MINISTERIUM FÜR FINANZEN UND WIRTSCHAFT
BADEN-WÜRTTEMBERG

Postfach 10 14 53 70013 Stuttgart
E-Mail: poststelle@mfw.bwl.de
FAX: 0711 123-4791

Präsidenten des Landtags
von Baden-Württemberg
Herrn Wilfried Klenk MdL
Haus des Landtags
Konrad-Adenauer-Str. 3
70173 Stuttgart

Stuttgart 07.05.2015
Name Reinhard Knödler
Telefon 0711 123-2216
Aktenzeichen 95-4203.26
(Bitte bei Antwort angeben)

nachrichtlich - ohne Anlagen -

Staatsministerium
Innenministerium
Ministerium für Ländlichen Raum
und Verbraucherschutz

Antrag der Abg. Karl Rombach u. a. CDU
- EU-Zahlungsdiensterichtlinie II (Payments Services Directive II, PSD II)
- Drucksache 15 / 6642

Ihr Schreiben vom 24. März 2015

Anlagen

Beschluss des Bundesrats BR-Drs. 602 /13 (B)

Sehr geehrter Herr Landtagspräsident,

das Ministerium für Finanzen und Wirtschaft nimmt zu dem oben genannten Antrag wie folgt Stellung:

Der Landtag wolle beschließen, die Landesregierung zu ersuchen, zu berichten,

1. *welche Änderungen durch die Überarbeitung der Zahlungsdiensterichtlinie der Europäischen Union (EU-Zahlungsdiensterichtlinie II, Payments Services Directive II, PSD II) erfolgen, die die Sicherheit des Zahlungsverkehrs betreffen;*

Zu 1.:

Die Zahlungsdiensterichtlinie II (PSD II) wird die ursprüngliche Zahlungsdiensterichtlinie (PSD I) aus dem Jahr 2007 ergänzen und ersetzen. Bislang liegt die PSD II allerdings lediglich im Entwurf vor. Dieser Entwurf kann im gegenwärtig stattfindenden Trilogverfahren noch geändert werden.

Die in die PSD II neu aufgenommenen Regelungen zielen darauf ab, für unterschiedliche Formen von Zahlungsdienstleistungen einen einheitlichen Binnenmarkt zu schaffen, Lücken im Verbraucherschutz zu schließen, die Sicherheit von Zahlungen zu verbessern und eine größere Konsistenz der Aufsichtsregimes in den Mitgliedstaaten der EU zu erreichen.

Insbesondere soll mit der PSD II der starken Zunahme von elektronischen und mobilen Zahlungen sowie dem Aufkommen innovativer Zahlungsdienstleistungen Rechnung getragen werden.

Zu diesem Zweck wird der Geltungsbereich der PSD II auf die sog. Dritten Zahlungsdienstleister (Third Party Payment Service Provider, TPP) ausgedehnt. Die TPPs führen im Auftrag des Verbrauchers (Zahlers) Dienstleistungen aus, bei denen sie Zugriff auf das Zahlungskonto des Verbrauchers bei dessen kontoführendem Kreditinstitut erhalten. Dadurch können insbesondere für den kontoführenden Zahlungsdienstleister neue Risiken entstehen.

Ein wichtiges Ziel der PSD II ist die Erhöhung der Sicherheit von Zahlungsdienstleistungen. Dem dienen insbesondere die Einführung sicherheitsbezogener Dokumentations- und Berichtspflichten für die unterschiedlichen Zahlungsdienstleister im Rahmen der Zulassung und im laufenden Geschäftsbetrieb bei sicherheitsrelevanten Vorfällen sowie die Einführung der verstärkten Kundenauthentifizierung bei elektronischen Zahlungsvorgängen. Zudem sollen die Möglichkeiten der Mitgliedsstaaten, durch die Ausübung von Wahlmöglichkeiten die Sicherheitsanforderungen zu senken, eingeschränkt werden.

