Seminar für Bankrecht 2017

13.6.2017

Univ.-Prof. Dr. Stefan Perner

SICHERHEIT BEIM ONLINE-BANKING

PATRONANZ

VKB BANK
ÖSTERREICHS UNABHÄNGIGE BANK

JKU | INSTITUT FÜR BANKRECHT

SICHERHEIT BEIM ONLINE-BANKING

Seminar für Bankrecht 2017
Linz, 13. Juni 2017

JOHANNES KEPLER UNIVERSITÄT LINZ

Univ.-Prof. Dr. Stefan Perner

SICHERHEITSASPEKTE BEIM ONLINE-BANKING

- **Kundenidentifikation**
  Sicherheit vor Geldwäsche und Terrorismus
- **Kundenauthentifikation**
  Sicherheit vor Missbrauch – Haftung bei Missbrauch
- **Kundenkommunikation**
  Sicherheit im rechtsgeschäftlichen Verkehr
- **Europäische Determinierung der Materien**
  - Identifikation: RL 2015/849/EU (4. Anti-Geldwäsche-RL)
  - Authentifikation: RL 2007/64/EG (PSD I) + RL 2015/2366/EU (PSD II)
  - Kommunikation: Verbraucherschutz-RL; EuGH C-375/15 (BAWAG)

JKU

KUNDENIDENTIFIKATION BEIM ONLINE-GESCHÄFT

JKU

KUNDENIDENTIFIKATION

- **§ 6 Abs 2 Z 1 FM-GwG: grundsätzlich persönliche Ausweisleistung**
- **§ 9 FM-GwG: verstärkte Sorgfalt bei erhöhtem Risiko (zB Ferngeschäft)**
  - ☐ elektronische Signatur
  - ☐ elektronischer Identitätsausweis
  - ☐ Ident. Brief (Post)
  - ☐ Überweisung von bestehendem Konto
- **§ 6 Abs 4 FM-GwG: Video-Identifizierung**
  - ☐ BaFin-Rundschreiben 1/2014: Fall persönlicher Anwesenheit
  - ☐ Online-IDV (BGBl II 5/2017): entspricht BaFin
  - ☐ Vereinbarkeit mit Art 18 iVm Anh III 4. Geldwäsche-RL?
  - ☐ EBA-Leitlinien Mitte 2017

JKU

KUNDENAUTHENTIFIKATION BEIM ONLINE-BANKING

JKU

UMWÄLZUNGEN DURCH PSD II?

- **Artt 54 ff PSD I: „Sicherstellung der Zustimmung“**
- **Art 4 Nr 30 iVm Art 97 PSD II (RL 2015/2366/EU): starke Kundenauthentifizierung (SCA)**
  - Wissen (etwas, das nur der Nutzer weiß: Passwort, PIN, Sicherheitsfrage)
  - Besitz (etwas, das nur der Nutzer hat: TAN, Codekarte)
  - Inhärenz (etwas, das der Nutzer ist: biometrische Merkmale)
  - 2 Kriterien, unabhängig voneinander
  - Bei Zugriff auf Zahlungskonto, elektronischem Zahlungsvorgang oder Missbrauchsrisiko
  - Hafungsfragen
- **Art 98 Abs 3 PSD II: Ausnahmen (EBA-RTS) nach Maßgabe von**
  - Risiko
  - Betrag, Periodizität oder beides
  - Zahlungsweg

JKU

EBA-REGULIERUNGSSTANDARDS

- **Stand des Verfahrens (6/2017): VO-Entwurf der KOM**
- **Information über Zahlungskonto (Art 10)**
  - ☐ Information über Kontostand
  - ☐ Information über Zahlungsvorgang (90 Tage)
  - ☐ Nicht bei Ersteinstieg und Inaktivität von 90 Tagen
- **Bagatellgeschäfte (Artt 11, 12, 16)**
  - ☐ Kontaktloses Zahlen: € 50 / 150 / 5 Zahlungsvorgänge
  - ☐ Beförderungsentgelte: unbeaufsichtigt
  - ☐ Parkgebühr: unbeaufsichtigt
  - ☐ Kleinbetragstransaktionen: € 30 / 100 / 5 Zahlungsvorgänge

JKU

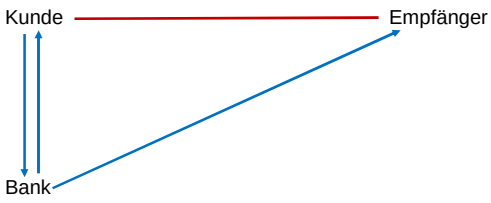
EU-GESETZGEBUNG: STRUKTURFRAGEN

- **Entstehungsgeschichte der starken Kundenauthentifizierung**
  - ☐ Artt 54 ff PSD I: „Sicherstellung der Zustimmung“
  - ☐ EBA/GL/2014/12 zur Sicherheit von Internetzahlungen
  - ☐ Art 4 Nr 30, Art 97 PSD II
  - ☐ EBA-Regulierungsstandards auf Basis von Art 98 PSD II
- **Rolle der EBA im Prozess?**
  - ☐ EBA-VO 2010/1093/EU
  - ☐ Art 10 & Art 15: Technische Standards (Art 290 & 291 AEUV)
  - ☐ Art 16: Meta-Ebene der EU-Bankenaufsicht: Leitlinien & Empfehlungen
  - ☐ EG 26: Subsidiarität von Leitlinien!
- **Praktische Bedeutung: Vertragsänderung**
  - ☐ Bsp: Restriktive Rsp zur Erklärungsfiktion (OGH 1 Ob 210/12g & 2 Ob 131/12x)
  - ☐ Technische Standards als gesetzliches Gebot oder Verbot

JKU

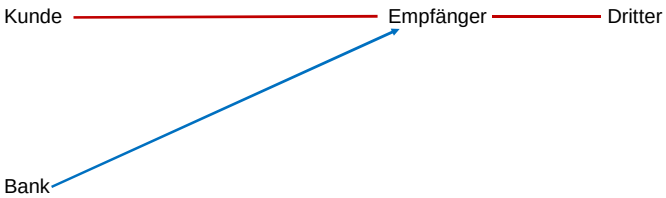
KUNDENAUTHENTIFIKATION UND HAFTUNG

JKU



1. Unautorisierter Vorgang (zB Phishing)
2. Wirksamkeit der Überweisung (Rechtsverhältnis Bank – Empfänger)?
3. Interner Ausgleich (Rechtsverhältnis Bank – Kunde)?

JKU



- OGH 2 Ob 107/08m
- Wirksamer Rechtsschein einer Überweisung?
- OGH bejaht Rückforderungsanspruch der Bank
- zust ÖBA 2009/1551, *P. Bydlinski* = EvBl 2009/98, *Perner*

- OGH 10 Ob 102/15w (EvBl 2016/111, *Kellner* = JBl 2017, 316, *Dullinger*)
- Ausgleich Kunde – Bank (§ 44 ZaDiG)
- Haftung nur bei grober FL; Erweiterung außerhalb B-2-C zulässig
- OGH bejaht schadenersatzrechtliche Haftung des Kunden

- PSD I: Haftung bei leichter Fahrlässigkeit bis 150 € / PSD II: € 50
- PSD I & PSD II: Unbegrenzte Haftung bei grober Fahrlässigkeit
- PSD I & PSD II: Ausschluss ab Anzeige, Verschärfung bei Betrug
- PSD II: Ausschluss bei Verzicht auf starke Kundenauthentifikation

JKU

SORGFALTSMAßSTAB DES KUNDEN

- **Phishing-Attacke: OGH 10 Ob 102/15w**
  - „soweit ersichtlich“ keine Rechtsprechung zum Verschuldensgrad
  - *Dullinger* und *Kellner*: Grobe Fahrlässigkeit (Dauer und Häufigkeit der Verwendung)
  - OLG München 17 U 3257/11: Grobe Sorgfaltswidrigkeit
  - LG Hannover 11 O 229/15: Grobe Sorgfaltswidrigkeit
- **Beweisfragen**
  - Anscheinsbeweis für Authentifizierung bei fehlerfreiem System: BGH XI ZR 91/14
  - kein Anscheinsbeweis der (groben) Fahrlässigkeit bei Phishing: BGH XI ZR 91/14
  - vgl OGH 2 Ob 107/08m, 9 Ob 3/08v
  - siehe nun Art 72 Abs 2 PSD II
- **Gestaltungsmöglichkeiten der Bank**
  - Mitteilungen und Warnungen der Bank
  - keine „rechtsgeschäftliche“ Konstruktion ieS

JKU

KUNDENKOMMUNIKATION BEIM ONLINE-BANKING

JKU

KUNDENKOMMUNIKATION

- **EuGH C-375/15 (BAWAG)**
  - Funktionsweise der „E-Banking-Box“
  - Mitteilung auf dauerhaftem Datenträger?
  - *Caks*, ÖBA 2017, 316; *Spitzer/Wilfinger*, ÖBA 2017, 230
- **Dauerhafter Datenträger**
  - zahlreiche Verbraucherschutz-RL (vgl § 126b BGB)
  - Dauerhafte Speicherbarkeit, Unveränderbarkeit
  - Box & Nachricht in Box als dauerhafte Datenträger
- **Mitteilung**
  - Unabhängig vom Format
  - Effektive Übermittlung in Kenntnissphäre des Benutzers
  - ZB: SMS-Benachrichtigung

JKU

SICHERHEIT BEIM ONLINE-BANKING

Seminar für Bankrecht 2017
Linz, 13. Juni 2017

JOHANNES KEPLER
UNIVERSITÄT LINZ

Univ.-Prof. Dr. Stefan Perner

Gesetzesbestimmungen

FM-GwG

Umfang der Sorgfaltspflichten

§ 6. (4) Die persönliche Vorlage des amtlichen Lichtbildausweises im Sinne Abs. 2 kann bei Geschäftsbeziehungen oder Transaktionen ohne persönliche Kontakte durch Sicherungsmaßnahmen ersetzt werden. Den Verpflichteten müssen jedenfalls Name, Geburtsdatum und Adresse des Kunden, bei juristischen Personen die Firma und der Sitz bekannt sein. Als Sicherungsmaßnahmen sind zulässig:

1. die Vorlage des amtlichen Lichtbildausweises im Rahmen eines videogestützten elektronischen Verfahrens (Online-Identifikation),

2. ein gesetzlich vorgesehenes Verfahren, das gesichert dieselbe Information wie mit der Vorlage eines amtlichen Lichtbildausweises zur Verfügung stellt (elektronischer Ausweis),

3. die Abgabe der rechtsgeschäftliche Erklärung des Kunden in Form einer qualifizierten elektronischen Signatur gemäß Art. 3 Z 12 der Verordnung (EU) Nr. 910/2014 oder die Zustellung der rechtsgeschäftlichen Erklärung des Verpflichteten mit eingeschriebener Postzustellung an diejenige Kundenadresse, die als Wohnsitz oder Sitz des Kunden angegeben worden ist, wenn zusätzlich

a) bei juristischen Personen der Sitz zugleich der Sitz der zentralen Verwaltung ist, worüber der Kunde eine schriftliche Erklärung abzugeben hat, b) eine Kopie des amtlichen Lichtbildausweises des Kunden oder seines gesetzlichen Vertreters oder bei juristischen Personen des vertretungsbefugten Organs dem Verpflichteten vor dem Zeitpunkt des Vertragsabschlusses vorliegt, sofern nicht das Rechtsgeschäft elektronisch an Hand einer qualifizierten elektronischen Signatur abgeschlossen wird und

c) bei Kunden mit Sitz oder Wohnsitz in einem Drittland, eine schriftliche Bestätigung eines anderen Kreditinstitutes, mit dem der Kunde eine dauernde Geschäftsverbindung hat, vorliegt, dass die Identität des Kunde im Sinne dieses Bundesgesetzes festgestellt und überprüft wurde und dass die dauernde Geschäftsverbindung aufrecht ist. Hat das bestätigende Kreditinstitut seinen Sitz in einem Drittland, so muss dieses Drittland die Anforderungen gemäß § 13 Abs. 4 erfüllen. An Stelle einer Identifizierung und Bestätigung durch ein Kreditinstitut ist auch eine Identifizierung und schriftliche Bestätigung durch die österreichische Vertretungsbehörde im betreffenden Drittland oder einer anerkannten Beglaubigungsstelle zulässig,

oder

4. die erste Zahlung im Rahmen der Transaktionen über ein Konto abgewickelt wird, das im Namen des Kunden bei einem Kreditinstitut im Sinne des § 13 eröffnet wurde und ihnen Kopien von Dokumenten des Kunden vorliegen, aufgrund derer die Angaben des Kunden bzw. seiner vertretungsbefugten natürlichen Person glaubhaft nachvollzogen werden können. Anstelle dieser Kopien ist es ausreichend, wenn eine schriftliche Bestätigung des Kreditinstitutes vorliegt, über das die erste Zahlung abgewickelt werden soll, dass die Identität des Kunden im Sinne dieses Bundesgesetzes oder der Richtlinie (EU) 2015/849 festgestellt und überprüft wurde.

Die FMA hat mit Zustimmung des Bundesministers für Finanzen mit Verordnung festzulegen, welche Maßnahmen bei der Online-Identifikation zum Ausgleich des erhöhten Risikos erforderlich sind und dabei insbesondere Anforderungen an die Datensicherheit, Fälschungssicherheit und an jene Personen, die die Online-Identifikation durchführen festzulegen.

Gesamte Rechtsvorschrift für Online-Identifikationsverordnung, Fassung vom 08.06.2017

Langtitel

Verordnung der Finanzmarktaufsichtsbehörde (FMA) über die videogestützte Online-Identifikation von Kunden (Online-Identifikationsverordnung – Online-IDV)
StF: BGBl. II Nr. 5/2017

Präambel/Promulgationsklausel

Auf Grund des § 6 Abs. 4 des Finanzmarkt-Geldwäschegesetzes – FM-GwG, BGBl. I Nr. 118/2016, wird mit Zustimmung des Bundesministers für Finanzen verordnet:

Text

1. Teil
Allgemeine Bestimmungen
Gegenstand

§ 1. (1) Diese Verordnung regelt die erforderlichen Sicherungsmaßnahmen, um das erhöhte Risiko auszugleichen, das sich aus der Feststellung und Überprüfung der Identität einer Person ergibt, die oder deren vertretungsbefugte natürliche Person nicht physisch anwesend ist, wenn stattdessen ein videogestütztes elektronisches Verfahren (Online-Identifikation) verwendet wird.

(2) Die gemäß dieser Verordnung zu setzenden erforderlichen Sicherungsmaßnahmen gelten unbeschadet der weiteren Sorgfaltspflichten zur Prävention von Geldwäscherei oder Terrorismusfinanzierung gemäß dem FM-GwG.

(3) Die Verpflichteten können unbeschadet der nach dieser Verordnung zu setzenden erforderlichen Sicherungsmaßnahmen weitere Sicherungsmaßnahmen zur Anhebung des Sicherheitsniveaus setzen.

(4) Die Bestimmungen dieser Verordnung gelten unbeschadet der auf die Online-Identifikation anzuwendenden datenschutzrechtlichen Anforderungen.

Begriffsbestimmungen

§ 2. Im Sinne dieser Verordnung bezeichnet der Ausdruck

1. Bildschirmkopie: eine mittels elektronischer Datenverarbeitung gefertigte und gespeicherte Graphik, die den Bildschirminhalt als visuelle Komponente der Online-Identifikation bezogen auf den Zeitpunkt ihrer Erstellung in einer Qualität wiedergibt, die den jeweiligen Überprüfungs- und Dokumentationszwecken entspricht;
2. amtlicher Lichtbildausweis: ein amtlicher Lichtbildausweis im Sinne von § 6 Abs. 2 Z 1 FM-GwG, der über optische Sicherheitsmerkmale verfügt, welche im Vergleich zu bewegungsoptisch wirksamen (holographischen) Elementen zumindest gleichwertig sind.

2. Teil
Sicherungsmaßnahmen
Organisatorische Sicherungsmaßnahmen

§ 3. (1) Der Verpflichtete darf für die Online-Identifikation nur Mitarbeiter einsetzen, die für die Durchführung der Online-Identifikation hinreichend geschult und zuverlässig sind. Diese Schulung hat zumindest den rechtlichen Rahmen, die technischen Voraussetzungen sowie die praktische Sicherstellung der Überprüfung zu umfassen.

(2) Der Verpflichtete hat sicherzustellen, dass die im Rahmen der Online-Identifikation herangezogenen Anwendungen sowie die übertragenen Daten zu keinem Konflikt mit anderen Prozessen des Verpflichteten führen, eine Beeinflussung ausgeschlossen ist und die Anwendungen sowie die Daten vor einem unbefugten Zugriff geschützt sind.

(3) Mitarbeiter des Verpflichteten dürfen die Online-Identifikation nur in einem abgetrennten, mit einer Zugangskontrolle ausgestatteten Raum durchführen.

Verfahrensbezogene Sicherungsmaßnahmen

§ 4. (1) Soweit personenbezogene Daten nach den Bestimmungen dieser Verordnung verarbeitet werden, geschieht dies aufgrund von § 6 Abs. 4 FM-GwG für die Zwecke der Verhinderung von Geldwäscherei und Terrorismusfinanzierung (§ 21 Abs. 4 FM-GwG).

(2) Das Gespräch oder der Gesprächsteil, das oder der dem Zwecke der Online-Identifikation dient, ist jedenfalls akustisch in seiner Gesamtheit aufzuzeichnen; § 50a Abs. 5 DSG 2000 ist anzuwenden. Darüber hinaus sind Bildschirmkopien anzufertigen, die bei geeigneten Belichtungsverhältnissen Folgendes aus der Online-Identifikation graphisch abbilden:

1. Jedenfalls das Gesicht des potentiellen Kunden oder der vertretungsbefugten natürlichen Person des potentiellen Kunden,
2. die Präsentation der Vorderseite des amtlichen Lichtbildausweises oder von dessen Datenseite und
3. die Präsentation der Rückseite des amtlichen Lichtbildausweises oder von dessen Datenseite.

Die Bildschirmkopien haben dabei jedenfalls von einer solchen Qualität zu sein, dass der potentielle Kunde oder die vertretungsbefugte natürliche Person des potentiellen Kunden und die auf dem amtlichen Lichtbildausweis enthaltenen Daten vollständig und zweifelsfrei erkennbar sind.

(3) Der potentielle Kunde oder dessen vertretungsbefugte natürliche Person hat während der Online-Identifikation nach Aufforderung

1. seinen Kopf unter Präsentation des Gesichts zu bewegen und getrennt davon
2. die Seriennummer seines amtlichen Lichtbildausweises mitzuteilen.

(4) Der Mitarbeiter, der die Online-Identifikation durchführt, hat sich von der Authentizität des amtlichen Lichtbildausweises wie folgt zu vergewissern:

1. Visuelle Überprüfung des Vorhandenseins der optischen Sicherheitsmerkmale einschließlich bewegungsoptischer (holographischer) oder gleichwertiger Sicherheitsmerkmale, die nach Aufforderung zum horizontalen und vertikalen Kippen des amtlichen Lichtbildausweises deutlich erkennbar sein müssen,
2. Überprüfung der korrekten alphanumerischen Ziffernorthographie der Seriennummer,
3. Überprüfung der Unversehrtheit der Laminierung, die den amtlichen Lichtbildausweis umschließt, oder vergleichbarer Merkmale, die für die Unversehrtheit des Dokumentes sprechen,
4. Überprüfung zum Zwecke des Ausschlusses, dass es sich nur um ein nachträglich mit dem amtlichen Lichtbildausweis verbundenes Lichtbild handelt,
5. Überprüfung der logischen Konsistenz
   a) der Merkmale des potentiellen Kunden oder der vertretungsbefugten natürlichen Person des potentiellen Kunden einerseits und der Personenbeschreibung sowie des Lichtbildes im amtlichen Lichtbildausweis andererseits, außerdem
   b) des Lichtbildes, des Ausstellungsdatums und des Geburtsdatums im amtlichen Lichtbildausweis zueinander, außerdem
   c) aller weiterer unter Umständen bereits vorhandener Kundendaten einerseits und der entsprechenden weiteren Angaben auf dem amtlichen Lichtbildausweis andererseits.

(5) Der potentielle Kunde oder dessen vertretungsbefugte natürliche Person hat während der laufenden Videoübertragung eine eigens für den Zweck der Online-Identifikation gültige, zentral generierte und an ihn per E-Mail oder SMS übermittelte Ziffernfolge unmittelbar einzugeben und an den Mitarbeiter elektronisch zurückzusenden.

Zwingender Abbruch der Online-Identifikation

§ 5. (1) Der Vorgang der Online-Identifikation ist vorbehaltlich der Fälle gemäß Abs. 2 abzubrechen, wenn

1. eine für die Anfertigung einer Bildschirmkopie geeignete visuelle Überprüfung des potentiellen Kunden oder des amtlichen Lichtbildausweises oder von beiden nicht möglich ist,
2. bei Vorliegen sonstiger Unstimmigkeiten,
3. bei Vorliegen sonstiger Unsicherheiten.

(2) Trifft den Verpflichteten die Sorgfaltspflicht gegenüber dem Kunden, dessen Identität und diejenige seiner vertretungsberechtigten natürlichen Person festzustellen und zu überprüfen, bei Vorliegen

eines Falles gemäß § 5 Z 4 oder 5 FM-GwG, so ist die Online-Identifikation zu Ende zu führen und zu erwägen, eine Verdachtsmeldung gemäß § 16 FM-GwG an die Geldwäschemeldestelle zu erstatten.

Ausführung der Online-Identifikation durch Dienstleister

§ 6. (1) Bedient sich ein Verpflichteter für die Ausführung der Online-Identifikation gemäß dieser Verordnung eines Dienstleisters, hat er dafür Sorge zu tragen, dass der Dienstleister Sicherungsmaßnahmen ergreift, die sowohl hinsichtlich des Umfanges als auch der Qualität, den Anforderungen in dieser Verordnung entsprechen. Die endgültige Verantwortung für die Erfüllung dieser Anforderungen verbleibt jedoch beim Verpflichteten, der auf den Dienstleister zurückgreift. Bei Abschluss, Durchführung und Kündigung der Vereinbarung mit einem Dienstleister ist mit der gebotenen Professionalität und Sorgfalt zu verfahren und namentlich eine klare Aufteilung der Rechte und Pflichten schriftlich zu vereinbaren. § 11 DSG 2000 ist anzuwenden.

(2) Auslagerungs- und Vertretungsverhältnisse im Sinne von § 15 FM-GwG dürfen weder die Qualität der internen Kontrolle noch die Möglichkeit der FMA zur Prüfung der Einhaltung aller Anforderungen an die Online-Identifikation wesentlich beeinträchtigen.

3. Teil

Schlussbestimmungen

Verweise

§ 7. (1) Soweit auf Bestimmungen des FM-GwG verwiesen wird, ist das Finanzmarkt-Geldwäschegesetz – FM-GwG, BGBl. I Nr. 118/2016, in seiner Stammfassung anzuwenden.

(2) Soweit auf Bestimmungen des DSG 2000 verwiesen wird, ist das Datenschutzgesetz 2000 – DSG 2000, BGBl. I Nr. 165/1999, in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 und der Kundmachung BGBl. I Nr. 132/2015 anzuwenden.

Personenbezogene Bezeichnungen

§ 8. Soweit sich die in dieser Verordnung verwendeten Bezeichnungen auf natürliche Personen beziehen, gilt die gewählte Form für beide Geschlechter.

