Stellungnahme

Bitkom Stellungnahme zum Entwurf eines Gesetzes zur Umsetzung der aufsichtsrechtlichen Vorschriften der Zweiten Zahlungsdiensterichtlinie (ZDUG) des BMF

4. Januar 2017

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Marco Liesenjohann
Referent Wissenschaftlicher Dienst
Vertretungsweise Betreuung Banking, Financial Services & FinTechs
T +49 30 27576-207
m.liesenjohann@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Bitkom bedankt sich beim Bundesministerium für Finanzen für die Gelegenheit zur Stellungnahme zum Entwurf eines Gesetzes zur Umsetzung der aufsichtsrechtlichen Vorschriften der Zweiten Zahlungsdiensterichtlinie (ZDUG).

Bitkom unterstützt die Ziele, die der Umsetzung der Zweiten Zahlungsdiensterichtlinie zugrunde liegen, in vollem Umfang:

- Förderung von Innovationen im Zahlungsverkehr,
- Erhöhung der Sicherheit des Zahlungsverkehrs und von Zahlungsdiensten,
- Konkretisierung des Anwendungsbereichs und der Ausnahmetatbestände und
- Verbesserung des Verbraucherschutzes.

Bei der Umsetzung in deutsches Recht unter der Vorgabe der Vollharmonisierung möchte Bitkom mit dieser Stellungnahme einen Beitrag dazu leisten, dass diese Ziele

erreicht werden.

Wir möchten insbesondere zur starken Kundenauthentifizierung im jetzigen Gesetzesentwurf zu Änderungen und Präzisierungen anregen, die letztlich zur Verbesserung der Sicherheit für Verbraucher bei der Zahlungsabwicklung führen. Außerdem möchten wir den Gesetzgeber auf potenzielle Mehrfach-Regulierung im Zusammenhang mit dem aktuellen Entwurf des Geldwäschegesetzes unter anderem im Hinblick auf Einrichtung einer zentralen Kontaktstelle und auf potenzielle Doppelprüfung durch Zahlungsauslösedienstleister hinweisen. Unsere Vorschläge zu Bußgeldvorschriften und Übergangsmodalitäten sollen dazu motivieren, bei der Ausgestaltung des Gesetzes wirtschafts- sowie wettbewerbsfördernde Anpassungen nicht auszuschließen, sofern diese nicht im Widerspruch mit den Zielen der Zweiten Zahlungsdiensterichtlinie stehen.

Zu § 27 ZAG-E – Interne Kontrollmechanismen

Im Rahmen der Registrierung für Kontoinformationsdienstleister nach § 34 ZAG-E ist sachgemäß (vgl. auch Artikel 33 Absatz 1 der Zweiten Zahlungsdiensterichtlinie) nicht die Einreichung einer Beschreibung der internen Kontrollmechanismen i.S.d. § 27 ZAG-E vorgesehen. Allerdings ist der § 27 ZAG-E für Nur-Kontoinformationsdienstleister in § 2 Absatz 6 ZAG-E nicht als Ausnahme aufgeführt und somit seine Anwendungsreichweite für Kontoinformationsdienstleister unklar. Bitkom schlägt vor dies über eine vollständige oder teilweise Ausnahme ebenda zu heilen.

Zudem würde das Geldwäschegesetz nach aktuellem Entwurfsstand auf Institute im Sinne des § 1 Absatz 3 ZAG-E als Verpflichtete verweisen und Kontoinformationsdienstleister sind von diesem Begriff erfasst (vgl. § 1 Absatz 1 Nummer 1 ZAG-E). Bitkom regt an auf Basis der Geschäftsausrichtung von Kontoinformationsdienstleistern nochmals kritisch zu hinterfragen, ob für das Geldwäschegesetz eine entsprechende Verweisregelung sinnvoller wäre, die Institute, welche ausschließlich diese betreiben, von der Vollanwendung explizit ausnimmt. Alternativ wäre nur zielführend das Potential auszunutzen, welches eine gezielte Geldwäscheprävention für Kontoinformationsdienstleister mit sich bringen würde, d.h. insbesondere mittels weniger aber spezifischer Monitoringindizien (Stichwort: Rundumblick auf den Zahlungsdienstnutzer im Rahmen von Multibankingdiensten).

