SICHEREN ZAHLUNGSVERKEHR FÜR VERBRAUCHER GEWÄHRLEISTEN

Stellungnahme zum Referentenentwurf eines Gesetzes zur Umsetzung der aufsichtsrechtlichen Vorschriften der Zweiten Zahlungsdiensterichtlinie

(Zahlungsdienstumsetzungsgesetz – ZDUG)

4. Januar 2017

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Finanzmarkt

Markgrafenstraße 66
10969 Berlin

finanzen@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. GEMEINSAME VORBEMERKUNG

Der Verbraucherzentrale Bundesverband (vzbv) bedankt sich für die Gelegenheit zur Stellungnahme zu den Referentenentwürfen des Bundesministeriums der Finanzen (BMF) und des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) zur Umsetzung der zweiten Zahlungsdiensterichtlinie - EU/2015/2366 - (PSD II).

Zahlungsdienste gehören zu den wichtigsten Finanzdienstleistungen für Verbraucherinnen und Verbraucher[1], auch wenn sie im Alltag häufig nur als Nebensache erscheinen. Marktdaten zufolge geht es dabei um einen Rechtsbereich, in dem es nur alleine bezogen auf das Zahlen im Einzelhandel jährlich bereits um bis zu 9,5 Milliarden unbare Transaktionen[2] geht. Davon entfällt erfahrungsgemäß ein erheblicher Anteil auf Verbraucher. Der Entwurf des BMJV beziffert zusätzlich rund 133 Millionen Zahlungsdienstrahmenverträgen (Girokonten und Kreditkartenverträge), die von diesem Gesetzesvorhaben reguliert werden. Die Richtlinie erfasst beides, den Rahmenvertrag als auch den einzelnen Zahlungsvorgang.

Nachdem das Zahlungsverkehrsrecht zuletzt 2009 auf Basis der ersten Zahlungsdiensterichtlinie (PSD I) umfassend neu gefasst wurde, erfährt dieses Rechtsgebiet mit der Umsetzung der Folgerichtlinie abermals wichtige Neuerungen, wie

- die Abschaffung des Zusatzentgeltes für das Bezahlen mit gängigen unbaren Zahlungsmitteln,
- verbesserten Verbraucherschutz bei unbefugten Zahlungsvorgängen, aber auch neue Sicherheitsanforderungen,
- mehr Drittkostentransparenz und
- die Regulierung von Zahlungsauslöse- und Kontoinformationsdiensten.

Die PSD II umfasst dabei wie ihr Vorgänger einen aufsichtsrechtlichen Teil, umzusetzen im Wesentlichen im Zahlungsdiensteaufsichtsgesetz (ZAG), und einen zivilrechtlichen Teil, dem im Bürgerlichen Gesetzbuch seit 2009 ein eigener Abschnitt im Schuldrecht gewidmet wurde. Folgerichtig wurden zwei Entwürfe von den beiden jeweils für ihren Bereich federführenden Ministerien vorgelegt. Auf beide geht der vzbv mit zwei Stellungnahmen gesondert ein.

Es gibt aber übergreifende Themen, die keine gänzlich getrennte Sicht nur auf einen der beiden Rechtsbereiche zulässt.

Jede einzelne als Zahlungsdienst im Aufsichtsrecht zu definierende Leistung auch im Zivilrecht als einzeln abrechenbaren Zahlungsdienst zuzulassen, wird dem Gedanken des Rahmenvertrages und der bisher entwickelten Grundsätze zum Girokonto nicht gerecht. Auch wenn die Begriffe aufeinander abzustimmen sind, sollte im Zivilrecht besser zwischen einer überwachten Dienstleistung und einer einzeln abrechnungsfähigen Leistung unterschieden werden.

Auch die Fragen von Sicherheitsvorgaben und Haftungsregelungen lassen sich nicht gänzlich entkoppeln.

---

[1] Die gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

[2] Jährliche Erhebung des EHI Retail Institute, vorgestellt auf dem Kartenkongress in Bonn 2016: Geschätzte 18-20 Mrd. Transaktionen insgesamt, davon 2015 erhoben unbar 47,6 Prozent, die unter die Rechtsvorschriften hier fallen.

