EUROPÄISCHE
KOMMISSION

Brüssel, den 28.6.2023
COM(2023) 367 final

2023/0210 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/2010

(Text von Bedeutung für den EWR)

{COM(2023) 366 final} - {SEC(2023) 256 final} - {SWD(2023) 231 final} - {SWD(2023) 232 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Mit der zweiten Zahlungsdiensterichtlinie (PSD2[1]) wurde ein Rechtsrahmen für alle Massenzahlungen in der EU geschaffen, sowohl für den Euro als auch für andere Währungen und sowohl für inländische als auch für grenzüberschreitende Zahlungen. Mit der ersten Zahlungsdiensterichtlinie (PSD1)[2], die 2007 verabschiedet wurde, wurde ein harmonisierter Rechtsrahmen für die Schaffung eines integrierten EU-Zahlungsverkehrsmarkts geschaffen. Aufbauend auf der PSD1 wurden mit der PSD2 Hindernisse für neue Arten von Zahlungsdiensten beseitigt und das Niveau des Verbraucherschutzes und der Sicherheit verbessert. Die meisten Vorschriften der PSD2 gelten seit Januar 2018, einige Vorschriften wie die Vorschriften zur starken Kundenauthentifizierung gelten jedoch erst seit September 2019.

Die PSD2 enthält Vorschriften über die Erbringung von Zahlungsdiensten sowie Vorschriften über die Zulassung und Beaufsichtigung einer Kategorie von Zahlungsdienstleistern, nämlich Zahlungsinstituten. Zu den anderen Kategorien von Zahlungsdienstleistern gehören Kreditinstitute, die unter das EU-Bankenrecht[3] fallen, und E-Geld-Institute, die unter die E-Geld-Richtlinie[4] fallen.

In der Mitteilung der Kommission über eine EU-Strategie für den Massenzahlungsverkehr aus dem Jahr 2020[5] wurden die Prioritäten der Kommission in Bezug auf den Massenzahlungsverkehr für die Amtszeit des derzeitigen Kollegiums der Kommissionsmitglieder (2019–2024) festgelegt. Begleitet wurde sie von einer Strategie für ein digitales Finanzwesen, in der Prioritäten für die digitale, über Zahlungen hinausgehende Agenda im Finanzsektor festgelegt wurden. In der EU-Strategie für den Massenzahlungsverkehr wurde angekündigt, dass die Kommission Ende 2021 „*eine umfassende Überprüfung der Anwendung und der Auswirkungen der PSD2 einleiten*“ wird. Diese Überprüfung wurde im Wesentlichen im Jahr 2022 ordnungsgemäß durchgeführt und führte zu einem Beschluss der Kommission, legislative Änderungen der PSD2 vorzuschlagen, um deren Funktionsweise zu verbessern. Diese Änderungen sind in zwei Vorschlägen enthalten: dem vorliegenden Vorschlag für eine Verordnung über Zahlungsdienste in der EU und einem Vorschlag für eine Richtlinie über Zahlungsdienste und E-Geld-Dienste mit Schwerpunkt auf der Zulassung und Beaufsichtigung von Zahlungsinstituten (und zur Änderung einiger anderer Richtlinien).

Die vorgeschlagene Überarbeitung der PSD2 ist im Arbeitsprogramm der Kommission für 2023 enthalten, zusammen mit einer geplanten Gesetzgebungsinitiative für einen Rahmen für den Zugang zu Finanzdaten, mit der der Zugang zu Finanzdaten und deren Nutzung über Zahlungskonten hinaus auf mehr Finanzdienstleistungen ausgeweitet werden.

---

1 Richtlinie (EU) 2015/2366 vom 25. November 2015 über Zahlungsdienste im Binnenmarkt.

2 Richtlinie 2007/64/EG vom 13. November 2007 über Zahlungsdienste im Binnenmarkt.

3 Verordnung (EU) Nr. 575/2013 über Aufsichtsanforderungen an Kreditinstitute, Richtlinie 2013/36/EU über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten.

4 Richtlinie 2009/110/EG über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten.

5 COM(2020) 592 final vom 24. September 2020.

- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Zu den bestehenden politischen Bestimmungen, die für diese Initiative relevant sind, gehören andere Rechtsvorschriften im Bereich des Zahlungsverkehrs, andere Rechtsvorschriften für Finanzdienstleistungen, die auch Zahlungsdienstleister abdecken, und EU-Rechtsvorschriften mit horizontaler Geltung, die sich auf den Zahlungsverkehrsraum auswirken. Bei der Ausarbeitung dieses Vorschlags wurde darauf geachtet, die Kohärenz mit diesen Vorschriften sicherzustellen.

Weitere Rechtsvorschriften im Bereich des Massenzahlungsverkehrs sind, neben den oben genannten, die Verordnung über den einheitlichen Euro-Zahlungsverkehrsraum (SEPA) von 2012, mit der die technischen Anforderungen für Überweisungen und Lastschriften in Euro harmonisiert werden[6]. Am 26. Oktober 2022 schlug die Kommission eine Änderung der SEPA-Verordnung vor, um die Verwendung von Sofortzahlungen in Euro in der EU zu beschleunigen und zu erleichtern[7]; laut diesem Vorschlag müssen Zahlungsdienstleister, die Sofortzahlungen in Euro anbieten, Nutzern einen „Dienst zur Überprüfung von IBAN/Namen“ anbieten, und mit dem vorliegenden Vorschlag wird diese Anforderung auf Zahlungsdienstleister ausgeweitet, die Überweisungen in einer beliebigen EU-Währung anbieten. Mit der Verordnung über grenzüberschreitende Zahlungen werden die Preise für inländische und grenzüberschreitende Überweisungen in Euro angeglichen[8]. In der Verordnung über Interbankenentgelte sind Höchstbeträge für solche Entgelte festgelegt[9]. Der vorliegende Vorschlag steht im Einklang mit dem Ziel, den Zugang zu Barmitteln zu verbessern, indem es Händlern ermöglicht wird, in physischen Geschäften Bargeldbereitstellungsdienste anzubieten, auch wenn ein Kunde keinen Kauf getätigt hat. Die Arbeiten zum Zugang zu Barmitteln sind auch im Zusammenhang mit der Strategie für den Massenzahlungsverkehr der Kommission zu sehen, in der als politisches Ziel festgelegt wurde, dass Barmittel weithin zugänglich bleiben sollten.

Weitere einschlägige Rechtsvorschriften über Finanzdienstleistungen sind u. a. die Richtlinie über die Wirksamkeit von Abrechnungen[10], an der der diesem Vorschlag beigefügte Richtlinienvorschlag eine gezielte Änderung enthält. Weitere einschlägige Rechtsvorschriften sind die Verordnung über Märkte für Kryptowerte (MiCA)[11], das Gesetz über die digitale operationale Resilienz im Finanzsektor in Bezug auf die Cybersicherheit (DORA)[12] und die Richtlinie zur Bekämpfung der Geldwäsche, zu denen derzeit ein Paket von Änderungsvorschlägen von den Gesetzgebern erörtert wird[13].

Die Initiative steht gänzlich in Einklang mit anderen Initiativen, die die Kommission in ihrer Strategie für ein digitales Finanzwesen in der EU angekündigt hat[14]. Diese Strategie wurde zusammen mit der EU-Strategie für den Massenzahlungsverkehr vorgestellt und zielt darauf

6 Verordnung (EU) Nr. 260/2012 vom 14. März 2012.
7 COM(2022) 546 final.
8 Verordnung (EU) 2021/1230 vom 14. Juli 2021 über grenzüberschreitende Zahlungen in der Union.
9 Verordnung (EU) 2015/751 vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge.
10 Richtlinie 98/26/EG vom 19. Mai 1998 über die Wirksamkeit von Abrechnungen in Zahlungs- sowie Wertpapierliefer- und -abrechnungssystemen.
11 Verordnung (EU) 2023/1114 vom 31. Mai 2023 über Märkte für Kryptowerte.
12 Verordnung (EU) 2022/2554 vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor.
13 Zahlungsdienstleister sind Verpflichtete im Sinne der EU-Gesetzgebung zur Bekämpfung der Geldwäsche.
14 COM(2020) 591 final vom 24. September 2020.

ab, die Digitalisierung des Finanzwesens und der EU-Wirtschaft voranzutreiben und die Fragmentierung des digitalen Binnenmarkts zu verringern.