Daneben möchte Bitkom auch auf die absehbare Doppelprüfung hinsichtlich der Prävention von Geldwäsche und Terrorismusfinanzierung durch Zahlungsauslösedienstleister hinweisen. Das Geldwäschegesetz bzw. der § 27 Absatz 1 Nummer 5 ZAG-E erfasst nach aktuellem Entwurfsstand Institute im Sinne des § 1 Absatz 3 ZAG-E und somit auch Zahlungsauslösedienstleister als Verpflichtete. Die vollständige Anwendbarkeit der Geldwäscheanforderungen für Zahlungsauslösedienstleister erscheint auch hier wenig sachgerecht. Insbesondere ein entsprechendes Monitoring durch Zahlungsauslösedienste, die eine Art „Transaktionsvermittlerrolle“ zwischen Zahlungsdienstnutzern und kontoführenden Instituten vornehmen, führt im Ergebnis zu einer Doppelprüfung und Meldung des gleichen Sachverhalts aber zu keinerlei Mehrwert für die Geldwäscheprävention. Im Gegenteil: es wäre von einer ziellosen Mehrbelastung für die ohnehin bereits stark ausgelasteten Ermittlungsbehörden auszugehen.

Schließlich erscheint eine vollständige Anwendbarkeit des § 27 ZAG-E auf Zahlungsauslösedienstleister insgesamt nicht sachgerecht. Dies betrifft neben § 27 Absatz 1 Nummer 5 ZAG-E insbesondere auch § 27 Absatz 1 Nummer 4 und § 27 Absatz 2 ZAG-E in Verbindung mit § 24c Kreditwesengesetz.

Zu § 41 ZAG-E – Zentrale Kontaktstelle

Gemäß Artikel 29 Absatz 4 der Zweiten Zahlungsdiensterichtlinie können die Behörden des Aufnahmemitgliedstaats gegenüber ausländischen Zahlungsinstituten, die ihr Niederlassungsrecht über Agenten ausüben und deren Sitz sich in einem anderen Mitgliedstaat befindet, anordnen, dass eine zentrale Kontaktstelle benannt wird, um die Kommunikation und Berichterstattung zu erleichtern. Die Europäische Bankenaufsichtsbehörde ist aufgefordert, hierzu technische Regulierungsstandards zu entwerfen.

§ 41 Absatz 4 zielt jedoch darauf ab, dass parallel zu dieser mit § 41 ZAG-E umgesetzten Option im ebenfalls zur Konsultation vorliegenden Entwurf des Gesetzes zur Umsetzung der Vierten EU-Geldwäscherichtlinie erwogen wird, mit einem neuen § 26 Absatz 4a ZAG-E die Vorkehrungen für eine weitere Kontaktstelle auf Basis des Artikel 45 Absatz 9 der Vierten Geldwäscherichtlinie zu treffen. Das Bundesministerium der Finanzen wird ermächtigt, durch eine Rechtsverordnung Zahlungsdienstleistern und E-Geld-Emittenten, die im Inland in anderer Form als einer Zweigniederlassung niedergelassen sind, aufzuerlegen, eine Kontaktstelle einzurichten und die Aufgaben dieser Kontaktstelle näher zu bestimmen.