RICHTLINIE (EU) 2015/2366 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 25. November 2015

über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG

Artikel 4

Begriffsbestimmungen

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck:

1. „Herkunftsmitgliedstaat“

a) den Mitgliedstaat, in dem sich der Sitz des Zahlungsdienstleisters befindet, oder

b) wenn der Zahlungsdienstleister nach dem für ihn geltenden nationalen Recht keinen Sitz hat, den Mitgliedstaat, in dem sich seine Hauptverwaltung befindet;

2. „Aufnahmemitgliedstaat“ den Mitgliedstaat, in dem ein Zahlungsdienstleister einen Agenten oder eine Zweigniederlassung hat oder Zahlungsdienste erbringt und der nicht der Herkunftsmitgliedstaat dieses Zahlungsdienstleisters ist;

3. „Zahlungsdienst“ eine oder mehrere der in Anhang I aufgeführten gewerblichen Tätigkeiten;

4. „Zahlungsinstitut“ eine juristische Person, der nach Artikel 11 eine Zulassung für die unionsweite Erbringung und Ausführung von Zahlungsdiensten erteilt wurde;

5. „Zahlungsvorgang“ die bzw. den vom Zahler, im Namen des Zahlers oder vom Zahlungsempfänger ausgelöste(n) Bereitstellung, Transfer oder Abhebung eines Geldbetrags, unabhängig von etwaigen zugrunde liegenden Verpflichtungen im Verhältnis zwischen Zahler und Zahlungsempfänger;

6. „Fernzahlungsvorgang“ einen Zahlungsvorgang, der über das Internet oder mittels eines Geräts, das für die Fernkommunikation verwendet werden kann, ausgelöst wird;

7. „Zahlungssystem“ ein System zum Transfer von Geldbeträgen mit formalen und standardisierten Regeln und einheitlichen Vorschriften für die Verarbeitung, das Clearing und/oder die Verrechnung von Zahlungsvorgängen;

8. „Zahler“ eine natürliche oder juristische Person, die Inhaber eines Zahlungskontos ist und die einen Zahlungsauftrag von diesem Zahlungskonto gestattet oder — falls kein Zahlungskonto vorhanden ist — eine natürliche oder juristische Person, die den Auftrag für einen Zahlungsvorgang erteilt;

9. „Zahlungsempfänger“ eine natürliche oder juristische Person, die den Geldbetrag, der Gegenstand eines Zahlungsvorgangs ist, als Empfänger erhalten soll;

10. „Zahlungsdienstnutzer“ eine natürliche oder juristische Person, die einen Zahlungsdienst als Zahler oder Zahlungsempfänger oder in beiden Eigenschaften in Anspruch nimmt;

11. „Zahlungsdienstleister“ eine Stelle im Sinne des Artikels 1 Absatz 1 oder eine natürliche oder juristische Personen, für die die Ausnahme gemäß Artikel 32 oder 33 gilt;

12. „Zahlungskonto“ ein auf den Namen eines oder mehrerer Zahlungsdienstnutzer(s) lautendes Konto, das für die Ausführung von Zahlungsvorgängen genutzt wird;

13. „Zahlungsauftrag“ einen Auftrag, den ein Zahler oder Zahlungsempfänger seinem Zahlungsdienstleister zur Ausführung eines Zahlungsvorgangs erteilt;

14. „Zahlungsinstrument“ jedes personalisierte Instrument und/oder jeden personalisierten Verfahrensablauf, das bzw. der zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister vereinbart wurde und zur Erteilung eines Zahlungsauftrags verwendet wird;

15. „Zahlungsauslösedienst“ einen Dienst, der auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto auslöst;

16. „Kontoinformationsdienst“ einen Online-Dienst zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten, das/die ein Zahlungsdienstnutzer entweder bei einem anderen Zahlungsdienstleister oder bei mehr als einem Zahlungsdienstleister hält;

17. „kontoführender Zahlungsdienstleister“ einen Zahlungsdienstleister, der für einen Zahler ein Zahlungskonto bereitstellt und führt;

18. „Zahlungsauslösedienstleister“ einen Zahlungsdienstleister, der gewerbliche Tätigkeiten nach Anhang I Nummer 7 ausübt;

19. „Kontoinformationsdienstleister“ einen Zahlungsdienstleister, der gewerbliche Tätigkeiten nach Anhang I Nummer 8 ausübt;

20. „Verbraucher“ eine natürliche Person, die bei den von dieser Richtlinie erfassten Zahlungsdienstverträgen zu Zwecken handelt, die nicht ihrer gewerblichen oder beruflichen Tätigkeit zugerechnet werden können;

21. „Rahmenvertrag“ einen Zahlungsdienstvertrag, der die zukünftige Ausführung einzelner und aufeinander folgender Zahlungsvorgänge regelt und die Verpflichtung zur Einrichtung eines Zahlungskontos und die entsprechenden Bedingungen enthalten kann;

22. „Finanztransfer“ einen Zahlungsdienst, bei dem ohne Einrichtung eines Zahlungskontos auf den Namen des Zahlers oder des Zahlungsempfängers ein Geldbetrag eines Zahlers nur zum Transfer eines entsprechenden Betrags an einen Zahlungsempfänger oder an einen anderen, im Namen des Zahlungsempfängers handelnden Zahlungsdienstleister entgegengenommen wird und/oder bei dem der Geldbetrag im Namen des Zahlungsempfängers entgegengenommen und diesem verfügbar gemacht wird;

23. „Lastschrift“ einen Zahlungsdienst zur Belastung des Zahlungskontos des Zahlers, wenn ein Zahlungsvorgang vom Zahlungsempfänger aufgrund der Zustimmung des Zahlers gegenüber dem Zahlungsempfänger, dessen Zahlungsdienstleister oder seinem eigenen Zahlungsdienstleister ausgelöst wird;

24. „Überweisung“ einen auf Aufforderung des Zahlers ausgelösten Zahlungsdienst zur Erteilung einer Gutschrift auf das Zahlungskonto des Zahlungsempfängers zulasten des Zahlungskontos des Zahlers in Ausführung eines oder mehrerer Zahlungsvorgänge durch den Zahlungsdienstleister, der das Zahlungskonto des Zahlers führt;

25. „Geldbetrag“ Banknoten und Münzen, Giralgeld oder E-Geld im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/110/EG;

26. „Wertstellungsdatum“ den Zeitpunkt, den ein Zahlungsdienstleister für die Berechnung der Zinsen bei Gutschrift oder Belastung eines Betrags auf einem Zahlungskonto zugrunde legt;

27. „Referenzwechselkurs“ den Wechselkurs, der bei jedem Währungsumtausch zugrunde gelegt und vom Zahlungsdienstleister zugänglich gemacht wird oder aus einer öffentlich zugänglichen Quelle stammt;

28. „Referenzzinssatz“ den Zinssatz, der bei der Zinsberechnung zugrunde gelegt wird und aus einer öffentlich zugänglichen und für beide Parteien eines Zahlungsdienstvertrags überprüfbaren Quelle stammt;

29. „Authentifizierung“ ein Verfahren, mit dessen Hilfe der Zahlungsdienstleister die Identität eines Zahlungsdienstnutzers oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments, einschließlich der Verwendung der personalisierten Sicherheitsmerkmale des Nutzers, überprüfen kann;

30. „starke Kundenauthentifizierung“ eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas, das nur der Nutzer besitzt) oder Inhärenz (etwas, das der Nutzer ist), die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist;

31. „personalisierte Sicherheitsmerkmale“ personalisierte Merkmale, die der Zahlungsdienstleister einem Zahlungsdienstnutzer zum Zwecke der Authentifizierung bereitstellt;

32. „sensible Zahlungsdaten“ Daten, einschließlich personalisierter Sicherheitsmerkmale, die für betrügerische Handlungen verwendet werden können. Für die Tätigkeiten von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern stellen der Name des Kontoinhabers und die Kontonummer keine sensiblen Zahlungsdaten dar;

33. „Kundenidentifikator“ eine Kombination aus Buchstaben, Zahlen oder Symbolen, die dem Zahlungsdienstnutzer vom Zahlungsdienstleister mitgeteilt wird und die der Zahlungsdienstnutzer angeben muss, damit ein anderer am Zahlungsvorgang beteiligter Zahlungsdienstnutzer und/oder dessen Zahlungskonto bei einem Zahlungsvorgang zweifelsfrei ermittelt werden kann;

34. „Fernkommunikationsmittel“ ein Verfahren, das ohne gleichzeitige körperliche Anwesenheit von Zahlungsdienstleister und Zahlungsdienstnutzer für den Abschluss eines Vertrags über die Erbringung von Zahlungsdiensten eingesetzt werden kann;

35. „dauerhafter Datenträger“ jedes Medium, das es dem Zahlungsdienstnutzer gestattet, an ihn persönlich gerichtete Informationen derart zu speichern, dass die Information für eine für die Zwecke der Informationen angemessene Dauer zugänglich bleibt, und das die unveränderte Wiedergabe der gespeicherten Informationen ermöglicht;

36. „Kleinstunternehmen“ ein Unternehmen, das zum Zeitpunkt des Abschlusses des Zahlungsdienstvertrags ein Unternehmen im Sinne des Artikels 1 und des Artikels 2 Absätze 1 und 3 des Anhangs der Empfehlung 2003/361/EG ist;

37. „Geschäftstag“ einen Tag, an dem der an der Ausführung eines Zahlungsvorgangs beteiligte Zahlungsdienstleister des Zahlers bzw. des Zahlungsempfängers den für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb unterhält;

38. „Agent“ eine natürliche oder juristische Person, die im Namen eines Zahlungsinstituts Zahlungsdienste ausführt;

39. „Zweigniederlassung“ eine Geschäftsstelle, die nicht die Hauptverwaltung ist und die einen Teil eines Zahlungsinstituts bildet, keine Rechtspersönlichkeit hat und unmittelbar sämtliche oder einen Teil der Geschäfte betreibt, die mit der Tätigkeit eines Zahlungsinstituts verbunden sind; alle Geschäftsstellen eines Kredit- bzw. Zahlungsinstituts mit Hauptverwaltung in einem anderen Mitgliedstaat, die sich in ein und demselben Mitgliedstaat befinden, gelten als eine einzige Zweigniederlassung;

40. „Gruppe“ eine Gruppe von Unternehmen, die untereinander durch eine in Artikel 22 Absätze 1, 2 oder 7 der Richtlinie 2013/34/EU genannte Beziehung verbunden sind, oder Unternehmen im Sinne der Artikel 4, 5, 6 und 7 der delegierten Verordnung (EU) Nr. 241/2014 der Kommission (29), die untereinander durch eine in Artikel 10 Absatz 1 oder Artikel 113 Absätze 6 oder 7 der Verordnung (EU) Nr. 575/2013 genannte Beziehung verbunden sind;

41. „elektronisches Kommunikationsnetz“ ein Netz im Sinne des Artikels 2 Buchstabe a der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates (30);

42. „elektronische Kommunikationsdienste“ ein Dienst im Sinne des Artikels 2 Buchstabe c der Richtlinie 2002/21/EG;

43. „digitale Inhalte“ Waren oder Dienstleistungen, die in digitaler Form hergestellt und bereitgestellt werden, deren Nutzung oder Verbrauch auf ein technisches Gerät beschränkt ist und die in keiner Weise die Nutzung oder den Verbrauch von Waren oder Dienstleistungen in physischer Form einschließen;

44. „Annahme und Abrechnung von Zahlungsvorgängen (Acquiring)“ einen den Transfer von Geldbeträgen zum Zahlungsempfänger bewirkenden Zahlungsdienst eines Zahlungsdienstleisters, der mit einem Zahlungsempfänger eine vertragliche Vereinbarung über die Annahme und die Verarbeitung von Zahlungsvorgängen schließt;

45. „Ausgabe von Zahlungsinstrumenten“ einen Zahlungsdienst, bei dem ein Zahlungsdienstleister eine vertragliche Vereinbarung schließt, um einem Zahler ein Zahlungsinstrument zur Auslösung und Verarbeitung der Zahlungsvorgänge des Zahlers zur Verfügung zu stellen;

46. „Eigenmittel“ Mittel im Sinne des Artikels 4 Absatz 1 Nummer 118 der Verordnung (EU) Nr. 575/2013, wobei mindestens 75 % des Kernkapitals in Form von hartem Kernkapital nach Artikel 50 der genannten Verordnung gehalten werden und das Ergänzungskapital höchstens ein Drittel des harten Kernkapitals beträgt;

47. „Zahlungsmarke“ jeder reale oder digitale Name, jeder reale oder digitale Begriff, jedes reale oder digitale Zeichen, jedes reale oder digitale Symbol oder jede Kombination davon, mittels dem oder der bezeichnet werden kann, unter welchem Zahlungskartensystem kartengebundene Zahlungsvorgänge ausgeführt werden;

48. „Co-badging“ das Aufnehmen von zwei oder mehr Zahlungsmarken oder Zahlungsanwendungen derselben Zahlungsmarke auf dasselbe Zahlungsinstrument.

Artikel 72

Nachweis der Authentifizierung und Ausführung von Zahlungsvorgängen

(1) Die Mitgliedstaaten schreiben vor, dass ein Zahlungsdienstleister in dem Fall, dass ein Zahlungsdienstnutzer bestreitet, einen ausgeführten Zahlungsvorgang autorisiert zu haben, oder geltend macht, dass der Zahlungsvorgang nicht ordnungsgemäß ausgeführt wurde, nachweisen muss, dass der Zahlungsvorgang authentifiziert war, ordnungsgemäß aufgezeichnet und verbucht und nicht durch eine technische Panne oder einen anderen Mangel des von dem Zahlungsdienstleister erbrachten Dienstes beeinträchtigt wurde.

Wird der Zahlungsvorgang über einen Zahlungsauslösedienstleister ausgelöst, so muss der Zahlungsauslösedienstleister nachweisen, dass der Zahlungsvorgang — innerhalb seines Zuständigkeitsbereichs — authentifiziert, ordnungsgemäß aufgezeichnet und nicht durch eine technische Panne oder einen anderen Mangel im Zusammenhang mit dem von ihm verantworteten Zahlungsdienst beeinträchtigt wurde.

(2) Bestreitet ein Zahlungsdienstnutzer, einen ausgeführten Zahlungsvorgang autorisiert zu haben, so reicht die vom Zahlungsdienstleister, gegebenenfalls einschließlich des Zahlungsauslösedienstleisters aufgezeichnete Nutzung eines Zahlungsinstruments für sich gesehen nicht notwendigerweise aus, um nachzuweisen, dass der Zahler entweder den Zahlungsvorgang autorisiert oder aber in betrügerischer Absicht gehandelt oder eine oder mehrere seiner Pflichten nach Artikel 69 vorsätzlich oder grob fahrlässig verletzt hat. Der Zahlungsdienstleister, gegebenenfalls einschließlich des Zahlungsauslösedienstleisters, muss unterstützende Beweismittel vorlegen, um Betrug oder grobe Fahrlässigkeit des Zahlungsdienstnutzers nachzuweisen.

Artikel 74

Haftung des Zahlers für nicht autorisierte Zahlungsvorgänge

(1) Abweichend von Artikel 73 kann der Zahler dazu verpflichtet werden, Schäden, die infolge eines nicht autorisierten Zahlungsvorgangs unter Nutzung eines verlorenen oder gestohlenen Zahlungsinstruments oder infolge der missbräuchlichen Verwendung eines Zahlungsinstruments entstehen, bis höchstens 50 EUR zu tragen.

Unterabsatz 1 findet keine Anwendung, wenn

a) der Verlust, der Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments für den Zahler vor einer Zahlung nicht bemerkbar war, es sei denn, der Zahler hat selbst in betrügerischer Absicht gehandelt oder

b) der Verlust durch Handlungen oder Unterlassungen eines Angestellten oder eines Agenten, einer Zweigniederlassung eines Zahlungsdienstleisters oder einer Stelle, an den bzw. die Tätigkeiten ausgelagert werden, verursacht wurde.

Der Zahler trägt alle Verluste, die in Verbindung mit nicht autorisierten Zahlungsvorgängen entstanden sind, wenn er sie in betrügerischer Absicht oder durch vorsätzliche oder grob fahrlässige Verletzung einer oder mehrerer der Pflichten nach Artikel 69 herbeigeführt hat.

In diesen Fällen findet der Höchstbetrag nach Unterabsatz 1 keine Anwendung.

Wenn der Zahler weder in betrügerischer Absicht gehandelt hat noch seinen Pflichten nach Artikel 69 vorsätzlich nicht nachgekommen ist, können die Mitgliedstaaten die Haftung nach dem vorliegenden Absatz einschränken, wobei sie insbesondere der Art der personalisierten Sicherheitsmerkmale sowie den besonderen Umständen Rechnung tragen, unter denen der Verlust, der Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments stattgefunden hat.

(2) Verlangt der Zahlungsdienstleister des Zahlers keine starke Kundenauthentifizierung, so trägt der Zahler einen finanziellen Verlust nur, wenn der Zahler in betrügerischer Absicht gehandelt hat. Akzeptiert der Zahlungsempfänger oder der Zahlungsdienstleister des Zahlungsempfängers eine starke Kundenauthentifizierung nicht, muss er dem Zahlungsdienstleister des Zahlers den finanziellen Schaden ersetzen.

(3) Nach einer Anzeige gemäß Artikel 69 Absatz 1 Buchstabe b trägt der Zahler keine finanziellen Folgen der Nutzung des verlorenen, gestohlenen oder missbräuchlich verwendeten Zahlungsinstruments, es sei denn, er hat in betrügerischer Absicht gehandelt.

Stellt der Zahlungsdienstleister nicht nach Artikel 70 Absatz 1 Buchstabe c geeignete Mittel bereit, um jederzeit den Verlust, Diebstahl oder die missbräuchliche Verwendung eines Zahlungsinstruments anzeigen zu können, so haftet der Zahler nicht für die finanziellen Folgen der Nutzung dieses Zahlungsinstruments, es sei denn, er hat in betrügerischer Absicht gehandelt.

Artikel 97

Authentifizierung

(1) Die Mitgliedstaaten stellen sicher, dass ein Zahlungsdienstleister eine starke Kundenauthentifizierung verlangt, wenn der Zahler

a) online auf sein Zahlungskonto zugreift,

b) einen elektronischen Zahlungsvorgang auslöst,

c) über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs birgt.

(2) Im Fall der Einleitung elektronischer Fernzahlungsvorgänge nach Absatz 1 Buchstabe b stellen die Mitgliedstaaten sicher, dass die Zahlungsdienstleister für elektronische Fernzahlungsvorgänge eine starke Kundenauthentifizierung verlangen, die Elemente umfasst, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen.

(3) Im Fall des Absatzes 1 stellen die Mitgliedstaaten sicher, dass die Zahlungsdienstleister über angemessene Sicherheitsvorkehrungen verfügen, um die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer zu schützen.

(4) Die Absätze 2 und 3 gelten auch, wenn Zahlungen über einen Zahlungsauslösedienstleister ausgelöst werden. Die Absätze 1 und 3 gelten auch, wenn die Informationen über einen Kontoinformationsdienstleister angefordert werden.

(5) Die Mitgliedstaaten stellen sicher, dass der kontoführende Zahlungsdienstleister dem Zahlungsauslösedienstleister und dem Kontoinformationsdienstleister gestattet, sich auf die Authentifizierungsverfahren zu stützen, die er dem Zahlungsdienstnutzer gemäß den Absätzen 1 und 3 sowie — in Fällen, in denen der Zahlungsauslösedienstleister beteiligt ist — auch gemäß den Absätzen 1, 2 und 3 bereitstellt.

Artikel 98

Technische Regulierungsstandards für die Authentifizierung und die Kommunikation

(1) Die EBA arbeitet im Einklang mit Artikel 10 der Verordnung (EU) Nr. 1093/2010 in enger Zusammenarbeit mit der EZB und nach Anhörung aller maßgeblichen Akteure, einschließlich des Zahlungsverkehrsmarktes, unter Berücksichtigung der Interessen aller Beteiligten für Zahlungsdienstleister im Sinne des Artikels 1 Absatz 1 dieser Richtlinie technische Regulierungsstandards aus, in denen Folgendes präzisiert wird:

a) die Erfordernisse des Verfahrens zur starken Kundenauthentifizierung gemäß Artikel 97 Absätze 1 und 2,

b) die Ausnahmen von der Anwendung des Artikels 97 Absätze 1, 2 und 3 unter Zugrundelegung der Kriterien des Absatzes 3 dieses Artikels,

c) die Anforderungen, die Sicherheitsmaßnahmen gemäß Artikel 97 Absatz 3 erfüllen müssen, um die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer zu schützen, und

d) die Anforderungen an gemeinsame und sichere offene Standards für die Kommunikation zwischen kontoführenden Zahlungsdienstleistern, Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern, Zahlern, Zahlungsempfängern und anderen Zahlungsdienstleistern zum Zwecke der Identifizierung, der Authentifizierung, der Meldung und der Weitergabe von Informationen sowie der Anwendung von Sicherheitsmaßnahmen.

(2) Die Entwürfe technischer Regulierungsstandards gemäß Absatz 1 werden von der EBA mit folgender Zielsetzung ausgearbeitet:

a) Sicherstellung eines angemessenen Sicherheitsniveaus für Zahlungsdienstnutzer und Zahlungsdienstleister durch die Festlegung wirksamer und risikobasierter Anforderungen,

b) Gewährleistung der Sicherheit für die Gelder und die personenbezogenen Daten der Zahlungsdienstnutzer,

c) Sicherstellung und Aufrechterhaltung eines fairen Wettbewerbs zwischen allen Zahlungsdienstleistern,

d) Gewährleistung der Neutralität im Hinblick auf die Technologie und das Geschäftsmodell,

e) Ermöglichung der Entwicklung benutzerfreundlicher, allgemein zugänglicher und innovativer Zahlungsmittel.

(3) Die Ausnahmen nach Absatz 1 Buchstabe b werden unter Zugrundelegung folgender Kriterien gewährt:

a) mit der Dienstleistung verbundenes Risikoniveau,

b) der Betrag des Zahlungsvorgangs oder dessen Periodizität, oder beide,

c) für die Ausführung des Zahlungsvorgangs genutzter Zahlungsweg.

(4) Die EBA übermittelt der Kommission diese in Absatz 1 genannten Entwürfe technischer Regulierungsstandards bis zum 13. Januar 2017.

Der Kommission wird die Befugnis übertragen, die technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010 zu erlassen.

(5) Gemäß Artikel 10 der Verordnung (EU) Nr. 1093/2010 überprüft und aktualisiert die EBA — soweit erforderlich — die technischen Regulierungsstandards regelmäßig, um unter anderem der Innovation und den technologischen Entwicklungen Rechnung zu tragen.

EUROPEAN
COMMISSION

Brussels, XXX
[…](2017) XXX draft

COMMISSION DELEGATED REGULATION (EU) No …/..

of XXX

supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

Article 98(4) of Directive (EU) No 2015/2366 empowers the Commission to adopt, following submission of draft standards by the European Banking Authority (EBA), and in accordance with Articles 10 to 14 of Regulation No (EU) 1093/2010, delegated acts specifying the requirements of the strong customer authentication, the exemptions from its application and common and secure open standards of communication.

In accordance with Article 10(1) of Regulation No (EU) 1093/2010 establishing the EBA, the Commission shall decide within three months of receipt of the draft standards whether to endorse the drafts submitted. The Commission may also endorse the draft standards in part only, or with amendments, where the Union's interests so require, having regard to the specific procedure laid down in those Articles.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

In accordance with the third subparagraph of Article 10(1) of Regulation No (EU) 1093/2010, the EBA has carried out a public consultation on the draft technical standards submitted to the Commission in accordance with Article 98(4) of Directive (EU) No 2015/2366. A consultation paper was published on the EBA internet site on 12 August 2016, and the consultation closed on 12 October 2016. Moreover, the EBA invited the EBA's Banking Stakeholder Group set up in accordance with Article 37 of Regulation No (EU) 1093/2010 to provide advice on them. Together with the draft technical standards, the EBA has submitted an explanation on how the outcome of these consultations has been taken into account in the development of the final draft technical standards submitted to the Commission.

