PSD II: Die Frist zur Umsetzung läuft

Von Christian Conreder und Ulrike Schild

Mit der Veröffentlichung der PSD II im Amtsblatt der Europäischen Union am 23. Dezember 2015 hat die zweijährige Frist bis zur Umsetzung begonnen. Ab dem 13. Januar 2018 gelten dann die neuen Regelungen, zu denen unter anderem der Kontozugang für Drittanbieter, die Haftung des kontoführenden Zahlungsdienstleisters bei missbräuchlichen Transaktionen und die starke Kundenauthentifizierung zählen. Weil die Zeit zur Ermittlung der nötigen Anpassungen knapp bemessen ist, raten die Autoren dazu, schnellstmöglich Maßnahmen in die Wege zu leiten. Red.

Zur Verbesserung des grenzüberschreitenden Dienstleistungs- und Warenverkehrs wurde in den letzten Jahren das Zahlungsverkehrsrecht unionsweit stark vereinheitlicht. Durch den harmonisierten Zahlungsverkehrsmarkt sollen nicht nur der Wettbewerb gefördert und die technischen Neuerungen im Zahlungsverkehr berücksichtigt, sondern auch der Verbraucherschutz und die Sicherheit von Zahlungsdiensten erhöht werden.

Im Zuge dieser Harmonisierungsmaßnahmen wurde auch die Zahlungsdiensterichtlinie 2007/64/EG (PSD I) einer grundlegenden Prüfung unterzogen, in deren Folge am 24. Juli 2013 ein Vorschlag für eine überarbeitete Zahlungsdiensterichtlinie (PSD II) von der Europäischen Kommission veröffentlicht wurde. Die finale PSD II wurde am 23. Dezember 2015 im Amtsblatt der Europäischen Union veröffentlicht (Richtlinie (EU) 2015/2366).

Die bislang geltende PSD I beschränkte sich auf die Regulierung der Tätigkeiten von Kreditinstituten, E-Geld-Instituten sowie Zahlungsinstituten, die Zahlungsdienste erbringen. Sie sah hauptsächlich Regelungen für die Erteilung und den Entzug der Zulassung, Eigenmittel- und Sicherungsanforderungen sowie für erlaubte und nicht erlaubte Tätigkeiten vor. Um die Sicherheit im elektronischen Zahlungsverkehr weiter zu erhöhen, wurden mit der PSD II neue Regelungen unter anderem für eine verstärkte Kundenauthentifizierung, für sogenannte Drittdienste und im Hinblick auf Haftungsfragen eingeführt.

Durch den erhöhten Verbraucherschutz sowie die neuen aufsichtsrechtlichen Anforderungen werden den Zahlungsdienstleistern neue Pflichten und Herausforderungen auferlegt. Dieser neue Pflichtenkreis wird durch die PSD II auch auf sogenannte dritte Zahlungsdienstleister erweitert, die Zahlungsauslöse- und/oder Kontoinformationsdienste anbieten. Einige Neuerungen sind dabei besonders hervorzuheben.

Zu den Autoren

Dr. Christian Conreder, Hamburg, und **Ulrike Schild**, Frankfurt am Main, beide KPMG Rechtsanwaltsgesellschaft mbH

Anwendungsbereich erweitert auf „one-leg-out-transactions"

Der Anwendungsbereich der PSD II wird erweitert. So sind die Bestimmungen der PSD II zu Transparenz- und Informationspflichten (Titel III der PSD II) sowie die Bestimmungen über Rechte und Pflichten im Zusammenhang mit der Bereitstellung und Nutzung von Zahlungsdiensten (Titel IV der PSD II) auch bei sogenannten „one-leg-out-transactions" anwendbar.

„One-leg-out-transactions" bezeichnen Zahlungsvorgänge, bei denen nur einer der beteiligten Zahlungsdienstleister in der Europäischen Union ansässig ist. Dabei spielt die Währungseinheit (wie US-Dollar, Euro, Britische Pfund) keine Rolle. Zahlungstransaktionen mit einem Drittstaatenbezug müssen, jedenfalls im Hinblick auf die Zahlungsdienste, die in der Europäischen Union erbracht werden, die oben beschriebenen Kriterien erfüllen.