2. *wie die Sicherheit im Zahlungsverkehr durch die EU-Zahlungsdiensterichtlinie II sichergestellt werden soll;*

Zu 2.:

Wie in 1. dargestellt, soll die Sicherheit im Zahlungsverkehr insbesondere durch die Schaffung sicherheitsbezogener Dokumentations- und Berichtspflichten, die Ausweitung des Geltungsbereichs der PSD II auf TPPs und durch die Einführung einer verstärkten Kundenauthentifizierung erhöht werden.

Im Antrag auf Zu*lassung als Zahlungsinstitut* müssen bspw. Verfahren zur Überwachung, Handhabung und Folgemaßnahmen bei Sicherheitsvorfällen und sicherheitsbezogenen Kundenbeschwerden (Art. 5 Abs. 1f PSD II) und Mechanismen für die Überwachung, die Rückverfolgung und den Zugang zu sensiblen Zahlungsdaten (Art. 5 Abs. 1g PSD II) dokumentiert werden.

Alle Zahlungsdienstleister müssen sicherheitsrelevante Vorfälle im *laufenden Geschäftsbetrieb* an die Aufsichtsbehörden berichten. Wenn ein Sicherheitsvorfall die finanziellen Interessen der Kunden tangiert, dann muss der Zahlungsdienstleister direkt und unverzüglich die Kunden darüber in Kenntnis setzen und sie über Maßnahmen zur Schadensabwehr informieren (Artikel 85).

Den mit dem Zugriff der *Dritten Zahlungsdiensteanbieter* (TPPs) auf die Zahlungskonten bei den kreditführenden Zahlungsdienstleistern verbundenen Risiken soll dadurch entgegengewirkt werden, dass die TPPs durch die PSD II erstmals aufsichtsrechtlich erlaubnispflichtig werden. Damit gelten auch für die TPPs die von der PSD II vorgesehenen Dokumentations- und Berichtspflichten und sie sind den zivilrechtlichen Regelungen des Zahlungsverkehrs unterworfen. Der EU-Gesetzgeber hat hierdurch die sich aus der Zwischenschaltung solcher Dienstleister in dem jeweiligen Zahlungsvorgang ergebenden Sicherheitsrisiken für den Zahlungsverkehr lösen wollen. Dritte Zahlungsdienstleister müssen deshalb ähnliche Pflichten erfüllen wie das kontoführende Institut selbst. Löst ein dritter Zahlungsdienstleister auf Verlangen des Zahlers einen Zahlungsauftrag aus, so ist er nach Art. 39 PSD II zur Übermittlung von bestimmten zusätzlichen Informationen an den Zahler und an den Zahlungsempfänger nach Auslösung verpflichtet. Nach Art. 40 PSD II hat der dritte Zahlungsdienstleister im Falle von Betrug oder anderweitigen Streitigkeiten dem Zahler und dem kontoführenden Zahlungsdienstleister die Referenz der Zahlungsvorgänge und die Zulassungsinformationen zur Verfügung zu stellen.

Durch die Mitwirkung am Zahlungsvorgang erhalten die dritten Zahlungsdienstleister Zugang zu sensiblen Kundendaten. Nach Art. 58 und 59 PSD II unterliegen die dritten Zahlungsdienstleister bestimmten Pflichten zum Schutz dieser sensiblen Daten und der Information an den Zahler über die eingesehenen Daten. Daher hat ein dritter Zahlungsdienstleister bei Erbringung eines Zahlungsauslösedienstes u.a. zu gewährleisten,