- **Kohärenz mit anderen Politikbereichen der EU**

Die Initiative steht im Einklang mit der Mitteilung der Kommission „Das europäische Wirtschafts- und Finanzsystem: Mehr Offenheit, Stärke und Resilienz“[15] von 2021, in der die Bedeutung der Strategie für den Massenzahlungsverkehr der Kommission und der digitalen Innovation im Finanzwesen für die Stärkung des Binnenmarkts für Finanzdienstleistungen bekräftigt wurde. In derselben Mitteilung wurde auch noch einmal bestätigt, dass die Dienststellen der Kommission und der Europäischen Zentralbank auf fachlicher Ebene gemeinsam ein breites Spektrum politischer, rechtlicher und technischer Fragen im Zusammenhang mit der möglichen Einführung eines digitalen Euro prüfen und dabei ihren jeweiligen Zuständigkeiten nach den EU-Verträgen Rechnung tragen würden.

Die Kommission legt in Verbindung mit den Vorschlägen zur Änderung der PSD2 einen Vorschlag für einen EU-Rechtsrahmen für den Zugang zu Finanzdaten vor; dieser Vorschlag betrifft den Zugang zu anderen Finanzdaten als Zahlungskontodaten, die weiterhin unter die Rechtsvorschriften über Zahlungen fallen.

Allgemeinere einschlägige EU-Rechtsvorschriften umfassen die DSGVO[16], den europäischen Rechtsakt zur Barrierefreiheit[17] und den Vorschlag für ein Datengesetz, das für das offene Bankwesen („Open Banking“) relevant ist[18]. Insbesondere ist in den Kapiteln III und IV des vorgeschlagenen Datengesetzes ein horizontaler Rahmen für die Rechte und Pflichten in Bezug auf die Bedingungen für die Bereitstellung von Daten in Geschäftsbeziehungen zwischen Unternehmen vorgesehen.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

- **Rechtsgrundlage**

Die Rechtsgrundlage der PSD2 ist Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), wonach die Organe der EU für die Verwirklichung der Ziele des Artikels 26 AEUV die Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten erlassen, welche die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben.

- **Subsidiarität (bei nicht ausschließlicher Zuständigkeit)**

Zahlungsdienste können auch grenzüberschreitend von Zahlungsdienstleistern innerhalb des Binnenmarkts für Zahlungsdienste erbracht werden. Die Dienstleistungsfreiheit und die

15 COM(2021) 32 final vom 19. Januar 2021.

16 Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Siehe auch unten unter „Grundrechte“.

17 Richtlinie (EU) 2019/882 vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen. Dies ist für Maßnahmen zur Verbesserung des Zugangs zur starken Kundenauthentifizierung relevant, die so konzipiert sind, dass sie mit der genannten Richtlinie in Einklang stehen.

18 Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM(2022) 68 final. Der Vorschlag für ein Datengesetz enthält horizontale Vorschriften für den Datenzugang und die Datennutzung. In diesem Zusammenhang können erforderlichenfalls sektorspezifische Vorschriften für den Zugang zu Daten erlassen werden, auch im Hinblick auf Vorschriften für Open Banking.

Niederlassungsfreiheit werden von Zahlungsdienstleistern weithin genutzt. Um harmonische Voraussetzungen und gleiche Wettbewerbsbedingungen im Binnenmarkt für Massenzahlungsdienste sicherzustellen, sind Rechtsvorschriften auf EU-Ebene erforderlich. Diese Logik liegt der ersten und der zweiten Zahlungsdiensterichtlinie zugrunde und gilt für diesen Vorschlag weiterhin.

- **Verhältnismäßigkeit**

Der Vorschlag enthält gezielte Maßnahmen zur Verhältnismäßigkeit, z. B. die Möglichkeit, dass ein kontoführender Zahlungsdienstleister im Bereich des Open Banking von seiner zuständigen nationalen Behörde eine Ausnahme von der Anforderung erhält, über eine spezielle Schnittstelle für den Datenzugang verfügen zu müssen.

- **Wahl des Instruments**

Die PSD2 ist eine Richtlinie, die derzeit in Rechtsvorschriften in den Mitgliedstaaten umgesetzt wird. In verschiedenen Bereichen der EU-Rechtsvorschriften über Finanzdienstleistungen[19] wurde es jedoch als angemessen erachtet, Vorschriften für Finanzunternehmen in eine unmittelbar anwendbare Verordnung aufzunehmen, um die Kohärenz der Umsetzung in den Mitgliedstaaten zu verbessern. Die Überprüfung der PSD2 ergab, dass dieser Ansatz auch in den Rechtsvorschriften über Zahlungen angemessen wäre, was dazu geführt hat, dass die vorgeschlagenen Änderungen der PSD2 in zwei verschiedenen Rechtsakten enthalten sind: dem vorliegenden Vorschlag für eine Verordnung mit Vorschriften für Zahlungsdienstleister und Verbraucher und dem Vorschlag für eine Richtlinie, die insbesondere Vorschriften für die Zulassung und Beaufsichtigung von Zahlungsinstituten enthält.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften**

Im Jahr 2022 wurde eine Bewertung der PSD2 durchgeführt. In die Bewertung flossen ein Bericht eines unabhängigen Auftragnehmers und die Ansichten der Interessenträger bei verschiedenen öffentlichen Konsultationen ein. Der Bewertungsbericht wird als Anhang der Folgenabschätzung zu dem vorliegenden Vorschlag veröffentlicht[20].

Der Bewertungsbericht kommt zu dem Schluss, dass die Ziele der PSD2 in unterschiedlichem Maße erreicht wurden. Ein Bereich mit positiven Auswirkungen war die Betrugsprävention durch die Einführung einer starken Kundenauthentifizierung; auch wenn sich die Umsetzung als schwieriger erwies als erwartet, hat die starke Kundenauthentifizierung bereits erheblich zur Eindämmung von Betrug beigetragen. Die PSD2 war auch im Hinblick auf ihr Ziel, die Effizienz und die Transparenz zu erhöhen und die Auswahl an Zahlungsinstrumenten für Zahlungsdienstnutzer zu erweitern, besonders wirksam. Die Wirksamkeit der PSD2 im Hinblick auf die Schaffung gleicher Wettbewerbsbedingungen ist jedoch begrenzt, insbesondere angesichts des anhaltenden Ungleichgewichts zwischen Banken und Nichtbanken als Zahlungsdienstleister, das sich aus dem mangelnden direkten Zugang letzterer zu bestimmten wichtigen Zahlungssystemen ergibt. Bei der Einführung des „Open Banking“ waren gemischte Erfolge zu verzeichnen, wobei trotz der Kosten für die Umsetzung

[19] Z. B. Aufsichtsvorschriften für Banken oder Vorschriften über Wertpapiermärkte.

[20] SWD(2023) 231 final.

der Bestimmungen der PSD2 über Open-Banking-Dienste weiterhin Probleme im Zusammenhang mit den Schnittstellen für den Datenzugang von Open-Banking-Dienstleistern bestehen. Was das Binnenmarktziel betrifft, so nimmt zwar die grenzüberschreitende Erbringung von Zahlungsdiensten zu, doch bleiben viele Zahlungssysteme (insbesondere Debitkartensysteme) nach wie vor national. Die erwarteten Kostensenkungen für Händler aufgrund neuer und billigerer Zahlungsmittel haben sich nicht vollständig verwirklicht. Insgesamt kommt die Bewertung zu dem Schluss, dass der derzeitige PSD2-Rahmen trotz bestimmter Mängel Fortschritte bei der Verwirklichung seiner Ziele ermöglicht hat, während er im Hinblick auf seine Kosten relativ effizient ist und einen EU-Mehrwert erbringt.