Together with the draft technical standards, and in accordance with the third subparagraph of Article 10(1) of Regulation No (EU) 1093/2010, the EBA has submitted its Impact Assessment, including its analysis of the costs and benefits, related to the draft technical standards submitted to the Commission. This analysis is available at (------ link to be provided by Communications), pages 40-44 of the Final Draft Regulatory Technical Standards package.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

These Regulatory Technical Standards (RTS) specify the requirements, under Article 98 of Directive (EU) No 2015/2366 (PSD2), of the strong customer authentication (SCA), the exemptions from the application of SCA, the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials, and the requirements for common and secure open standards of communication (CSC) between account servicing payment service providers (ASPSPs), payment initiation service providers (PISPs), account information service providers (AISPs), payers, payees and other payment service providers (PSPs).

These RTS take into account the various objectives of PSD2, including enhancing security, promoting competition, ensuring technology and business-model neutrality, contributing to the integration of payments in the EU, protecting consumers, facilitating innovation and enhancing customer convenience.

The RTS are technology and business-model neutral. The RTS contain a number of exemptions, including two exemptions for remote payments, one on transaction-risk analysis and the other on low value payments (below EUR 30). It also contains exemptions for

proximity payments. Considering the fact that the exemption based on transaction risk analysis is based on the observance of pre-set reference fraud rates, it is appropriate that the adequacy of the fraud level monitoring mechanism(s) of the payment service provider is scrutinized by a statutory auditor to ensure an impartial assessment of the correctness of the data. The actually achieved fraud levels should not only be reported to the competent authorities, for the purpose of ensuring an effective enforcement of the exemptions; they should also be reported directly to EBA enabling it to conduct a review of the reference fraud rates in the RTS within 18 months after the RTS enters into force.

Due to their very nature, payments made through the use of an anonymous payment instruments are not subject to the obligation of strong customer authentication. It goes without saying that where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from Directive (EU) 2015/2366 and this Regulatory Technical Standard.

The RTS also establish requirements on the communication between ASPSPs, AISPs and PISPs, among which the obligation for the ASPSPs to offer at least one interface for AISPs and PISPs for access to payment account information. With regard to the communication between ASPSPs, AISPs and PISPs, accordingly, the existing practice of third-party access without identification referred to in market jargon as 'screen scraping' or, mistakenly, as 'direct access' will no longer be allowed once the transition period under Article 115(4) PSD2 has elapsed and the RTS apply. However, the RTS establish requirements for ASPSPs to develop and maintain a communication interface to allow PISPs, AISPs and payment service providers issuing card-based payment instruments to access the data they need in compliance with PSD2. The RTS only apply to payment accounts, in accordance with the scope of PSD2. The RTS thus does not cover the access to accounts other than payment accounts, which falls under the competence of the Member States.

Where the ASPSP decides to use a dedicated interface, it shall ensure that this interface provides the same level of availability and performance as the interfaces offered to, and used by, their own customers. In order to ensure that these third parties can continue their service when the dedicated interface is not functioning properly, they should be able to use the customer facing interfaces as a contingency measure. Relevant provisions of PSD2 (Articles 65-67) should apply, including identification and authentication procedures. Payment initiation services and account information services providers should in particular comply with their obligations under Articles 66(3) and 67(2) of PSD2. The use of the contingency measures should be fully documented and reported to the authorities by the relevant providers, upon request. Once the dedicated interface is restored to full service, payment initiation services and account information services providers should be obliged to use it. For reasons of legal certainty, and in view of the requirement of harmonising a multitude of different rules to achieve a genuine single market in this domain, the RTS and the security measures referred to in Articles 65, 66, 67 and 97 of Directive (EU) 2015/2366 should become applicable from the same date.

COMMISSION DELEGATED REGULATION (EU) No …/..

of XXX

supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, and in particular the second subparagraph of Article 98(4) thereof[1],

Whereas:

(1) Payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. The authentication procedure should include, in general, transaction monitoring mechanisms to detect attempts to use a payment service user's personalised security credentials that were lost, stolen, or misappropriated and should also ensure that the payment service user is the legitimate user and therefore is giving consent for the transfer of funds and access to its account information through a normal use of the personalised security credentials. Furthermore, it is necessary to specify the requirements of the strong customer authentication that should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse, by requiring the generation of an authentication code which should be resistant against the risk of being forged in its entirety or by disclosure of any of the elements upon which the code was generated.

(2) As fraud methods are constantly changing, the requirements of strong customer authentication should allow for innovation in the technical solutions addressing the emergence of new threats to the security of electronic payments. To ensure that the requirements to be laid down are effectively implemented on a continuous basis, it is also appropriate to require that the security measures for the application of strong customer authentication and its exemptions, the measures to protect confidentiality and integrity of the personalised security credentials, and the measures establishing common and secure open standards of communication are documented, periodically tested, evaluated and audited by internal or statutory auditors. In order to allow

[1] OJ L 337, 23.12.2015 p. 35.

competent authorities to monitor the quality of the review of these measures, such reviews should be made available to them upon their request.

(3) As electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to introduce additional requirements for the strong customer authentication of such transactions, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction.

(4) Dynamic linking is possible through the generation of authentication codes which is subject to a set of strict security requirements. To remain technologically neutral a specific technology for the implementation of authentication codes should not be required. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.

(5) It is necessary to lay down specific requirements for the situation where the final amount is not known at the moment the payer initiates an electronic remote payment transaction, in order to ensure that the strong customer authentication is specific to the maximum amount that the payer has given consent for as referred to in Directive (EU) 2015/2366.

(6) In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as knowledge (something only the user knows), such as length or complexity, for the elements categorised as possession (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorized as inherence (something the user is) such as algorithm specifications, biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to lay down the requirements to ensure that those elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device,namely a device such as a tablet or a mobile phone which can be used both for giving the instruction to make the payment and in the authentication process.

(7) In accordance with Directive (EU) 2015/2366, exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.

(8) Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider, pose a low level of risk, thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Articles 65, 66 and 67 Directive (EU) 2015/2366, payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service

providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

(9) Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user friendly and low risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).

(10) Similar to the exemption for low value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase is posing a slightly higher security risk.

(11) The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which can guarantee the high levels of payment security that Directive (EU) 2015/2366 aims to reach through strong customer authentication. When the competent authorities establish that those corporate payment processes and protocols achieve the objectives of Directive (EU) 2015/2366 in terms of security, payment service providers may be exempted from the strong customer authentication requirements.

(12) In the case of real-time transaction risk analysis that categorise a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk based exemption should be set in a manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

(13) For the purpose of ensuring an effective enforcement, payment service providers, that wish to benefit from the exemptions from strong customer authentication based on risk analysis, should regularly monitor and make available to competent authorities and to the European Banking Authority (EBA), for each payment instrument and payment transaction, the value of unauthorised payment transactions and the observed fraud

rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.

(14) The collection of this new historical evidence on the fraud rates of electronic payment transactions will also provide evidence contributing to an effective review by the EBA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The EBA should review and submit draft updates to the Commission of these regulatory technical standards, where appropriate, by submitting new draft thresholds and corresponding fraud rates with the aim of enhancing the security of remote electronic payments, in accordance with Article 98(5) of Directive (EU) 2015/2366 and with Article 10 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council[2].

(15) Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions. In the case of remote payments, consumers should also have the choice to revert back to strong customer authentication where, in a given case, they consider this more safe and secure.

(16) The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.

(17) In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availabilty of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers.

(18) Each account servicing payment service provider with payment accounts that are accessible online should offer at least one interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user. Directive (EU) 2015/2366 provides for the access and use of payment account information by account information service providers. This regulation therefore does not change the rules of access to accounts other than payment accounts.

[2] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

(19) In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. Moreover, the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international or European standardisation organisations. To ensure technology and business-model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

(20) Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in Directive (EU) 2015/2366, it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. To ensure that the payment service providers who are making use of the dedicated interface can continue to provide their services in case of problems with availability or inadequate performance, it is necessary to provide a fallback mechanism that will allow such providers to use the interface for the identification and communication with the account servicing payment service providers' payment service users under certain conditions and requirements.

(21) In order to allow competent authorities to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the competent authorities with documentation of the solutions in case of emergencies. Where the account servicing payment service provider has implemented a dedicated interface, it should also provide the competent authority, on its request, with the statistics on the availability and performance of that interface.

(22) In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

(23) To improve user confidence and ensure strong customer authentication, the use of electronic identification means and trust services as set out in Regulation (EU) No

910/2014 of the European Parliament and of the Council[3] should be taken into account, in particular with regard to notified electronic identification schemes

(24) For reasons of legal certainty, it is appropriate that this Regulation be applicable from the same date as Articles 65, 66, 67 and 97 of Directive 2015/2366.

(25) This Regulation is based on the draft regulatory technical standards submitted by the EBA to the Commission.

(26) EBA has conducted open and transparent public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the opinion of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010.

HAS ADOPTED THIS REGULATION:

CHAPTER I
GENERAL PROVISIONS

Article 1
Subject matter

This Regulation establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to do the following:

(a) apply the procedure of strong customer authentication in accordance with Article 97 of Directive (EU) 2015/2366;

(b) exempt the application of the security requirements of strong customer authentication, subject to specified and limited conditions based on the level of risk, the amount and the recurrence of the payment transaction and of the payment channel used for its execution;

(c) protect the confidentiality and the integrity of the payment service user's personalised security credentials;

(d) establish common and secure open standards for the communication between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers in relation to the provision and use of payment services in application of Title IV of Directive (EU) 2015/2366.

Article 2
General authentication requirements

1. Payment service providers shall have transaction monitoring mechanisms in place that enable them detect unauthorised or fraudulent payment transactions for the purpose of the implementation of the security measures referred to in points (a) and (b) of Article 1.

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 53).

Those mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials.

2. Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:

(a) lists of compromised or stolen authentication elements;

(b) the amount of each payment transaction;

(c) known fraud scenarios in the provision of payment services;

(d) signs of malware infection in any sessions of the authentication procedure.

Article 3
Review of the security measures

1. The implementation of the security measures referred to in Article 1 shall be documented, periodically tested, evaluated and audited by internal or statutory auditors in accordance with the applicable audit framework of the payment service provider.

2. The period between the audit reviews referred to in paragraph 1 shall be determined taking into account the relevant accounting and statutory audit framework applicable to the payment service provider.

However, payment service providers that make use of the exemption referred to in Article 18 shall perform a statutory audit for the methodology, the model and the reported fraud rates at a minimum on a yearly basis.

3. The audit review shall evaluate and report on the compliance of the payment service provider's security measures with the requirements set out in this Regulation.

The entire report shall be made available to competent authorities upon their request.

CHAPTER II
SECURITY MEASURES FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION

Article 4
Authentication code

1. Where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code.

The authentication code shall be only accepted once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2. For the purpose of paragraph 1, payment service providers shall adopt security measures ensuring that each of the following requirements is met:

(a) no information on any of the elements referred to in paragraph 1 can be derived from the disclosure of the authentication code;

(b) it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;

(c) the authentication code cannot be forged.

3. Payment service providers shall ensure that the authentication by means of generating an authentication code includes each of the following measures:

(a) where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1, it shall not be possible to identify which of the elements referred to in that paragraph was incorrect;

(b) the number of failed authentication attempts that can take place consecutively, after which the actions referred to in Article 97(1) of Directive (EU) 2015/2366 shall be temporarily or permanently blocked, shall not exceed five times within a given period of time;

(c) the communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements in Chapter V;

(d) a maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed five minutes.

4. Where the block referred to in paragraph 3(b) is temporary, the duration of that block and the number of retries shall be established based on the characteristics of the service provided to the payer and all the relevant risks involved, taking into account, at a minimum, the factors referred to in Article 2(3).

The payer shall be alerted before the block is made permanent.

Where the block has been made permanent, a secure procedure shall be established allowing the payer to regain use of the blocked electronic payment instruments.

Article 5
Dynamic linking

1. Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this Regulation, they shall also adopt security measures that meet each of the following requirements:

(a) the payer is made aware of the amount of the payment transaction and of the payee*;*

(b) the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;

(c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;

(d) any change to the amount or the payee results in the invalidation of the authentication code generated.

2. For the purpose of paragraph 1, payment service providers shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:

(a) the amount of the transaction and the payee throughout all of the phases of the authentication;

(b) the information displayed to the payer throughout all of the phases of the authentication including the generation, transmission and use of the authentication code.

3. For the purpose of paragraph 1(b) and where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366 the following requirements for the authentication code shall apply:

(a) in relation to a card-based payment transaction for which the payer has given consent to the exact amount of the funds to be blocked pursuant to Article 75(1) of that Directive, the authentication code shall be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction;

(b) in relation to payment transactions for which the payer has given consent to execute a batch of remote electronic payment transactions to one or several payees, the authentication code shall be specific to the total amount of the batch of payment transactions and to the specified payees.

Article 6
Requirements of the elements categorised as knowledge

1. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as knowledge are uncovered by, or disclosed to, unauthorised parties.

2. The use by the payer of those elements shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties.

Article 7
Requirements of the elements categorised as possession

1. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as possession are used by unauthorised parties.

2. The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.

Article 8
Requirements of devices and software linked to elements categorised as inherence

1. Payment service providers shall adopt measures to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties. At a

minimum, the payment service providers shall ensure that those access devices and software have a very low probability of an unauthorised party being authenticated as the payer.

2. The use by the payer of those elements shall be subject to measures ensuring that those devices and the software guarantee resistance against unauthorised use of the elements through access to the devices and the software.

Article 9
Independence of the elements

1. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.

2. Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.

3. For the purposes of paragraph 2, the mitigating measures shall include each of the following:

   (a) the use of separated secure execution environments through the software installed inside the multi-purpose device;

   (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party;

   (c) where alterations have taken place, mechanisms to mitigate the consequences thereof.

CHAPTER III
EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION

Article 10
Payment account information

1. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 and to paragraph 2 of this Article and, where a payment service user is limited to accessing either or both of the following items online without disclosure of sensitive payment data:

   (a) the balance of one or more designated payment accounts;

   (b) the payment transactions executed in the last 90 days through one or more designated payment accounts.

2. For the purpose of paragraph 1, payment service providers shall not be exempted from the application of strong customer authentication where either of the following condition is met:

(a) the payment service user is accessing online the information specified in paragraph 1 for the first time;

(b) more than 90 days have elapsed since the last time the payment service user accessed online the information specified in paragraph 1(b) and strong customer authentication was applied .

Article 11
Contactless payments at point of sale

Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, where the payer initiates a contactless electronic payment transaction provided that each of the following conditions is met:

(a) the individual amount of the contactless electronic payment transaction does not exceed EUR 50;

(b) the cumulative amount of previous contactless electronic payment transactions initiated by means of a payment instrument with a contactless functionality from the date of the last application of strong customer authentication does not exceed EUR 150;

(c) the number of consecutive transactions initiated via the payment instrument offering a contactless functionality since the last application of strong customer authentication does not exceed five.

Article 12
Transport fares and parking fees

Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

Article 13
Trusted beneficiaries

1. Payment service providers shall apply strong customer authentication where a payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider.

2. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, where the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

Article 14
Recurring transactions

1. Payment service providers shall apply strong customer authentication when a payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee.

2. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred to in paragraph 1.

Article 15
Credit transfers between accounts held by the same natural or legal person

Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, where the payer initiates a credit transfer in circumstances where the payer and the payee are the same natural or legal person and both payment accounts are held by the same account servicing payment service provider.

Article 16
Low-value transactions

Payment service providers shall be allowed not to apply strong customer authentication, where the payer initiates a remote electronic payment transaction provided that the following conditions are met:

(a) the amount of the remote electronic payment transaction does not exceed EUR 30;

(b) the cumulative amount of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not, exceed EUR 100

(c) the number of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed 5 consecutive individual remote electronic payment transactions.

Article 17
Secure corporate payment systems

Payment service providers shall be allowed not to apply strong customer authentication in respect of legal persons initiating electronic payment transactions through the use of dedicated corporate payment processes or protocols where the competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those aimed for by Directive 2015/2366.

Article 18
Transaction risk analysis

1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 3 of this Article.

2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:

   (a) where the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is below the

reference fraud rates specified in the table set out in the Annex for 'remote electronic card-based payments' and 'remote electronic credit transfers' respectively;

(b) where the amount of the transaction does not exceed the relevant Exemption Threshold Value ('ETV') specified in the table set out in the Annex;

(c) where the following conditions, assessed on the basis of the transaction monitoring mechanisms referred to in paragraph 3, are met:

(i) no abnormal spending or behavioural pattern of the payer has been identified;

(ii) no unusual information about the payer's device/software access has been identified;

(iii) no malware infection in any session of the authentication procedure has been identified;

(iv) no known fraud scenario in the provision of payment services has been identified;

(v) the location of the payer is not abnormal;

(vi) the location of the payee is not identified as high risk.

3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall have in place transaction monitoring mechanisms that enable those providers to perform a real-time risk analysis of those transactions which takes into account, at a minimum, the risk-based factors set out in Article 2(2) and assesses, the following risk-based factors: the previous spending patterns of the individual payment service user;

(a) the payment transaction history of each of the payment service provider's payment service users;

(b) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;

(c) abnormal payment patterns of the payment service user in relation to the user's payment transaction history;

(d) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

The assessment made by a payment service provider shall combine all those risk-based factors into a detailed risk scoring of each transaction, which would enable the assessment of the level of risk of each payment transaction.

Article 19
Calculation of fraud rates

1. For each type of transaction referred to in the table set out in the Annex, the payment service provider shall ensure that the overall fraud rates covering both payment transactions authenticated through strong customer authentication and those executed

under any of the exemptions referred to in Articles 13 to 18 are equivalent to, or lower than, the reference fraud rate for the same type of payment transaction indicated in the table set out in the Annex.

The overall fraud rate for each type of transaction shall be calculated as the total value of unauthorised or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of transactions, whether authenticated with the application of strong customer authentication or executed under any exemption referred to in Articles 13 to 18 on a rolling quarterly basis.

2. The calculation of the fraud rates and resulting figures shall be assessed by the audit review referred to in Article 3(2), which shall ensure that they are complete and accurate.

3. The methodology and any model, used by the payment service provider to calculate the fraud rates, as well as the fraud rates themselves, shall be adequately documented and made fully available to competent authorities and to EBA.

Article 20
Cessation of exemptions based on transaction risk analysis

1. Payment service providers that make use of the exemption referred to in Article 18 shall immediately report to the competent authorities where one of their monitored fraud rates, for any given payment instrument or type of payment transaction, exceeds the applicable reference fraud rate and shall provide to the competent authorities a description of the measures that they intend to adopt to restore compliance of their monitored fraud rate with the applicable reference fraud rates.

2. Payment service providers shall immediately cease to make use of the exemption referred to in Article 18 for a given payment instrument or type of payment transaction in the specific exemption threshold range where their monitored fraud rate exceeds for two consecutive quarters the reference fraud rate applicable for that payment instrument or type of payment transaction in that exemption threshold range.

3. Following the cessation of the exemption referred to in Article 18 in accordance with paragraph 2 of this Article, payment service providers shall not use that exemption again, until their calculated fraud rate equals to, or is below, the reference fraud rates applicable for that payment instrument or type of payment transaction in that exemption threshold range for two consecutive quarters.

4. Where payment service providers intend to make use again of the exemption referred to in Article 18, they shall notify the competent authorities in a reasonable timeframe and shall before making use again of the exemption, provide evidence of the restoration of compliance of their monitored fraud rate with the applicable reference fraud rate for that exemption threshold range in accordance with paragraph 3 of this Article.

Article 21
Monitoring

1. In order to make use of the exemptions set out in Articles 10 to 18, payment service providers shall record and monitor the following data for each payment instrument

and type of payment transaction, with a breakdown for both remote and non-remote payment transactions, at least on a quarterly basis:

(a) the total value of unauthorised payment transactions in accordance with Article 64(2) of Directive (EU) 2015/2366, the total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated through strong customer authentication and under the exemptions;

(b) the average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and under the exemptions;

(c) the number of payment transactions where any of the exemptions was applied and their percentage in respect of the total number of payment transactions.

2. Payment service providers shall make the results of the monitoring in accordance with paragraph 1 available to competent authorities and to EBA.

CHAPTER IV
CONFIDENTIALITY AND INTEGRITY OF THE PAYMENT SERVICE USERS' PERSONALISED SECURITY CREDENTIALS

Article 22
General requirements

1. Payment service providers shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication.

2. For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:

(a) personalised security credentials are masked when displayed and are not readable in their full extent when input by the payment service user during the authentication;

(b) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plaintext;

(c) secret cryptographic material is protected from unauthorised disclosure.

3. Payment service providers shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials.

4. Payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter II take place in secure environments in accordance with strong and widely recognised industry standards.

Article 23
Creation and transmission of credentials

Payment service providers shall ensure that the creation of personalised security credentials is performed in a secure environment.

They shall mitigate the risks of unauthorised use of the personalised security credentials and of the authentication devices and software following their loss, theft or copying before their delivery to the payer.

Article 24
Association with the payment service user

1. Payment service providers shall ensure that only the payment service user is associated, in a secure manner, with the personalised security credentials, the authentication devices and the software.

2. For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:

   (a) the association of the payment service user's identity with personalised security credentials, authentication devices and software is carried out in secure environments under the payment service provider's responsibility comprising at least the payment service provider's premises, the internet environment provided by the payment service provider or other similar secure websites used by the payment service provider and its automated teller machine services, and taking into account risks associated with devices and underlying components used during the association process that are not under the responsibility of the payment service provider;

   (b) the association by means of a remote channel of the payment service user's identity with the personalised security credentials and with authentication devices or software is performed using strong customer authentication.

Article 25
Delivery of credentials, authentication devices and software

1. Payment service providers shall ensure that the delivery of personalised security credentials, authentication devices and software to the payment service user is carried out in a secure manner designed to address the risks related to their unauthorised use due to their loss, theft or copying.

2. For the purpose of paragraph 1, payment service providers shall at least apply each of the following measures:

   (a) effective and secure delivery mechanisms ensuring that the personalised security credentials, authentication devices and software are delivered to the legitimate payment service user ;

   (b) mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user by means of the internet;

   (c) arrangements ensuring that, where the delivery of personalised security credentials is executed outside the premises of the payment service provider or through a remote channel:

      (i) no unauthorised party can obtain more than one feature of the personalised security credentials, the authentication devices or software when delivered through the same channel;

(ii) the delivered personalised security credentials, authentication devices or software require activation before usage;

(d) arrangements ensuring that, in cases where the personalised security credentials, the authentication devices or software have to be activated before their first use, the activation shall take place in a secure environment in accordance with the association procedures referred to in Article 24.

Article 26
Renewal of personalised security credentials

Payment service providers shall ensure that the renewal or re-activation of personalised security credentials adhere to the procedures for the creation, association and delivery of the credentials and of the authentication devices in accordance with Articles 23, 24 and 25.

Article 27
Destruction, deactivation and revocation

Payment service providers shall ensure that they have effective processes in place to apply each of the following security measures:

(a) the secure destruction, deactivation or revocation of the personalised security credentials, authentication devices and software;

(b) where the payment service provider distributes reusable authentication devices and software, the secure re-use of a device or software is established, documented and implemented before making it available to another payment services user;

(c) the deactivation or revocation of information related to personalised security credentials stored in the payment service provider's systems and databases and, where relevant, in public repositories.

CHAPTER V
COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION

SECTION 1
GENERAL REQUIREMENTS FOR COMMUNICATION

Article 28
Requirements for identification

1. Payment service providers shall ensure secure identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals.

2. Payment service providers shall ensure that the risks of misdirection of communication to unauthorised parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.

Article 29
Traceability

1. Payment service providers shall have processes in place which ensure that all payment transactions and other interactions with the payment services user, with other payment service providers and with other entities, including merchants, in the context of the provision of the payment service are traceable, ensuring knowledge ex-post of all events relevant to the electronic transaction in all the various stages.