Entscheidet sich der Gesetzgeber für den Gebrauch der Option, sollten die Kriterien für die Kontaktstelle so gefasst werden, dass die Qualität der Maßnahmen zur Geldwäscheprävention und zur Verhinderung der Terrorismusfinanzierung bestmöglich gewährleistet werden kann, aber zugleich so flexibel sein, dass die Verpflichteten die Vorschriften einhalten können, ohne überzogenen Belastungen ausgesetzt zu werden. Wir sind in diesem Zusammenhang der Meinung, dass Artikel 45 Absatz 9 nicht zwingend vorschreibt, die zentrale Kontaktstelle im eigenen Hoheitsgebiet vorzusehen. Es ist durchaus denkbar, dass die bis Juni 2017 vorzulegenden technischen Regulierungsstandards der Europäischen Finanzaufsichtsbehörden auch andere Lösungsmöglichkeiten anbieten. Vor diesem Hintergrund plädieren wir nachdrücklich dafür, es den Zahlungsdienstleistern und E-Geld-Emittenten, die im Inland in anderer Form als einer Zweigniederlassung niedergelassen sind, auch zu ermöglichen, als zentrale Kontaktstelle geschulte, kenntnisreiche zentrale Kontaktstellen in einem anderen Mitgliedstaat zu benennen.

Zu § 55 ZAG-E – Meldung schwerwiegender Betriebs- oder Sicherheitsvorfälle

Wir empfehlen, dass die Vorschrift im Zusammenhang mit den derzeit stattfindenden Arbeiten zur Umsetzung des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 gesehen wird, das teilweise ähnliche Regelungen enthält. Insofern droht mit einer parallelen Verpflichtung von Zahlungsdienstleistern zu vergleichbaren Maßnahmen nach dem IT-Sicherheitsgesetz und dem § 55 ZAG-E eine vermeidbare Doppelbelastung. Wir plädieren daher dafür, in Abstimmung mit dem Bundesministerium des Innern zu

prüfen, ob wegen der bereits bestehenden Verpflichtungen durch das IT-Sicherheitsgesetzes auf eine gesonderte Umsetzung der Vorgaben aus § 55 ZAG-E verzichtet werden kann.

Außerdem gab es während der Umsetzung der MaSI bezüglich Meldung schwerwiegender Betriebs- oder Sicherheitsvorfälle bereits große Unsicherheiten, welche durch die FAQ der BaFin am 28.10.2015 adressiert wurden. Wir regen an, dass die Definitionen in der ZAG auch auf diesen Erfahrungswerten aufbauen. Erweiterungen sollten neben Anwendungsfällen auch Aussagen zur Betroffenheit von Systemen enthalten.

Zu § 56 ZAG-E – Starke Kundenauthentifizierung

Für innovative „payment wallets", die nur technisch durch Apps oder andere Softwarelösungen auf Smartphones oder sonstige IT-/Kommunikationsgeräte geladen werden, sollte klargestellt werden, dass sich die Anforderungen der starken Kundenauthentifizierung nur auf die Autorisierung des Zahlungsdienstes selbst erstrecken kann. Um doppelte und damit unverhältnismäßige Authentifizierungsmechanismen zu vermeiden, die insbesondere zukunftsorientierte Zahlungsinnovationen behindern könnten, sollte bei Regulierung des Authentifizierungsvorgangs zwischen der Autorisierung des (regulierten) Zahlungsdiensts selbst – je nach Risikolage, mit starker Kundenauthentifizierung – einerseits und dem bloßen Zugang zur technischen Lösung einer wallet oder sonstigen payment App auf dem Smartphone, Tablet oder sonstigen IT-Gerät (ohne starke Kundenauthentifizierung) andererseits unterschieden werden.

Zu Absatz 1 – 5

Wir sehen die Gefahr, dass mit dem Zahlungsdiensteumsetzungsgesetz Vorfestlegungen stattfinden, die im Nachhinein zu Interpretationsschwierigkeiten führen könnten. Nach der Zweiten Zahlungsdiensterichtlinie ist die starke Kundenauthentifizierung künftig immer dann erforderlich, wenn nicht der delegierte Rechtsakts der EU-Kommission nach Artikel 98 Zweite Zahlungsdiensterichtlinie Abweichungen hiervon gestattet. Im Auftrag des Artikels 98 an die Europäische Bankenaufsichtsbehörde (EBA) ist ausdrücklich niedergelegt, dass darin auch Ausnahmen von der Anwendung des Artikels 97 Absätze 1, 2 und 3 formuliert werden sollen. Wir regen daher an, Absatz 1 Satz 1 entsprechend anzupassen:

„Der Zahlungsdienstleister verlangt eine starke Kundenauthentifizierung oder alternativ ein zulässiges Vorgehen entsprechend den Vorgaben des delegierten Rechtsaktes gemäß Absatz 5, wenn der Zahler"

Ebenso sollte Absatz 2 neu gefasst werden, in:

„Handelt es sich im Falle des Absatzes 1 Satz 1 Nummer 2 um einen elektronischen Fernzahlungsvorgang, hat der Zahlungsdienstleister eine starke Kundenauthentifizierung ~~zu verlangen~~, die Elemente umfasst, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen,

zu verlangen oder alternativ ein zulässiges Vorgehen entsprechend den Vorgaben des delegierten Rechtsaktes gemäß Absatz 5 anzuwenden."

Zu Absatz 6

Eine Verordnung für eine begrenzte Übergangszeit kann erheblichen Schaden anrichten. Die Marktteilnehmer müssten sich dann unter Umständen nach der bereits erfolgten Anpassung ihrer Systeme an die Anforderungen des Rundschreibens der Bundesanstalt zu den Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) einen aufwändigen Zwischenschritt einlegen, um sich danach auf das Inkrafttreten des delegierten Rechtsakts nach Artikel 98 der EU-Kommission auf der Basis der technischen Regulierungsstandards für die Kundenauthentifizierung und Kommunikation der Europäischen Bankenaufsichtsbehörde vorzubereiten. Das halten wir für deutlich unverhältnismäßig.

Aus der Formulierung der Verordnungsermächtigung für das Bundesministerium der Finanzen wird zudem nicht deutlich, dass es, wie in der Gesetzesbegründung dann ausgeführt, um eine Übergangsmaßnahme bis zum Inkrafttreten des delegierten Rechtsakts gehen soll. Dies sollte daher in Absatz 6 deutlicher zum Ausdruck kommen, etwa durch die folgende Formulierung:

„Das Bundesministerium der Finanzen kann durch Rechtsverordnung nähere Bestimmungen über die bis zum Inkrafttreten des delegierten Rechtsakts gemäß Absatz 5 geltenden"

Zu § 57 ZAG-E - Zugang zu Zahlungskontodiensten bei CRR-Kreditinstituten

Bitkom möchte darauf hinweisen, dass der Regelungsinhalt des § 57 ZAG-E über eine Umsetzung des Artikels 36 der Zweiten Zahlungsdiensterichtlinie deutlich hinausgeht und so die Vorgabe des Erwägungsgrundes 39, wonach der Zugang zu Konten so sein soll, dass „das Zahlungsinstitut seine Dienstleistungen ungehindert und effizient erbringen kann", stark einschränkt.

Anders als in der Gesetzesbegründung dargelegt, stellt ein Kreditinstitut, das ein Sammelzahlungskonto für ein Zahlungsinstitut führt, lediglich die Zahlungsverkehrsinfrastruktur zur Verfügung, auf deren Basis durch den Drittdienst geprüfte Zahlungen ausgeführt werden. Kreditinstitute, wenn sie Sammelzahlungskonten führen, müssen sich darauf verlassen, dass die geldwäscherechtlichen Sorgfaltspflichten des Instituts von diesem eingehalten werden. Mit dem Kunden des Drittdienstes verbindet das Kreditinstitut aufgrund der Führung des Kontos für den Drittdienst keine Geschäftsbeziehung. Eine andere Interpretation verstieße gegen den Grundsatz der Trennung von Zahlungsverkehr und Grundgeschäft. Das Kreditinstitut, das ein Sammelzahlungskonto führt, hat zudem keinen Einfluss darauf, wer Zahlungen über das Konto vornimmt. Das Kreditinstitut hat auch keinerlei Verfügungsbefugnis über das Konto, kann Gelder also nicht zurücküberweisen. Erfolgen hier Zahlungen von Kunden des Drittdienstes, bestehen weder technische noch rechtliche Möglichkeiten, dies zu verhindern.