Regulierung weiterer Zahlungsdienstleister

Neben den nach der PSD I bisher regulierten Zahlungsdienstleistern (unter anderem

Kreditinstitute, Zahlungsinstitute und E-Geld-Institute) werden künftig auch sogenannte dritte Zahlungsdienstleister reguliert. Dritte Zahlungsdienstleister sind nach der PSD II Zahlungsauslösedienste, Kontoinformationsdienste sowie weitere Drittdienste.

Solche dritten Zahlungsdienstleister bieten typischerweise kein Zahlungskonto an, sondern stellen vielmehr eine Softwarebrücke zwischen Händler und Webportal des kontoführenden Zahlungsdienstleisters her, um den Zugang zu dem Konto oder zu Informationen zu ermöglichen.

Zahlungsauslösediensten, wie beispielsweise Sofort-Überweisung oder Giropay, ist nach den Anforderungen der PSD II vom kontoführenden Institut ein Zugang zum Online-Zahlungskonto des Kunden bei diesem zu gewähren. Hierzu baut der Zahlungsauslösedienst zwischen der Webseite des Online-Händlers und dem Internetportal des kontoführenden Zahlungsinstituts eine Softwarebrücke auf. Über diese Softwarebrücke kann der Zahler selbst den Zahlungsvorgang auslösen oder seine persönlichen Zahlungsauthentifikationsmerkmale (in der Regel PIN und TAN) an den Zahlungsauslösedienst weitergeben, der mit diesen Daten den Zahlungsvorgang für den Zahler auslöst.

Anforderungen an Zahlungsauslösedienste

Der Zahlungsauslösedienst ist in den Zahlungsvorgang nur zu dem Zweck der tatsächlichen Zahlungsauslösung eingebunden. Hierzu stellt die PSD II verschiedene Regelungen auf.

- So darf der Zahlungsauslösedienst beispielsweise zu keiner Zeit Geldbeträge des Zahlers im Zusammenhang mit der Bereitstellung des Zahlungsauslösedienstes halten.

- Er muss unter anderem sicherstellen, dass die persönlichen Sicherheitsmerkmale des Zahlers keiner anderen Partei außer dem Zahler selbst sowie dem Herausgeber der Sicherheitsmerkmale zugänglich sind und dass sie vom Zahlungsauslösedienst über sichere Kanäle übermittelt werden.

- Zudem muss gewährleistet werden, dass alle weiteren bei der Bereitstellung des Zahlungsauslösedienstes erlangten Informationen über den Zahler nur mit ausdrücklicher Zustimmung des Zahlers dem Zahlungsempfänger mitgeteilt werden dürfen.

- Ferner darf der Zahlungsauslösedienst keine sensiblen Zahlungsdaten des Zahlers speichern.

Kontozugang für Zahlungsauslöse- und Kontoinformationsdienste

Auch an das kontoführende Institut des Zahlungsdienstnutzers werden neue Anforderungen gestellt. So muss es vor allem den Zugang zum Konto ermöglichen. Eine Ablehnung des Zugangs kommt nur unter objektiven und gebührend nachgewiesenen Gründen im Zusammenhang mit nicht autorisiertem oder betrügerischem Zugang zum Zahlungskonto in Betracht. In solchen Fällen ist der Zahler unverzüglich nach der Zugangsverweigerung, in der vorab vereinbarten Form über die Verweigerung des Zugangs sowie deren Gründe zu informieren.

Zahlungsaufträge, die über den Zahlungsauslösedienst übermittelt werden, müssen hinsichtlich der zeitlichen Abwicklung, der Prioritäten und der Entgelte in derselben Weise behandelt werden wie Zahlungsaufträge, die direkt über den Zahler übermittelt werden. Die zuständige Behörde ist ebenfalls unverzüglich über den Vorfall, einschließlich der Einzelheiten und der Gründe, zu informieren. Schließlich kann die Zahlung nach Abschluss des Zahlungsvorgangs bei dem Zahlungsauslösedienst nicht mehr vom Zahler rückgängig gemacht werden.