2. For the purpose of paragraph 1, payment service providers shall ensure that any communication session established with the payment services user, other payment service providers and other entities, including merchants, relies on each of the following:

   (a) a unique identifier of the session;

   (b) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data;

   (c) timestamps which shall be based on a unified time-reference system and which shall be synchronised according to an official time signal.

SECTION 2
SPECIFIC REQUIREMENTS FOR THE COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION

Article 30
General obligations for communication interfaces

1. Account servicing payment service providers that offer to a payer a payment account that is accessible online shall have in place at least one interface which meets each of the following requirements:

   (a) account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments are able to identify themselves towards the account servicing payment service provider;

   (b) account information service providers are able to communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions;

   (c) payment initiation service providers are able to communicate securely to initiate a payment order from the payer's payment account and receive all information on the initiation of the payment transaction and all information accessible to the account servicing payment service providers regarding the execution of the payment transaction.

2. For the purposes of authentication of the payment service user, the interface referred to in paragraph 1 shall allow account information service providers and payment initiation service providers to rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user.

   The interface shall at least meet all of the following requirements:

   (a) a payment initiation service provider or an account information service provider shall be able to instruct the account servicing payment service

provider to start the authentication based on the consent of the payment service user;

(b) communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and any payment service users concerned shall be established and maintained throughout the authentication;

(c) the integrity and confidentiality of the personalised security credentials and of authentication codes transmitted by or through the payment initiation service provider or the account information service provider shall be ensured.

3. Account servicing payment service providers shall ensure that their interfaces follow standards of communication which are issued by international or European standardisation organisations.

Account servicing payment service providers shall also ensure that the technical specification of any of the interfaces is documented specifying a set of routines, protocols, and tools needed by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments for allowing their software and applications to interoperate with the systems of the account servicing payment service providers.

Account servicing payment service providers shall at a minimum make the documentation available, at no charge, upon request by authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or payment service providers that have applied to their competent authorities for the relevant authorisation, and shall make a summary of the documentation publicly available on their website.

4. In addition to paragraph 3, account servicing payment service providers shall ensure that, except for emergency situations, any change to the technical specification of their interface is made available to authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, or payment service providers that have applied to their competent authorities for the relevant authorisation, in advance as soon as possible and not less than 3 months before the change is implemented.

Payment service providers shall document emergency situations where changes were implemented and make the documentation available to competent authorities on request.

5. Account servicing payment service providers shall make available a testing facility, including support, for connection and functional testing to enable authorised payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers, or payment service providers that have applied for the relevant authorisation, to test their software and applications used for offering a payment service to users.

However, no sensitive information shall be shared through the testing facility.

Article 31
Communication interface options

Account servicing payment service providers shall establish the interface(s) referred to in Article 30 by means of a dedicated interface or by allowing the use by the payment service

providers referred to in Article 30(1) of the interfaces used for authentication and communication with the account servicing payment service provider's payment services users.

Article 32
Obligations for a dedicated interface

1. Subject to compliance with Article 30 and 31, account servicing payment service providers that have put in place a dedicated interface, shall ensure that the dedicated interface offers the same level of availability and performance, including support, as the interfaces made available to the payment service user for directly accessing its payment account online.

2. For the purpose of paragraph 1, account servicing payment service providers shall monitor the availability and performance of the dedicated interface, produce statistics from the monitoring and make those statistics available to the competent authorities upon their request.

Article 33
Contingency measures for a dedicated interface

1. Account servicing payment service providers shall include, in the design of the dedicated interface, a strategy and plans for contingency measures in the event of an inadequate performance, unplanned unavailability of the interface and systems breakdown.

2. Where the dedicated interface does not operate at the same level of availability and performance as the interfaces made available to the account servicing payment service provider's payment service users for accessing their payment accounts online, both the account servicing payment service provider and the payment service providers referred to in Article 30(1) shall report that fact to their respective competent national authorities without delay.

3. Where the dedicated interface is unavailable for more than 30 seconds during a communication session between payment service providers within the dedicated interface, or where it does not operate in compliance with the requirements under Articles 30 and 32, the payment service providers referred to in Article 30(1) shall be allowed to make use of the interfaces made available to the payment service users for directly accessing their payment account online, until the dedicated interface has resumed functioning at the level prescribed under Article 32(1), and only under the following conditions:

   (a) they ensure that they can be identified by the account servicing payment service provider;

   (b) they are enabled to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user;

   (c) they take the necessary measures to ensure that they do not access, store or process data for purposes other than for the provision of the service as requested by the payment service user;

   (d) they continue to comply with the obligations following from Article 66(3) and Article 67(2) of Directive (EU) 2015/2366 respectively;

(e) they document and provide, upon request and without undue delay, the log files of the data that are accessed through the interface operated by the account servicing payment service provider for its payment service users to the account servicing payment service provider, to their competent national authority;

(f) they duly justify, upon request and without undue delay, the use of the interface made available to the payment service users for directly accessing its payment account online to their competent national authority and inform the account servicing payment service provider accordingly;

For the purposes of point (a), the account servicing payment service provider shall ensure that the identification by the payment service providers referred to in Article 30(1) can be performed.

Article 34
Certificates

1. For the purpose of identification, as referred to in Article 22(2)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 of the European Parliament and of the Council or for website authentication as referred to in Article 3(39) of that Regulation.

2. For the purpose of this Regulation, the registration number as referred to in the official records in accordance with Annex III (c) or Annex IV (c) to Regulation (EU) No 910/2014 shall be the authorisation number of the payment service provider issuing card-based payment instruments, the account information service providers and payment initiation service providers, including account servicing payment service providers providing such services, available in the public register of the home Member State pursuant to Article 14 of Directive (EU) 2015/2366 or resulting from the notifications of every authorisation granted under Article 8 of Directive 2013/36/EU of the European Parliament and of the Council[4] in accordance with Article 20 of that Directive.

3. For the purposes of this Regulation, qualified certificates for electronic seals or for website authentication referred to in paragraph 1 shall include, in a language customary in the sphere of international finance, additional specific attributes in relation to each of the following:

(a) the role of the payment service provider, which maybe one or more of the following:

(i) account servicing;

(ii) payment initiation;

(iii) account information;

(iv) issuing of card-based payment instruments;

[4] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

(b) the name of the competent authorities where the payment service provider is registered.

4. The attributes referred to in paragraph 3 shall not affect the interoperability and recognition of qualified certificates for electronic seals or website authentication.

Article 35
Security of communication session

1. Account servicing payment service providers, payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall ensure that, when exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.

2. Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall keep the access sessions offered by account servicing payment service providers as short as possible and they shall actively terminate any such session as soon as the requested action has been completed.

3. When maintaining parallel network sessions with the account servicing payment service provider, account information service providers and payment initiation service providers shall ensure that those sessions are securely linked to relevant sessions established with the payment service user(s) in order to prevent the possibility that any message or information communicated between them could be misrouted.

4. Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments with the account servicing payment service provider shall contain unambiguous references to each of the following items:

(a) the payment service user or users and the corresponding communication session in order to distinguish several requests from the same payment service user or users;

(b) for payment initiation services, the uniquely identified payment transaction initiated;

(c) for confirmation on the availability of funds, the uniquely identified request related to the amount necessary for the execution of the card-based payment transaction.

5. Account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall ensure that where they communicate personalised security credentials and authentication codes, these are not readable by any staff at any time.

In case of loss of confidentiality of personalised security credentials under their sphere of competence, those providers shall inform without undue delay the payment services user associated with them and the issuer of the personalised security credentials.

Article 36
Data exchanges

1. Account servicing payment service providers shall comply with each of the following requirements:

   (a) they shall provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data;

   (b) they shall provide, immediately after receipt of the payment order, payment initiation service providers with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the latter;

   (c) they shall, upon request, immediately provide payment service providers with a confirmation in a simple 'yes' or 'no' format, whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer.

2. In case of an unexpected event or error occurring during the process of identification, authentication, or the exchange of the data elements, the account servicing payment service provider shall send a notification message to the payment initiation service provider or the account information service provider and the payment service provider issuing card-based payment instruments which explains the reason for the unexpected event or error.

   Where the account servicing payment service provider offers a dedicated interface in accordance with Article 32, the interface shall provide for notification messages concerning unexpected events or errors to be communicated by any payment service provider that detects the event or error to the other payment service providers participating in the communication session.

3. Account information service providers shall have in place suitable and effective mechanisms that prevent access to information other than from designated payment accounts and associated payment transactions, in accordance with the user’s explicit consent.

4. Payment initiation service providers shall provide account servicing payment service providers with the same information as requested from the payment service user when initiating the payment transaction directly.

5. Account information service providers shall be able to access information from designated payment accounts and associated payment transactions held by account servicing payment service providers for the purposes of performing the account information service in either of the following circumstances:

   (a) whenever the payment service user is actively requesting such information;

   (b) where the payment service user does not actively request such information, no more than four times in a 24 hour period, unless a higher frequency is agreed between the account information service provider and the account servicing payment service provider, with the payment service user’s consent.

CHAPTER VI
FINAL PROVISIONS

Article 37
Review

Without prejudice to Article 98(5) of Directive (EU) 2015/2366, EBA shall review by [*OP: please insert date corresponding to '18 months after the date of application referred to in Article 37(2)]* the fraud rates referred to in the Annex to this Regulation and, if appropriate, submit draft updates thereto to the Commission in accordance with Article 10 of Regulation (EU) No 1093/2010.

Article 38
Entry into force

1. This Regulation shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

2. This Regulation shall apply from [OP: please insert date corresponding to '18 months after entry into force date'].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President
Jean-Claude Juncker

СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

CVRIA
LUXEMBOURG

EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

URTEIL DES GERICHTSHOFS (Dritte Kammer)

25. Januar 2017*

„Vorlage zur Vorabentscheidung – Richtlinie 2007/64/EG – Zahlungsdienste im Binnenmarkt – Rahmenverträge – Allgemeine vorvertragliche Unterrichtung – Erfordernis der Unterrichtung auf Papier oder einem anderen dauerhaften Datenträger – Übermittlung von Informationen über eine Mailbox auf einer Website für Electronic-Banking“

In der Rechtssache C-375/15

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Obersten Gerichtshof (Österreich) mit Entscheidung vom 27. Mai 2015, beim Gerichtshof eingegangen am 15. Juli 2015, in dem Verfahren

BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG

gegen

Verein für Konsumenteninformation

erlässt

* Verfahrenssprache: Deutsch.

DER GERICHTSHOF (Dritte Kammer)

unter Mitwirkung des Kammerpräsidenten L. Bay Larsen sowie der Richter M. Vilaras, J. Malenovský, M. Safjan (Berichterstatter) und D. Šváby,

Generalanwalt: M. Bobek,

Kanzler: K. Malacek, Verwaltungsrat,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 30. Juni 2016,

unter Berücksichtigung der Erklärungen

– der BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG, vertreten durch Rechtsanwalt G. Schett,

– des Vereins für Konsumenteninformation, vertreten durch Rechtsanwalt S. Langer,

– der italienischen Regierung, vertreten durch G. Palmieri als Bevollmächtigte im Beistand von L. D'Ascia, avvocato dello Stato,

– der polnischen Regierung, vertreten durch B. Majczyna als Bevollmächtigten,

– der Europäischen Kommission, vertreten durch W. Mölls und H. Tserepa-Lacombe als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 15. September 2016

folgendes

Urteil

1 Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 36 Abs. 1 und Art. 41 Abs. 1 der Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG

sowie zur Aufhebung der Richtlinie 97/5/EG (ABl. 2007, L 319, S. 1) in der durch die Richtlinie 2009/111/EG des Europäischen Parlaments und des Rates vom 16. September 2009 (ABl. 2009, L 302, S. 97) geänderten Fassung (im Folgenden: Richtlinie 2007/64).

2 Dieses Ersuchen ergeht im Rahmen eines Rechtsstreits zwischen der BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG (im Folgenden: BAWAG) und dem Verein für Konsumenteninformation (im Folgenden: VKI) wegen einer von der BAWAG beim Abschluss von Verbraucherverträgen verwendeten Klausel.

Rechtlicher Rahmen

Unionsrecht

3 In den Erwägungsgründen 18, 21 bis 24, 27 und 46 der Richtlinie 2007/64 heißt es:

„(18) Es sollten Regeln eingeführt werden, die transparente Vertragsbedingungen und Informationsanforderungen bei Zahlungsdiensten sicherstellen.

…

(21) In dieser Richtlinie sollten die Informationspflichten der Zahlungsdienstleister gegenüber den Zahlungsdienstnutzern festgelegt werden, damit Letztere ein gleich hohes Maß an verständlichen Informationen über Zahlungsdienste erhalten und so die Konditionen der verschiedenen Anbieter in der EU vergleichen und ihre Wahl in voller Kenntnis der Sachlage treffen können. Im Interesse der Transparenz sollte diese Richtlinie die harmonisierten Anforderungen festlegen, die erforderlich sind, um sicherzustellen, dass der Zahlungsdienstnutzer sowohl zu dem mit dem Zahlungsdienstleister geschlossenen Vertrag als auch zum Zahlungsvorgang in ausreichendem Umfang alle notwendigen Informationen erhält. Damit der Binnenmarkt für Zahlungsdienste reibungslos funktionieren kann, sollten die Mitgliedstaaten nur solche Informationsvorschriften erlassen können, die in dieser Richtlinie vorgesehen sind.

(22) Nach der Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken [von Unternehmen gegenüber Verbrauchern im Binnenmarkt und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (‚Richtlinie über unlautere Geschäftspraktiken‘) (ABl. 2005, L 149, S. 22)] sowie der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (‚Richtlinie über den elektronischen Geschäftsverkehr‘) [(ABl. 2000, L 178, S. 1)] und der Richtlinie 2002/65/EG des Europäischen Parlaments und des Rates vom 23. September 2002 über den Fernabsatz von Finanzdienstleistungen an Verbraucher [und zur Änderung der Richtlinie 90/619/EWG des Rates und der Richtlinien 97/7/EG und 98/27/EG (ABl. 2002, L 271, S. 16) in der durch die Richtlinie 2005/29 geänderten Fassung] sollten die Verbraucher vor unlauteren oder irreführenden Praktiken geschützt werden. Die zusätzlichen Bestimmungen jener Richtlinien gelten weiterhin. Doch muss insbesondere verdeutlicht werden, in welchem Verhältnis die vorvertraglichen Informationspflichten dieser Richtlinie zu denen der Richtlinie 2002/65/EG stehen.

(23) Die Informationen sollten den Bedürfnissen der Nutzer angemessen sein und in standardisierter Form übermittelt werden. Allerdings sollten für Einzelzahlungen andere Informationspflichten gelten als für Rahmenverträge, die mehrere Zahlungsvorgänge betreffen.

(24) In der Praxis sind Rahmenverträge und darunter fallende Zahlungsvorgänge weitaus häufiger und fallen wirtschaftlich mehr ins Gewicht als Einzelzahlungen. Bei Zahlungskonten oder bestimmten Zahlungsinstrumenten ist ein Rahmenvertrag erforderlich. Daher sollten die Vorabinformationspflichten bei Rahmenverträgen recht umfassend sein[,] und die Informationen sollten immer auf Papier oder einem anderen dauerhaften Datenträger mitgeteilt werden, wie beispielsweise Ausdrucke von Kontoauszugsdruckern, Disketten, CD-ROMs, DVDs und PC-Festplattenlaufwerken, auf denen elektronische Post gespeichert werden kann, sowie Websites, sofern sie für einen dem Zweck der Information angemessenen Zeitraum konsultiert und unverändert reproduziert werden können. Allerdings sollten Zahlungsdienstleister und Zahlungsdienstnutzer in einem Rahmenvertrag vereinbaren können, in welcher Weise nachträgliche Information über die ausgeführten Zahlungsvorgänge erfolgen soll, beispielsweise dass beim Internetbanking alle das Zahlungskonto betreffenden Informationen online zugänglich gemacht werden.

…

(27) … [I]n dieser Richtlinie [sollte] zwischen zwei Arten unterschieden werden, auf [die] Informationen vom Zahlungsdienstleister gegeben werden müssen. Entweder sollte die Information mitgeteilt, d. h. vom Zahlungsdienstleister zu dem in dieser Richtlinie geforderten Zeitpunkt von sich aus übermittelt werden, ohne dass der Zahlungsdienstnutzer sie ausdrücklich anfordern muss, oder die Information sollte dem Zahlungsdienstnutzer unter Berücksichtigung seine[s] etwaigen Ersuchens um nähere Informationen zugänglich gemacht werden. In letzterem Fall sollte der Zahlungsdienstnutzer selbst aktiv werden, um sich die Informationen zu verschaffen, indem er sie beispielsweise ausdrücklich vom Zahlungsdienstleister anfordert, sich in die Mailbox des Bankkontos einloggt oder eine Bankkarte in den Drucker für Kontoauszüge einführt. …

…

(46) Ein reibungslos und zügig funktionierendes Zahlungssystem setzt voraus, dass der Nutzer sich auf die ordnungsgemäße und fristgerechte Ausführung seiner Zahlung durch den Zahlungsdienstleister verlassen kann. In der Regel ist der Zahlungsdienstleister in der Lage, die mit einem Zahlungsvorgang verbundenen Risiken einzuschätzen. Er ist es, der das Zahlungssystem vorgibt, Vorkehrungen trifft, um fehlgeleitete oder falsch zugewiesene Geldbeträge zurückzurufen, und in den meisten Fällen darüber entscheidet, welche zwischengeschalteten Stellen an der Ausführung eines Zahlungsvorgangs beteiligt werden. …“

4 In Art. 4 („Begriffsbestimmungen“) der Richtlinie 2007/64 heißt es:

„Für die Zwecke dieser Richtlinie bezeichnet der Begriff

…

12. ‚Rahmenvertrag‘ einen Zahlungsdienstvertrag, der die zukünftige Ausführung einzelner und aufeinander folgender Zahlungsvorgänge regelt und die Verpflichtung zur Einrichtung eines Zahlungskontos und die entsprechenden Bedingungen enthalten kann;

…

25. ‚dauerhafter Datenträger‘ jedes Medium, das es dem Zahlungsdienstnutzer gestattet, an ihn persönlich gerichtete Informationen derart zu speichern, dass er sie in der Folge für eine für die Zwecke der Informationen angemessene Dauer einsehen kann, und das die unveränderte Wiedergabe gespeicherter Informationen ermöglicht;

…“

5 Titel III („Transparenz der Vertragsbedingungen und Informationspflichten für Zahlungsdienste“) der Richtlinie enthält das Kapitel 1 („Allgemeine Vorschriften“). Zu den Bestimmungen dieses Kapitels gehören u. a. die Art. 30 und 31.

6 Art. 30 („Anwendungsbereich“) der Richtlinie bestimmt:

„(1) Dieser Titel gilt für Einzelzahlungen sowie für Rahmenverträge und die von ihnen erfassten Zahlungsvorgänge. Die Parteien können vereinbaren, dass dieser Titel insgesamt oder teilweise keine Anwendung findet, wenn es sich beim Zahlungsdienstnutzer nicht um einen Verbraucher handelt.

(2) Die Mitgliedstaaten können vorsehen, dass die Bestimmungen dieses Titels auf Kleinstunternehmen in gleicher Weise angewandt werden wie auf Verbraucher.

…“

7 Art. 31 („Sonstige Bestimmungen des Gemeinschaftsrechts“) der Richtlinie sieht vor:

„Dieser Titel lässt Bestimmungen des Gemeinschaftsrechts, die zusätzliche Anforderungen in Bezug auf die vorvertragliche Unterrichtung enthalten, unberührt.

In den Fällen jedoch, in denen auch die Richtlinie [2002/65 in der durch die Richtlinie 2005/29 geänderten Fassung] Anwendung findet, werden die Informationsbestimmungen des Artikels 3 Absatz 1 jener Richtlinie mit Ausnahme von Nummer 2 Buchstaben c bis g, Nummer 3 Buchstaben a, d und e sowie Nummer 4 Buchstabe b durch die Artikel 36, 37, 41 und 42 der vorliegenden Richtlinie ersetzt.“

8 Kapitel 2 („Einzelzahlungen“) des Titels III der Richtlinie 2007/64 enthält u. a. die Art. 35 bis 37.

9 Art. 35 („Anwendungsbereich“) der Richtlinie bestimmt:

„(1) Dieses Kapitel gilt für Einzelzahlungen, die nicht Gegenstand eines Rahmenvertrags sind.

(2) Wird ein Zahlungsauftrag für eine Einzelzahlung über ein rahmenvertraglich geregeltes Zahlungsinstrument übermittelt, so ist der Zahlungsdienstleister nicht verpflichtet, Informationen, die der Zahlungsdienstnutzer bereits aufgrund eines Rahmenvertrags mit einem anderen Zahlungsdienstleister erhalten hat oder erhalten wird, mitzuteilen oder zugänglich zu machen.“

10 Art. 36 („Allgemeine vorvertragliche Unterrichtung“) der Richtlinie sieht vor:

„(1) Die Mitgliedstaaten schreiben vor, dass der Zahlungsdienstleister dem Zahlungsdienstnutzer die Informationen und Vertragsbedingungen gemäß Artikel 37 in leicht zugänglicher Form zugänglich macht, bevor der Zahlungsdienstnutzer durch einen Vertrag oder ein Angebot über die Ausführung einer Einzelzahlung gebunden ist. Auf Verlangen des Zahlungsdienstnutzers stellt ihm der Zahlungsdienstleister die Informationen und Vertragsbedingungen in Papierform oder auf einem anderen dauerhaften Datenträger zur Verfügung. Die Informationen und Vertragsbedingungen sind in einer Amtssprache des Mitgliedstaats, in dem der Zahlungsdienst angeboten wird, oder in einer anderen zwischen den Parteien vereinbarten Sprache klar und verständlich abzufassen.

…

(3) Die Pflichten gemäß Absatz 1 können auch erfüllt werden, indem eine Kopie des Entwurfs für einen Vertrag über die Ausführung einer Einzelzahlung bzw. des Entwurfs für einen Zahlungsauftrag, die bzw. der die nach Artikel 37 erforderlichen Informationen und Vertragsbedingungen enthält, bereitgestellt wird.“

11 In Abs. 1 von Art. 37 („Informationen und Vertragsbedingungen“) der Richtlinie werden die Informationen und Vertragsbedingungen aufgezählt, die dem Zahlungsdienstnutzer mitgeteilt oder zugänglich gemacht werden müssen.

12 Kapitel 3 („Rahmenverträge“) von Titel III der Richtlinie 2007/64 enthält u. a. die Art. 40 bis 43.

13 Art. 40 („Anwendungsbereich“) der Richtlinie lautet:

„Dieses Kapitel gilt für Zahlungsvorgänge, die Gegenstand eines Rahmenvertrags sind.“

14 Art. 41 („Allgemeine vorvertragliche Unterrichtung“) der Richtlinie bestimmt:

„(1) Die Mitgliedstaaten schreiben vor, dass der Zahlungsdienstleister dem Zahlungsdienstnutzer rechtzeitig die Informationen und Vertragsbedingungen gemäß Artikel 42 in Papierform oder auf einem anderen dauerhaften Datenträger mitteilt, bevor der Zahlungsdienstnutzer durch einen Rahmenvertrag oder ein Vertragsangebot gebunden ist. Die Informationen und Vertragsbedingungen sind in einer Amtssprache des Mitgliedstaats, in dem der Zahlungsdienst angeboten wird, oder in einer anderen zwischen den Parteien vereinbarten Sprache klar und verständlich abzufassen.

(2) Wurde der Rahmenvertrag auf Verlangen des Zahlungsdienstnutzers mittels eines Fernkommunikationsmittels geschlossen, das es dem Zahlungsdienstleister nicht erlaubt, seinen Verpflichtungen aus Absatz 1 nachzukommen, so erfüllt der Zahlungsdienstleister diese Pflichten unverzüglich nach Abschluss des Rahmenvertrags.