II. WESENTLICHE AUFSICHTSRECHTLICHE FORDERUNGEN

- Von zentraler verbraucherpolitischer Bedeutung ist die sichere aber auch datenschutzrechtlich unbedenkliche Gestaltung der neu mit der Richtlinie zugelassenen Zahlungsauslöse- und Kontoinformationsdienste.

  Es ist wichtig, dass die Regelungen zur Versicherungspflicht und Haftung dieser Unternehmen auch das Risiko abdecken, dass Verbraucher auf gefälschte Zahlungsauslösedienste hereinfallen könnten.

  Noch wichtiger und besser wäre es aber, das verfahrenstechnisch ausgeschlossen wird, dass diese Dienste mehr Daten als sie für die Beauftragung einer Zahlung benötigen, überhaupt technisch einsehen können. Und um es Angreifern mit gefälschten Seiten möglichst schwer zu machen, sollte der Zugang für Zahlungsauslösediensten so vom gewöhnlichen Onlinebanking abweichen, dass Täter keine Möglichkeit haben, Zugangsdaten zu erlangen, mit denen sie über die echten Onlinebanking-Seiten Schaden auslösen können. Das kann bereits erreicht werden, wenn Auslösedienste, die sich einem Kontoinstitut gegenüber ohnehin besonders autorisieren müssen, keine PIN Angabe mehr abfragen dürfen, weil sie diese zum Zugang nur für einen Überweisungsvorgang nicht mehr benötigen.

- Bis heute fehlt es an einer Befugnis, aufsichtsrechtlich gegen Verstöße gegen Artikel 9 der SEPA-Migrationsverordnung vorzugehen. Darin ist geregelt, dass niemand, vorgeben darf, das sich ein Konto für Überweisungen und Lastschriften in Deutschland belegen befinden muss. Auch ein durch SEPA erreichbares Konto in einem anderen Mitgliedsland muss genügen. Bereits über zehn Abmahnungen musste der vzbv in kurzer Zeit aussprechen. Weitere werden zurzeit vorbereitet. Anbieter, die Verbrauchern in Deutschland die Nutzung eines Kontos in einem Nachbarland verweigern, ignorieren den Rechtsanspruch, nicht mehr in jedem Land ein eigenes Konto führen zu müssen, wenn man zum Beispiel in einem EU-Land arbeitet und im anderen wohnt.

  Der eigentlich zuständigen Bundesanstalt für Finanzdienstleistungsaufsicht fehlt die Kompetenz, dazu hoheitsrechtlich auch gegenüber Anbietern, die keine Finanzdienstleister sind, tätig werden zu dürfen.

- Viele Verbraucher werden überrascht, wenn sie eine dringende Überweisung zum nächsten Geschäftstag veranlassen müssen, dass bei vielen Instituten der Einlieferungsschluss bereits eher am frühen Nachmittag oder mittags gelegt ist. Die Richtlinien-Vorgabe, dass Zahlungen von einem auf den nächsten Geschäftstag auszuführen sind, wird durch diese Praxis in Frage gestellt.

  In einer gemeinsamen zivil- und aufsichtsrechtlichen Regelung sollte sichergestellt werden, dass der Annahmeschluss nicht willkürlich früh, sondern tatsächlich so gestaltet wird, wie das für einen ordnungsgemäßen Ablauf des Zahlungsverkehrs möglich ist.

Die näheren Ausführungen dazu befinden sich in der zivilrechtlichen Stellungnahme, auf die hierzu verwiesen wird.

III. ZU DEN REGELUNGEN IM EINZELNEN

Nachfolgend wird auf die aus Verbrauchersicht kritischen Punkte in der Reihenfolge der Vorschriften des Entwurfes jeweils gesondert eingegangen.

1. REGELUNGEN AUS DEM ENTWURF

1.1 Absicherung für den Haftungsfall von Zahlungsauslösediensten und Kontoinformationsdiensten (§§ 16 und 36 ZAG-E)

Mit der Umsetzung werden zwei neue Kategorien von Zahlungsdienstleistern geregelt, die es zwar schon seit längerem gibt, die bisher aber keine Regulierung und Überwachung erfahren haben, auch weil sie sich insofern von den üblichen Diensten unterscheiden, da sie keine Zahlungen selbst durchführen, also Gelder transferieren.