- dass er keinen Besitz an Geldern des Zahlungsdienstnutzers erlangt;
- dass keinerlei Informationen über den Zahlungsdienstnutzer, die er während des Zahlungsvorgangs erlangt hat, einer anderen Partei zugänglich sind;
- dass er sich gegenüber dem / den kontoführenden Zahlungsdienstleister(n) des Kontoinhabers jedes Mal, wenn eine Zahlung ausgelöst wird oder Kontoinformationen erfasst werden, über eine verstärkte Authentifizierung authentifiziert, es sei denn Ausnahmen iSd Art. 87a PSD II stehen zur Verfügung;
- dass er keine personalisierten Sicherheitsdaten des Zahlungsdienstenutzers speichert und von ihm keinerlei weitere Daten verlangt als solche, die für die Ausführung des Zahlungsvorgangs erforderlich sind; und
- dass er Daten nicht verwendet, sich zu ihnen Zugang verschafft oder speichert, es sei denn für die vom Zahler ausdrücklich geforderten Zahlungsvorgänge (Art. 58 Abs. 2 PSD II),
- dass er den Betrag, den Empfänger oder ein anderes Merkmal des Zahlungsvorgangs nicht verändert.

Zur Erhöhung der Sicherheit sieht die PSD II eine *verstärkte Kundenauthentifizierung* gegenüber dem kontoführenden Institut vor, wenn der Zahler (i) online Zugang zu seinem Zahlungskonto erhält, (ii) einen elektronischen Zahlungsvorgang auslöst oder (iii) eine andere Transaktion über einen Fernzugang durchführt, die das Risiko von Zahlungsbetrug oder anderem Missbrauch in sich birgt (Art. 87 Abs. 1 PSD II). Verstärkte Kundenauthentifizierung bezeichnet dabei ein Authentifizierungsverfahren, das auf der Verwendung zweier oder mehr Merkmale jeweils aus den Bereichen Wissen (bspw. PIN), Besitz (bspw. Verwendung des eigenen Smartphones) oder Biometrie beruht.

Elektronische Zahlungsvorgänge erfordern auch dann eine verstärkte Authentifizierung, wenn die Zahlung durch einen Dritten Zahlungsdienstleister ausgelöst wird (Art. 87 Abs. 1c PSD II).

Die Einhaltung der Sicherheitsstandards im Zahlungsverkehr soll durch die behördliche Aufsicht (in Deutschland voraussichtlich die BaFin) gewährleistet werden. Ein Verstoß gegen die Sicherheitsanforderungen soll sanktioniert werden können.

3. *welche Gefahren, insbesondere im Bereich der Cyberkriminalität, durch die in der EU-Zahlungsdiensterichtlinie II vorgesehene Weitergabe von PIN und TAN des Online-Bankings an dritte Zahlungsdienstleister entstehen;*

Zu 3.:

Das PIN/TAN-Verfahren unterteilt sich in den Zugang zum Konto, der mit der persönlichen Identifikationsnummer (PIN) erfolgt, und der eigentlichen geschäftlichen Transaktion, die mit der Transaktionsnummer (TAN) erfolgt. Da PIN und TAN in einem automatischen und geheimen Verfahren von den Banken an die Kunden übermittelt werden, erhält nur der Kunde selbst Kenntnis von PIN und TAN. Die derzeit relativ hohe Sicherheit des Online-Bankings basiert auf dem vertraulichen Umgang mit PIN und TAN zwischen dem Kunden und der Bank.

Bei der Weitergabe von PIN und TAN des Online-Bankings an dritte Zahlungsdienstleister besteht die Gefahr durch die Manipulation des Kunden (Social Engineering) insbesondere in folgenden Fällen:

- Der Zahler übergibt direkt PIN / TAN an gefälschten Zahlungsdienstleister via E-Mail. An dieser Stelle glaubt der Kunde einem dritten vertrauenswürdigen Zahlungsdienstleister seine Daten zu übermitteln. Jedoch werden diese Daten von den Dritten strafbar missbraucht. Die Pflicht des dritten Zahlungsdienstleisters, auch sich selbst jeweils gegenüber dem kontoführenden Zahlungsdienstleister über eine verstärkte Authentifizierung zu authentifizieren und mit dem Zahlungsdienstnutzer und dem kontoführenden Institut nur über sichere Wege zu kommunizieren (Art. 58 Abs. 1a PSD II), soll dieses Risiko verringern.