(3) Die Pflichten gemäß Absatz 1 können auch erfüllt werden, indem eine Kopie des Rahmenvertragsentwurfs, der die nach Artikel 42 erforderlichen Informationen und Vertragsbedingungen enthält, bereitgestellt wird.“

15 In Art. 42 („Informationen und Vertragsbedingungen“) der Richtlinie werden die Informationen und Vertragsbedingungen aufgezählt, die dem Zahlungsdienstnutzer mitgeteilt werden müssen.

16 Art. 43 („Zugänglichkeit der Informationen und der Vertragsbedingungen des Rahmenvertrags“) der Richtlinie 2007/64 lautet:

„Der Zahlungsdienstnutzer kann jederzeit während der Vertragslaufzeit die Vorlage der Vertragsbedingungen des Rahmenvertrags sowie der in Artikel 42 genannten Informationen und Vertragsbedingungen in Papierform oder auf einem anderen dauerhaften Datenträger verlangen.“

17 Art. 44 („Änderungen der Vertragsbedingungen“) der Richtlinie bestimmt:

„(1) Der Zahlungsdienstleister schlägt Änderungen des Rahmenvertrags sowie der in Artikel 42 genannten Informationen und Vertragsbedingungen in der in Artikel 41 Absatz 1 vorgesehenen Weise spätestens zwei Monate vor dem geplanten Zeitpunkt ihrer Anwendung vor.

Sofern dies gemäß Artikel 42 Nummer 6 Buchstabe a vereinbart wurde, muss der Zahlungsdienstleister den Zahlungsdienstnutzer davon in Kenntnis setzen, dass seine Zustimmung zu den Änderungen als erteilt gilt, wenn er dem Zahlungsdienstleister seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens der geänderten Bedingungen angezeigt hat. In diesem Fall weist der Zahlungsdienstleister auch darauf hin, dass der Zahlungsdienstnutzer das Recht hat, den Rahmenvertrag vor dem vorgeschlagenen Tag der Anwendung der Änderungen kostenlos fristlos zu kündigen.

(2) Änderungen der Zinssätze oder der Wechselkurse können unmittelbar und ohne vorherige Benachrichtigung angewandt werden, sofern dieses Recht im Rahmenvertrag vereinbart wurde und die Änderungen auf den nach Maßgabe des Artikels 42 … vereinbarten Referenzzinssätzen oder Referenzwechselkursen beruhen. Der Zahlungsdienstnutzer ist so rasch wie möglich in der in Artikel 41 Absatz 1 vorgesehenen Weise von jeder Änderung des Zinssatzes zu unterrichten, es sei denn, die Parteien haben eine Vereinbarung darüber getroffen, wie oft und wie die Informationen mitgeteilt oder zugänglich gemacht werden sollen. Änderungen der Zinssätze oder Wechselkurse, die für den Zahlungsdienstnutzer günstiger sind, können jedoch ohne Benachrichtigung angewandt werden.

…“

Österreichisches Recht

18 Durch das Bundesgesetz über die Erbringung von Zahlungsdiensten (Zahlungsdienstegesetz – ZaDiG) aus dem Jahr 2009 (BGBl. I Nr. 66/2009, im Folgenden: Zahlungsdienstegesetz) wird die Richtlinie 2007/64 in österreichisches Recht umgesetzt.

19 § 26 des Zahlungsdienstegesetzes bestimmt:

„(1) Der Zahlungsdienstleister hat dem Zahlungsdienstnutzer rechtzeitig, bevor der Zahlungsdienstnutzer durch einen Vertrag oder ein Vertragsangebot gebunden ist, die Informationen und Vertragsbedingungen

1. im Fall eines Rahmenvertrages gemäß § 28 in Papierform oder, sofern der Zahlungsdienstnutzer damit einverstanden ist, auf einem anderen dauerhaften Datenträger mitzuteilen …

…

(2) Die Informationen und Vertragsbedingungen sind klar und verständlich abzufassen …“

20 In § 29 Abs. 1 des Zahlungsdienstegesetzes heißt es:

„(1) Der Zahlungsdienstleister hat

1. dem Zahlungsdienstnutzer Änderungen des Rahmenvertrages spätestens zwei Monate vor dem geplanten Zeitpunkt ihrer Anwendung in der in § 26 Abs. 1 Z 1 und Abs. 2 vorgesehenen Weise vorzuschlagen …

…“

21 Durch das Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz – ECG), aus dem Jahr 2001 (BGBl. I Nr. 152/2001, im Folgenden: E-Commerce-Gesetz) wird die Richtlinie 2000/31 in österreichisches Recht umgesetzt.

22 § 11 des E-Commerce-Gesetzes lautet:

„Ein Diensteanbieter hat die Vertragsbestimmungen und die allgemeinen Geschäftsbedingungen dem Nutzer so zur Verfügung zu stellen, dass er sie speichern und wiedergeben kann. Diese Verpflichtung kann nicht zum Nachteil des Nutzers abbedungen werden.“

23 § 12 des E-Commerce-Gesetzes sieht vor:

„Elektronische Vertragserklärungen, andere rechtlich erhebliche elektronische Erklärungen und elektronische Empfangsbestätigungen gelten als zugegangen, wenn sie die Partei, für die sie bestimmt sind, unter gewöhnlichen Umständen abrufen kann. Diese Regelung kann nicht zum Nachteil von Verbrauchern abbedungen werden.“

Ausgangsverfahren und Vorlagefragen

24 Der VKI ist nach den österreichischen Rechtsvorschriften zum Schutz von Verbraucherinteressen klagebefugt.

25 Die BAWAG ist eine in ganz Österreich tätige Bank. Sie verwendet im geschäftlichen Verkehr mit Verbrauchern allgemeine Bedingungen für die Nutzung ihrer E-Banking-Website durch die Verbraucher.

26 Die allgemeinen Nutzungsbedingungen der E-Banking-Website enthalten folgende Klausel: „Mitteilungen und Erklärungen (insbesondere Kontonachrichten, Kontoauszüge, Kreditkartenabrechnungen, Änderungsmitteilungen etc.), die die Bank dem Kunden zu übermitteln oder zugänglich zu machen hat, erhält der Kunde, der E-Banking vereinbart hat, per Post oder durch Abrufbarkeit oder Übermittlung elektronisch im Wege des [BAWAG-]E-Bankings."

27 Der Zugang zu dieser Website wird aufgrund eines Vertrags gewährt, der neben einem Vertrag über die Eröffnung und das Führen eines Bankkontos abgeschlossen wird und damit Teil eines Rahmenvertrags ist.

28 Aus der Vorlageentscheidung geht hervor, dass Nachrichten, die an die auf der E-Banking-Website für die Verbraucher eingerichteten elektronischen Mailboxen geschickt werden, dort für einen dem Zweck der Information der Verbraucher angemessenen Zeitraum unverändert bestehen bleiben und nicht gelöscht werden, so dass sie auf elektronischem Weg konsultiert und unverändert reproduziert oder ausgedruckt werden können. Die Nachrichten können von den Verbrauchern verwaltet und gegebenenfalls gelöscht werden.

29 Der VKI erhob beim Handelsgericht Wien (Österreich) Klage gegen die BAWAG auf Unterlassung der Verwendung der oben genannten Klausel oder ihr entsprechender Klauseln in den allgemeinen Geschäftsbedingungen.

30 Diese Klauseln verstoßen nach Auffassung des VKI gegen die Vorschriften des Zahlungsdienstegesetzes.

31 Nachdem das Handelsgericht Wien der Klage des VKI mit Urteil vom 31. Oktober 2013 stattgegeben hatte, legte die BAWAG beim Oberlandesgericht Wien (Österreich) Berufung gegen dieses Urteil ein.

32 Mit Urteil vom 11. April 2014 änderte das Oberlandesgericht Wien das Urteil des Handelsgerichts Wien teilweise ab. Die BAWAG legte gegen diese Entscheidung des Oberlandesgerichts Wien Revision beim vorlegenden Gericht ein.

33 Da der Oberste Gerichtshof (Österreich) der Ansicht ist, dass die Entscheidung des bei ihm anhängigen Rechtsstreits von der Auslegung der Richtlinie 2007/64 abhängt, hat er beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Ist Art. 41 Abs. 1 in Verbindung mit Art. 36 Abs. 1 der Richtlinie 2007/64 dahin auszulegen, dass eine Information (in elektronischer Form), die von der Bank an die E-Mail-Box des Kunden im Rahmen des Onlinebanking (E-Banking) übermittelt wird, so dass der Kunde diese Information nach dem Einloggen auf der E-Banking-Website durch Anklicken abrufen kann, dem Kunden auf einem dauerhaften Datenträger mitgeteilt wird?

2. Wenn Frage 1 verneint wird:

   Ist Art. 41 Abs. 1 in Verbindung mit Art. 36 Abs. 1 der Richtlinie 2007/64 dahin auszulegen, dass in einem solchen Fall

   a) die Information von der Bank zwar auf einem dauerhaften Datenträger zur Verfügung gestellt, aber nicht dem Kunden mitgeteilt, sondern diesem nur zugänglich gemacht wird, oder

   b) es sich überhaupt nur um ein Zugänglichmachen der Information ohne Verwendung eines dauerhaften Datenträgers handelt?

Zu den Vorlagefragen

34 Mit seinen Fragen, die zusammen zu prüfen sind, möchte das vorlegende Gericht wissen, ob Art. 41 Abs. 1 und Art. 44 Abs. 1 der Richtlinie 2007/64 in Verbindung mit deren Art. 4 Nr. 25 dahin auszulegen sind, dass Änderungen der Informationen und Vertragsbedingungen im Sinne des Art. 42 der Richtlinie sowie Änderungen des Rahmenvertrags, die der Zahlungsdienstleister dem Zahlungsdienstnutzer über eine Mailbox auf einer E-Banking-Website übermittelt, im Sinne dieser Bestimmungen auf einem dauerhaften Datenträger mitgeteilt werden, oder dahin,

dass sie dem Nutzer lediglich, wie in Art. 36 Abs. 1 Satz 1 der Richtlinie in Bezug auf die in ihrem Art. 37 angeführten Informationen und Vertragsbedingungen vorgesehen, zugänglich gemacht werden.

35 Einleitend ist darauf hinzuweisen, dass in Bezug auf einen Vertrag oder ein Vertragsangebot über die Ausführung einer Einzelzahlung, die nicht Gegenstand eines Rahmenvertrags im Sinne von Art. 4 Nr. 12 der Richtlinie 2007/64 ist, nach Art. 36 Abs. 1 der Richtlinie eine Pflicht zur allgemeinen vorvertraglichen Unterrichtung des Zahlungsdienstnutzers besteht, während für Zahlungsvorgänge, die Gegenstand eines Rahmenvertrags sind, eine solche Pflicht in Art. 41 Abs. 1 der Richtlinie vorgesehen ist.

36 Der „Rahmenvertrag“ wird für die Zwecke der Richtlinie 2007/64 in deren Art. 4 Nr. 12 als ein Zahlungsdienstvertrag definiert, der die zukünftige Ausführung einzelner und aufeinanderfolgender Zahlungsvorgänge regelt und die Verpflichtung zur Einrichtung eines Zahlungskontos und die entsprechenden Bedingungen enthalten kann.

37 Nach Art. 41 Abs. 1 der Richtlinie schreiben die Mitgliedstaaten vor, dass der Zahlungsdienstleister dem Zahlungsdienstnutzer rechtzeitig die Informationen und Vertragsbedingungen gemäß Art. 42 der Richtlinie in Papierform oder auf einem anderen dauerhaften Datenträger mitteilt, bevor der Zahlungsdienstnutzer durch einen Rahmenvertrag oder ein Vertragsangebot gebunden ist.

38 Ferner geht aus Art. 44 Abs. 1 Unterabs. 1 der Richtlinie 2007/64 hervor, dass der Zahlungsdienstleister Änderungen des Rahmenvertrags sowie der in Art. 42 der Richtlinie genannten Informationen und Vertragsbedingungen in der in Art. 41 Abs. 1 der Richtlinie vorgesehenen Weise spätestens zwei Monate vor dem geplanten Zeitpunkt ihrer Anwendung vorschlägt.

39 Zur sachdienlichen Beantwortung der gestellten Fragen sind zwei in Art. 41 Abs. 1 der Richtlinie aufgestellte Erfordernisse zu prüfen, und zwar das Erfordernis, die betreffenden Informationen auf einem dauerhaften Datenträger festzuhalten, sowie das Erfordernis, diese Informationen dem Zahlungsdienstnutzer mitzuteilen.

40 Erstens ist zum Begriff „dauerhafter Datenträger“ in Art. 41 Abs. 1 der Richtlinie 2007/64 festzustellen, dass er in Art. 4 Nr. 25 der Richtlinie als jedes Medium definiert wird, das es dem Zahlungsdienstnutzer gestattet, an ihn persönlich gerichtete Informationen derart zu speichern, dass er sie in der Folge für eine für die Zwecke der Informationen angemessene Dauer einsehen kann, und das die unveränderte Wiedergabe gespeicherter Informationen ermöglicht.

41 Im 24. Erwägungsgrund der Richtlinie wird ausgeführt, dass die Vorabinformationspflichten bei Rahmenverträgen recht umfassend sein und die Informationen immer auf Papier oder einem anderen dauerhaften Datenträger mitgeteilt werden sollten, beispielsweise auf Ausdrucken von Kontoauszugsdruckern, Disketten, CD-ROMs, DVDs und PC-Festplattenlaufwerken, auf denen elektronische Post gespeichert werden kann, sowie Websites, sofern sie für einen dem Zweck der Information angemessenen Zeitraum konsultiert und unverändert reproduziert werden können.

42 Der Gerichtshof hat, unter Bezugnahme insbesondere auf die Definition des „dauerhaften Datenträgers“ in Art. 3 Buchst. m der Richtlinie 2008/48/EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87/102/EWG des Rates (ABl. 2008, L 133, S. 66, berichtigt im ABl. 2009, L 207, S. 14, im ABl. 2010, L 199, S. 40, und im ABl. 2011, L 234, S. 46), entschieden, dass ein solcher Datenträger dem Verbraucher entsprechend der Papierform den Besitz der erforderlichen Informationen garantieren muss, damit er gegebenenfalls seine Rechte geltend machen kann. Maßgebend sind insoweit die Möglichkeit für den Verbraucher, an ihn persönlich gerichtete Informationen zu speichern, die Gewähr dafür, dass ihr Inhalt und ihre Zugänglichkeit während einer angemessenen Dauer nicht verändert werden, und die Möglichkeit ihrer unveränderten Wiedergabe (vgl. in diesem Sinne Urteile vom 5. Juli 2012, Content Services, C-49/11, EU:C:2012:419, Rn. 42 bis 44, und vom 9. November 2016, Home Credit Slovakia, C-42/15, EU:C:2016:842, Rn. 35).

43 Wie der Generalanwalt in den Nrn. 51 bis 63 seiner Schlussanträge ausgeführt und der Gerichtshof der Europäischen Freihandelsassoziation (EFTA) in seinem Urteil vom 27. Januar 2010, Inconsult Anstalt/Finanzmarktaufsicht (E-04/09, EFTA Court Report 2009-2010, S. 86, Rn. 63 bis 66), entschieden hat, sind bestimmte Websites als „dauerhafte Datenträger“ im Sinne von Art. 4 Nr. 25 der Richtlinie 2007/64 anzusehen.

44 Im Hinblick insbesondere auf die Rn. 40 bis 42 des vorliegenden Urteils ist dies der Fall, wenn eine Website es dem Zahlungsdienstnutzer gestattet, an ihn persönlich gerichtete Informationen derart zu speichern, dass er sie in der Folge für eine für die Zwecke der Informationen angemessene Dauer einsehen kann, und die unveränderte Wiedergabe gespeicherter Informationen ermöglicht. Außerdem muss, damit eine Website als „dauerhafter Datenträger“ im Sinne von Art. 4 Nr. 25 der Richtlinie 2007/64 angesehen werden kann, jede Möglichkeit der einseitigen Änderung ihres Inhalts durch den Zahlungsdienstleister oder durch einen mit der Verwaltung der Website betrauten Administrator ausgeschlossen sein.

45 Diese Auslegung steht im Einklang mit den in den Erwägungsgründen 21 und 22 der Richtlinie 2007/64 genannten Zielen, nämlich dem Schutz der Zahlungsdienstnutzer und insbesondere der Verbraucher.

46 Es ist Sache des vorlegenden Gerichts, zu prüfen, ob im Ausgangsverfahren die in Rn. 44 des vorliegenden Urteils genannten Voraussetzungen erfüllt sind.

47 Zweitens ist in Bezug auf die Frage, wann Änderungen der Informationen und Vertragsbedingungen im Sinne des Art. 42 der Richtlinie 2007/64 sowie Änderungen des Rahmenvertrags als im Einklang mit Art. 41 Abs. 1 der Richtlinie auf einem dauerhaften Datenträger „mitgeteilt“ angesehen werden können, darauf hinzuweisen, dass in der Richtlinie, wie in ihrem 27. Erwägungsgrund ausgeführt wird, zwischen zwei Arten der Informationsübermittlung durch den Zahlungsdienstleister unterschieden werden sollte. Entweder sollten die betreffenden Informationen mitgeteilt, d. h. vom Zahlungsdienstleister von sich aus übermittelt werden, ohne dass der Zahlungsdienstnutzer sie ausdrücklich anfordern muss, oder sie sollten dem Zahlungsdienstnutzer unter Berücksichtigung seines etwaigen Ersuchens um nähere Informationen zugänglich gemacht werden. Im letztgenannten Fall sollte der Zahlungsdienstnutzer selbst aktiv werden, um sich die Informationen zu verschaffen, indem er sie beispielsweise ausdrücklich vom Zahlungsdienstleister anfordert, sich in die Mailbox des Bankkontos einloggt oder seine Bankkarte in den Kontoauszugsdrucker einführt.

48 Folglich muss der Zahlungsdienstleister, wenn die Richtlinie 2007/64 vorsieht, dass er dem Zahlungsdienstnutzer die betreffenden Informationen mitteilt, diese Informationen von sich aus übermitteln.

49 Zugleich kann, da der Schutz der Zahlungsdienstnutzer und insbesondere der Verbraucher – wie in Rn. 45 des vorliegenden Urteils dargelegt – zu den Zielen der Richtlinie 2007/64 gehört, von den Zahlungsdienstnutzern, wie der Generalanwalt in den Nrn. 75 bis 77 seiner Schlussanträge ausgeführt hat, vernünftigerweise nicht erwartet werden, dass sie regelmäßig alle elektronischen Kommunikationssysteme abfragen, bei denen sie registriert sind; dies gilt umso mehr, als nach Art. 44 Abs. 1 Unterabs. 2 der Richtlinie unter den dort genannten Umständen die Zustimmung der Zahlungsdienstnutzer zu den vom Zahlungsdienstleister vorgeschlagenen Änderungen der Bedingungen des Rahmenvertrags als erteilt gilt.

50 In Anbetracht dessen können die betreffenden Informationen, die der Zahlungsdienstleister dem Zahlungsdienstnutzer über eine E-Banking-Website übermittelt, als im Sinne von Art. 41 Abs. 1 der Richtlinie 2007/64 mitgeteilt angesehen werden, wenn mit einer solchen Übermittlung einhergeht, dass der

Zahlungsdienstleister von sich aus tätig wird, um den Zahlungsdienstnutzer davon in Kenntnis zu setzen, dass die Informationen auf der Website vorhanden und verfügbar sind.

51 Wie der Generalanwalt in Nr. 79 seiner Schlussanträge im Wesentlichen ausgeführt hat, kann dies u. a. durch die Übersendung eines Schreibens oder einer E-Mail an die vom Zahlungsdienstnutzer üblicherweise für die Kommunikation mit Dritten verwendete Adresse geschehen, deren Nutzung die Parteien in einem zwischen dem Zahlungsdienstleister und dem Nutzer geschlossenen Rahmenvertrag vereinbart haben. Dabei darf es sich jedoch nicht um die Adresse handeln, die dem Nutzer auf der vom Zahlungsdienstleister oder einem von ihm beauftragten Administrator verwalteten E-Banking-Website zugeteilt wurde, da diese Website, auch wenn sie eine elektronische Mailbox enthält, vom Nutzer nicht üblicherweise für seine Kommunikation mit anderen Personen als dem Zahlungsdienstleister genutzt wird.

52 Es ist Sache des vorlegenden Gerichts, zu prüfen, ob unter Berücksichtigung aller Umstände des Ausgangsverfahrens davon ausgegangen werden kann, dass der Zahlungsdienstleister dem Zahlungsdienstnutzer Änderungen der Informationen und Vertragsbedingungen im Sinne des Art. 42 der Richtlinie 2007/64 sowie Änderungen des entsprechenden Rahmenvertrags von sich aus übermittelt hat.

53 Nach alledem sind die Vorlagefragen wie folgt zu beantworten:

– Art. 41 Abs. 1 und Art. 44 Abs. 1 der Richtlinie 2007/64 sind in Verbindung mit Art. 4 Nr. 25 der Richtlinie dahin auszulegen, dass Änderungen der Informationen und Vertragsbedingungen im Sinne des Art. 42 der Richtlinie sowie Änderungen des Rahmenvertrags, die der Zahlungsdienstleister dem Zahlungsdienstnutzer über eine Mailbox auf einer E-Banking-Website übermittelt, nur dann im Sinne dieser Bestimmungen auf einem dauerhaften Datenträger mitgeteilt werden, wenn zwei Voraussetzungen erfüllt sind:

  – Die Website gestattet es dem Zahlungsdienstnutzer, an ihn persönlich gerichtete Informationen derart zu speichern, dass er sie in der Folge für eine angemessene Dauer einsehen kann und ihm die unveränderte Wiedergabe gespeicherter Informationen möglich ist, ohne dass ihr Inhalt durch den Zahlungsdienstleister oder einen Administrator einseitig geändert werden kann, und,

  – sofern der Zahlungsdienstnutzer die Website besuchen muss, um von den betreffenden Informationen Kenntnis zu erlangen, geht mit ihrer Übermittlung einher, dass der Zahlungsdienstleister von sich aus tätig

wird, um den Zahlungsdienstnutzer davon in Kenntnis zu setzen, dass die Informationen auf der Website vorhanden und verfügbar sind.

– Falls der Zahlungsdienstnutzer eine solche Website besuchen muss, um von den betreffenden Informationen Kenntnis zu erlangen, werden sie ihm lediglich im Sinne von Art. 36 Abs. 1 Satz 1 der Richtlinie 2007/64 zugänglich gemacht, wenn mit ihrer Übermittlung nicht einhergeht, dass der Zahlungsdienstleister in der genannten Weise von sich aus tätig wird.

Kosten

54 Für die Parteien des Ausgangsverfahrens ist das Verfahren ein Zwischenstreit in dem beim vorlegenden Gericht anhängigen Rechtsstreit; die Kostenentscheidung ist daher Sache dieses Gerichts. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Aus diesen Gründen hat der Gerichtshof (Dritte Kammer) für Recht erkannt:

Art. 41 Abs. 1 und Art. 44 Abs. 1 der Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG in der durch die Richtlinie 2009/111/EG des Europäischen Parlaments und des Rates vom 16. September 2009 geänderten Fassung sind in Verbindung mit Art. 4 Nr. 25 der Richtlinie dahin auszulegen, dass Änderungen der Informationen und Vertragsbedingungen im Sinne des Art. 42 der Richtlinie sowie Änderungen des Rahmenvertrags, die der Zahlungsdienstleister dem Zahlungsdienstnutzer über eine Mailbox auf einer E-Banking-Website übermittelt, nur dann im Sinne dieser Bestimmungen auf einem dauerhaften Datenträger mitgeteilt werden, wenn zwei Voraussetzungen erfüllt sind:

– **Die Website gestattet es dem Zahlungsdienstnutzer, an ihn persönlich gerichtete Informationen derart zu speichern, dass er sie in der Folge für eine angemessene Dauer einsehen kann und ihm die unveränderte Wiedergabe gespeicherter Informationen möglich ist, ohne dass ihr Inhalt durch den Zahlungsdienstleister oder einen Administrator einseitig geändert werden kann, und,**

– **sofern der Zahlungsdienstnutzer die Website besuchen muss, um von den betreffenden Informationen Kenntnis zu erlangen, geht mit ihrer Übermittlung einher, dass der Zahlungsdienstleister von sich aus tätig**

wird, um den Zahlungsdienstnutzer davon in Kenntnis zu setzen, dass die Informationen auf der Website vorhanden und verfügbar sind.