Eine weitere Gruppe sogenannter dritter Zahlungsdienstleister sind die Kontoinformationsdienste. Sie rufen Informationen im Auftrag ihres Kunden von einem oder mehreren Online-Zahlungskonten bei einem oder mehreren Zahlungsdienstleistern ab, um diese zusammenzufassen und dem Kontoinhaber einen Überblick über seine finanzielle Situation aufzuzeigen.

Damit Kontoinformationsdienstleister ihre Dienste anbieten können, ist auch ihnen ein Zugang zum Online-Zahlungskonto des Kunden zu gewähren. Das kontoführende Zahlungsinstitut ist verpflichtet, dem Kontoinformationsdienst ebenfalls einen diskriminierungsfreien Zugang zum Online-Zahlungskonto zu ermöglichen. Auch hier kommt eine Ablehnung nur bei Vorliegen objektiver Gründe in Betracht.

Daneben gibt es noch einen weiteren „Drittdienst". Ein Zahlungsdienstleister, der kartengebundene Zahlungsinstrumente herausgibt, ist berechtigt, bei dem kontoführenden Zahlungsinstitut eine Bestätigung anzufordern, ob der Betrag, der für einen konkreten kartengebundenen Zahlungsvorgang erforderlich ist, auf dem Online-Zahlungskonto des Zahlers verfügbar ist (Abfragedienst). Das kontoführende Institut ist nach den Regeln der PSD II verpflichtet, dem Abfragedienst unverzüglich mit einer „Ja"- oder „Nein"-Mitteilung zu antworten. Eine Mitteilung des Kontostandes sowie ein „Blocken" des angefragten Geldbetrages auf dem Zahlungskonto sind jedoch nicht erlaubt.

EBA-Register für Zahlungsdienstleister

Neu ist ebenfalls die Einführung eines zentralen elektronischen Registers der Europäischen Bankenaufsichtsbehörde (EBA-Register). Das zentrale EBA-Register soll die Namen der Stellen veröffentlichen, die Zahlungsdienste erbringen. Auch die Mitgliedstaaten der Europäischen Union werden zur Einrichtung öffentlicher Register

verpflichtet, in die unter anderem die jeweils national zugelassenen Zahlungsinstitute sowie die Zahlungsdienste, für die das jeweilige Institut zugelassen ist, einzutragen sind.

Zahlungsauslösedienstleister müssen in Zukunft eine Zulassung als Zahlungsinstitut beantragen, wobei sie nach Zulassung in das jeweilige nationale Register sowie das EBA-Register aufzunehmen sind. Kontoinformationsdienstleister bedürfen zwar keiner Zulassung, sie werden aber gemäß PSD II weitestgehend wie Zahlungsinstitute behandelt und müssen daher ebenfalls in das zukünftige EBA-Register eingetragen werden.

Das EBA-Register soll auf der Website der EBA kostenlos öffentlich zugänglich gemacht werden. Für die Erstellung des EBA-Registers wird die EBA Entwürfe technischer Durchführungsstandards im Hinblick auf die Einzelheiten und die Struktur der zu übermittelnden Informationen erarbeiten (inklusive eines gemeinsamen Formats und Musters) und wird diese bis zum 13. Juli 2017 an die Europäische Kommission übermitteln.

Starke Kundenauthentifizierung

Ein erheblicher Teil der neuen Anforderungen im Zusammenhang mit der starken Kundenauthentifizierung wurde bereits mit dem Rundschreiben „Mindestanforderung an die Sicherheit von Internetzahlungen" (MaSI) der BaFin vom Mai 2015 (Rundschreiben 4/2015), die seit dem 5. November 2015 in Kraft getreten sind, geregelt.[1)] Diese Anforderungen werden durch die PSD II nochmals verschärft.

Zukünftig muss der Zahlungsdienstleister eine starke Kundenauthentifizierung verlangen, wenn der Zahler zum Beispiel online auf sein Zahlungskonto zugreift oder einen elektronischen Zahlungsvorgang auslöst. Neu bei Letzterem ist, dass die Authentifizierung durch dynamische Codes bei der Auslösung eines elektronischen Zahlungsvorgangs erfolgen muss.

