettbewerb fördern und den Zahlungsverkehr sicherer machen. Bereits seit 2018 gilt die Vorgabe der PSD2, wonach keine Gebühren mehr für bestimmte Zahlarten verlangt werden dürfen (Surcharging-Verbot).

Starke Kundenauthentifizierung

Während es bei Open Banking um die Öffnung des Bankensystems durch Zugriff auf die Kontodaten für Drittanbieter über Schnittstellen geht („Access to Account" oder XS2A), die SMS-TAN mit ihrem nachvollziehbaren Tod neue Herausforderungen für den Verbraucher bringt, ist die starke Kundenauthentifizierung oder auch Zwei-Faktor Authentifizierung ein Thema, das der Handel fürchtet. Dabei sind nicht die Händler die Adressaten der neuen Verpflichtungen, sondern die Zahlungsdienstleister. Die müssen ab dem 14.09.2019 die starke Kundenauthentifizierung („Strong Customer Authentication") umsetzen. Zu den Zahlungsdienstleistern gehören auch Zahlungsauslösedienstleister.

Zusätzliche Eingaben für Kunden

Bei der starken Kundenauthentifizierung muss zur Benutzerkennung und Passwort (= Wissenskategorie) ein weiteres Merkmal aus der Kategorie Besitz (Karte, Smartphone) oder Inhärenz (Fingerabdruck, Stimme) treten, welches die Authentifizierung unterstützt. Meist ist dies ein weiterer Code. Der wird dann über Apps, wie Google Authenticator oder spezifische Banking-Apps erzeugt, denn vorgedruckte Listen (TAN-Listen) sind nicht mehr erlaubt. Einfach die Kreditkarten einzugeben oder über PayPal per Kennung und Passwort die Zahlung anzustoßen, reicht dann nicht mehr. Natürlich fürchtet der Handel Performanceverluste, denn jeder zusätzliche Klick stört die Konversion.

Die Implementierung benötigt Zeit und Ressourcen. Daher sahen die technischen Regulierungsstandards für eine starke Kundenauthentifizierung (Regulatory Technical Standard „RTS") eine längere Umsetzungsfrist vor, die aber eben im September abläuft. Selbst die Zahlungsdienstleister können zu Zeit noch nicht alle sagen, wie sie die Vorgaben umsetzen. Schon werden Stimmen nach Fristverlängerung laut.

PayPal gehört wie Amazon Pay, Paydirekt und Klarna zu den Anbietern, die noch keine konkreten Angaben machen. Vermutlich wird die Eingabe einer TAN Pflicht, über die auch heute schon der Kontenzugang abgesichert werden kann. Aber auch die PayPal-App bietet Möglichkeiten bis hin zur Implementierung einer Gesichtserkennung. Hier kann es aber auch Unterschiede je nach hinterlegter tatsächlicher Zahlart geben. Denn Einzugsermächtigungen müssen anders als Kreditkartenzahlungen nicht gesondert abgesichert werden. Die Händler sollen dabei nicht weiter belastet werden. Klarna sieht Rechnungs- und Ratenkauf als nicht betroffen an.

Weitere Ausnahmen von der Pflicht zur starken Kundenauthentifizierung betreffen neben vom Zahler als vertrauenswürdig eingestufte Empfänger (Whitelist), wiederkehrende Zahlungen und auch Kleinbetragszahlungen mit Transaktionen bis zu 30 Euro. Die Summe der Beträge darf seit der letzten starken Authentifizierung allerdings 100 Euro nicht übersteigen. Zudem ist diese Ausnahme auf maximal 5

Zahlungsvorgänge beschränkt. Ab der sechsten Zahlung wird also auch bei Kleinbeträgen wieder eine starke Authentifizierung erforderlich.

Händlerpflichten
Der Händler ist verpflichtet, nach § 312d Abs. 1 BGB, Art. 246a § 1 Abs. 1 Nr. 7 EGBGB Informationen zur Zahlung zu erteilen (Informationen über: „die Zahlungs-, Liefer- und Leistungsbedingungen, …“). Das bedeutet, dass – meist in den AGB – Ergänzungen zur starken Kundenauthentifizierung aufzunehmen sind. Je nach Zahlungsdienstleister dürften mehr Daten im Transfer vom Händler zum Zahlungsdienstleister anfallen. Hier sind die Informationspflichten nach der DSGVO berührt. Händler müssen deshalb ggf. ihre Datenschutzhinweise ergänzen und aufführen, welche (weiteren) Daten übermittelt werden.

Grundlage der Datenübermittlung
Unsicherheit besteht zudem noch, wie diese Datentransfers rechtlich legitimiert sein können. Neben interessenbasierten Grundlagen (Art. 6 Abs. 1 lit. f DSGVO) nennen Zahlungsdienstleister Auftragsverarbeitung (Art. 28 DSGVO) als Grundlage. Das ist aber dann nicht recht nachvollziehbar, wenn sich der Zahlungsdienstleister als Auftragsverarbeiter des Händlers sieht. Denn die starke Kundenauthentifizierung ist nicht die Pflicht des Händlers, sondern des Zahlungsdienstleisters. In Betracht kommt schließlich noch eine Datenerhebung und Verarbeitung auf der Basis einer gemeinsamen Verantwortung nach Art. 26 DSGVO. Auftragsverarbeitung und Datenaustausch in gemeinsamer Verantwortung setzen wieder gesonderte vertragliche Abreden voraus, die zwischen Händler und Zahlungsdienstleister getroffen werden müssen.

Welche Basis letztlich in den Datenschutzbedingungen genannt werden muss, hängt von dem Datenaustausch und seiner Organisation ab. Die wiederum verlangt eventuell nicht unerheblichen Implementierungsaufwand. Es wird also höchste Zeit für Händler, sich mit dem Thema zu beschäftigen.

Fazit:
Die Händler sind nicht direkt, aber indirekt betroffen. Zahlungsanbieter mauern noch, weil sie selbst noch an Lösungen basteln. Fakt ist, dass Händler AGB und eventuell auch Datenschutzhinweise ergänzen müssen.

Mit besten Grüßen

Rolf Becker

Über den Autor

Rechtsanwalt Rolf Becker ist Partner der Rechtsanwälte WIENKE & BECKER (www.kanzlei-wbk.de) in Köln und Autor von Fachbüchern und Fachartikeln zum Wettbewerbsrecht, Markenrecht und Vertriebsrecht, insbesondere im Fernabsatz. Als Mitglied im ECC-Club kommentiert Rechtsanwalt Becker für das ECC Köln regelmäßig aktuelle Urteile zum Onlinehandel und gibt Händlern praktische Tipps, wie sie mit den gesetzlichen Vorgaben umgehen sollen.

RA Becker auf Twitter: http://twitter.com/rolfbecker

Er ist auch Autor des Informationsdienstes www.Versandhandelsrecht.de.