Zahlungsauslösedienste wirken bei der Auslösung eines Zahlungsvorganges des Zahlenden an den Zahlungsempfänger mit und teilen dem Zahlungsempfänger noch vor Zugang der Zahlung und an Stelle einer Bestätigung durch die Zahlungsdienstleister selber mit, dass die Zahlung unwiderruflich auf den Weg gebracht wurde. Zahlungsauslösedienste umgehen damit für Onlinehändler und -dienstleister das Erfordernis, sich auf von den Kontoinstituten angebotene teurere Zahlungsinstrumente einlassen zu müssen, mit denen Zahlungsempfängern Garantien für den Erfolg der Zahlung ausgesprochen werden. Ein bereits am deutschen Markt etabliertes Angebot ist „Sofortüberweisung“.

Kontoinformationsdiensten wird dagegen Zugang zu einem oder mehreren Girokonten gewährt, um dem Kontoinhaber die Daten aus seiner Kontonutzung aufzubereiten. Solche Dienste gibt es im Ansatz schon sehr lange, seit es die Homebanking-Schnittstellen gibt. Dies geht noch in die Zeit vor dem allgemeinen Internetzugang zurück. Heute sind dies jedoch Onlinedienste und Apps, die damit aber außerhalb der unmittelbaren Einflusssphäre des eigenen Gerätes des Nutzers mit sensiblen Kontodaten arbeiten.

Dass nun die Zuständigkeit zur Überwachung und Kontrolle dieser Anbieter, die Zugriff auf die Konten von Verbrauchern nehmen, für die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) begründet wird, ist zu begrüßen. Es bestehen dennoch weiterhin Sicherheits- und Datenschutzbedenken, wenn Dienste, die lediglich Zahlungen auf den Weg bringen sollen und mit denen der Verbraucher in keiner weiteren Vertragsbeziehung steht, Zugang zu hoch sensiblen Kontozugangsdaten erhalten.

Die Problematik wird im Entwurf, wenn es um die Regelungen der Berufshaftpflichtversicherung geht, gesehen, aber nicht gelöst: Während für die Kontoinformationsdienste in § 36 Absatz 1 ZAG-E unmittelbar die zu versichernde Haftung auch auf den Fall unbefugter und betrügerischer Zugriffe auf das Konto über diese Dienste einbezogen wird, fehlen für Zahlungsauslösedienste in § 16 Absatz 1 ZAG-E solche konkreten Vorgaben völlig. Denn hier wird nur festgelegt, dass die Versicherung die Haftung „gemäß den Vorschriften des Bürgerlichen Gesetzbuches“ abzudecken hat.

Tatsächlich ist in Frage zu stellen, ob das eigentlich von diesen Diensten ausgehende Risiko in irgendeiner rechtlich relevanten Weise damit versicherungstechnisch überhaupt abgedeckt wird.

Solange Kontozugangsdaten abgefragt werden, mit denen auch jeder Dritte Zugang zum Konto erlangen kann, also die gewöhnliche Konto-PIN gepaart mit einer TAN, besteht vor allem auch das Risiko, dass Verbraucher durch manipulierte „gehackte" Onlineshops oder gänzlich gefälschte Angebote (sogenannte *fake shops*) auf Webseiten weitergeleitet werden, die sich nach außen so verhalten, als wenn sie ein Zahlungsauslösedienst wären. Nach den Erfahrungen mit Phishing und Pharming-Angriffen auf Verbraucherkonten bedarf es keiner Darlegung mehr, warum dies gefährlich ist.

Selbst wenn die neuen Vorgaben der PSD II zur starken Kundenauthentifizierung, die noch durch weitere Sicherheitsanforderungen aus sekundärem Recht über die Europäische Bankenaufsicht (EBA) zur Zeit zu konkretisieren sind, künftig das Risiko einschränken werden, dass Unbefugte beliebige Zahlungen ausführen können, wird dies das Risiko, Schaden zu nehmen, wenn man auf solche gefälschte Seiten hereinfällt, alleine noch nicht ausschließen.