Falls der Zahlungsdienstnutzer eine solche Website besuchen muss, um von den betreffenden Informationen Kenntnis zu erlangen, werden sie ihm lediglich im Sinne von Art. 36 Abs. 1 Satz 1 der Richtlinie 2007/64 in der durch die Richtlinie 2009/111 geänderten Fassung zugänglich gemacht, wenn mit ihrer Übermittlung nicht einhergeht, dass der Zahlungsdienstleister in der genannten Weise von sich aus tätig wird.

Bay Larsen Vilaras Malenovský

Safjan Šváby

Verkündet in öffentlicher Sitzung in Luxemburg am 25. Januar 2017.

Der Kanzler Der Präsident der Dritten Kammer

A. Calot Escobar L. Bay Larsen

SCHLUSSANTRÄGE DES GENERALANWALTS
MICHAL BOBEK
vom 15. September 2016(1)

Rechtssache C-375/15

BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG
gegen
Verein für Konsumenteninformation

(Vorabentscheidungsersuchen des Obersten Gerichtshofs [Österreich])

„Rechtsangleichung – Richtlinie 2007/64/EG – Zahlungsdienste im Binnenmarkt – Rahmenverträge – Allgemeine vorvertragliche Unterrichtung – Informationen über Änderungen der Rahmenvertragsbedingungen – Erfordernis der Mitteilung von Informationen auf einem dauerhaften Datenträger – ‚Mitteilen' oder ‚Zugänglichmachen' von Informationen – Übermittlung von Informationen über die Mailbox auf einer E-Banking-Website im Internet"

I – Einführung

1. Die Richtlinie 2007/64/EG über Zahlungsdienste im Binnenmarkt(2) schreibt vor, dass der Zahlungsdienstleister dem Zahlungsdienstnutzer Änderungen des Rahmenvertrags in Papierform oder auf einem anderen *dauerhaften Datenträger mitteilen muss.*

2. Bei der BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG (im Folgenden: BAWAG) handelt es sich um eine in Österreich tätige Bank. Sie bietet ihren Kunden Verträge für das E-Banking im Internet an. In ihren Allgemeinen Geschäftsbedingungen für solche E-Banking-Verträge verwendet die BAWAG eine Vertragsklausel, wonach dem Kunden „Änderungsmitteilungen" über die interne Mailbox ihres E-Banking-Systems im Internet übermittelt werden. Nach Ansicht des Vereins für Konsumenteninformation, eines Verbraucherverbands, steht eine solche Klausel nicht im Einklang mit der in der Richtlinie 2007/64 festgelegten Pflicht, Informationen auf einem „dauerhaften Datenträger" zur Verfügung zu stellen.

3. In der vorliegenden Rechtssache soll der Gerichtshof klarstellen, ob Informationen, die über eine E-Banking-Mailbox erteilt werden, im Sinne der Richtlinie 2007/64 durch einen „dauerhaften Datenträger" „mitgeteilt" (und nicht bloß „zugänglich gemacht") werden. Allgemeiner wird der Gerichtshof erneut(3) ersucht, ein Gleichgewicht herzustellen zwischen einerseits den Mindestanforderungen an die Unterrichtung und den Schutz der Verbraucher und andererseits den technischen Entwicklungen aufgrund der (zweifellos auch durch Verbraucherpräferenzen verursachten) wachsenden Neigung der Wirtschaftsbeteiligten, Online- und papierlose Lösungen für

die Kommunikation mit ihren Kunden einzurichten.

II – Rechtlicher Rahmen

A – *Unionsrecht*

4. Die Richtlinie 2007/64 enthält Regeln in Bezug auf die Transparenz der Vertragsbedingungen und die Informationspflichten für Zahlungsdienste(4). Diese Regeln legen die Informationspflichten der Zahlungsdienstleister gegenüber Zahlungsdienstnutzern fest, damit diese, wie es im 21. Erwägungsgrund heißt, „ein gleich hohes Maß an verständlichen Informationen … erhalten und so die Konditionen der verschiedenen Anbieter in der EU vergleichen und ihre Wahl in voller Kenntnis der Sachlage treffen können".

5. Gemäß dem 23. Erwägungsgrund sollten die Informationen den Bedürfnissen der Nutzer angemessen sein und in standardisierter Form übermittelt werden. Allerdings sollten, so heißt es dort weiter, für Einzelzahlungen andere Informationspflichten gelten als für Rahmenverträge (die mehrere Zahlungsvorgänge betreffen). Im 24. Erwägungsgrund werden die Vorabinformationspflichten bei Rahmenverträgen klargestellt; außerdem wird dort anhand von Beispielen verdeutlicht, was unter einem „dauerhaften Datenträger" zu verstehen ist. Im 25. Erwägungsgrund werden die Informationsanforderungen bei Einzelzahlungen im Gegensatz zu Rahmenverträgen dahin gehend präzisiert, dass die Informationen nicht in jedem Fall auf Papier oder einem anderen dauerhaften Datenträger gegeben werden müssen, es sei denn, dies wird vom Verbraucher verlangt.

6. Der 27. Erwägungsgrund der Richtlinie 2007/64 unterscheidet zwischen zwei Wegen der Erteilung von Informationen durch den Zahlungsdienstleister: „Entweder sollte die Information mitgeteilt, d. h. vom Zahlungsdienstleister zu dem in dieser Richtlinie geforderten Zeitpunkt von sich aus übermittelt werden, ohne dass der Zahlungsdienstnutzer sie ausdrücklich anfordern muss, oder die Information sollte dem Zahlungsdienstnutzer unter Berücksichtigung seine[s] etwaigen Ersuchens um nähere Informationen zugänglich gemacht werden." Des Weiteren werden in diesem Erwägungsgrund anhand von Beispielen weitere Fälle dargestellt, in denen Informationen „zugänglich gemacht" werden und der Verbraucher selbst aktiv werden muss, um Zugang zu ihnen zu erlangen.

7. Art. 4 der Richtlinie 2007/64 enthält Begriffsbestimmungen. Nach Art. 4 Nr. 12 bezeichnet der Begriff „‚Rahmenvertrag' einen Zahlungsdienstvertrag, der die zukünftige Ausführung einzelner und aufeinanderfolgender Zahlungsvorgänge regelt und die Verpflichtung zur Einrichtung eines Zahlungskontos und die entsprechenden Bedingungen enthalten kann". Gemäß Art. 4 Nr. 25 bezeichnet der Begriff „‚dauerhafter Datenträger' jedes Medium, das es dem Zahlungsdienstnutzer gestattet, an ihn persönlich gerichtete Informationen derart zu speichern, dass er sie in der Folge für eine für die Zwecke der Informationen angemessene Dauer einsehen kann, und das die unveränderte Wiedergabe gespeicherter Informationen ermöglicht".

8. Titel III („Transparenz der Vertragsbedingungen und Informationspflichten für Zahlungsdienste") der Richtlinie 2007/64 enthält in seinem Kapitel 2 die Bestimmungen für „Einzelzahlungen" (Art. 35 bis 39). In Kapitel 3 finden sich die Bestimmungen, die auf „Rahmenverträge" anwendbar sind (Art. 40 bis 48).

9. Der für „Rahmenverträge" geltende Art. 41 („Allgemeine vorvertragliche Unterrichtung") der Richtlinie 2007/64 lautet:

„(1) Die Mitgliedstaaten schreiben vor, dass der Zahlungsdienstleister dem Zahlungsdienstnutzer rechtzeitig die Informationen und Vertragsbedingungen gemäß Artikel 42 in Papierform oder auf

einem anderen dauerhaften Datenträger mitteilt, bevor der Zahlungsdienstnutzer durch einen Rahmenvertrag oder ein Vertragsangebot gebunden ist. Die Informationen und Vertragsbedingungen sind in einer Amtssprache des Mitgliedstaats, in dem der Zahlungsdienst angeboten wird, oder in einer anderen zwischen den Parteien vereinbarten Sprache klar und verständlich abzufassen.

…“

10. Art. 44 der Richtlinie 2007/64 betrifft Änderungen der Rahmenvertragsbedingungen. Art. 44 Abs. 1 Unterabs. 1 lautet: „Der Zahlungsdienstleister schlägt Änderungen des Rahmenvertrags sowie der in Artikel 42 genannten Informationen und Vertragsbedingungen in der in Artikel 41 Absatz 1 vorgesehenen Weise spätestens zwei Monate vor dem geplanten Zeitpunkt ihrer Anwendung vor.“ Art. 44 Abs. 1 Unterabs. 2 bestimmt: „Sofern dies gemäß Artikel 42 Nummer 6 Buchstabe a vereinbart wurde, muss der Zahlungsdienstleister den Zahlungsdienstnutzer davon in Kenntnis setzen, dass seine Zustimmung zu den Änderungen als erteilt gilt, wenn er dem Zahlungsdienstleister seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens der geänderten Bedingungen angezeigt hat. In diesem Fall weist der Zahlungsdienstleister auch darauf hin, dass der Zahlungsdienstnutzer das Recht hat, den Rahmenvertrag vor dem vorgeschlagenen Tag der Anwendung der Änderungen kostenlos fristlos zu kündigen.“

B – *Österreichisches Recht*

11. Die Richtlinie 2007/64 wurde durch das Bundesgesetz über die Erbringung von Zahlungsdiensten (Zahlungsdienstegesetz, BGBl I Nr. 66/2009) in österreichisches Recht umgesetzt. § 26 dieses Gesetzes lautet:

„(1) Der Zahlungsdienstleister hat dem Zahlungsdienstnutzer rechtzeitig, bevor der Zahlungsdienstnutzer durch einen Vertrag oder ein Vertragsangebot gebunden ist, die Informationen und Vertragsbedingungen

1. im Fall eines Rahmenvertrages gemäß § 28 in Papierform oder, sofern der Zahlungsdienstnutzer damit einverstanden ist, auf einem anderen dauerhaften Datenträger mitzuteilen …

…“

12. § 29 des Zahlungsdienstegesetzes betrifft Änderungen des Rahmenvertrags und hat folgenden Wortlaut:

„(1) Der Zahlungsdienstleister hat

1. dem Zahlungsdienstnutzer Änderungen des Rahmenvertrages spätestens zwei Monate vor dem geplanten Zeitpunkt ihrer Anwendung in der in § 26 Abs. 1 Z 1 und Abs. 2 vorgesehenen Weise vorzuschlagen und,

2. sofern eine Vereinbarung gemäß § 28 Abs. 1 Z 6 lit. a getroffen wurde, darauf hinzuweisen,

a) dass die Zustimmung des Zahlungsdienstnutzers zu den Änderungen als erteilt gilt, wenn er dem Zahlungsdienstleister seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt der Anwendung der Änderungen angezeigt hat, und

b) dass der Zahlungsdienstnutzer das Recht hat, den Rahmenvertrag vor dem Inkrafttreten der Änderungen kostenlos fristlos zu kündigen.“

III – Ausgangsrechtsstreit, Vorlagefragen und Verfahren vor dem Gerichtshof

13. Die BAWAG verwendet für Kundenverträge über Bankdienstleistungen vorformulierte Verträge mit Allgemeinen Geschäftsbedingungen. Die im Ausgangsverfahren streitige Vertragsklausel betrifft insbesondere die Teilnahme der Kunden am E-Banking-System der BAWAG im Internet. Sie lautet wie folgt:

„Mitteilungen und Erklärungen (insbesondere Kontonachrichten, Kontoauszüge, Kreditkartenabrechnungen, Änderungsmitteilungen etc.), die die Bank dem Kunden zu übermitteln oder zugänglich zu machen hat, erhält der Kunde, der E-Banking vereinbart hat, per Post oder durch Abrufbarkeit oder Übermittlung elektronisch im Wege des BAWAG P.S.K. E-Bankings."

14. Die Kommunikation über das in Rede stehende E-Banking-System geht nach Darstellung des vorlegenden Gerichts wie folgt vonstatten: Im Rahmen ihres E-Banking-Systems richtet die BAWAG für jeden Kunden eine Mailbox ein. Auf diese können die Kunden durch Einloggen mit ihrem persönlichen Passwort auf der E-Banking-Website zugreifen. Elektronische Nachrichten werden dann von der Bank an die Mailbox übermittelt. Ergänzende Mitteilungen, wie etwa Nachrichten an die private E-Mail-Adresse des Kunden, mit denen dieser darüber informiert wird, dass eine Nachricht an die E-Banking-Mailbox versandt worden ist, erfolgen nicht.

15. Im Ausgangsverfahren erhob der Verein für Konsumenteninformation Klage mit dem Antrag, der BAWAG die Aufnahme der streitigen Vertragsklausel in die Verträge, die sie mit ihren Kunden schließt, und die Anwendung der Klausel auf diese Kunden zu untersagen. Die Klage hatte in der ersten Instanz Erfolg; auch das Berufungsgericht entschied im Sinne des Klägers. Die Vertragsklausel stelle einen Verstoß gegen die zwingenden Vorschriften des § 26 Abs. 1 Z 1 in Verbindung mit § 29 Abs. 1 Z 1 des Zahlungsdienstegesetzes dar. Die BAWAG legte Revision beim Obersten Gerichtshof (Österreich) ein. In diesem Kontext hat der Oberste Gerichtshof das Verfahren ausgesetzt und folgende Fragen zur Vorabentscheidung vorgelegt:

1. Ist Art. 41 Abs. 1 in Verbindung mit Art. 36 Abs. 1 der Richtlinie 2007/64 dahin auszulegen, dass eine Information (in elektronischer Form), die von der Bank an die E-Mail-Box des Kunden im Rahmen des Online-Banking (E-Banking) übermittelt wird, so dass der Kunde diese Information nach dem Einloggen auf der E-Banking-Website durch Anklicken abrufen kann, dem Kunden auf einem dauerhaften Datenträger mitgeteilt wird?

2. Wenn Frage 1 verneint wird:

   Ist Art. 41 Abs. 1 in Verbindung mit Art. 36 Abs. 1 der Richtlinie 2007/64 dahin auszulegen, dass in einem solchen Fall

   a) die Information von der Bank zwar auf einem dauerhaften Datenträger zur Verfügung gestellt, aber nicht dem Kunden mitgeteilt, sondern diesem nur zugänglich gemacht wird, oder

   b) es sich überhaupt nur um ein Zugänglichmachen der Information ohne Verwendung eines dauerhaften Datenträgers handelt?

16. Das Vorabentscheidungsersuchen ist am 15. Juli 2015 beim Gerichtshof eingegangen. Die BAWAG, der Verein für Konsumenteninformation, die italienische und die polnische Regierung sowie die Europäische Kommission haben schriftliche Erklärungen eingereicht. Am 30. Juni 2016 hat eine Sitzung stattgefunden, in der der Verein für Konsumenteninformation, die BAWAG und die Kommission mündlich verhandelt haben.

IV – Würdigung

A – *Vorbemerkungen*

17. Vor der inhaltlichen Würdigung der vom Obersten Gerichtshof (Österreich) gestellten Fragen bedürfen drei Punkte der Klarstellung.

1. Einschlägige Bestimmungen der Richtlinie 2007/64

18. Erstens ist, auch wenn das vorlegende Gericht in seinen Fragen auf Art. 41 Abs. 1 der Richtlinie 2007/64 „in Verbindung mit" deren Art. 36 Abs. 1 abstellt, lediglich die erstgenannte Bestimmung für die vorliegende Rechtssache unmittelbar relevant.

19. Den Angaben im Vorabentscheidungsersuchen lässt sich entnehmen, dass die hier in Rede stehende Vertragsklausel in einer E-Banking-Vereinbarung enthalten ist. Die E-Banking-Vereinbarung wird ergänzend zu einem Rahmenvertrag geschlossen. Somit betrifft die streitige Vertragsklausel die Mitteilung von Informationen nach Maßgabe eines Rahmenvertrags. Folglich ist Art. 36 Abs. 1 der Richtlinie 2007/64, der ausschließlich für Einzelzahlungen, d. h. nicht von einem Rahmenvertrag erfasste Zahlungen, gilt, auf den vorliegenden Fall nicht unmittelbar anwendbar.

20. Gleichwohl ist Art. 36 Abs. 1 für die systematische Auslegung der Richtlinie insgesamt von Bedeutung. Die Bestimmung regelt die Art und Weise, in der Informationen über Einzelzahlungen zugänglich zu machen sind; sie unterscheidet sich ausdrücklich von der Art und Weise, in der die Informationen bei Rahmenverträgen mitgeteilt werden müssen. Die Bezugnahme auf Art. 36 Abs. 1 in den Fragen des vorlegenden Gerichts ist daher als ein Ersuchen um Auslegung des Verhältnisses zwischen beiden Bestimmungen zu verstehen, da diese die Informationsanforderungen regelnden Vorschriften – Art. 36 und Art. 41 – nach der Systematik der Richtlinie miteinander verknüpft sind.

21. Zweitens liegt auf der Hand, dass die streitige Vertragsklausel – aus dem Blickwinkel der Richtlinie 2007/64 – auf eine Reihe recht unterschiedlicher Elemente Bezug nimmt, und zwar auf „Mitteilungen und Erklärungen (insbesondere Kontonachrichten, Kontoauszüge, Kreditkartenabrechnungen, Änderungsmitteilungen etc.) …". Wie jedoch in den beim Gerichtshof eingereichten schriftlichen und mündlichen Erklärungen bestätigt worden ist, geht es vorliegend allein um das zuletzt genannte Element, also um Änderungsmitteilungen; dabei handelt es sich um das einzige Element, das zu Änderungen von Rahmenverträgen führen kann.

22. Die für Änderungen von Rahmenverträgen maßgebende Bestimmung der Richtlinie 2007/64 ist Art. 44. Nach Art. 44 Abs. 1 schlägt „[d]er Zahlungsdienstleister … Änderungen des Rahmenvertrags … in der in Artikel 41 Absatz 1 vorgesehenen Weise … vor". Ich gelange daher zu dem Ergebnis, dass im vorliegenden Fall die Art. 41 Abs. 1 und 44 Abs. 1 der Richtlinie 2007/64 relevant sind.

2. Formulierung der gestellten Fragen

23. Nach der Formulierung des Vorlagebeschlusses im vorliegenden Fall ist davon auszugehen, dass ein Zusammenhang zwischen der Art des für die Kommunikation verwendeten *Trägers* und dem *Weg* besteht, auf dem Informationen kommuniziert werden. Bedeutet der Umstand, dass ein dauerhafter Datenträger existiert, zwangsläufig auch, dass die Informationen „mitgeteilt" werden? Falls die Informationen nicht auf einem dauerhaften Datenträger kommuniziert werden, werden sie dann lediglich „zugänglich gemacht"?

24. Meines Erachtens sind diese beiden Elemente – die Art des für die Kommunikation verwendeten Trägers und der Weg, auf dem Informationen kommuniziert werden – getrennt zu prüfen. Das Medium ist zu trennen von dem Weg, auf dem Informationen geliefert werden.

25. Die Richtlinie 2007/64 enthält keinen Anhaltspunkt dafür, dass der für Informationen verwendete Träger und der Weg der Informationsübermittlung Hand in Hand gehen müssen. Im Gegenteil: In verschiedenen Erwägungsgründen der Richtlinie wird erläutert, dass es sich um zwei verschiedene Fragen handelt. Im 24. Erwägungsgrund wird unter Nennung von Beispielen dargelegt, was unter einem „dauerhaften Datenträger“ zu verstehen ist. Der 27. Erwägungsgrund bezeichnet die beiden in der Richtlinie vorgesehenen Wege für die Kommunikation von Informationen („Mitteilen“ und „Zugänglichmachen“). Denkbar sind daher Fälle, in denen Informationen, selbst wenn sie sich auf einem „dauerhaften Datenträger“ befinden, dem Verbraucher nicht wirksam „mitgeteilt“, sondern lediglich „zugänglich gemacht“ werden, wie dies in verschiedenen Bestimmungen der Richtlinie beispielhaft zum Ausdruck kommt(5).

26. Deshalb lassen sich die beiden Fragen des vorlegenden Gerichts vereinfachen und wie folgt umformulieren: 1. Handelt es sich bei den Informationen in der E-Banking-Mailbox um Informationen auf einem „dauerhaften Datenträger“? und 2. Werden diese Informationen von der Bank „mitgeteilt“ (und nicht nur „zugänglich gemacht“)?

3. Sachverhaltsdarstellung durch das nationale Gericht

27. Nach den Feststellungen des vorlegenden Gerichts ist für das vorliegende Verfahren davon auszugehen, dass die von der Bank über ihr E-Banking-System an die E-Banking-Mailbox der Kunden übermittelten elektronischen Nachrichten nicht verändert werden können. Sie werden während eines für die Zwecke der Information angemessenen Zeitraums von der Bank nicht gelöscht. Die Information kann auf dieselbe Art und Weise konsultiert und reproduziert (elektronisch wiedergegeben bzw. ausgedruckt) werden. Der Kunde kann die Nachrichten verwalten und auch löschen.

28. Diese Darstellung wird allerdings vom Verein für Konsumenteninformation bestritten. Seiner Ansicht nach nimmt das vorlegende Gericht bereits eine rechtliche Würdigung der Tatsachen vor.

29. Nach ständiger Rechtsprechung beruht das Verfahren nach Art. 267 AEUV auf einer klaren Aufgabentrennung zwischen den nationalen Gerichten und dem Gerichtshof. Die Feststellung und Beurteilung des Sachverhalts des Ausgangsrechtsstreits ist allein Sache des nationalen Gerichts(6).

30. Im vorliegenden Fall hat das vorlegende Gericht die Merkmale des in Rede stehenden Mailbox- und E-Banking-Systems recht eingehend geprüft. Mit der nachfolgenden Würdigung in Abschnitt B.1 der vorliegenden Schlussanträge soll daher die Tragweite des Begriffs „dauerhafter Datenträger“ in der Richtlinie 2007/64 klargestellt werden.

31. In den beim Gerichtshof eingereichten Erklärungen werden Fragen zu den Voraussetzungen aufgeworfen, die internetbasierte Kommunikationssysteme erfüllen müssen, um als „dauerhafter Datenträger“ gelten zu können. Vor diesem Hintergrund können, auch wenn die Beurteilung der technischen Merkmale des E-Banking-Systems der BAWAG als Sachverhaltselemente allein Sache des nationalen Gerichts ist, durch die Auslegung der Definition „dauerhafter Datenträger“ in der Richtlinie 2007/64 einige sachdienliche Kriterien aufgezeigt werden.

B – *Würdigung*

1. Dauerhafter Datenträger

32. Die materiellen Voraussetzungen, die erfüllt sein müssen, um einen Träger oder ein Instrument als „dauerhaften Datenträger“ qualifizieren zu können, finden sich in der Begriffsbestimmung in Art. 4 Nr. 25 der Richtlinie 2007/64: a) Der Datenträger muss es ermöglichen, an den Kunden persönlich gerichtete Informationen derart zu speichern, dass er sie in

der Folge für eine angemessene Dauer einsehen kann, und b) er muss die unveränderte Wiedergabe gespeicherter Informationen gewährleisten.