- **Konsultation der Interessenträger**

Um sicherzustellen, dass der Vorschlag der Kommission den Standpunkten aller Interessenträger Rechnung trägt, wurden zu dieser Initiative folgende Konsultationen durchgeführt:

– eine öffentliche Online-Konsultation im Zeitraum vom 10. Mai bis 2. August 2022[21];

– eine gezielte (aber dennoch öffentliche) Konsultation mit detaillierteren Fragen als die öffentliche Konsultation, im Zeitraum vom 10. Mai 2022 bis zum 5. Juli 2022[22];

– eine Sondierung im Zeitraum vom 10. Mai 2022 bis zum 2. August 2022[23];

– eine gezielte Konsultation zur Richtlinie über die Wirksamkeit von Abrechnungen im Zeitraum vom 12. Februar 2021 bis zum 7. Mai 2021;

– eine Konsultation der Interessenträger in der Expertengruppe „Zahlungsverkehrsmarkt“ der Kommission;

– Konsultationen im Rahmen von Ad-hoc-Kontakten mit verschiedenen Interessenträgern, auf deren Initiative oder auf Initiative der Kommission;

– eine Konsultation der Sachverständigen der Mitgliedstaaten in der Expertengruppe für Bankwesen, Zahlungsverkehr und Versicherungswesen der Kommission.

Die Ergebnisse dieser Konsultationen werden in Anhang 2 der Folgenabschätzung zu diesem Vorschlag zusammengefasst.

- **Einholung und Nutzung von Expertenwissen**

Zur Ausarbeitung dieser Initiative wurden verschiedene Expertenbeiträge und -quellen herangezogen, darunter:

– Nachweise, die im Rahmen der oben genannten Konsultationen und auf Ad-hoc-Basis von Interessenträgern vorgelegt wurden;

– von der Europäischen Bankenaufsichtsbehörde in ihrer Empfehlung angeführte Nachweise[24];

– eine von einem Auftragnehmer, Valdani Vicari & Associati Consulting, im September 2022 durchgeführte Studie mit dem Titel „A study on the application and

21 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation_de

22 https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_de

23 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules_de

24 EBA/Op/2022/06 vom 23. Juni 2022. Referenznummer FISMA/2021/OP/0002.

impact of Directive (EU) 2015/2366 on payment services (PSD2)“ (Studie über die Anwendung und Auswirkungen der Richtlinie (EU) 2015/2366 über Zahlungsdienste (PSD2))[25];

– Daten, die von privatwirtschaftlichen Akteuren, z. B. im Bereich des Open Banking, und von Verbraucherorganisationen erhoben wurden.

• **Folgenabschätzung**

Diesen beiden Vorschlägen ist eine Folgenabschätzung beigefügt, die vom Ausschuss für Regulierungskontrolle am 1. März 2023 geprüft wurde. Der Ausschuss für Regulierungskontrolle gab am 3. März 2023 eine befürwortende Stellungnahme mit Vorbehalten ab.

Die Folgenabschätzung ergab, dass es trotz der Erfolge der PSD2 vier Hauptprobleme auf dem EU-Zahlungsverkehrsmarkt gibt:

– Die Verbraucher sind dem Risiko von Betrug ausgesetzt und haben mangelndes Vertrauen in Zahlungen;

– der Rahmen für Open Banking funktioniert unvollkommen;

– die EU-Aufsichtsbehörden haben uneinheitliche Befugnisse und Pflichten;

– es bestehen ungleiche Wettbewerbsbedingungen zwischen Banken und Nichtbanken als Zahlungsdienstleister.

Diese Probleme haben unter anderem nachstehende Folgen:

– Die Nutzer (insbesondere Verbraucher, Händler und KMU) sind nach wie vor einem Betrugsrisiko ausgesetzt;

– Open-Banking-Dienstleister stoßen auf Hindernisse, wenn es darum geht, grundlegende Open-Banking-Dienste anzubieten, und tun sich schwerer, Innovationen zu verwirklichen und mit etablierten Akteuren wie Kartensystemen in Wettbewerb zu treten;

– Zahlungsdienstleister sind mit Blick auf ihre Pflichten generell verunsichert und Zahlungsdienstleister, die keine Banken sind, sind gegenüber Banken im Wettbewerb benachteiligt;

– es entstehen wirtschaftliche Ineffizienzen und höhere Kosten für Geschäftstätigkeiten, was sich negativ auf die Wettbewerbsfähigkeit der EU auswirkt;

– der Binnenmarkt für Zahlungen ist zersplittert, und es kommt zu „Forum Shopping“ (Wahl des günstigsten Gerichtsstands).

Mit der Initiative werden vier spezifische Ziele verfolgt, die den festgestellten Problemen entsprechen:

1. Stärkung des Nutzerschutzes und des Vertrauens in Zahlungen;
2. Verbesserung der Wettbewerbsfähigkeit bei Open-Banking-Dienstleistungen;
3. Verbesserung der Durchsetzung und Umsetzung in den Mitgliedstaaten;
4. Verbesserung des (direkten oder indirekten) Zugangs zu Zahlungssystemen und Bankkonten für Zahlungsdienstleister, die keine Banken sind.

[25] Abrufbar über diesen Link: https://data.europa.eu/doi/10.2874/996945.

In der Folgenabschätzung wird ein Paket bevorzugter Optionen vorgestellt, mit denen die spezifischen Ziele erreicht werden sollen (die nachstehende Liste deckt beide in dieser Verordnung und in der begleitenden Richtlinie enthaltenen Maßnahmen ab):

– Für das spezifische Ziel 1 Verbesserungen bei der Anwendung der starken Kundenauthentifizierung, eine Rechtsgrundlage für den Austausch von Informationen über Betrug und eine Verpflichtung zur Aufklärung der Kunden über Betrug, Ausweitung der IBAN-Überprüfung auf alle Überweisungen und bedingte Umkehr der Haftung für Betrug bei autorisierten Push-Zahlungen; eine Verpflichtung der Zahlungsdienstleister, den Zugang zur starken Kundenauthentifizierung für Nutzer mit Behinderungen, ältere Menschen und andere Menschen, die mit Herausforderungen bei der Nutzung der starken Kundenauthentifizierung konfrontiert sind, zu verbessern; Maßnahmen zur Verbesserung der Verfügbarkeit von Barmitteln; Verbesserung der Nutzerrechte und -information.

– Für das spezifische Ziel 2 eine Anforderung an kontoführende Zahlungsdienstleister, eine spezielle Schnittstelle für den Datenzugang einzurichten; „Erlaubnis-Dashboards“, die es den Nutzern ermöglichen, ihre gewährten Open-Banking-Zugangserlaubnisse zu verwalten; detailliertere Spezifikationen der Mindestanforderungen an Open-Banking-Datenschnittstellen.

– Für das spezifische Ziel 3 Ersetzung des überwiegenden Teils der PSD2 durch eine unmittelbar anwendbare Verordnung zur Klärung unklarer oder mehrdeutiger Aspekte der PSD2; Verschärfung der Bestimmungen über Sanktionen; Integration der Zulassungsregelungen für Zahlungsinstitute und E-Geld-Institute.

– Für das spezifische Ziel 4 Stärkung der Rechte von Zahlungsinstituten und E-Geld-Instituten auf ein Bankkonto; Gewährung der Möglichkeit der direkten Beteiligung von Zahlungsinstituten und E-Geld-Instituten an allen Zahlungssystemen, einschließlich derjenigen, die von den Mitgliedstaaten gemäß der Richtlinie über die Wirksamkeit von Abrechnungen benannt wurden, mit zusätzlichen Klarstellungen zu Zulassungs- und Risikobewertungsverfahren.