- Täter können weiterhin eine selbstgewählte Kontoverbindung nutzen, um den vom Kunden gewünschten Zahlvorgang umzuleiten. Denn niemand kann wirklich als Verbraucherkunde ausschließen, dass das Konto, das im Rahmen eines vorgeblichen Zahlungsauslösedienstes als Ziel angegeben wird, dem intendierten Berechtigten gehört.
- Täter können, nachdem sie sich für das Onlinebanking anmelden konnten, die Verbindung offen halten und Zugriff auf diverse Kontodaten nehmen. Neben wertvollen Daten, um den Verbraucher für weitere Straftaten auszuforschen, ist es sogar vorstellbar, dass Täter völlig neue Zahlungskonten auf den Namen des Betroffenen einrichten und die bei manchen Anbietern noch üblich Ein-Cent-Überweisung zur Übermittlung eines Passwortes nutzen, um das zur Identifizierung des Kunden und Freischaltung des neuen Kontos mit dieser Überweisung übertragene Passwort auszulesen. Ein argloser Verbraucher wird sich der Tragweite einer solchen „Fehlüberweisung" zu seinen Gunsten möglicherweise noch nicht einmal bewusst, wenn er sie später wahrnimmt. Damit sind auch Straftaten nach dem Geldwäschegesetz Tür und Tor geöffnet, und es besteht das Risiko, dass arglose Verbraucher ins Visier der Fahndung geraten.

Damit besteht das Dilemma, dass der europäische Gesetzgeber den Zahlungsauslösediensten zwar nun eine Plattform geschaffen hat, um mit eigenem Rechtsanspruch die Schnittstellen zum Onlinebanking der Banken nutzen zu können. Haftung und Kosten für diese Dienstleistungen werden jedoch auf alle anderen Marktteilnehmer, insbesondere auch Verbraucher verteilt:

- Kommt es zu Vermögens- oder Geldwäschedelikten, weil Täter Verbraucher zur Dateneingabe auf gefälschten Seiten locken konnten, bleibt entweder die Bank und damit im Ergebnis auch die Gemeinschaft ihrer Kunden auf den Kosten sitzen. Oder es wird dem Betroffenen sogar grobe Fahrlässigkeit vorgeworfen, was zur Folge hat, dass der Einzelne den Schaden alleine zu tragen hat.
- Nehmen solche initiierten Zahlungen über Onlinebanking zu, ist damit zu rechnen, dass Institute vermehrt Einzelnutzungsgebühren für Onlinebanking erheben werden. Erste Institute haben dies bereits getan. Durch die Praxis dieser

Anbieter wird damit für Verbraucher die Nutzung des Girokontos selbst dann teurer, wenn sie Auslösedienste gar nicht nutzen oder sogar ablehnen.

Der Gesetzgeber muss sicherstellen, dass zumindest die Gefahren, die von solchen Dienstleistungen ausgehen, nicht auf Verbraucher verlagert werden. Mehrere Wege stehen dafür zur Verfügung, wenigstens einer wäre zwingend umzusetzen:

- Gefährdungshaftung für Auslösedienste oder Haftungsausschluss für Verbraucher

  Es reicht nicht aus, eine Haftpflichtversicherungspflicht lediglich auf jene Handlungen vorzugeben, die nach dem geltenden Recht des BGB den Anbietern von Zahlungsauslösediensten zuzuweisen ist. Wollte man die realistische Gefahr, die von Nachahmern ausgeht versichern, müsste man einen dazu passenden Gefährdungshaftungstatbestand entwickeln. Oder es müsste auf Kosten dieser Dienste ein Fonds geschaffen werden, aus dem diese Schäden getragen werden. Alternativ könnte man auch ausschließen, dass Verbrauchern bei der Nutzung eines gefälschten Zugangs grobe Fahrlässigkeit vorgeworfen werden kann, wenn der gefälschte Dienst nicht hinreichend klar als falsch erkennbar war. Das würde aber nur den Einzelnen entlasten.