33. Dieselben Kriterien finden sich auch in mehreren anderen Rechtsakten des abgeleiteten Unionsrechts, in denen der Begriff „dauerhafter Datenträger“ verwendet wird. Dieser erstmals in der Richtlinie 97/7/EG über Vertragsabschlüsse im Fernabsatz(7) enthaltene Begriff bezeichnet eine Alternative zu Papier als Informationsträger bzw. -medium. Die Richtlinie 97/7 enthielt zwar keine Definition des Begriffs „dauerhafter Datenträger“, doch hat der Gerichtshof das einheitliche Verständnis dieses Begriffs im Unionsrecht durch Heranziehung der vom Unionsgesetzgeber in anderen Rechtstexten angegebenen Definitionsmerkmale des Begriffs „dauerhafter Datenträger“ bestätigt(8). Die oben in Nr. 32 genannten Definitionsmerkmale finden sich auch in anschließenden Bestimmungen des abgeleiteten Rechts(9) und in Durchführungsvorschriften(10).

34. Die Kernelemente der Definition – Speicherbarkeit und Reproduzierbarkeit – finden sich auch in anderen Rechtsakten, in denen der Begriff „dauerhafter Datenträger“ nicht ausdrücklich verwendet wird, etwa in der Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr(11).

a) Dauerhafte Datenträger und das Internet

35. Die Einführung des Begriffs „dauerhafter Datenträger“ und die Elemente seiner Definition zeugen vom Willen des Unionsgesetzgebers, das Spannungsverhältnis aufzulösen, das zwischen i) dem Erfordernis, sich der Entwicklung der Technologie, die den Geschäftsverkehr über das Internet beschleunigt, und anderer elektronischer Kommunikationsmittel anzupassen, und ii) dem Schutz der Verbraucherrechte durch Verbraucheraufklärung besteht. Durch die Gleichstellung von Papier als Träger mit anderen „dauerhaften Datenträgern“ in bestimmten Fällen trägt das Unionsrecht der technologischen Entwicklung und den wirtschaftlichen Interessen sowohl der Verbraucher als auch der Dienstleister an einem Wegfall von Papier als Träger Rechnung.

36. Gleichzeitig soll aber mit den Definitionsmerkmalen des Begriffs „dauerhafter Datenträger“ – Speicherbarkeit und unveränderte Wiedergabe – der Schutz der Verbraucher als der schutzbedürftigeren Partei bei Vertragsverhältnissen dadurch erreicht werden, dass ein nur vorübergehender Erhalt der Verbraucherinformationen(12) und deren einseitige Änderung durch die Dienstleister verhindert werden. Diese Merkmale gewährleisten, wie es Generalanwalt Mengozzi formuliert hat, „dass die Informationen der Kontrolle des Kunden, nicht aber der Kontrolle desjenigen unterliegen, der sie erteilt hat“(13).

37. Trotz der verhältnismäßig klaren Definition des Begriffs „dauerhafter Datenträger“ ist in der vorliegenden Rechtssache streitig, ob über eine E-Banking-Mailbox übermittelte Nachrichten die oben in Nr. 32 dargelegten Merkmale eines „dauerhaften Datenträgers“ erfüllen.

38. Zunächst können nach Ansicht des Vereins für Konsumenteninformation E-Mails und Websites im Internet nicht als „dauerhafte Datenträger“ eingestuft werden, da sie kein körperliches Speicherinstrument darstellen können.

39. Diesem Argument kann meines Erachtens nicht gefolgt werden.

40. Nunmehr steht fest, dass der Begriff „dauerhafter Datenträger“ flexibel definiert wird. Der Gerichtshof hat ihn als der Papierform „funktional gleichwertig“ bezeichnet(14) und ihn damit von jeder Vorgabe hinsichtlich der Gestalt des Informationsträgers gelöst.

41. Außerdem spricht die Bezugnahme in Art. 4 Nr. 25 der Richtlinie 2007/64 auf „jedes Medium“ dafür, dass der Begriff „dauerhafter Datenträger“ weit zu verstehen ist und *a priori* keine bestimmte Kommunikationsform ausschließt.

42. Der Begriff „dauerhafter Datenträger“ ist daher unabhängig von der physischen Struktur oder den Hardware-Eigenschaften eines Mediums oder Trägers. Er knüpft vielmehr an die *funktionalen* Merkmale an, die für seine Wirkungsweise bestimmend sind und es ihm ermöglichen, die Erfordernisse der Speicherbarkeit und der unveränderten Wiedergabe im Sinne von Art. 4 Nr. 25 der Richtlinie zu erfüllen. Solange also diese Bedingungen erfüllt sind, kann sich die tatsächliche Art und Form eines „dauerhaften Datenträgers“ mit der Entwicklung der technischen Möglichkeiten im Laufe der Zeit verändern.

43. Zugegebenermaßen zeigt die Entwicklung der Unionsvorschriften in der Frage, ob internetbasierte Kommunikation die Voraussetzungen für „dauerhafte Datenträger“ erfüllen kann, einen gewissen Grad der Unsicherheit. So lässt sich dem 20. Erwägungsgrund der Richtlinie 2002/65 und Art. 2 Nr. 12 der Richtlinie 2002/92 eine gewisse Zurückhaltung gegenüber dem Internet entnehmen, denn dort heißt es, dass Internet-Websites nicht zu den „dauerhaften Datenträgern“ gehören, es sei denn, sie entsprechen den in der Definition enthaltenen Kriterien.

44. Im 23. Erwägungsgrund der Richtlinie 2011/83 werden E-Mails jedoch zu den Beispielen für dauerhafte Datenträger gezählt. Zudem wurde in der Richtlinie 2007/64 die zurückhaltende Einstellung gegenüber Internet-Websites wohl aufgegeben. In ihrem 24. Erwägungsgrund sind als Beispiel für „dauerhafte Datenträger“ nunmehr ausdrücklich Websites genannt, die „für einen dem Zweck der Information angemessenen Zeitraum konsultiert und unverändert reproduziert werden können“.

45. Die Qualifizierung einer Internet-Website als „dauerhafter Datenträger“ aufgrund ihrer funktionalen Eigenschaften ist schließlich auch vom EFTA-Gerichtshof im Urteil Inconsult Anstalt/Finanzmarktaufsicht(15) im Kontext einer Rechtssache bestätigt worden, in der es um die Auslegung des Begriffs „dauerhafter Datenträger“ in der Richtlinie 2002/92 ging. Dort hat der EFTA-Gerichtshof entschieden, dass „gewöhnliche“ Websites nicht den Anforderungen entsprächen, um als „dauerhafter Datenträger“ angesehen werden zu können(16), während dies bei „fortgeschrittenen“ Websites durchaus der Fall sein könne, wenn sie die in der einschlägigen Definition vorgesehenen Anforderungen erfüllten(17).

46. An dieser Stelle ist also festzuhalten, dass die Einstufung internetbasierter Kommunikationssysteme als „dauerhafte Datenträger“ nicht *per se* ausgeschlossen ist. Voraussetzung ist jedoch, dass ihre Funktionalität und ihr Betrieb den in Nr. 32 der vorliegenden Schlussanträge dargelegten Anforderungen von Art. 4 Nr. 25 der Richtlinie 2007/64 entsprechen.

b) „E-Banking-Mailbox“ als dauerhafter Datenträger

47. Die BAWAG und die Kommission sind der Auffassung, dass angesichts der Angaben im Vorabentscheidungsersuchen die in Rede stehende E-Banking-Mailbox den Anforderungen von Art. 4 Nr. 25 der Richtlinie entspreche.

48. Der Verein für Konsumenteninformation macht dagegen geltend, dass das in Rede stehende E-Banking-System die vorgenannten Anforderungen nicht erfülle, da der Server, auf dem sich die Mailbox befinde, von der BAWAG selbst verwaltet werde. Es sei daher nicht gewährleistet, dass die in der Mailbox gespeicherten Informationen unverändert blieben. Außerdem sei der Dienstleister in der Lage, den Zugang für Nutzer zu sperren. Im gleichen Sinne vertritt die polnische Regierung die Ansicht, dass sich E-Mails von den im Wege des E-Banking übermittelten Nachrichten unterschieden, da der Zahlungsdienstleister bei Letzteren in der Regel insbesondere nach Vertragsende die Möglichkeit habe, sie einseitig zu ändern oder den Zugang zu ihnen zu sperren, so dass eine unveränderte Wiedergabe der Informationen nicht gewährleistet sei.

49. Meines Erachtens hängt die Antwort auf die Frage, ob eine E-Banking-Mailbox als „dauerhafter Datenträger“ angesehen werden kann, von der Erfüllung der in Art. 4 Nr. 25 der Richtlinie 2007/64 festgelegten Voraussetzungen ab, was das nationale Gericht im Licht der vom Gerichtshof aufgestellten Auslegungskriterien zu beurteilen hat.

50. Das Urteil Content Services des Gerichtshofs ist dabei von begrenztem Nutzen. Darin hat der Gerichtshof im Kontext der Richtlinie 97/7 entschieden, dass Informationen, die dem Verbraucher nur über einen Hyperlink auf einer Website übermittelt würden, nicht als „dauerhafter Datenträger“ im Sinne von Art. 5 Abs. 1 der Richtlinie angesehen werden könnten(18). Allerdings war der Gerichtshof nicht mit dem Fall befasst, in dem eine Website gewährleistet, dass der Verbraucher Informationen speichern, auf sie zugreifen und sie wiedergeben kann(19). Um einen solchen Fall ging es jedoch im Urteil Inconsult Anstalt/Finanzmarktaufsicht des EFTA-Gerichtshofs(20).

51. Anknüpfend an den Ansatz des EFTA-Gerichtshofs im Urteil Inconsult Anstalt/Finanzmarktaufsicht bin ich der Meinung, dass verschiedene Arten technischer Vorkehrungen wie internetbasierte Mailbox-Systeme je nach ihren Merkmalen und Funktionalitäten die Anforderungen an „dauerhafte Datenträger“ erfüllen können.

52. Ohne eine erschöpfende Aufzählung geben oder das Spektrum der bestehenden oder möglichen technischen Vorkehrungen eingrenzen zu wollen, die den Voraussetzungen von Art. 4 Nr. 25 der Richtlinie 2007/64 entsprechen könnten, sind meines Erachtens zwei Szenarien denkbar, bei denen eine E-Banking-Mailbox als „dauerhafter Datenträger“ angesehen werden könnte(21). Erstens könnte davon ausgegangen werden, dass eine E-Banking-Mailbox *per se* die Anforderungen an einen „dauerhaften Datenträger“ erfüllt. Zweitens könnte ein solches System als Weg zur Übermittlung elektronischer Dokumente angesehen werden, die, sofern sie in einem entsprechenden Format bereitgestellt werden, als solche „dauerhafte Datenträger“ darstellen können. In beiden Fällen lautet die entscheidende Frage, ob die Informationen für eine angemessene Dauer gespeichert werden können und ob ihre unveränderte Wiedergabe gewährleistet ist. Bei beiden Szenarien setzt das Bestehen einer „Mailbox“ jedoch einen eigenständigen abgesicherten Speicherbereich voraus, auf den die Nutzer mittels Benutzernamen und Passwort zugreifen können.

53. Beim ersten Szenario stellt eine E-Banking-Mailbox ein System dar, das dem Zahlungsdienstleister die Übermittlung von Informationen und dem Zahlungsdienstnutzer die Speicherung und Wiedergabe der Informationen erlaubt. In diesem Fall werden jedoch die gesonderten Funktionen der Mailbox als „dauerhafter Datenträger“ einerseits und als „Speicherträger“ andererseits in erheblichem Umfang aufgehoben.

54. Was das Erfordernis der Speicherbarkeit betrifft, müssen die Informationen während einer für die Zwecke der betreffenden Information angemessene Dauer zugänglich sein, d. h. so lange, wie sie für den Zahlungsdienstnutzer zur Wahrung seiner Interessen gegenüber dem Zahlungsdienstleister relevant sind(22). Die Dauer der Verfügbarkeit der Informationen kann daher je nach deren Inhalt und den betroffenen vertraglichen Rechten und Pflichten variieren(23). Bei Änderungen der Rahmenvertragsbedingungen kann der Zeitraum der Zugänglichkeit über die Löschung des Kontos oder die Beendigung des Vertrags hinausgehen, um dem Zahlungsdienstnutzer die Kenntnisnahme seiner vertraglichen Rechte und erforderlichenfalls die Geltendmachung von Ersatzansprüchen zu ermöglichen.

55. Neben dem Kriterium der Speicherbarkeit der Informationen für eine angemessene Dauer muss auch das Erfordernis der „unveränderten Wiedergabe“ erfüllt sein. Unter unveränderter Wiedergabe ist zu verstehen, dass der Zahlungsdienstleister technisch keine Möglichkeit hat, Informationen nach der Übermittlung an den Nutzer einseitig zu ändern oder zu löschen(24). Infolgedessen dürfte eine Mailbox, die sich auf dem Server des Zahlungsdienstleisters befindet und

von diesem verwaltet wird, wohl kaum das Erfordernis der Gewährleistung einer „unveränderten Wiedergabe“ erfüllen, da sie technisch der Kontrolle des Zahlungsdienstleisters unterliegt.

56. Trotz der augenscheinlichen Komplexität neuer Technologien bleibt der Ausgangspunkt bemerkenswert einfach: Das grundlegende Ziel der Rechtsvorschriften über die Unterrichtung der Verbraucher bei Vertragsschluss oder -änderungen besteht darin, die Verbraucher auf bestimmte Weise zu unterrichten und ihnen die Möglichkeit zu geben, die Informationen in einem sicheren Format zu späteren Beweiszwecken aufzubewahren. Ohne einer der Vertragsparteien bösen Willen zu unterstellen, kann durch eine der Kontrolle des Dienstleisters unterliegende „Mailbox“ definitionsgemäß nicht sichergestellt werden, dass die Verbraucher die an diese Mailbox gelieferten Informationen in der Folge in einem sicheren Format einsehen oder nutzen können. Um eine Parallele zu „prävirtuellen“ Zeiten zu ziehen: Eine solche Mailbox ähnelt einer Situation, in der den Kunden Papierfassungen ihrer Verträge mit einer Bank ausgehändigt wurden, alle Vertragsdokumente aber zwingend in einem Archivraum in der Bank selbst aufbewahrt werden mussten. Auch wenn Papier recht dauerhaft ist, kann aus der Sicht des Kunden wohl kaum davon die Rede sein, dass er die Informationen in den archivierten Vertragsdokumenten „in der Folge … einsehen kann“ und dass ihm eine „unveränderte Wiedergabe“ im Sinne von Art. 4 Nr. 25 der Richtlinie 2007/64 ermöglicht wird.

57. Allerdings gibt es noch das zweite oben erwähnte Szenario. Beim ersten Szenario – und ebenso in den meisten der in der vorliegenden Rechtssache eingereichten Erklärungen – hat sich die Diskussion darauf konzentriert, ob die Mailbox als solche als „dauerhafter Datenträger“ angesehen werden kann. Die Konzentration auf diese Frage mag jedoch etwas in die Irre führen. Eine Mailbox lässt sich als Portal für die Mitteilung von Informationen auffassen. Dann ist die Mailbox nicht selbst als der Informationsträger anzusehen. Mit anderen Worten: Die Mailbox eines E-Banking-Systems könnte als „Gateway“ betrachtet werden, über das die betreffenden Informationen in Form elektronischer Dokumente übermittelt werden. Bei dieser Sichtweise lautet die entscheidende Frage nicht „Welche technischen Eigenschaften weist die Mailbox auf?“, sondern „Wie sehen die individuellen Nachrichten aus, die über die Mailbox versendet werden?“.

58. Was das Format angeht, in dem die Informationen mitzuteilen sind, so müssen die an den Kunden persönlich gerichteten Informationen in einem elektronischen Dokument erteilt werden, dessen Format die unveränderte Wiedergabe der Informationen garantiert. Ohne mögliche technische Lösungen vorab beurteilen zu wollen, könnte dies durch ein elektronisches Format gewährleistet werden, das Änderungen grundsätzlich unmöglich macht und ein hinreichendes Maß an Authentizität der Informationen garantiert, wenn der Kunde sich später möglicherweise auf sie stützt.

59. Da die Mailbox beim zweiten Szenario den Kanal für die Übermittlung von Dokumenten darstellt, selbst aber keine Speichereinrichtung ist, muss die Möglichkeit bestehen, die elektronischen Dokumente gesondert in einer Weise zu speichern, die es dem Nutzer erlaubt, das Dokument herunterzuladen und/oder auszudrucken. Angesichts der begrifflichen Trennung zwischen der Mailbox als Gateway und der Speichereinrichtung bedeutet bei diesem Szenario das Erfordernis der Speicherbarkeit nämlich, dass die Mailbox die sie passierenden Nachrichten und die Speichermöglichkeiten dem Kunden über eine benutzerfreundliche Schnittstelle zur Kenntnis bringen muss. Wie der EFTA-Gerichtshof hervorgehoben hat, muss sie „Elemente enthalten, die den Verbraucher mit an Sicherheit grenzender Wahrscheinlichkeit dazu anhalten, die Informationen in Papierform zu sichern oder auf einem anderen dauerhaften Datenträger zu speichern“(25).

60. Wurden die betreffenden Informationen in Form eines elektronischen Dokuments übermittelt, das selbst einen „dauerhaften Datenträger“ darstellt, wäre das die Dauer der Zugänglichkeit der gespeicherten Informationen betreffende Kriterium aufgrund der Möglichkeit, das elektronische

Dokument auf der eigenen Festplatte des Kunden zu speichern oder einen Ausdruck in einer eigenen Akte des Kunden aufzubewahren, grundsätzlich erfüllt. Es ist jedoch darauf hinzuweisen, dass der Zahlungsdienstleister durch die Einrichtung einer „Mailbox“ den Eindruck erweckt, dass es sich um einen eigenen Bereich mit bestimmter Speicherkapazität für den Kunden handelt. Das bedeutet, dass die Dauer der Zugänglichkeit der Nachrichten in Form elektronischer Dokumente in der Mailbox selbst für die Zwecke der betreffenden Informationen angemessen sein muss, es sei denn, dem Kunden wird klar angezeigt, dass das elektronische Dokument nur für begrenzte Zeit in der E-Banking-Mailbox gespeichert werden kann und nach Ablauf einer ausdrücklich bezeichneten gebührenden Frist entfernt wird.

61. Somit ist meines Erachtens das Erfordernis, dass sich Informationen auf einem „dauerhaften Datenträger“ im Sinne von Art. 4 Nr. 25 der Richtlinie 2007/64 befinden müssen, erfüllt, wenn die Informationen den Kunden in einem leicht zugänglichen und sicheren Format über eine elektronische Mailbox erteilt werden und es den Kunden freisteht, mit den Informationen nach Gutdünken zu verfahren. Um diese Situation mit einem Postamt zu vergleichen: Sie entspricht *de facto* dem Fall, dass dem Kunden ein „Brief“ ausgehändigt wird. Wie der einzelne Kunde dann damit verfährt – ob er ihn aufbewahrt oder wegwirft –, ist allein seine Sache.

62. Abschließend ist hinzuzufügen, dass die beiden vorstehend dargestellten Szenarien sich nicht gegenseitig ausschließen. Meines Erachtens muss auf jeden Fall mindestens eines von ihnen vorliegen, damit dem Erfordernis der Kommunikation über einen „dauerhaften Datenträger“ Genüge getan wird. Allerdings lassen sich die technischen Merkmale beider Varianten auch kombinieren. So kann z. B. ein E-Banking-System, bei dem die Kontrolle des Dienstnutzers über seine Mailbox gewährleistet ist und bei dem der Dienstleister keine Möglichkeit hat, den Inhalt einseitig zu ändern oder zu löschen, zugleich als Gateway fungieren, über das die betreffenden Informationen in Form elektronischer Dokumente in einem Format geliefert werden, das ihre Unveränderbarkeit und Speicherbarkeit garantiert, und als Gateway, das dem Nutzer die Speicherung des Dokuments durch Ausdrucken oder Herunterladen ermöglicht.

63. Infolgedessen bin ich der Auffassung, dass Art. 44 Abs. 1 in Verbindung mit Art. 41 Abs. 1 und Art. 4 Nr. 25 der Richtlinie 2007/64 dahin auszulegen ist, dass Informationen, die ein Zahlungsdienstleister an die E-Banking-Mailbox des Kunden übermittelt, Informationen auf einem „dauerhaften Datenträger“ darstellen, sofern die E-Banking-Mailbox es dem Zahlungsdienstnutzer ermöglicht, an ihn persönlich gerichtete Informationen so zu speichern, dass er sie in der Folge für eine für die Zwecke der Informationen angemessene Dauer einsehen kann. Sie muss außerdem die unveränderte Wiedergabe der gespeicherten Informationen erlauben und somit verhindern, dass der Dienstleister auf die Informationen zugreift, sie verändert oder löscht. Eine E-Banking-Mailbox kann außerdem einen geeigneten Kanal für die Übermittlung von Informationen in Form elektronischer Dokumente darstellen, wenn diese Dokumente selbst die Anforderungen an einen „dauerhaften Datenträger“ erfüllen und wenn ein solches System den Nutzer dazu anhält, die Dokumente mit Hilfe einer leicht zugänglichen Funktion elektronisch zu speichern und/oder auszudrucken.

2. „Mitteilen“ oder „Zugänglichmachen“ von Informationen

64. Sollte das nationale Gericht feststellen, dass die in Rede stehende E-Banking-Mailbox oder die darin zur Verfügung gestellten Informationen die Anforderungen erfüllen, um als „dauerhafter Datenträger“ angesehen zu werden, bleibt noch zu prüfen, ob die Informationen über „Änderungsmitteilungen“ als im Sinne von Art. 41 Abs. 1 der Richtlinie 2007/64 „mitgeteilt“ anzusehen sind.

65. Wie bereits in Nr. 25 der vorliegenden Schlussanträge dargelegt, sieht die Richtlinie 2007/64

zwei verschiedene Regelungen für die Kommunikation vor, für die jeweils unterschiedliche Anforderungen gelten.

66. Wie die italienische Regierung in ihren schriftlichen Erklärungen zutreffend ausgeführt hat, kommen in den unterschiedlichen Formulierungen der Art. 36 und 37 („Zugänglichmachen" von Informationen) im Gegensatz zu den Art. 41 und 42 („Mitteilen" von Informationen) der Richtlinie 2007/64 zwei verschiedene Standards für die Übermittlung von Informationen an Zahlungsdienstnutzer zum Ausdruck. In Fällen, in denen die Richtlinie das Verb „mitteilen" verwendet, ist meines Erachtens eine verstärkte Informationspflicht gemeint.

67. Informationen über Rahmenvertragsänderungen, um die es im vorliegenden Fall geht, sind in Art. 44 Abs. 1 der Richtlinie 2007/64 geregelt. In dessen Unterabs. 1 heißt es, dass der Zahlungsdienstleister Änderungen des Rahmenvertrags sowie der in Art. 42 genannten Informationen und Vertragsbedingungen in der in Art. 41 Abs. 1 vorgesehenen Weise spätestens zwei Monate vor dem geplanten Zeitpunkt ihrer Anwendung vorschlägt. Diese Informationen müssen im Sinne von Art. 41 Abs. 1 der Richtlinie „mitgeteilt" werden.

68. Im 27. Erwägungsgrund der Richtlinie 2007/64 finden sich aufschlussreiche Hinweise zu den Begriffen „mitteilen" und „zugänglich machen". Darin heißt es, dass die Informationen „*mitgeteilt*" werden, wenn sie „vom Zahlungsdienstleister zu dem … geforderten Zeitpunkt von sich aus übermittelt werden, ohne dass der Zahlungsdienstnutzer sie ausdrücklich anfordern muss".