Eine Reihe von Optionen wurde in der Folgenabschätzung aufgrund hoher Umsetzungskosten und ungewisser Vorteile verworfen. Bei den Kosten der ausgewählten Optionen handelt es sich hauptsächlich um einmalige Kosten, die größtenteils von kontoführenden Zahlungsdienstleistern (im Wesentlichen Banken) getragen werden. Im Bereich des Open Banking werden die Kosten durch Einsparungen (z. B. durch die Abschaffung einer permanenten „Fallback“-Schnittstelle und des entsprechenden Befreiungsverfahrens) und durch die Annahme von Maßnahmen zur Verhältnismäßigkeit (mögliche Ausnahmen für kontoführende Zahlungsdienstleister im Nischenbereich) ausgeglichen. Die Kosten, die den Mitgliedstaaten durch eine verbesserte Durchsetzung und Umsetzung entstehen, werden begrenzt sein. Die Kosten für den direkten Zugang zu wichtigen Zahlungssystemen für Zahlungsinstitute werden begrenzt sein und gehen zulasten der betreffenden Zahlungssysteme. Die Vorteile werden hingegen einem breiten Spektrum von Interessenträgern zugutekommen, darunter den Nutzern von Zahlungsdiensten (Verbrauchern, Unternehmen, Händlern und öffentlichen Verwaltungen) und auch den Zahlungsdienstleistern selbst (insbesondere Zahlungsdienstleistern, die keine Banken sind, aus dem FinTech-Sektor). Der Nutzen wird wiederkehrender Natur sein, während es sich bei den Kosten hauptsächlich um einmalige Anpassungskosten handelt, weshalb der kumulierte Nutzen die Gesamtkosten langfristig übersteigen dürfte.

- **Effizienz der Rechtsetzung und Vereinfachung**

Der vorliegende Vorschlag ist keine Initiative im Rahmen von REFIT (Programm zur Gewährleistung der Effizienz und Leistungsfähigkeit der Rechtsetzung). Dennoch wurden im Rahmen des Bewertungs- und Überprüfungsprozesses Möglichkeiten zur Verwaltungsvereinfachung gesucht. Die Präzisierung der Vorschriften für die starke Kundenauthentifizierung und andere Klarstellungen sowie die Beseitigung von Abweichungen, die sich aus der nationalen Umsetzung einer Richtlinie ergeben, werden zur Vereinfachung beitragen.

- **Grundrechte**

Das Grundrecht, das von dieser Initiative besonders betroffen ist, ist der Schutz personenbezogener Daten. Soweit die Verarbeitung personenbezogener Daten für die Einhaltung dieser Initiative erforderlich ist, ist es verhältnismäßig, das reibungslose Funktionieren des Binnenmarkts für digitale Zahlungen sicherzustellen. Im Rahmen dieser Initiative muss die Verarbeitung personenbezogener Daten im Einklang mit der Datenschutz-Grundverordnung (DSGVO) erfolgen, die unmittelbar für alle von diesem Vorschlag betroffenen Zahlungsdienste gilt.

- **Anwendung des „One-in-one-out"-Grundsatzes**

Die vorliegende Initiative verursacht keine Verwaltungskosten für Unternehmen oder Verbraucher, da die Initiative weder zu einer verstärkten Überwachung oder Beaufsichtigung von Zahlungsdienstleistern noch zu spezifischen neuen Berichtspflichten führen wird, die nicht bereits in der PSD2 enthalten sind. Auch zu einer Gebühren- oder Entgelterhebung kommt es durch diese Initiative nicht. Die Kommission ist daher der Auffassung, dass diese Initiative keine Verwaltungskosten verursacht, die einen Ausgleich nach dem „One-in-one-out"-Grundsatz erfordern, obwohl sie hierfür relevant ist, da sie Durchführungskosten verursacht. Die Zusammenführung der Rechtsvorschriften für E-Geld-Institute und für Zahlungsinstitute wird die Verwaltungskosten senken, indem beispielsweise die Anforderung, unter bestimmten Umständen eine neue Zulassung zu erhalten, abgeschafft wird.

- **Klima und Nachhaltigkeit**

Es wurden keine negativen Auswirkungen der Initiative auf das Klima festgestellt. Die Initiative wird zu Ziel 8.2 der Ziele für nachhaltige Entwicklung der Vereinten Nationen beitragen: „*Eine höhere wirtschaftliche Produktivität durch Diversifizierung, technologische Modernisierung und Innovation erreichen, einschließlich durch Konzentration auf mit hoher Wertschöpfung verbundene und arbeitsintensive Sektoren*".

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Der vorliegende Vorschlag hat keine Auswirkungen auf den EU-Haushalt.

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Die Initiative sieht eine Überprüfung fünf Jahre nach Geltungsbeginn vor. Besondere Aufmerksamkeit gilt dabei den Bestimmungen über Open Banking, Gebühren und Entgelte

für Zahlungsdienste sowie Vorschriften über die Haftung und Entschädigung bei betrügerischen Transaktionen.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Der Vorschlag enthält Vorschriften für Zahlungsdienstleister im Zusammenhang mit Zahlungen. Durch den Vorschlag ergeben sich keine Änderungen an der in der PSD2 festgelegten Liste der Zahlungsdienste. Die Liste der Ausschlüsse ist weitgehend unverändert. Es gibt eine Liste von Begriffsbestimmungen, die von der Liste in der PSD2 erweitert wird und mehr Begriffe und Klarstellungen zu bestimmten Begriffen enthält. Es werden Definitionen der Begriffe „von Händlern ausgelöste Zahlungsvorgänge“ und „Bestellungen per Post oder Telefon“ eingeführt. Die Definition des Begriffs „Fernzahlungsvorgang“ in der PSD2 wird optimiert, um eine klarere Abgrenzung der Begriffe „Initiierung eines Zahlungsvorgangs“ und „Fernauslösung eines Zahlungsvorgangs“ zu ermöglichen.

Zahlungssysteme und Zugang zu Konten bei Kreditinstituten

Was die Betreiber von Zahlungssystemen betrifft, so wird die Anforderung, über Zugangsregeln und -verfahren zu verfügen, die verhältnismäßig und nichtdiskriminierend sind, auch auf Zahlungssysteme ausgedehnt, die von einem Mitgliedstaat gemäß der Richtlinie 98/26 (Richtlinie über die Wirksamkeit von Abrechnungen[26]) benannt wurden. Betreiber von Zahlungssystemen sind verpflichtet, bei der Prüfung eines Antrags auf Teilnahme eines Zahlungsdienstleisters eine Bewertung der relevanten Risiken vorzunehmen. Eine Entscheidung über einen Antrag muss schriftlich erfolgen und es wird ein Recht auf Einlegung eines Rechtsbehelfs festgelegt. In Fällen, in denen keine Aufsicht durch das Europäische System der Zentralbanken besteht, müssen die zuständigen Behörden von den Mitgliedstaaten benannt werden; wo eine Aufsicht durch den ESZB besteht, kann diese herangezogen werden, um Unzulänglichkeiten bei den Zulassungsvorschriften und -verfahren von Zahlungssystemen zu beheben.

Die Vorschriften für den Zugang (Eröffnen und Schließen) eines Zahlungsinstituts zu einem Konto bei einem Kreditinstitut werden gegenüber der PSD2 verschärft. Auch Antragsteller, die eine Zulassung als Zahlungsinstitut beantragen (da sie über ein Bankkonto verfügen müssen, um ihre Zulassung zu erhalten), sowie die Agenten und Vertriebsstellen des Zahlungsinstituts fallen ebenfalls darunter. Die Verweigerung oder der Entzug des Zugangs muss auf schwerwiegende Gründe gestützt werden, z. B. auf den begründeten Verdacht einer rechtswidrigen Tätigkeit oder eines Risikos für das Kreditinstitut. Die Gründe für die Verweigerung oder den Entzug des Zugangs sind schriftlich und ausführlich im Hinblick auf die besondere Situation des betreffenden Zahlungsinstituts anzugeben.

Transparenz der Vertragsbedingungen und Informationspflichten für Zahlungsdienste

In Bezug auf die Ausnahme von den Informationspflichten für Zahlungsinstrumente von geringem Wert und E-Geld für nationale Zahlungsvorgänge wird die Möglichkeit für die Mitgliedstaaten gestrichen, die Ausgabenobergrenzen anzupassen.

Um interne Kohärenz sicherzustellen, wird die Verpflichtung, den Zahlungsdienstnutzer in Rahmenverträgen über alternative Streitbeilegungsverfahren zu informieren, auf Einzelzahlungen ausgeweitet.

[26] Diese Änderung muss zusammen mit einer gezielten Änderung der Richtlinie über die Wirksamkeit von Abrechnungen geprüft werden, die im begleitenden Vorschlag für eine Zahlungsdiensterichtlinie enthalten ist.