- Zugang für Auslösedienste sicherer gestalten

  Vielversprechender ist es, den Zugang für Zahlungsauslösedienste durch eine Abwandlung zu gestalten.
  Die geltenden Vorgaben der PSD II sehen in Artikel 66 Absatz 3 vor, dass Auslösedienste Daten nur für das Auslösen von Zahlungen nutzen dürfen. Auch die Datenschutzgrundverordnung zwingt die Kontoinstitute, die sensiblen weiteren Daten vor dem Zugriff durch Dritte zu schützen. Hinzu kommt nach Artikel 66 Absätze 3, Buchstabe d, dass Auslösedienste sich auch stets als solche zu identifizieren haben. Mindestens ein Dienstleister in Deutschland tut dies bisher nicht, weil er sich bisher Home- und Onlinebanking-Schnittstellen zu Dienste macht und diese ausliest und bearbeitet, als würde dies der Kontoinhaber selbst tun. (*Screenscraping*-Technologie).
  Im Kontext der weiteren Vorbereitung und Implementierung der Sicherheitsvorgaben wäre darauf zu drängen, solche Technologien zu beschränken. Wenn ein kontoführendes Institut künftig zu erkennen hat, dass ein Auslösedienst und nicht der Kunde selbst die Bank anspricht, dann sollte es auch keinen Zugriff auf alle Informationen mehr geben dürfen, die im Onlinebanking und Homebanking zur allgemeinen Kontoführung zur Verfügung gestellt werden. Ein Auslöseanbieter darf nach den Vorgaben nur Zugriff auf den Überweisungsauftrag haben. Erfolgt eine hinreichend sichere Authentifizierung dieser Anbieter über diese Schnittstelle, bedürfte es dann aber auch keiner Verwendung und Abfrage eines Konto-PIN mehr. Der Zahlungsvorgang könnte ähnlich wie bei einer Kartenzahlung mit dem 3DS Sicherheitsverfahren über die dynamisch verlinkte TAN gesichert werden, also jene Freigabenummer, die auf einen Zahlungsempfänger und einen Zahlbetrag schon spezifisch festgelegt wurden. Vorteile: Ohne PIN Abfrage kann kein Täter außerhalb der sicheren Anmeldung eines Auslösedienstes über das normale Onlinebanking Zugriff auf ein fremdes Konto nehmen. Und die über das Onlinebanking zu schützenden sensiblen Daten bleiben

technisch beim Nutzen eines Auslösedienstes weiter geschützt, weil sie vor diesen Diensten grundsätzlich verborgen bleiben.

Zur Umsetzung dieser Alternative wird auf die aktuelle Diskussion mit der EBA über die Sicherheitsstandards und über die Frage der weiteren Zulassung von Verfahren, die auf dem Markt heute dazu angewendet werden, verwiesen. Diese ist über den § 56 Absatz 4 und 5 ZAG-E im Rahmen der Vorgaben zur starken Kundenauthentifizierung antizipiert. Darin wird auf die nähere Ausgestaltung des Zugangs für Auslösedienste durch Vorgaben aus europäischem Sekundärrecht eingegangen. Die Vorgabe der Richtlinie, dass Auslösedienste die Sicherheitsvorgaben für das Onlinebanking nutzen können sollen, schreibt in diesem Kontext nicht verbindlich vor, dass sie alle Kontozugangsmerkmale nutzen können müssen. Ziel der Norm ist es nur, dass ein Auslösedienst durchgeführt werden kann. Der vzbv hat sich an der Konsultation zu den Sicherheitsfragen beteiligt. Dem vzbv ist bekannt, dass über die Details weiterhin diskutiert wird, dass aber selbst das Bundesamt für Sicherheit in der Informationstechnik hier Sicherheitsbedenken anmeldet. Mit der Schaffung des Rechtsanspruches für Zahlungsauslösedienste entfällt die Notwendigkeit für diese Dienste, sich als Kontoinhaber bei der Nutzung quasi zu tarnen. Damit ist der Anforderung zum Wettbewerbszugang auch für dritte Dienste zu Konten mehr als genüge getan. Es ist dann aber wichtig, nun die Sicherheitsgefahren zu begrenzen. Diese müssen sich nicht erst in Massen realisiert haben, um ihnen heute schon vorzubeugen.