Mindestens eines der Merkmale muss also dynamisch mit dem bestimmten Betrag und dem bestimmten Zahlungsempfänger verknüpft sein. Dies kann beispielsweise per SMS als Mobile TAN geschehen. Die zu verwendende Mobile TAN muss mit dem Betrag und dem Zahlungsempfänger der konkreten Zahlungstransaktion verbunden sein.

Zudem wird die EBA in enger Zusammenarbeit mit der Europäischen Zentralbank (EZB) Entwürfe technischer Regulierungsstandards unter anderem zu den Erfordernissen des Verfahrens zur starken Kundenauthentifizierung und der Ausnahmen von der starken Kundenauthentifizierung bis zum 13. Januar 2017 an die Europäische Kommission übermitteln.

Neben den aufsichtsrechtlichen Regelungen, enthält die PSD II auch neue zivilrechtliche Haftungsregelungen. Bestreitet der Zahlungsdienstnutzer eine Zahlung „autorisiert" zu haben, hat der Zahlungsdienstleister nachzuweisen, dass der Zahlungsvorgang vom Zahlungsdienstnutzer autorisiert war, ordnungsgemäß aufgezeichnet und verbucht und nicht durch eine technische Panne oder einen anderen Fehler des von dem Zahlungsdienstleisters erbrachten Dienstes beeinträchtigt wurde.

Kontoführender Zahlungsdienstleister haftet

Gelingt dieser Nachweis nicht, muss der Zahlungsdienstleister den Betrag des nichtautorisierten Zahlungsvorgangs unverzüglich, spätestens jedoch zum Ende des folgenden Geschäftstages, dem Zahlungsdienstnutzer erstatten. Diese Pflicht trifft den kontoführenden Zahlungsdienstleister auch, wenn der Zahlungsvorgang über einen Zahlungsauslösedienst ausgelöst wurde. Der kontoführende Zahlungsdienstleister kann dann bei Haftung des Zahlungsauslösedienstes von diesem eine Entschädigung verlangen. Die Haftungsbeteiligung des Kunden für Schäden, die infolge eines nicht autorisierten Zahlungsvorgangs unter Nutzung eines verlorenen oder gestohlenen Zahlungsinstruments oder infolge der missbräuchlichen Verwendung eines Zahlungsinstruments entstehen, wird durch die PSD II von 150 Euro auf 50 Euro erheblich reduziert.

Hat der Zahler in betrügerischer Absicht gehandelt oder vorsätzlich oder grob fahrlässig eine oder mehrere Pflichten in Bezug auf den Umgang mit den Zahlungsinstrumenten oder personalisierten Sicherheitsmerkmalen verletzt, findet die Haftungshöchstgrenze keine Anwendung. Der Zahler hat in diesem Fall die Schäden selbst zu tragen.

Die Umsetzungszeit hat begonnen

Spätestens jetzt sollten sich die Zahlungsdienstleister, die von der PSD II betroffen sind, mit den auf sie zukommenden neuen Herausforderungen auseinandersetzen. Die Zeit zur Ermittlung der erforderlichen Anpassungen ist knapp bemessen und beginnt mit der nun im Amtsblatt der Europäischen Union veröffentlichten PSD II (23. Dezember 2015) zu laufen.

Nach Inkrafttreten der PSD II haben die Mitgliedstaaten nur zwei Jahre – bis zum 13. Januar 2018 – Zeit, um die Neuerungen in nationales Recht zu überführen. Ab dem 13. Januar 2018 müssen die neuen Vorschriften angewendet werden. Dies bedeutet, dass alle betroffenen Zahlungsdienstleister am 13. Januar 2018 die neuen Herausforderungen der PSD II umgesetzt haben und anwenden müssen. Daher sollten schnellstmöglich die ersten Maßnahmen ergriffen werden.

Fußnote:

1) Siehe hierzu Prescher/Schild, Internetzahlungen: Die MaSI sind in Kraft, cards Karten cartes, 3/2015, S. 14 ff.