Es wird klargestellt, dass Zahlungsdienstleister in die Kontoauszüge die zur eindeutigen Identifizierung des Zahlungsempfängers erforderlichen Angaben, einschließlich eines Verweises auf den Handelsnamen des Zahlungsempfängers, eintragen.

Es wird klargestellt, dass Zahlungsdienste, die gemeinsam mit technischen Diensten angeboten werden, die die Erbringung von Zahlungsdiensten unterstützen und von dem Zahlungsdienstleister oder einem Dritten erbracht werden, mit dem sie zusammenarbeiten, den Anforderungen des Rahmenvertrags in Bezug auf Kündigungsgebühren unterliegen sollten.

Zusätzliche Informationsanforderungen für inländische Geldautomatenabhebungen werden für verschiedene Szenarien eingeführt.

In Bezug auf Überweisungen und Finanztransfers aus der EU in ein Nicht-EU-Land wird eine Verpflichtung für Zahlungsdienstleister eingeführt, dem Zahlungsdienstnutzer die voraussichtliche Frist bis zum Eingang des Geldes bei den Zahlungsdienstleistern des Zahlungsempfängers mit Sitz außerhalb der EU zur Verfügung zu stellen. Um eine bessere Vergleichbarkeit zu erreichen, müssen die geschätzten Währungsumrechnungsentgelte solcher internationaler Transaktionen in derselben Weise ausgedrückt werden wie für Überweisungen innerhalb der EU, d. h. als prozentualer Aufschlag gegenüber den neuesten verfügbaren Euro-Referenzwechselkursen der EZB.

Rechte und Pflichten bei der Erbringung und Nutzung von Zahlungsdiensten

Gemeinsame Bestimmungen

Gemäß der PSD2 ist das Verbot von Entgeltaufschlägen, das Zahlungsdienste umfasst, für die die Interbankenentgelt-Verordnung[27] gilt, in der PSD2 auf Überweisungen und Lastschriften beschränkt, die auf Euro und nicht auf andere Währungen der EU lauten. Es werden Änderungen eingeführt, um das Verbot von Aufschlägen auf Überweisungen und Lastschriften in allen Währungen der EU auszuweiten.

Die Vorschriften für von Händlern ausgelöste Zahlungsvorgänge und Lastschriften werden angeglichen und es werden dieselben Verbraucherschutzmaßnahmen wie Erstattungen auf Lastschriften und von Händlern ausgelöste Zahlungsvorgänge angewendet, da beide vom Zahlungsempfänger veranlasste Transaktionen sind.

Open Banking (Kontoinformationsdienste und Zahlungsauslösedienste)

Die Bestimmungen zum Open Banking enthalten eine Reihe von Änderungen gegenüber der PSD2 und es werden einige Bestimmungen aufgenommen, die derzeit in einem technischen Regulierungsstandard enthalten sind[28]. Zu den wichtigsten Änderungen gehören – außer in Ausnahmefällen – die Einführung einer speziellen Schnittstelle für den Zugang zu Open-Banking-Daten und die Aufhebung – außer unter genehmigten außergewöhnlichen Umständen – der Anforderung, dass kontoführende Zahlungsdienstleister dauerhaft eine „Fallback"-Schnittstelle unterhalten müssen. Es werden zusätzliche Anforderungen an dedizierte Schnittstellen in Bezug auf Leistung und Funktionen eingeführt. Um Open-Banking-Nutzer in die Lage zu versetzen, ihre Open-Banking-Erlaubnisse auf bequeme Weise zu verwalten, müssen kontoführende Zahlungsdienstleister ihnen ein „Dashboard" zur

[27] Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge.

[28] Delegierte Verordnung 2018/389 der Kommission zu technischen Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation.

Verfügung stellen, das es ermöglicht, jedem Open-Banking-Anbieter die Datenzugangserlaubnis wieder zu entziehen.

Es gab keine nennenswerte Nachfrage auf dem Markt für die spezifische Dienstleistung der Bestätigung der Verfügbarkeit von Mitteln, die von Artikel 65 der PSD2 als Open-Banking-Dienst neben Kontoinformationen und Zahlungsauslösediensten abgedeckt wurde. Auf der Grundlage dieses Dienstes wurden, wenn überhaupt, nur sehr wenige Geschäftsmodelle entwickelt, da der Markt auf die Nutzung von Kontoinformationsdiensten als Alternative zur Überprüfung der Verfügbarkeit von Mitteln angewiesen ist. Diese Bestimmung wurde daher als eigenständiger Open-Banking-Dienst gestrichen.

Autorisierung von Zahlungsvorgängen

Der Zahlungsdienstleister des Zahlungsempfängers ist verpflichtet, seinem Zahlungsdienstnutzer auf Anfrage einen Service zur Verfügung zu stellen, mit dem überprüft wird, ob der Kundenidentifikator des Zahlungsempfängers mit dem vom Zahler angegebenen Namen des Zahlungsempfängers übereinstimmt, und dem Zahlungsdienstleister des Zahlers jede festgestellte Abweichung mitgeteilt wird. Stimmen diese nicht überein, so teilt der Zahlungsdienstleister des Zahlers dem Zahler jedwede Abweichung und den festgestellten Grad der Abweichung mit. In dem Vorschlag der Kommission über Sofortzahlungen zur Änderung der SEPA-Verordnung[29], der derzeit von den Gesetzgebern erörtert wird, wird eine ähnliche Bestimmung in Bezug auf die Diskrepanzen zwischen dem Namen und dem Kundenidentifikator eines Zahlungsempfängers bei Sofortüberweisungen in Euro vorgeschlagen. Um einen kohärenten Rahmen für alle Überweisungen zu schaffen, gilt die Bestimmung dieses Vorschlags für Überweisungen, bei denen es sich nicht um Sofortüberweisungen in Währungen der Union handelt, und für Sofortüberweisungen in anderen Währungen als dem Euro. Eine solche Benachrichtigung muss erfolgen, bevor der Zahler den Zahlungsauftrag abschließt und bevor der Zahlungsdienstleister die Überweisung ausführt. Dem Nutzer bleibt in jedem Fall freigestellt, ob er den Zahlungsauftrag für eine Überweisung dennoch erteilen will.

In Bezug auf die Bestimmung über die Obergrenzen für die Nutzung eines Zahlungsinstruments wird klargestellt, dass Zahlungsdienstleister die mit ihren Zahlungsdienstnutzern vereinbarten Ausgabenobergrenzen nicht einseitig erhöhen dürfen.

In der Bestimmung über die Haftung des Zahlungsdienstleisters für nicht autorisierte Zahlungsvorgänge wird klargestellt, dass nur ein begründeter Verdacht auf Betrug durch den Zahler zu einer Verweigerung der Erstattung durch den Zahlungsdienstleister führen kann. In einem solchen Fall muss der Zahlungsdienstleister eine Begründung für die Ablehnung der Erstattung vorlegen und die Stellen angeben, an die sich der Zahler wenden kann.

Der Zahlungsdienstleister des Zahlers haftet für den vollen Betrag der Überweisung, wenn der Zahlungsdienstleister es versäumt hat, dem Zahler eine festgestellte Diskrepanz zwischen dem vom Zahler angegebenen Kundenidentifikator und dem vom Zahler angegebenen Namen des Zahlungsempfängers mitzuteilen. Ein Zahlungsdienstleister haftet, wenn ein Verbraucher von einem Dritten, der sich als Mitarbeiter des Zahlungsdienstleisters des Verbrauchers ausgibt, durch Lügen oder Täuschung zur Autorisierung eines Zahlungsvorgangs verleitet wurde. Es wird eine Verpflichtung für Anbieter elektronischer Kommunikationsdienste eingeführt, mit den Zahlungsdienstleistern zusammenzuarbeiten, um solchen Betrug zu verhindern.

[29] Vorschlag COM(2022) 546 final vom 26. Oktober 2022 zur Änderung der Verordnung (EU) Nr. 260/2012.

Ist die Haftung dem Zahlungsdienstleister des Zahlungsempfängers zuzurechnen, so hat dieser den finanziellen Schaden zu erstatten, der dem Zahlungsdienstleister des Zahlers entstanden ist. Die Bestimmungen über die Anzeige und Korrektur nicht autorisierter oder fehlerhaft ausgeführter Zahlungsvorgänge, die Informationspflichten und der Regressanspruch werden aktualisiert, um der neuen Haftungsregelung für die fehlerhafte Anwendung des Abgleichservice Rechnung zu tragen.