> Der vzbv fordert, es in § 16 Absatz 1 ZAG-E nicht bei einem Verweis auf die sich ergebende Haftung nach den Vorschriften des Bürgerlichen Gesetzbuches zu belassen, wenn es nicht gelingt, die Sicherheitsvorgaben für den Zugang von Zahlungsauslösediensten mit der EBA sicher vor Trittbrettfahrern zu gestalten. Das setzt aus Sicht des vzbv voraus, dass Auslösedienste nicht jener Daten, vor allem nicht der PIN bedürfen und diese vom Verbraucher abfragen, die nicht auch von jedem anderen, dann aber Unbefugten, zum Kontozugang verwendet werden könnten.

1.2 Sicherheitsanforderungen bei der Ausgabe von E-Geld (§ 18 ZAG-E)

In § 18 ZAG-E ist ohne dafür in der Begründung aufzufindenden näheren Grund vorgesehen, dass Zahlungen für die Ausgabe von E-Geld spätestens nach fünf Geschäftstagen zu sichern sind. Nicht erkennbar ist, warum es dieser Frist und solange bedarf. Die Sicherung von E-Geld muss zu jedem Zeitpunkt bedeuten, dass Mittel, die dazu bei einer Stelle, die E-Geld ausgibt, getrennt als Kundengelder insolvenzsicher handzuhaben sind.

> Der vzbv erwartet eine Prüfung und, sollte es dieser Frist bedürfen, eine Erklärung, wie ausgeschlossen wird, dass Verbraucher, die E-Geld tauschen, deswegen keiner Schutzlücke in diesem Zeitraum unterfallen.

1.3 Pflichten des Zahlungsauslösedienstes (§ 50 ZAG-E)

In § 50 Absatz 1 Ziffer 3 ZAG-E werden Zahlungsauslösediensten viel mehr Rechte eingeräumt, als dies selbst für herkömmliche Zahlungsdienstleister vorgesehen ist oder von der Richtlinie gestattet wird.

Denn in diesem Absatz wird dem Zahlungsauslösedienst eingeräumt, dass er auch alle anderen mit dem Auslösedienst erlangten Informationen an den Zahlungsempfänger weitergeben darf, solange der Zahlungsdienstnutzer dem nur ausdrücklich zugestimmt hat.

Einen Einwilligungsvorbehalt kennt die Richtlinie nicht. Vielmehr bestimmen die zugehörigen Vorgaben in Artikel 66 Absatz 3 zu den Buchstaben f und g, dass Zahlungsauslösedienstleister weder andere Daten, als die für das Ausführen des Auslösedienstes erforderlichen, verlangen dürfen, noch das diese Daten für andere Zwecke als den Zahlungsauslösevorgang verwenden dürfen. Dies wird zwar nachfolgend in den Ziffern 6 und 7 in § 50 Absatz 1 ZAG-E wiederholt. Es steht dann aber im Widerspruch zur Ziffer 3. In Ziffer 3 wird sogar wörtlich auf die Weitergabe „aller anderen Daten“ Bezug genommen, die es nach Ziffer 6 und 7 gar nicht geben darf.

Dies steht auch im Widerspruch zu § 46 Absatz 2 ZAG-E. In dieser Norm gibt es strenge Vorgaben für Zahlungsdienstleister selbst, wenn es um die Kontoabfrage im Vorfeld einer Kartenzahlung geht. Denn hier wird vorgegeben, dass dem Ersuchen, ob ein zu einer Karte gehöriges Konto einen deckungsfähigen Kontostand ausweist, nur mit Ja oder Nein aber nie mit dem Kontostand geantwortet werden darf. Ein Auslösedienst, der sich diese Frage selbständig beantwortet, indem er auf den Kontostand Zugriff nimmt, umgeht diese Vorgabe bereits, die aus Sicht des vzbv zu Recht zur Sicherstellung des Datenschutzes aufgestellt wurde. Nun würden diese Dienste sogar mehr dürfen, als selbst Zahlungsdienstleistern gestattet wird.