Die Vornahme von Konkretisierungen der europarechtlichen Regelung nach § 57 ZAG-E erscheinen auch aus den folgenden Gründen wenig zielführend:

Nach Artikel 97 Absatz 5 der Zweiten Zahlungsdiensterichtlinie bzw. § 56 Absatz 4 ZAG-E muss sichergestellt sein, dass der kontoführende Zahlungsdienstleister dem Zahlungsauslösedienstleister und dem Kontoinformationsdienstleister gestattet, sich auf die Authentifizierungsverfahren zu stützen, die er dem Zahlungsdienstnutzer selbst entsprechend der weiteren Vorgaben des Artikel 97 Absatz 1 bis 3 der Zweiten Zahlungsdiensterichtlinie bereitstellt. In der Praxis und so auch im Sinne der Zweiten Zahlungsdiensterichtlinie in anderen Vorschriften des ZAG-E abgebildet, findet technisch eine reine Weitergabe der personifizierten Sicherheitsmerkmale des Nutzers bei Einbindung eines Zahlungsauslösedienstleisters (§ 50 Absatz 1 Nummer 2 ZAG-E) bzw. eines Kontoinformationsdienstleisters (§ 52 Nummer 2 ZAG-E) an den kontoführenden Zahlungsdienstleister statt.

Dies heißt in der Konsequenz, auch bei Einbindung der neuen Zahlungsdienstleister verfügt das kontoführende Institut über die gleichen Informationen des Nutzers als würde sich dieser direkt im Onlinebanking mit seinen persönlichen Sicherheitsmerkmalen für ein persönliches oder ein Konto, für das er eine Verfügungsberechtigung besitzt, einloggen. Der in der Begründung zum ZDUG angeführte Hinweis auf Sammelkonten ist in diesem Zusammenhang unklar und bedürfte einer näheren Erläuterung. Würde von der Zweiten Zahlungsdiensterichtlinie-Praxis, d.h. der Weiterleitung von Sicherheitsmerkmalen im Rahmen der Zahlungsauslösung durch Sammelkonten für Drittdienste, abgewichen, wäre der Anwendungsbereich der Zweiten Zahlungsdiensterichtlinie nicht mehr gegeben und bilaterale Vereinbarungen zwischen Drittdienst und kontoführendem Institut notwendig, die z.B. auch entsprechende Sicherheitsvorkehrungen regeln müssten, die die derzeitigen Konkretisierungen vorsehen (vgl. hierzu Rational 19 des “EBA-Consultation Paper on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2”).

Die Konkretisierung der Regelung des Artikels 36 der Zweiten Zahlungsdiensterichtlinie in § 57 ZAG-E ist daher insgesamt unsachgemäß.

Zu § 61 ZAG-E – Beschwerden über Zahlungsdienstleister

Bitkom schlägt bezüglich der Umsetzung des Artikel 95 (1) der Zweiten Zahlungsdiensterichtlinie zur Spezifizierung der Zahlungsdienste, welche in den Geltungsbereich des Artikel fallen und analog der Vorgaben der MaSI (Mindestanforderungen zur Sicherheit von Internetzahlungen) im Kapitel 2 Risikobewertung und Kapitel 4 Risikominderung und – kontrolle sind, vor, dass die Erwartungshaltung der Regulierungsstelle in § 61 ZAG-E stärker zum Ausdruck kommt.

Zu § 66 ZAG-E – Bußgeldvorschriften

Die Etablierung eines neuen Bußgeldtatbestandes für Fälle, in denen eine starke Kundenauthentifizierung gemäß § 56 Absatz 1 und 2 unterlassen wird, geht über die Vorgaben der Zweite Zahlungsdiensterichtlinie hinaus, ohne dass hinreichende Gründe erkennbar sind. Die Pflicht zur starken Kundenauthentifizierung wird im Entwurf des Gesetzes zur Umsetzung des zivilrechtlichen Teils der Zweiten Zahlungsdiensterichtlinie durch Haftungsvorschriften (§ 675v BGB-E) unterlegt. Damit besteht bereits eine deutlich fühlbare Sanktion.