- Betrüger fangen die Daten ab, wenn ein Zahler die PIN / die TAN an einen vertrauenswürdigen dritten Zahlungsdienstleister übermitteln will (sog. Man-in-the-Middle-Angriff). Hier ist zum einen der Zahler selbst zu sensibilisieren. Zum anderen müssen die verantwortlichen dritten Zahlungsdienstleister bzw. Zahlungsinsti-

tute für eine sichere IT-Umgebung sorgen, in der solche Angriffe nicht möglich sind bzw. verhindert werden.

- Auch im Rahmen von Apps besteht die Gefahr, dass Betrüger Apps erstellen und so als vertrauenswürdiger dritter Zahlungsdienstleister auftreten und PIN / TAN des Zahlers abfangen. Zur Vermeidung dieser Gefahr könnten Zahlungsinstitute App-Dienste zulassen bzw. eine Authentifizierung anfordern und über die zugelassenen App-Dienste die Zahler informieren. Nicht zugelassenen / authentifizierten App-Diensten wäre sodann der Zugriff auf das Zahlungskonto zu versagen. Derartige Praktiken will die PSD II durch Erlaubnispflicht für dritte Zahlungsdienstleister und die Auflagen für deren Dienstleistungen unterbinden.

Werden die Systeme der Dritten Zahlungsdienstleister oder der Online-Händler gehackt, ist es durchaus möglich, dass das Authentifizierungsverfahren umgangen werden kann. Kommt ein Hacker in den Besitz von PIN und TAN, hat er die Möglichkeit, sich gegenüber dem kontoführenden Zahlungsdienstleister zu authentifizieren, ohne dass dies zunächst bemerkt wird. Bis der Schaden entdeckt wird, kann es wegen der Flüchtigkeit der digitalen Spuren für die Wiedererlangung des Geldes oder eine erfolgreiche Ermittlung der Täter bereits zu spät sein.

Um die Risiken eines Schadens zu minimieren und den Tätern den Erfolg zu erschweren, müsste in solchen Verfahren die TAN stets dynamisch generiert und an die jeweilige Transaktion gebunden werden, wie beispielsweise bei dem ChipTAN- oder dem mTAN-Verfahren.

Mit dem vermehrten Einsatz Dritter Zahlungsdienstleister steigt auch gleichzeitig die Gefahr für Kunden, Opfer einer Phishing-Straftat zu werden. Sollte - begünstigt durch den Erlass der EU-Zahlungsdiensterichtlinie II - die Anzahl derartiger Dienstleister stark ansteigen, kann es für den Endkunden zunehmend schwierig werden, zwischen der Plattform eines seriösen Zahlungsdienstleisters und einer täuschend echt aussehenden Phishing-Webseite zu unterscheiden. Gibt der Kunde auf einer gefälschten Seite des Dritten Zahlungsdienstleisters die PIN zu seinem Konto ein, hat der Täter den vollen Lesezugriff. Das ermöglicht ihm die Manipulation weiterer Authentifizierungsattribute, einschließlich der Mobilfunknummer für das m-TAN-Verfahren.

4. *wie die Haftung in der EU-Zahlungsdiensterichtlinie II zwischen drittem Zahlungsdienstleister und dem Kreditinstitut, das das Konto des Kunden führt, geregelt ist;*

Zu 4.:

Die Änderungen, die durch die überarbeitete Zahlungsdiensterichtlinie erfolgen werden, stehen noch nicht fest (siehe 1.). Nach dem Ratsbeschluss vom 1. Dezember 2014 soll zwischen der Haftung für *unautorisierte Zahlungen* und der Haftung für *nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen* unterschieden werden.