69. Beim „*Zugänglichmachen*" von Informationen muss der Nutzer eine aktivere Rolle spielen und die Informationen vom Zahlungsdienstleister anfordern. Im 27. Erwägungsgrund der Richtlinie 2007/64 werden folgende Beispiele für das „Zugänglichmachen" angeführt: ausdrückliches Anfordern der Informationen vom Zahlungsdienstleister, *sich in die Mailbox des Bankkontos einloggen* oder eine Bankkarte in den Drucker für Kontoauszüge einführen. Der Begriff „zugänglich machen" sieht also eine aktivere Rolle des Zahlungsdienstnutzers vor, der sich an den Dienstleister wenden muss, um die Informationen zu erlangen.

70. Soweit im 27. Erwägungsgrund als Beispiel für das „Zugänglichmachen" von Informationen der Fall genannt wird, dass der Zahlungsdienstnutzer „sich in die Mailbox des Bankkontos einloggt", steht dies entgegen der vom vorlegenden Gericht vertretenen Ansicht nicht im Widerspruch zum 24. Erwägungsgrund der Richtlinie, in dem Websites als mögliche „dauerhafte Datenträger" bezeichnet werden. Dass eine E-Banking-Mailbox die Voraussetzungen erfüllen kann, um als „dauerhafter Datenträger" angesehen zu werden, bedeutet nicht, dass die Bank dem Kunden die Informationen „mitgeteilt" hat. Wie bereits in den Nrn. 23 bis 26 der vorliegenden Schlussanträge dargelegt, ist der Träger, auf dem die Informationen mitgeteilt werden, von dem Weg zu unterscheiden, auf dem die Informationen übermittelt werden.

71. Die Nennung der „Mailbox des Bankkontos" als Beispiel für Informationen, die „zugänglich gemacht" werden, im 27. Erwägungsgrund der Richtlinie hat ihren Grund gerade in den besonderen Merkmalen der Kommunikation über E-Banking-Systeme.

72. Nach Ansicht der BAWAG (und auch des vorlegenden Gerichts) kommt es entscheidend darauf an, wer die Initiative zur Kommunikation der Information ergriffen hat. Wenn man dieser Argumentation folgt, wurde die Information im Sinne von Art. 41 Abs. 1 der Richtlinie 2007/64 „mitgeteilt", weil vom Zahlungsdienstleister die Initiative zur Übermittlung der Information an den Kunden mittels der E-Banking-Mailbox ausging.

73. Ich teile diese Ansicht nicht. Meiner Meinung nach ist die ursprüngliche Initiative weder der einzige noch der ausschlaggebende Faktor für die Beurteilung, ob die Information „mitgeteilt" oder lediglich „zugänglich gemacht" wurde. Wichtiger ist die effektive Übermittlung der Information.

Die Information muss aus dem Bereich des Dienstleisters heraustreten und in die Kenntnissphäre des Nutzers gelangen. Selbst wenn also die Initiative zur Übermittlung der Information über eine interne E-Banking-Mailbox vom Zahlungsdienstleister ausgehen mag, stellt dieser Kanal als solcher nicht die effektive Übermittlung der Information in die Sphäre des Kunden sicher, so dass dieser Kenntnis von ihr erlangt.

74. Um auf die bereits herangezogene Parallele zur „prävirtuellen“ Welt zurückzukommen: Eine vom Dienstleister verwaltete E-Banking-Mailbox ist weitgehend mit einem Postfach in einem Postamt oder mit einem persönlichen Schließfach in den Räumlichkeiten einer Bank vergleichbar. Ohne eine Mitteilung oder einen Hinweis kann man von Briefen, die in ein solches Fach gelegt werden und an den Kunden gerichtet sind, wohl kaum sagen, dass sie effektiv die persönliche Sphäre des Kunden erreicht haben.

75. Ich bin ebenso wie die polnische Regierung der Meinung, dass zwischen einer persönlichen E-Mail und dem internen Posteingang eines E-Banking-Systems unterschieden werden muss. Ein E-Mail-Konto stellt heutzutage eine regelmäßige und übliche Kommunikationsform dar und gehört zum Alltag der meisten Durchschnittsverbraucher. Die Mailbox im E-Banking, selbst wenn sie – wenn auch mit einigen Vorbehalten – technisch letztlich als mit einer E-Mail vergleichbar angesehen werden könnte, lässt sich hingegen kaum einem regelmäßig genutzten Instrument für die allgemeine und alltägliche Kommunikation der Verbraucher gleichstellen. Es handelt sich um eine für ihr Verhältnis zu einem speziellen Unternehmen (im vorliegenden Fall eine Bank) im speziellen Rahmen ihrer Bankgeschäfte eigentümliche Einrichtung. In der Regel besteht dabei jedoch keine Möglichkeit zur allgemeinen Kommunikation mit Dritten. Außerdem kann von den Verbrauchern vernünftigerweise nicht erwartet werden, dass sie die immer zahlreicher werdenden elektronischen Kommunikationssysteme jedes Dienstleisters im Rahmen ihrer vielgestaltigen Vertragsbeziehungen täglich abfragen.

76. Demnach verlassen in einer E-Banking-Mailbox abgelegte Informationen, auch wenn dies auf Initiative des Zahlungsdienstleisters geschieht, nicht die besondere Sphäre der Bank, um in den Bereich der von den Kunden im Alltag regelmäßig genutzten Kommunikationsinstrumente zu gelangen. In diesem Sinne werden die Informationen nicht „mitgeteilt“.

77. Dies gilt umso mehr, als in Fällen, in denen der Verbraucher im Einklang mit Art. 44 Abs. 1 Unterabs. 2 (bei entsprechender Vereinbarung nach Art. 42 Nr. 6 Buchst. a der Richtlinie) unterrichtet wird, seine Zustimmung zu Änderungen der Rahmenvertragsbedingungen als erteilt gilt, wenn er dem Zahlungsdienstleister seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens der geänderten Bedingungen angezeigt hat. Wie die polnische Regierung ausführt, ist es, wenn die Informationen lediglich über eine interne E-Banking-Mailbox kommuniziert werden, möglich oder sogar recht wahrscheinlich, dass die Kunden nicht erfahren, dass ihnen neue wichtige Informationen zur Verfügung stehen.

78. Der Vollständigkeit halber ist jedoch darauf hinzuweisen, dass auch mittels anderer technischer Lösungen gewährleistet werden kann, dass Zahlungsdienstleister ihren Nutzern Informationen effektiv „mitteilen“.

79. Meines Erachtens kann die „Mitteilung“ von Informationen „zweistufig“ erfolgen. Möglich wäre ein System, bei dem eine Mitteilung oder ein Hinweis an die private E-Mail-Adresse des Kunden (oder eine SMS an sein privates Telefon oder auch ein schlichtes Hinweisschreiben) versandt wird, um den Kunden auf die Verfügbarkeit neuer Nachrichten in seiner E-Banking-Mailbox aufmerksam zu machen. Meiner Meinung nach wäre ein solches Verfahren eine geeignete Ergänzung zur Kommunikation von Informationen über eine E-Banking-Mailbox auf einem dauerhaften Datenträger, so dass dann eine „Mitteilung“ der Informationen vorläge. Eine technische

Lösung dieser Art würde die effektive Mitteilung von Informationen an den Zahlungsdienstnutzer gewährleisten und zugleich die Vorteile des E-Banking-Mailbox-Systems wahren, wie etwa die Möglichkeit, den Erhalt einer Empfangsbestätigung sicherzustellen.

80. Meiner Ansicht nach liefe eine solche Lösung nicht den Feststellungen des Gerichtshofs im Urteil Content Services entgegen. Dort hat der Gerichtshof zwar ausgeführt, dass auf einer Website befindliche Informationen, die durch einen dem Verbraucher per E-Mail übermittelten Link zugänglich gemacht würden, dem Verbraucher weder im Sinne von Art. 5 Abs. 1 der Richtlinie 97/7 „erteilt“ würden, noch er sie im Sinne dieser Bestimmung „erhalten“ habe(26). Jedoch verfolgt die Richtlinie 97/7 nicht nur ein anderes Ziel als die Richtlinie 2007/64, sondern der Wortlaut der betreffenden Bestimmungen in beiden Richtlinien scheint auch nicht demselben Muster zu folgen(27). Außerdem unterscheidet sich der dem Urteil Content Services zugrunde liegende Sachverhalt, bei dem die Informationen nur über einen Link zu einer Website versandt wurden und die Merkmale eines „dauerhaften Datenträgers“ nicht vorlagen, grundlegend vom Sachverhalt der vorliegenden Rechtssache(28).

81. Ich pflichte dem vorlegenden Gericht bei, dass die Zahl der für den Zugriff auf die betreffenden Informationen erforderlichen (Maus-)Klicks nicht maßgebend dafür ist, ob die Informationen „mitgeteilt“ wurden. Denn im Fall von Rahmenverträgen im Sinne der Richtlinie 2007/64 besteht ja eine Vereinbarung zwischen dem Kunden und der Bank, wonach die Kommunikation über eine E-Banking-Mailbox erfolgt. Mehrere Klicks oder auch die Eingabe eines Benutzernamens und Passworts sind Handlungen, die nicht über das hinausgehen, was von Kunden zur Erlangung an sie versendeter Informationen erwartet wird.

82. Schließlich hat die Kommission geltend gemacht, da der Zahlungsdienstnutzer dem Erhalt von Informationen über die E-Banking-Mailbox zugestimmt habe, seien die für den Zugriff auf die Mailbox erforderlichen Schritte nicht als auf Initiative des Kunden erfolgt anzusehen. Wollte man diesem Argument folgen, hätte dies zweierlei zur Folge: Erstens müsste dann jede Kommunikation über die interne Mailbox als „mitgeteilt“ gelten. Zweitens stünde es den Verbrauchern *de facto* frei, durch Unterzeichnung einer E-Banking-Vereinbarung den in der Richtlinie 2007/64 vorgesehenen Schutz vertraglich abzubedingen.

83. Meines Erachtens ist dieses Vorbringen zurückzuweisen.

84. Verbraucher und Unternehmen befinden sich, wie es im 20. Erwägungsgrund heißt, nicht in derselben Situation und brauchen nicht im selben Umfang geschützt zu werden. Unter Anerkennung der in der Realität naturgemäß ungleichen Kräfteverhältnisse wird dort ferner darauf hingewiesen, dass die Verbraucherrechte durch Vorschriften geschützt werden müssen, von denen vertraglich nicht abgewichen werden darf(29). Ohne die Verbraucher übermäßig bevormunden zu wollen: Genau dies ist das Kernanliegen des Verbraucherschutzrechts.

85. Zugegebenermaßen ergibt sich aus Art. 42 Nr. 4 Buchst. a der Richtlinie, dass die Parteien die Kommunikationsmittel für die Informationsübermittlung oder Anzeigepflichten vereinbaren können. Dazu heißt es im 24. Erwägungsgrund, dass „Zahlungsdienstleister und Zahlungsdienstnutzer in einem Rahmenvertrag vereinbaren können [sollten], in welcher Weise nachträgliche Information über die ausgeführten Zahlungsvorgänge erfolgen soll, beispielsweise dass beim Internetbanking alle das Zahlungskonto betreffenden Informationen online zugänglich gemacht werden“. Diese die „nachträgliche Information über die ausgeführten Zahlungsvorgänge“ betreffende Feststellung lässt jedoch sowohl die Erfordernisse bezüglich der allgemeinen vorvertraglichen Unterrichtung nach Art. 41 Abs. 1 als auch die Informationspflichten bei Änderungen der Vertragsbedingungen nach Art. 44 der Richtlinie 2007/64 unberührt.

86. Ferner sieht Art. 34 der Richtlinie 2007/64 ausdrücklich Ausnahmen von den in ihrem Titel III aufgestellten Informationspflichten vor. Nach ihrer Überschrift bezieht sich die genannte Vorschrift lediglich auf Kleinbetragszahlungsinstrumente und elektronisches Geld. Nach Art. 34 Abs. 1 Buchst. b der Richtlinie sind Abweichungen von den nach Art. 44 vereinbarten Informationsanforderungen nur in dem konkreten Rahmenvertrag zulässig(30). Zudem sind hinsichtlich der Informationen über Änderungen des Rahmenvertrags nach Art. 44 Abs. 1 keine vertraglichen Abweichungen erlaubt, wie dies etwa bei Änderungen der Zinssätze und Wechselkurse vorbehaltlich der Sonderregelung in Art. 44 Abs. 2 der Richtlinie 2007/64 möglich ist.

87. Angesichts dessen bin ich der Ansicht, dass Art. 44 Abs. 1 in Verbindung mit Art. 41 Abs. 1 der Richtlinie 2007/64 dahin auszulegen ist, dass Informationen über Änderungen eines Rahmenvertrags, die ein Zahlungsdienstleister ausschließlich über eine E-Banking-Mailbox übermittelt, nicht im Sinne von Art. 41 Abs. 1 der Richtlinie „mitgeteilt“, sondern dem Zahlungsdienstnutzer lediglich „zugänglich gemacht“ werden.

V – Ergebnis

88. Nach alledem schlage ich dem Gerichtshof vor, die vom Obersten Gerichtshof (Österreich) vorgelegten Fragen wie folgt zu beantworten:

1. Art. 44 Abs. 1 in Verbindung mit Art. 41 Abs. 1 und Art. 4 Nr. 25 der Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG ist dahin auszulegen, dass Informationen, die ein Zahlungsdienstleister an die E-Banking-Mailbox des Kunden übermittelt, Informationen auf einem „dauerhaften Datenträger“ darstellen, sofern die E-Banking-Mailbox es dem Zahlungsdienstnutzer ermöglicht, an ihn persönlich gerichtete Informationen so zu speichern, dass er sie in der Folge für eine für die Zwecke der Informationen angemessene Dauer einsehen kann. Sie muss außerdem die unveränderte Wiedergabe der gespeicherten Informationen erlauben und somit verhindern, dass der Dienstleister auf die Informationen zugreift, sie verändert oder löscht. Eine E-Banking-Mailbox kann außerdem einen geeigneten Kanal für die Übermittlung von Informationen in Form elektronischer Dokumente darstellen, wenn diese Dokumente selbst die Anforderungen an einen „dauerhaften Datenträger“ erfüllen und wenn ein solches System den Nutzer dazu anhält, die Dokumente mit Hilfe einer leicht zugänglichen Funktion elektronisch zu speichern und/oder auszudrucken.

2. Art. 44 Abs. 1 in Verbindung mit Art. 41 Abs. 1 der Richtlinie 2007/64 ist dahin auszulegen, dass Informationen über Änderungen eines Rahmenvertrags, die ein Zahlungsdienstleister ausschließlich über eine E-Banking-Mailbox übermittelt, nicht im Sinne von Art. 41 Abs. 1 der Richtlinie „mitgeteilt“, sondern dem Zahlungsdienstnutzer lediglich „zugänglich gemacht“ werden.

---

1 – Originalsprache: Englisch.

---

2 – Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG (ABl. 2007, L 319, S. 1). Die Richtlinie 2007/64 wird mit Wirkung vom 13. Januar 2018 aufgehoben und ersetzt durch die Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der

Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64 (ABl. 2015, L 337, S. 35).

---

3 – Vgl. Urteil vom 5. Juli 2012, Content Services (C-49/11, EU:C:2012:419). Zur Auslegung der Wendung „auf Papier oder auf einem anderen dauerhaften Datenträger“ im Kontext von Art. 10 der Richtlinie 2008/48/EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87/102/EWG des Rates (ABl. 2008, L 133, S. 66) vgl. Schlussanträge der Generalanwältin Sharpston in der Rechtssache Home Credit Slovakia (C-42/15, EU:C:2016:431). Zur Auslegung von Art. 23 Abs. 2 der Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (ABl. 2001, L 12, S. 1) (Brüssel-I-Verordnung), in dem von „[e]lektronische[n] Übermittlungen, die eine dauerhafte Aufzeichnung … ermöglichen“, die Rede ist, hatte sich der Gerichtshof im Urteil vom 21. Mai 2015, El Majdoub (C-322/14, EU:C:2015:334), geäußert.

---

4 – Vgl. Art. 1 Abs. 2 und 18. Erwägungsgrund.

---

5 – So heißt es z. B. in Art. 43, dass der Zahlungsdienstnutzer die Vertragsbedingungen „in Papierform oder auf einem anderen dauerhaften Datenträger“ verlangen kann (d. h. der Kunde muss die Initiative ergreifen).

---

6 – Vgl. z. B. Urteile vom 18. Februar 2016, Finanmadrid EFC (C-49/14, EU:C:2016:98, Rn. 27 und die dort angeführte Rechtsprechung), und vom 3. September 2015, Costea (C-110/14, EU:C:2015:538, Rn. 13 und die dort angeführte Rechtsprechung).

---

7 – Richtlinie des Europäischen Parlaments und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz (ABl. 1997, L 144, S. 19), aufgehoben durch die Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates (ABl. 2011, L 304, S. 64). Art. 5 der Richtlinie 97/7 sah vor, dass der Verbraucher eine Bestätigung der Informationen gemäß Art. 4 Abs. 1 Buchst. a bis f der Richtlinie vorab schriftlich oder auf einem anderen für ihn verfügbaren dauerhaften Datenträger erhalten muss.

---

8 – Urteil vom 5. Juli 2012, Content Services (C-49/11, EU:C:2012:419, Rn. 44). Der Gerichtshof verwies auf Art. 2 Buchst. f der Richtlinie 2002/65/EG des Europäischen Parlaments und des Rates vom 23. September 2002 über den Fernabsatz von Finanzdienstleistungen an Verbraucher und zur Änderung der Richtlinie 90/619/EWG des Rates und der Richtlinien 97/7/EG und 98/27/EG (ABl. 2002, L 271, S. 16), auf Art. 2 Nr. 12 der Richtlinie 2002/92/EG des Europäischen Parlaments und des Rates vom 9. Dezember 2002 über Versicherungsvermittlung (ABl. 2003, L 9, S. 3), auf Art. 3 Buchst. m der Richtlinie 2008/48 sowie auf Art. 2 Nr. 10 der Richtlinie 2011/83.

---

9 – Vgl. z. B. Art. 2 Abs. 1 Buchst. h der Richtlinie 2008/122/EG des Europäischen Parlaments und des Rates vom 14. Januar 2009 über den Schutz der Verbraucher im Hinblick auf bestimmte Aspekte von Teilzeitnutzungsverträgen, Verträgen über langfristige Urlaubsprodukte sowie Wiederverkaufs- und Tauschverträgen (ABl. 2009, L 33, S. 10), Art. 2 Abs. 1 Buchst. m der Richtlinie 2009/65/EG des

Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) (ABl. 2009, L 302, S. 32), Art. 2 Nr. 17 der Richtlinie 2014/92/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten und den Zugang zu Zahlungskonten mit grundlegenden Funktionen (ABl. 2014, L 257, S. 214), Art. 4 Abs. 1 Nr. 62 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. 2014, L 173, S. 349) und Art. 2 Abs. 1 Nr. 18 der Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb (Neufassung) (ABl. 2016, L 26, S. 19).

---

10 – Vgl. z. B. Art. 2 Abs. 2 der Richtlinie 2006/73/EG der Kommission vom 10. August 2006 zur Durchführung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie (ABl. 2006, L 241, S. 26).

---

11 – Richtlinie des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (ABl. 2000, L 178, S. 1), die in ihrem Art. 10 Abs. 3 vorsieht, dass „[d]ie Vertragsbestimmungen und die allgemeinen Geschäftsbedingungen … dem Nutzer so zur Verfügung gestellt werden [müssen], dass er sie speichern und reproduzieren kann“.

---

12 – Vgl. entsprechend Schlussanträge der Generalanwältin Sharpston in der Rechtssache Home Credit Slovakia (C-42/15, EU:C:2016:431, Nr. 24).

---

13 – Schlussanträge des Generalanwalts Mengozzi in der Rechtssache Content Services (C-49/11, EU:C:2012:126, Nr. 42).

---

14 – Urteil vom 5. Juli 2012, Content Services (C-49/11, EU:C:2012:419, Rn. 40 und 42).

---

15 – Urteil vom 27. Januar 2010 (E-4/09, EFTA Court Report 2010, S. 86).

---

16 – In Rn. 63 seines Urteils vom 27. Januar 2010, Inconsult Anstalt/Finanzmarktaufsicht (E-4/09, EFTA Court Report 2010, S. 86), hat der EFTA-Gerichtshof entschieden, dass eine „gewöhnliche Website“ – die als dynamischer elektronischer Host oder als Portal für die Bereitstellung von Informationen diene, die im Allgemeinen vom Betreiber der Website beliebig geändert werden könnten – nicht den Anforderungen an die Gewährleistung einer unveränderten Wiedergabe entspreche und daher nicht als dauerhafter Datenträger angesehen werden könne.

---

17 – Diese Unterscheidung findet sich im Bericht der European Securities Markets Expert Group (ESME) von 2007 „On durable medium – Distance Marketing Directive and Markets in Financial Instruments Directive“, abrufbar unter http://ec.europa.eu/finance/securities/docs/esme/durable_medium_en.pdf.

---

18 – Urteil vom 5. Juli 2012, Content Services (C-49/11, EU:C:2012:419, Rn. 51).

19 – Urteil vom 5. Juli 2012, Content Services (C-49/11, EU:C:2012:419, Rn. 46).

20 – Urteil des EFTA-Gerichtshofs vom 27. Januar 2010, Inconsult Anstalt/Finanzmarktaufsicht (E-4/09, EFTA Court Report 2010, S. 86).

21 – Im Urteil des EFTA-Gerichtshofs vom 27. Januar 2010, Inconsult Anstalt/Finanzmarktaufsicht (E-4/09, EFTA Court Report 2010, S. 86), werden allgemein zwei Szenarien im Kontext von Websites angesprochen. Vgl. Rn. 64 ff. des Urteils.

22 – Vgl. entsprechend Urteil des EFTA-Gerichtshofs vom 27. Januar 2010, Inconsult Anstalt/Finanzmarktaufsicht (E-4/09, EFTA Court Report 2010, S. 86, Rn. 44).

23 – Ebd.

24 – Vgl. entsprechend Urteil des EFTA-Gerichtshofs vom 27. Januar 2010, Inconsult Anstalt/Finanzmarktaufsicht (E-4/09, EFTA Court Report 2010, S. 86, Rn. 66).

25 – Urteil des EFTA-Gerichtshofs vom 27. Januar 2010, Inconsult Anstalt/Finanzmarktaufsicht (E-4/09, EFTA Court Report 2010, S. 86, Rn. 64 und 65).

26 – Urteil vom 5. Juli 2012, Content Services (C-49/11, EU:C:2012:419, Rn. 37).

27 – In den verschiedenen Sprachfassungen von Art. 5 Abs. 1 und Art. 4 Abs. 1 der Richtlinie 97/7 werden andere Begriffe verwendet als in den Art. 41 Abs. 1 und 36 Abs. 1 der Richtlinie 2007/64. Vgl. Urteil vom 5. Juli 2012, Content Services (C-49/11, EU:C:2012:419, Rn. 35).

28 – Vgl. Urteil vom 5. Juli 2012, Content Services (C-49/11, EU:C:2012:419, Rn. 46).

29 – Weiter heißt es in diesem Erwägungsgrund, dass es den Unternehmen und Organisationen allerdings freistehen sollte, abweichende Vereinbarungen zu schließen. Die Mitgliedstaaten sollten jedoch vorsehen können, dass Kleinstunternehmen wie Verbraucher behandelt werden.

30 – Gemäß der genannten Bestimmung sind Ausnahmen nur vorgesehen für „einzelne Zahlungsvorgänge bis höchstens 30 EUR … oder [für Zahlungsinstrumente,] die entweder eine Ausgabenobergrenze von 150 EUR haben oder Geldbeträge speichern, die zu keiner Zeit 150 EUR übersteigen“. Gemäß Art. 34 Abs. 2 können diese Grenzwerte für innerstaatliche Zahlungsvorgänge verringert oder verdoppelt und für Zahlungsinstrumente auf Guthabenbasis erhöht werden.