Wenn Verbraucher zahlen wollen, wollen sie kurzfristig einen Kauf- bzw. Bestellvorgang abschließen. Ihr Ziel ist es, sich auf diesen Vorgang zu konzentrieren und nicht viel weitergehende rechtliche Erklärungen abzugeben. Zahlen muss möglich bleiben, ohne zugleich in weitergehende Datennutzungen einwilligen zu müssen. Denn der Grundsatz der Einwilligung als solches wäre gefährdet, wenn Zahlen nur noch bedingt ohne die zusätzliche Datenverwertung möglich wäre. Zum Beispiel weil gar keine Zahlungswege als solche, die zusätzlichen Einwilligungen verlangen, von einem Anbieter mehr angeboten werden. Völlig zu Recht verbietet die Richtlinie eine weitergehende Nutzung der Daten, die mit dem Zahlungsauslösevorgang angefallen sind. Auch das deutsche Gesetz darf diese Möglichkeit nicht schaffen.

> Der vzbv fordert, den richtlinienwidrigen und für den Datenschutz sehr gefährlichen § 50 Absatz 1 Ziffer 3 ZAG-E zu streichen. Zahlungen auszuführen und darüber hinaus Daten zu sammeln müssen zwei klar getrennte Vorgänge bleiben. Wenn es einer besonderen Einwilligung bedarf, darf diese nicht anders als in § 60 Absatz 2 ZAG-E für Zahlungsdienstleister geregelt werden. Dort ist das Zustimmungsbedürfnis zugleich auf die für die Erbringung des Zahlungsdienstes notwendigen Daten begrenzt.

2. FEHLENDE REGELUNG IM ENTWURF

Aufsichtsgrundlage zur Überwachung von Artikel 9 SEPA Migrationsverordnung

Im Zuge der SEPA-Migrationsverordnung (EU/260/2012) wurde in Artikel 9 die Pflicht formuliert, dass weder Zahler noch Zahlungsempfänger Vorgaben machen darf, dass sich ein Konto, dass für SEPA erreichbar ist, in einem bestimmten Land befinden muss. Dieses Recht soll es unter anderem Verbrauchern ermöglichen, nicht mehr als ein Konto führen zu müssen, wenn sie als Grenzgänger in einem Mitgliedsstaat arbeiten aber in einem anderen wohnen, wenn sie zeitweilig in ein anderes Mitgliedsland umziehen oder wenn sie den Markt an Zahlungskontodienstleistern im Binnenmarkt und insbesondere unter SEPA diskriminierungsfrei nutzen wollen.

Der vzbv mahnt derzeit zahlreiche Unternehmen ab, die gegen diese Vorgabe verstoßen. Die Unternehmen zeigen sich einerseits überrascht durch diese Norm, streiten teilweise sogar ab, dass es sich um eine verbraucherschützende Norm handele, die wir verfolgen können, oder sie machen geltend, dass es ihnen auf Grund anderer Normen verboten sei, die Verordnung zu befolgen, etwa aus Gründen des Geldwäschegesetzes.

Der vzbv wird ungeachtet dieser Einwände seine Möglichkeiten zur Rechtsdurchsetzung wahrnehmen. Allerdings wird es kaum möglich sein, auf diesem Wege jedes Unternehmen unverzüglich zur Einhaltung der Rechtsvorgaben zu zwingen.

Tatsächlich fehlt es in Deutschland an der vorgeschriebenen zuständigen Behörde für die Durchsetzung auch des Artikels 9 der Verordnung, da es der BaFin bislang an der Kompetenz fehlt, aufsichtsrechtlich auch an gewerbliche Zahlungsdienstnutzer heranzutreten. In diesem Kontext bedarf es dann auch eines Bußgeldtatbestand zur Sanktionsbewehrung der Vorgaben. Beides sind Pflichten der Bundesrepublik aus der Verordnung nach den Artikeln 10 und 11.

> Der vzbv erwartet, dass im Rahmen der Umsetzung der PSD II dafür Sorge getragen wird, dass die Umsetzung von Artikel 9 der SEPA-Migrationsverordnung auch aufsichtsrechtlich im Verantwortungsumfeld der BaFin wahrgenommen werden und Verstöße als Ordnungswidrigkeit geahndet werden können.