Bei *unautorisierten Zahlungen* erstattet der kontoführende Zahlungsdienstleister unverzüglich den Betrag des nicht autorisierten Zahlungsvorgangs und bringt das belastete Zahlungskonto gegebenenfalls wieder auf den Stand, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte (Art. 65 Abs. 2 PSD II). Haftet der Zahlungsauslösedienstleister für den nicht autorisierten Zahlungsvorgang, so entschädigt er den kontoführenden Zahlungsdienstleister auf dessen Verlangen unverzüglich für alle infolge der Erstattung an den Zahler erlittenen Verluste oder gezahlten Beträge, einschließlich des Betrags, der Gegenstand des nicht autorisierten Zahlungsvorgangs war. Der Zahlungsauslösedienstleister muss nachweisen, dass der Zahlungsvorgang – innerhalb seines Zuständigkeitsbereichs – authentifiziert, ordnungsgemäß aufgezeichnet und nicht durch eine technische Panne oder einen anderen Mangel im Zusammenhang mit seinem Zahlungsdienst beeinträchtigt wurde. Eine darüber hinausgehende finanzielle Entschädigung kann nach dem auf den Vertrag zwischen dem Zahler und dem Zahlungsdienstleister anwendbaren Recht oder gegebenenfalls nach dem Vertrag zwischen dem Zahler und dem Zahlungsauslösedienstleister festgelegt werden.

Bei *nicht erfolgter, fehlerhafter oder verspäteter Ausführung von Zahlungsvorgängen* haftet der kontoführende Zahlungsdienstleister gegenüber dem Zahler für die korrekte Ausführung des Zahlungsvorgangs und erstattet gegebenenfalls den Betrag, der Gegenstand des nicht oder fehlerhaft ausgeführten Zahlungsvorgangs ist, bzw. er bringt erforderlichenfalls das belastete Zahlungskonto wieder auf den Stand, auf dem es sich ohne den fehlerhaft ausgeführten Zahlungsvorgang befunden hätte. Haftet der Zahlungsauslösedienstleister für die fehlerhafte Ausführung des Zahlungsvorgangs, entschädigt er den kontoführenden Zahlungsdienstleister auf dessen Verlangen unverzüglich für alle infolge der Erstattung an den Zahler erlittenen Verluste oder gezahlten Beträge. Der Zahlungsauslösedienstleister muss nachweisen, dass der

Zahlungsauftrag beim kontoführenden Zahlungsdienstleister des Zahlers eingegangen ist. Haftet der Zahlungsdienstleister des Zahlungsempfängers, stellt er dem Zahlungsempfänger den Betrag, der Gegenstand des Zahlungsvorgangs ist, unverzüglich zur Verfügung und schreibt gegebenenfalls dem Zahlungskonto des Zahlungsempfängers den entsprechenden Betrag gut. Der Betrag wird spätestens zu dem Datum wertgestellt, zu dem der Betrag bei korrekter Ausführung wertgestellt worden wäre.

5. *wie diese Haftung sachgerecht geregelt werden muss;*

Zu 5.:

Mit den unter 4. beschriebenen Haftungs- und Erstattungsregelungen soll sichergestellt werden, dass kontoführendes Institut und Zahlungsauslösedienst nur für ihr eigenes Verhalten haften, der Bürger jedoch eine einzige Anlaufstelle hat, nämlich sein kontoführendes Institut. Zu diesem hat er eine dauerhafte Geschäftsbeziehung. Der Haftungsausgleich erfolgt dann zwischen kontoführendem Institut und Zahlungsauslösedienst.

Im Übrigen teilt die Landesregierung die Haltung des Bundesrats (BR-Drs. 602/13(B)), der die Notwendigkeit betont, dass grundsätzlich sichergestellt sein muss, dass Verbraucherinnen und Verbraucher ausreichend geschützt sind. Das umfasst im Zusammenhang mit Zahlungsinitialisierungsdiensten insbesondere die technische Absicherung sowie den Ausschluss zusätzlicher Haftungsrisiken. Darüber hinaus ist von Bedeutung, dass die mit der Übermittlung von Authentifizierungsmerkmalen derzeit verbundene Rechtsunsicherheit für die Kunden beseitigt wird.