Neue Haftungsbestimmungen für Anbieter technischer Dienste und Betreiber von Zahlungssystemen werden vorgesehen, wenn eine starke Kundenauthentifizierung nicht unterstützt wird, da die Bewertung der PSD2 ergeben hat, dass es Probleme bei der Umsetzung der starken Kundenauthentifizierung gab, die mit den Rollen dieser Interessenträger bei der Einführung der starken Kundenauthentifizierung in Zusammenhang standen, was sogar dazu beigetragen hat, dass die Anwendung der starken Kundenauthentifizierung von 2018 auf 2020 verschoben wurde.

Es wird klargestellt, dass der Zahler keine finanziellen Verluste zu tragen hat, wenn entweder der Zahlungsdienstleister des Zahlers oder des Zahlungsempfängers von der Anwendung einer starken Kundenauthentifizierung befreit sind.

Für Zahlungsvorgänge, bei denen der Transaktionsbetrag nicht im Voraus bekannt ist und Geld auf einem Zahlungsinstrument blockiert wird, wird eine rechtliche Verpflichtung für den Zahlungsempfänger eingeführt, dem Zahlungsdienstleister den genauen Betrag des Zahlungsvorgangs unmittelbar nach Erbringung der Dienstleistung bzw. Lieferung der Waren an den Zahler mitzuteilen, und die Anforderung, dass der blockierte Geldbetrag in angemessenem Verhältnis zum Betrag des künftigen Zahlungsvorgangs stehen muss, der zum Zeitpunkt der Blockierung vernünftigerweise zu erwarten ist.

Ausführung von Zahlungsvorgängen

In Fällen, in denen ein Zahlungsauslösedienstleister einen falschen Kundenidentifikator eines Zahlungsempfängers bereitstellt, wird dieser Zahlungsauslösedienstleister für den Betrag des Zahlungsvorgangs haftbar gemacht.

Datenschutz

Es wird eine neue Bestimmung aufgenommen, um ein wesentliches öffentliches Interesse, für das die Verarbeitung besonderer Kategorien personenbezogener Daten im Zusammenhang mit dieser vorgeschlagenen Verordnung erforderlich sein könnte, ausdrücklich zu definieren.

Operationelle und sicherheitsrelevante Risiken und Authentifizierung

Es wird eine neue Bestimmung hinzugefügt, wonach Zahlungsdienstleister über Mechanismen zur Überwachung von Transaktionen verfügen müssen, um die Anwendung einer starken Kundenauthentifizierung sicherzustellen und betrügerische Transaktionen besser zu verhindern und aufzudecken. Mit dieser Bestimmung wird der Begriff „Inhärenz“ klarer gefasst, indem präzisiert wird, dass solche Mechanismen zur Überwachung von Transaktionen auf der Analyse von Zahlungsvorgängen beruhen müssen, wobei Elemente zu berücksichtigen sind, die für den Zahlungsdienstnutzer bei einer normalen Verwendung der personalisierten Sicherheitsmerkmale typisch sind, einschließlich umgebungs- und verhaltensbezogener Merkmale, z. B. im Zusammenhang mit dem Standort des Zahlungsdienstnutzers, dem Zeitpunkt der Transaktion, der Nutzung des Geräts, den Ausgabengewohnheiten und dem Online-Geschäft, in dem der Kauf getätigt wird.

Für die Zwecke der Transaktionsüberwachung wurden Bestimmungen hinzugefügt, die es Zahlungsdienstleistern ermöglichen, auf freiwilliger Basis personenbezogene Daten wie Kundenidentifikatoren eines Zahlungsempfängers auszutauschen, die Vereinbarungen über

den Informationsaustausch unterliegen. In diesen Vereinbarungen über den Informationsaustausch müssen Einzelheiten für die Teilnahme und die operativen Elemente, einschließlich der Nutzung spezieller IT-Plattformen, festgelegt werden. Vor dem Abschluss solcher Vereinbarungen müssen die Zahlungsdienstleister gemäß der Verordnung (EU) 2016/679 eine Datenschutz-Folgenabschätzung durchführen und gegebenenfalls vorab die Aufsichtsbehörde konsultieren.

In Bezug auf die Anwendung der starken Kundenauthentifizierung bei von Händlern ausgelösten Zahlungsvorgängen wird klargestellt, dass bei der Festlegung des Mandats eine starke Kundenauthentifizierung erforderlich ist, ohne dass sie jedoch bei nachfolgenden von Händlern ausgelösten Zahlungsvorgängen angewendet werden muss. In Bezug auf die Anwendung der starken Kundenauthentifizierung im Falle von Bestellungen per Post oder Telefon wird klargestellt, dass es ausreicht, wenn die Auslösung eines Zahlungsvorgangs nicht digital ist, damit dieser Vorgang nicht unter die Verpflichtungen zur starken Kundenauthentifizierung fällt. Zahlungsvorgänge auf der Grundlage von beleghaften Zahlungsaufträgen oder Bestellungen per Post oder Telefon des Zahlers sollten jedoch Sicherheitsstandards und Kontrollen durch den Zahlungsdienstleister des Zahlers unterworfen werden, die eine Authentifizierung des Zahlungsvorgangs ermöglichen, um eine missbräuchliche Umgehung der Anforderungen an die starke Authentifizierung zu verhindern. Darüber hinaus wurde der Anwendungsbereich der Befreiung von der starken Kundenauthentifizierung bei Zahlungsvorgängen eingeschränkt, bei denen der Zahlungsempfänger Zahlungsaufträge auf der Grundlage eines vom Zahler erteilten Mandats erteilt (Lastschriften), während eine Verpflichtung zur Anforderung der starken Kundenauthentifizierung in Fällen eingeführt wurde, in denen ein Mandat über einen Fernzugang unter direkter Beteiligung eines Zahlungsdienstleisters erteilt wird.

Eine starke Kundenauthentifizierung ist nur für Kontoinformationsdienste anlässlich des ersten Datenzugangs erforderlich; Kontoinformationsdienstleister müssen jedoch mindestens alle 180 Tage eine starke Kundenauthentifizierung verlangen, wenn ihre Kunden auf aggregierte Kontodaten auf der Domain des Kontoinformationsdienstleisters zugreifen.

Es wurden Bestimmungen hinzugefügt, um die Zugänglichkeit der starken Kundenauthentifizierung zu verbessern, insbesondere um sicherzustellen, dass alle Kunden, einschließlich Menschen mit Behinderungen, ältere Menschen, Menschen mit geringen digitalen Kompetenzen und Personen, die keinen Zugang zu digitalen Kanälen oder einem Smartphone haben, über mindestens ein Mittel verfügen, das ihnen eine starke Kundenauthentifizierung ermöglicht.

In Bezug auf die Anforderung von „Fernzahlungen“ für Zahlungsdienstleister, eine starke Kundenauthentifizierung anzuwenden, die Elemente umfasst, die die Transaktion dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen, wird klargestellt, dass diese Verpflichtung für elektronische Zahlungsvorgänge gilt, für die ein Zahlungsauftrag über ein Gerät eines Zahlers unter Verwendung von Nahbereichstechnik für den Informationsaustausch mit der Infrastruktur des Zahlungsempfängers erteilt wird und bei denen die Durchführung einer starken Kundenauthentifizierung die Nutzung des Internets auf dem Gerät des Zahlers erfordert.

Es gibt eine Bestimmung, nach der Zahlungsdienstleister und technische Dienstleister verpflichtet sind, Outsourcing-Vereinbarungen zu schließen, wenn letztere die Elemente einer starken Kundenauthentifizierung bereitstellen und überprüfen.

Produktinterventionsbefugnisse der Europäischen Bankenaufsichtsbehörde

Mit diesem Vorschlag werden der EBA im Einklang mit Artikel 9 Absatz 5 der Verordnung (EU) Nr. 1093/2010 Befugnisse zur Produktintervention übertragen. Dies wird es der EBA ermöglichen, auf der Grundlage einer Reihe von Kriterien den Verkauf bestimmter Zahlungsprodukte, die mit bestimmten Risiken verbunden wären, vorübergehend zu untersagen.

