

## ECC-Rechtstipp

von RA Rolf Becker ([rbecker@kanzlei-wbk.de](mailto:rbecker@kanzlei-wbk.de))

### Sicherheit von Internetzahlungen



„Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSi)“ sollen ab dem 5. November 2015 verbindlich gelten. Sie stammen aus einer Leitlinie der europäischen Bankenaufsichtsbehörde (EBA) und wurden von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) im Mai für verbindlich erklärt. Mit dem Rundschreiben wird die Zeit bis zum Inkrafttreten der PSD II (Payment Services Directive II – Zahlungsdiensterichtlinie II) überbrückt. Damit kommen einige dort vorgesehene Neuerungen schneller als gedacht. Sechs Monate Umsetzungsfrist laufen Anfang November ab.

Der Handel befürchtet, dass man sich mit diesen Anforderungen vermehrte Kaufabbrüche einhandelt, weil kompliziertere Zahlungsabwicklungen frustrierte Kunden produzieren. Zwar werden auch Händler eine größere Sicherheit beim Bezahlen befürworten, aber damit einhergehende Umsatzverluste werden natürlich ungern in Kauf genommen. Hintergrund der Befürchtungen sind vor allem die neuen Anforderungen an eine sog. „starke Kundenauthentifizierung“.

Auszug aus dem Rundschreiben der BaFin:

*„Starke Kundenauthentifizierung ist im Sinne dieses Rundschreibens ein Verfahren, das auf der Verwendung zweier oder mehrerer der folgenden Elemente basiert, die als Wissen, Besitz und Inhärenz kategorisiert werden: i) etwas, das nur der Nutzer weiß, z. B. ein statisches Passwort, ein Code, eine persönliche Identifikationsnummer, ii) etwas, das nur der Nutzer besitzt, z. B. ein Token, eine Smartcard, ein Mobiltelefon, iii) eine Eigenschaft des Nutzers, z. B. ein biometrisches Charakteristikum, etwa ein Fingerabdruck. Außerdem müssen die gewählten Elemente unabhängig voneinander sein, d. h. die Verletzung eines Elements darf keinen Einfluss auf das andere bzw. die anderen haben. Mindestens eines der Elemente sollte nicht wiederverwendbar und nicht reproduzierbar (die Inhärenz ausgenommen) sein und nicht heimlich über das Internet entwendet werden können. Das starke Authentifizierungsverfahren sollte so gestaltet sein, dass die Vertraulichkeit der Authentifizierungsdaten gewahrt bleibt.“*

Zahlungsdienstleister werden gezwungen, diese starken Authentifizierungen in vielen Fällen einzusetzen. Klar ist allerdings, dass eine 2-Faktor-Authentifizierung viele Kunden abschrecken

wird. Schon heute scheitern viele Käufer an einem Passwort. Erst recht wird dies der Fall sein, wenn bei einem Bezahlvorgang noch weitere Sicherungsmittel präsentiert werden müssen. Müssen erst das Mobilgerät hergeholt werden, etwa eine App gestartet oder per SMS übermittelte Codes abgelesen und wieder am Computer eingegeben werden, sind Kaufabbrüche vorprogrammiert.

Händler sind unmittelbar nicht angesprochen und für sie gibt es allenfalls mittelbaren Handlungsbedarf. Adressaten der neuen Regelung sind im Wesentlichen die Zahlungsdienstleister, z. B. Internetzahlungsdienste wie PayPal, die browserbasierte Zahlungsdienstleistungen erbringen. Diese müssen dann gegebenenfalls Online-Händlern Vorgaben machen, um starke Authentifizierungen künftig zu ermöglichen. Gewohnte Services, wie man sie etwa bei Amazon und Co. kennt, bei denen man etwa eine einmal hinterlegte Kreditkarte oder Bankdaten bei weiteren Zahlungen für einen Kauf einfach nur kurz auswählt oder auch nur vorausgewählt und meist kaum reflektiert bestehen lässt, könnten damit künftig auf der Strecke bleiben.

Die BaFin, welche die Einhaltung der Mindestanforderungen künftig überwacht, hat in den letzten Tagen noch einmal bestätigt, dass sie ausschließlich Zahlungsdienstleister im Fokus hat. Man darf gespannt sein, wie sich die Lage in drei Wochen entwickelt.

Insgesamt sollen Zahlungen im Online-Bereich auch nach Auffassung des europäischen Richtliniengebers bald noch transparenter und sicherer werden. Vor wenigen Tagen wurde die überarbeitete Zahlungsdiensterichtlinie (Payment Services Directive II oder PSD2) angenommen. Die neuen Vorschriften, die im Jahr 2013 von der EU-Kommission vorgeschlagen wurden, sollen den Verbraucherschutz verbessern, Innovationen fördern und die Sicherheit von Zahlungsdiensten erhöhen und Zahlungen billiger machen. Sie enthält daher z. B. Verbote für Händler, Entgelte für bestimmte Zahlungskarten zu erheben (erlaubt nur noch für Drei-Parteien-Kreditkartensysteme). Nach Verabschiedung der Richtlinie durch den Ministerrat der EU und deren Veröffentlichung im Amtsblatt haben die Mitgliedsstaaten zwei Jahre Zeit, um die erforderlichen Anpassungen der nationalen Rechtsvorschriften vorzunehmen. Dann wird man sehen, wie man z. B. Deutschland mit den Möglichkeiten umgeht.

### **Über den Autor**

Rechtsanwalt Rolf Becker ([www.rolfbecker.de](http://www.rolfbecker.de)) ist Partner der Rechtsanwälte WIENKE & BECKER ([www.kanzlei-wbk.de](http://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 Online-Handel 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 auf den Informationsdiensten [www.Versandhandelsrecht.de](http://www.Versandhandelsrecht.de) und [www.fernabsatz-gesetz.de](http://www.fernabsatz-gesetz.de).

Dieser Rechtstipp ist Teil des Informationsangebots des E-Commerce-Center Köln (ECC Köln) an der IFH Institut für Handelsforschung GmbH, Köln.

Kontakt:

E-Commerce-Center Köln  
c/o IFH Institut für Handelsforschung GmbH  
Dürener Str. 401 b  
50858 Köln  
Telefon: +49 (0) 221 943607-70  
Telefax: +49 (0) 221 943607-59

[info@ecckoeln.de](mailto:info@ecckoeln.de) | [www.ecckoeln.de](http://www.ecckoeln.de) und [www.ifhkoeln.de](http://www.ifhkoeln.de)

Erscheinungsdatum: Oktober 2015