6. *welche Bezahlung der dritte Zahlungsdienstleister dem Kreditinstitut, dessen Infrastruktur, Datenbanken und Dienstleistungen er nutzt, laut der EU-Zahlungsdiensterichtlinie II entrichten muss;*

Zu 6.:

Zum Thema, welche Bezahlung der dritte Zahlungsdienstleister dem kontoführenden Zahlungsdienstleister für die Nutzung dessen Infrastruktur, Datenbanken und Dienstleistungen leisten muss, enthält die PSD II keine Regelungen. Insofern sollte es je-

dem Kreditinstitut unbenommen bleiben, Gebühren oder Entgelte für die entsprechenden Leistungen im gesetzlichen Rahmen zu fordern.

7. *wie eine Bezahlung der Dienstleistungen des Kreditinstituts, die der dritte Zahlungsanbieter nutzt, gestaltet werden kann;*

Zu 7.:

Vertragliche Preisabsprachen sind grundsätzlich zwischen allen Beteiligten möglich (kontoführendes Institut, Zahlungsauslösedienst, Kunde). Zunächst ist zu erwägen, wem die Leistung in Rechnung gestellt werden soll: den Kunden oder den Dritten Zahlungsdienstleistern. Sodann ist zu erwägen, wie das Preismodell gestaltet werden soll. Dabei kann auf bestehende Preismodelle für Zahlungsdienstleistungen der Kreditinstitute zurückgegriffen werden. Die im Markt existierenden Modelle reichen von der Bepreisung der Services (z. Bsp. Zahlungsauftrag) bis zu Pauschalen, die ggf. in der Grundgebühr des Kontos enthalten ist. Aus Verbrauchersicht sind die Kosten für diese Leistungen auf eine angemessene Höhe zu begrenzen.

8. *auf welchem Stand der Beratung innerhalb der EU-Institutionen die Überarbeitung der Zahlungsdiensterichtlinie ist und wann eine abschließende Beschlussfassung vorgesehen ist;*

Zu 8.:

Der Vorschlag der Kommission zur PSD II wurde in der ersten Lesung des Europäischen Parlaments am 3. April 2014 mit Änderungsvorschlägen versehen. Im Dezember 2014 hat sich der Rat auf Ebene des Ausschusses der Ständigen Vertreter auf eine "Allgemeine Ausrichtung" zur PSD II geeinigt und der Ratspräsidentschaft das Mandat für die Aufnahme von Trilogverhandlungen mit Parlament und Kommission erteilt. Diese Trilogverhandlungen haben Anfang Februar 2015 begonnen. Für den 12. Mai 2015 ist die politische Einigung des Rats vorgesehen.

Derzeit ist damit zu rechnen, dass die PSD II bis Ende des zweiten Quartals 2015 in Kraft treten kann. Für die nationale Umsetzung der Richtlinie werden den Mitglied-

staaten maximal 24 Monate zugestanden. Somit dürften die Regelungen der PSD II voraussichtlich Mitte des Jahres 2017 in nationale Gesetze umgesetzt sein.

9. *welche Haltung sie zur geplanten EU-Zahlungsdienstleistungsrichtlinie II mit Blick auf das Drei-Säulen-Modell des Bankwesens und den Verbraucherschutz einnimmt;*

Zu 9.:

Grundsätzlich begrüßt die Landesregierung das Bestreben der EU-Kommission, durch die PSD II die Schaffung eines einheitlichen Binnenmarktes auch für Online-Zahlungsvorgänge und innovative Zahlungsdienstleistungen voranzutreiben. Die sich daraus für die Verbraucher und den Online-Handel ergebenen Vorteile wie bspw. eine höhere Transaktionssicherheit und eine schnellere Transaktionsabwicklung sind positiv zu bewerten. Ob es allerdings, wie von der EU-Kommission erwartet, zu einer generellen Absenkung der Kosten für Zahlungsdienstleistungen kommen wird, bleibt in Anbetracht der Vielschichtigkeit des Marktes abzuwarten.

Die Landesregierung legt großen Wert darauf, dass den Belangen des Verbraucherschutzes auch bei den Neuregelungen im Bereich der online-Zahlungen und bei den innovativen Zahlungsdienstleistungen Rechnung getragen wird. Allerdings anerkennt sie die Bestrebungen der EU-Kommission, in der PSD II Regelungen zu schaffen, die insbesondere im Hinblick auf die Sicherheit der Zahlungsvorgänge zu sachgerechten Lösungen führen sollen.