Sonstige Bestimmungen

Ermächtigungen sind für technische Regulierungsstandards, die von der EBA ausgearbeitet werden, einschließlich bestehender technischer Regulierungsstandards, und in bestimmten Fällen für neue technische Regulierungsstandards vorgesehen. Die EBA kann bestehende technische Regulierungsstandards ändern; geschieht dies jedoch nicht, bleiben sie in Kraft.

Die vorgeschlagene Verordnung wird am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt in Kraft treten und 18 Monate danach zur Anwendung kommen[30]. Eine Entsprechungstabelle der Artikel in Bezug auf die entsprechenden Artikel der PSD2 und der E-Geld-Richtlinie ist beigefügt.

[30] Dieses Datum ist auf die Umsetzungsfrist der begleitenden Zahlungsdiensterichtlinie abgestimmt.

2023/0210 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/2010

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[31],

nach Stellungnahme der Europäischen Zentralbank[32],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Seit der Annahme der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates[33] hat sich der Markt für Massenzahlungsdienste vor allem durch die zunehmende Nutzung von Karten und anderen digitalen Zahlungsmitteln, die abnehmende Verwendung von Bargeld und die zunehmende Präsenz neuer Akteure und Dienste, einschließlich digitaler Brieftaschen und kontaktloser Zahlungen, erheblich verändert. Die COVID-19-Pandemie und der damit einhergehende Wandel im Hinblick auf Konsum- und Zahlungspraktiken haben dazu geführt, dass sichere und effiziente Zahlungen immer wichtiger geworden sind.

(2) In der Mitteilung der Kommission über eine EU-Strategie für den Massenzahlungsverkehr[34] wurde die Einleitung einer umfassenden Überprüfung der Anwendung und der Auswirkungen der Richtlinie (EU) 2015/2366 angekündigt, „*die eine Gesamtbewertung der Frage umfassen sollte, ob sie unter Berücksichtigung der Marktentwicklungen noch zweckmäßig ist*“.

(3) Mit der Richtlinie (EU) 2015/2366 wurde das Ziel verfolgt, Hindernisse für neue Arten von Zahlungsdiensten zu beseitigen und das Niveau des Verbraucherschutzes

---

31 ABl. C … vom …, S. ….

32 ABl. C … vom …, S. ….

33 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, 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

34 COM(2020) 592 final.

und der Sicherheit zu verbessern. Die Bewertung der Auswirkungen und der Anwendung der Richtlinie (EU) 2015/2366 durch die Kommission ergab, dass die Richtlinie (EU) 2015/2366 in Bezug auf viele ihrer Ziele weitgehend erfolgreich war, es wurden jedoch auch bestimmte Bereiche ermittelt, in denen die Ziele dieser Richtlinie nicht vollständig erreicht wurden. So wurde in der Bewertung beispielsweise festgestellt, dass die Zunahme neuer Arten von Betrug ein Problem darstellt, das im Hinblick auf die Ziele des Verbraucherschutzes Anlass zur Sorge gibt. Mängel wurden auch im Hinblick auf das Ziel festgestellt, den Wettbewerb auf dem Markt dank der sogenannten „Open-Banking-Dienste“ (Kontoinformationsdienste und Zahlungsauslösedienste) zu verbessern, indem Markthindernisse für Drittanbieter abgebaut werden. Auch bei der Verwirklichung des Ziels, die Erbringung grenzüberschreitender Zahlungsdienste zu verbessern, wurden nur begrenzte Fortschritte erzielt, was vor allem auf uneinheitliche Aufsichtspraktiken und Rechtsdurchsetzung in der Union zurückzuführen ist. Bei der Bewertung wurden auch Faktoren ermittelt, die die Fortschritte im Hinblick auf das Ziel, gleiche Wettbewerbsbedingungen für alle Zahlungsdienstleister zu schaffen, behindern.

(4) Bei der Bewertung wurden auch Probleme im Zusammenhang mit der unterschiedlichen Umsetzung und Durchsetzung der Richtlinie (EU) 2015/2366 festgestellt, die sich unmittelbar auf den Wettbewerb zwischen Zahlungsdienstleistern auswirken, indem in den einzelnen Mitgliedstaaten unterschiedliche Regulierungsbedingungen geschaffen werden, was Aufsichtsarbitrage begünstigt. Es sollte keinen Raum für „Forum Shopping“ geben, bei dem sich Zahlungsdienstleister als „Herkunftsland“ diejenigen Mitgliedstaaten aussuchen, in denen die Anwendung der Unionsvorschriften über Zahlungsdienste für sie vorteilhafter ist, und grenzüberschreitende Dienste in anderen Mitgliedstaaten erbringen, die die Vorschriften strenger auslegen oder aktivere Durchsetzungsmaßnahmen auf dort niedergelassene Zahlungsdienstleister anwenden. Diese Praxis verfälscht den Wettbewerb. Die Unionsvorschriften über Zahlungsdienste sollten daher weiter harmonisiert werden, indem Vorschriften über die Ausübung der Zahlungsdienstetätigkeit, einschließlich der Rechte und Pflichten der Beteiligten, in eine Verordnung aufgenommen werden. Diese Vorschriften, mit Ausnahme der Vorschriften über die Zulassung und Beaufsichtigung von Zahlungsinstituten, die in einer Richtlinie verbleiben sollten, sollten präzisiert und detaillierter formuliert werden, um die Auslegungsspielräume so gering wie möglich zu halten.

(5) Obwohl die Ausgabe von E-Geld durch die Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates[35] geregelt ist, wird die Verwendung von E-Geld zur Finanzierung von Zahlungsvorgängen weitgehend durch die Richtlinie (EU) 2015/2366 geregelt. Folglich ist der Rechtsrahmen für E-Geld-Institute und Zahlungsinstitute, insbesondere in Bezug auf die Wohlverhaltensregeln, bereits weitgehend angeglichen. Um die externen Kohärenzfragen anzugehen und angesichts der Tatsache, dass E-Geld-Dienste und Zahlungsdienste immer schwieriger voneinander zu unterscheiden sind, sollten die rechtlichen Rahmenbedingungen für E-Geld-Institute und Zahlungsinstitute einander angenähert werden. Allerdings unterscheiden sich die Zulassungsanforderungen, insbesondere das Anfangskapital

[35] Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG (ABl. L 267 vom 10.10.2009, S. 7).

und die Eigenmittel, und einige grundlegende Schlüsselkonzepte für das E-Geld-Geschäft, wie z. B. die Ausgabe, Verteilung und Rücktauschbarkeit von E-Geld, von den von Zahlungsinstituten erbrachten Dienstleistungen. Diese Besonderheiten sollten daher bei der Zusammenführung der Bestimmungen der Richtlinie (EU) 2015/2366 und der Richtlinie 2009/110/EG beibehalten werden. Da die Richtlinie 2009/110/EG durch die Richtlinie (EU) XXXX [PSD3] aufgehoben wird, sollten ihre Vorschriften, mit Ausnahme der Zulassungs- und Aufsichtsvorschriften, die in die Richtlinie (EU) XXX [PSD3] aufgenommen wurden, mit geeigneten Anpassungen in einen einheitlichen Rahmen gemäß der vorliegenden Verordnung gebracht werden.

(6) Um Rechtssicherheit und einen klaren Anwendungsbereich der Wohlverhaltensregeln bei der Erbringung von Zahlungs- und E-Geld-Diensten sicherzustellen, ist es erforderlich, die Kategorien von Zahlungsdienstleistern zu spezifizieren, die den Pflichten in Bezug auf die Ausübung der Geschäftstätigkeit bei der Erbringung von Zahlungsdiensten und E-Geld-Diensten in der gesamten Union unterliegen.