Daneben wird in § 66 keine Einschränkung für den Fall vorgenommen, dass der Zahlungsdienstleister von einer starken Kundenauthentifizierung gemäß § 56 Absatz 1 und 2 absehen darf. Damit würden – unseres Erachtens entgegen der Intention des Gesetzgebers - Ausnahmen von der starken Kundenauthentifizierung letztlich komplett ausgeschlossen, etwa bei Transaktionen mit geringem Risiko. Hier sollte in der Gesetzesbegründung Klarheit hergestellt werden.

Schließlich ist nicht nachvollziehbar, warum der Katalog der Bußgeldvorschriften in § 66 Absatz 2 ZAG-E zwar neue Bußgeldtatbestände enthält, aber keinen für die Fälle vorsieht, in denen ein CRR-Kreditinstitut Instituten entgegen § 57 ZAG-E die Möglichkeit des Zugangs zu Zahlungskontodiensten auf nicht-objektiver, diskriminierender oder unverhältnismäßiger Grundlage verweigert. Der Aufsicht sollten insbesondere für diesen kritischen Neuregelungsbereich des ZAG angemessene Sanktionsmittel zur Verfügung stehen. Der aktuelle Entwurf des § 675k BGB-E (Gesetz zur Umsetzung des zivilrechtlichen Teils der Zweiten Zahlungsdiensterichtlinie) sieht bisher ebenfalls lediglich eine Informationspflicht an den Zahlungdienstnutzer im Fall der Verweigerung vor.

Schlussbemerkung zu Übergangsfristen

Bitkom möchte abschließend betonen, wie wichtig klar definierte Übergangsfristen und etwaige abhängige Interimsvorgaben für die Wirtschaft sind. Das zeitlich spätere Wirksamwerden des delegierten Rechtsaktes der Europäischen Kommission auf Basis der technischen Regulierungsstandards der EBA für die Kundenauthentifizierung gegenüber dem des ZDUG führt zu Unsicherheiten, die vermeidbar erscheinen.

Zu den §§ 46 bis 52 ZAG-E – Inkrafttreten

In diesem Zusammenhang möchten wir insbesondere auf die noch zu regelnde Interimsphase eingehen, die sich daraus ergibt, dass die in den Titeln 1-3 des Abschnittes 10 (§§ 46 – 52 ZAG-E) enthaltenen Pflichten bei der Zusammenarbeit von kontoführenden Zahlungsdienstleistern mit Kontoinformationsdiensten bzw. Zahlungsauslösediensten durchsetzt sind mit Vorgaben, die sich auf Methoden der Authentifizierung und sicheren Kommunikation gemäß Artikel 98 der Zweiten Zahlungsdiensterichtlinie beziehen. Das gilt etwa für § 47 Satz ZAG-E, § 49 Absatz 1 Satz 1 ZAG-E, § 50 Absatz 1 Nr. 2b und Nr. 4 ZAG-E, § 51 Absatz 1 Nummer 1 ZAG-E sowie § 52 Nummer 3 ZAG-E. Angesichts der unterschiedlichen zeitlichen Wirksamkeit des ZDUG (zum 13. Januar 2018) und des delegierten Rechtsaktes der Europäischen Kommission auf Basis der technischen Regulierungsstandards der EBA für

die Kundenauthentifizierung und Kommunikation (frühestens zum September 2018) sind diese Vorschriften sinnvoll erst anwendbar, wenn der delegierte Rechtsakt vorliegt. Daher sollten unseres Erachtens auch die §§ 46 – 52 TAG-E erst zu diesem Zeitpunkt in Kraft gesetzt werden.