Zweifellos wird der intensivere Wettbewerb den Druck auf den Bankensektor, der bislang den Markt für Zahlungsdienstleistungen beherrscht, verstärken. Im Hinblick auf das Drei-Säulen-Modell des Bankensektors bleibt jedoch festzuhalten, dass gerade die Zahlungsdienstleistungen auch bei den öffentlich-rechtlichen Kreditinstituten und bei den genossenschaftlichen Banken weitgehend zentralisiert sind. Damit kann davon ausgegangen werden, dass diese beiden Bereiche, die für die flächendeckende Versorgung von Bevölkerung und Wirtschaft von so überragender Bedeutung sind, ebenso wie die gesamte Kreditwirtschaft in der Lage sein werden, die Herausforderungen aus der PSD II zu bewältigen.

Gerade in Anbetracht der sehr technischen Fragestellungen, die sich im Zusammenhang mit der PSD II ergeben, ist die Kreditwirtschaft aufgerufen, sich mit ihrer Exper-

tise wie bereits in der Vergangenheit auch in den weiteren europäischen Gesetzgebungsprozess direkt einzubringen.

10. *inwieweit sie bereits im Bundesrat bzw. auf EU-Ebene in dieser Angelegenheit aktiv geworden ist.*

Zu 10.:

Im Zuge der Behandlung des Entwurfs der PSD II im Bundesrat hat dieser am 20.9.2013 mit den Stimmen Baden-Württembergs eine Stellungnahme beschlossen (BR-Drs. 602/13(B); in der Anlage beigefügt).

Der Bundesrat forderte, dass die Eigenbeteiligung im Falle einer missbräuchlichen Verwendung eines Zahlungsinstruments lediglich bei der nicht sicheren Aufbewahrung persönlicher Sicherheitsmerkmale angewendet werden soll.

Im Hinblick auf die Einbeziehung von TPPs hat der Bundesrat darauf hingewiesen, dass sich Verbraucher durch Preisgabe ihrer Online-Banking-Zugangsdaten gegenüber Dritten erheblichen Risiken und Missbrauchsgefahren aussetzen. Daher hat der Bundesrat die Notwendigkeit betont, dass im Zusammenhang mit Zahlungsinitialisierungsdiensten insbesondere die technische Absicherung sowie der Ausschluss zusätzlicher Haftungsrisiken gewährleistet sein muss, damit die Verbraucher ausreichend geschützt sind und die mit der Übermittlung von Authentifizierungsmerkmalen derzeit verbundene Rechtsunsicherheit für die Kunden beseitigt wird.

Zudem wies der Bundesrat darauf hin, dass dem Schutz der Verbraucher vor Sicherheitslücken im System der Zahlungsdienstleister eine hohe Bedeutung zukommt. Deshalb sollen die Zahlungsdienstleister zu einer adäquaten und raschen Anpassung ihrer Sicherheitsverfahren verpflichtet werden. Es wird außerdem angeregt, dass spätestens zwei Jahre nach Dokumentation einer bestimmten Angriffsform in der EU ein Haftungsausschluss seitens der Verbraucher vorgesehen wird, wenn diese trotz der Erkenntnisse über die Sicherheitslücken noch Opfer eines solchen Angriffs werden konnten.

Die Stellungnahme wurde direkt an die Kommission übermittelt.

Im Rahmen des derzeitigen Trilogverfahrens ist keine weitere Beteiligung des Bundesrats am europäischen Gesetzgebungsprozess vorgesehen.

Die Antwort ist mit dem Innenministerium und dem Ministerium für Ländlichen Raum und Verbraucherschutz abgestimmt.

Das Innenministerium hat die Antwort zu Ziffer 3 mitgezeichnet.

Mit freundlichen Grüßen
in Vertretung des Ministers

gez. Guido Rebstock
Ministerialdirektor