(7) Es gibt mehrere Kategorien von Zahlungsdienstleistern. Kreditinstitute nehmen Einlagen von Nutzern entgegen, die zur Ausführung von Zahlungsvorgängen verwendet werden können. Sie sind gemäß der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates[36] zugelassen. Zahlungsinstitute nehmen keine Einlagen entgegen. Sie können Nutzergeld halten und E-Geld ausgeben, das zur Ausführung von Zahlungsvorgängen verwendet werden kann. Sie sind gemäß der Richtlinie (EU) XXX [PSD3] zugelassen. Postscheckämter, die nach einzelstaatlichem Recht hierzu berechtigt sind, können auch E-Geld-Dienste und Zahlungsdienste erbringen. Weitere Kategorien von Zahlungsdienstleistern sind die Europäische Zentralbank (EZB) und die nationalen Zentralbanken, wenn sie nicht in ihrer Eigenschaft als Währungsbehörde oder andere Behörden handeln, und Mitgliedstaaten oder ihre regionalen oder lokalen Gebietskörperschaften, wenn sie nicht in ihrer Eigenschaft als Behörden handeln.

(8) Es ist angezeigt, den Dienst, der die Möglichkeit bietet, Bargeld von einem Zahlungskonto abzuheben, von der Tätigkeit der Führung eines Zahlungskontos zu trennen, da die Anbieter von Bargeldabhebungsdiensten keine Zahlungskonten führen dürfen. Die unter Nummer 5 des Anhangs der Richtlinie (EU) 2015/2366 zusammen aufgeführten Dienste der Ausgabe von Zahlungsinstrumenten sowie der Annahme und Abrechnung („Acquiring“) von Zahlungsvorgängen sollten als zwei verschiedene Zahlungsdienste dargestellt werden, als ob eine Dienstleistung ohne die andere nicht angeboten werden könnte. Eine gesonderte Auflistung der Ausgabe- und Acquiring-Dienste sollte zusammen mit unterschiedlichen Definitionen der einzelnen Dienste klarstellen, dass die Ausgabe- und Acquiring-Dienste von Zahlungsdienstleistern getrennt angeboten werden können.

(9) Der Ausschluss bestimmter Kategorien von Betreibern von Geldautomaten aus dem Anwendungsbereich der Richtlinie (EU) 2015/2366 hat sich in der Praxis als schwierig erwiesen. Daher sollte die Kategorie der Geldautomatenbetreiber, die gemäß der Richtlinie (EU) 2015/2366 von der Anforderung einer Zulassung als Zahlungsdienstleister ausgenommen waren, durch eine neue Kategorie von

[36] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

Geldautomatenbetreibern ersetzt werden, die keine Zahlungskonten führen. Diese Betreiber unterliegen zwar nicht den Zulassungsanforderungen der Richtlinie (EU) XXX [PSD3], sollten jedoch dann, wenn diese Geldautomatenbetreiber für Bargeldabhebungen Entgelte erheben, den Anforderungen an die Gebührentransparenz unterliegen.

(10) Um den Zugang zu Bargeld weiter zu verbessern, was eine Priorität der Kommission darstellt, sollte es Händlern gestattet sein, im stationären Handel, auch wenn der Kunde keinen Kauf tätigt, Bargeldbereitstellungsdienste anzubieten, ohne eine Zulassung als Zahlungsdienstleister beantragen oder als Agent eines Zahlungsinstituts auftreten zu müssen. Diese Bargeldbereitstellungsdienste sollten jedoch der Verpflichtung unterliegen, dem Kunden gegebenenfalls in Rechnung gestellte Entgelte offenzulegen. Diese Dienstleistungen sollten von Einzelhändlern auf freiwilliger Basis erbracht werden und von der Verfügbarkeit von Bargeld beim betreffenden Einzelhändler abhängen.

(11) Die Ausnahme vom Anwendungsbereich der Richtlinie (EU) 2015/2366 für Zahlungsvorgänge zwischen Zahler und Zahlungsempfänger über einen im Auftrag des Zahlers oder des Zahlungsempfängers handelnden Handelsvertreter wurde in den Mitgliedstaaten sehr unterschiedlich angewandt. Der Begriff des Handelsvertreters wird typischerweise im nationalen Zivilrecht definiert, das von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein kann, was zu einer uneinheitlichen Behandlung derselben Dienstleistungen in verschiedenen Rechtsräumen führt. Der Begriff des Handelsvertreters, der unter diese Ausnahme fällt, sollte daher harmonisiert und präzisiert werden, indem auf die Definition des Handelsvertreters gemäß der Richtlinie 86/653/EWG des Rates[37] verwiesen wird. Darüber hinaus sollte mehr Klarheit darüber geschaffen werden, unter welchen Bedingungen Zahlungsvorgänge vom Zahler an den Zahlungsempfänger über Handelsvertreter vom Anwendungsbereich dieser Verordnung ausgenommen werden können. Dies wird dadurch erreicht, dass Vertreter durch eine Vereinbarung mit dem Zahler oder dem Zahlungsempfänger ermächtigt werden sollten, den Verkauf oder den Kauf von Waren oder Dienstleistungen allein im Namen des Zahlers oder des Zahlungsempfängers, aber nicht beider, auszuhandeln oder abzuschließen, unabhängig davon, ob der Handelsvertreter im Besitz des Geldes des Kunden ist oder nicht. Plattformen für den elektronischen Geschäftsverkehr, die sowohl für einzelne Käufer als auch für Verkäufer als Handelsvertreter fungieren, ohne dass Käufer oder Verkäufer über eine echte Marge oder Autonomie verfügen, um den Verkauf oder den Kauf von Waren oder Dienstleistungen auszuhandeln oder abzuschließen, sollten nicht vom Anwendungsbereich dieser Verordnung ausgenommen werden. Die Europäische Bankenaufsichtsbehörde (EBA) sollte Leitlinien für den Ausschluss von Zahlungsvorgängen vom Zahler zum Zahlungsempfänger über einen Handelsvertreter ausarbeiten, um für mehr Klarheit und Konvergenz zwischen den zuständigen Behörden zu sorgen. Diese Leitlinien können ein Verzeichnis der Anwendungsfälle umfassen, die typischerweise unter die Ausnahme für Handelsvertreter fallen.

(12) Die Ausnahme vom Anwendungsbereich der Richtlinie (EU) 2015/2366 in Bezug auf Instrumente mit besonderer Zweckbestimmung wurde in den Mitgliedstaaten unterschiedlich angewandt, obwohl Dienstleister, deren Instrumente unter diese Ausnahme fielen, verpflichtet waren, ihre Tätigkeit den zuständigen Behörden zu

[37] Richtlinie 86/653/EWG des Rates vom 18. Dezember 1986 zur Koordinierung der Rechtsvorschriften der Mitgliedstaaten betreffend die selbstständigen Handelsvertreter (ABl. L 382 vom 31.12.1986, S. 17).

melden. Weitere Empfehlungen gab die EBA in ihren „*Leitlinien über die Ausnahme für begrenzte Netze gemäß der PSD2*“ vom 24. Februar 2022[38]. Trotz dieser Versuche, die Anwendung der Ausnahme in Bezug auf spezielle Instrumente zu klären, gibt es nach wie vor Dienstleister, die Dienste anbieten, die erhebliche Zahlungsvolumen mit sich bringen, und eine Vielzahl von Produkten, die einer großen Zahl von Kunden angeboten werden, die beabsichtigen, von dieser Ausnahme Gebrauch zu machen. In diesen Fällen profitieren die Verbraucher nicht von den erforderlichen Schutzvorkehrungen und die Dienste sollten nicht von der Ausnahme für spezielle Instrumente profitieren. Daher muss klargestellt werden, dass dasselbe zweckbestimmte Instrument nicht für Zahlungsvorgänge zum Erwerb von Waren und Dienstleistungen in mehr als einem begrenzten Netz oder zum Erwerb eines unbegrenzten Waren- oder Dienstleistungsspektrums verwendet werden kann.

(13) Um zu beurteilen, ob ein begrenztes Netz vom Anwendungsbereich ausgenommen werden sollte, sollten die geografische Lage der Annahmestellen eines solchen Netzes sowie die Zahl der Annahmestellen berücksichtigt werden. Zweckbestimmte Instrumente sollten es dem Inhaber ermöglichen, Waren oder Dienstleistungen nur in den stationären Räumlichkeiten des Ausstellers zu erwerben, während die Nutzung in der Umgebung eines Online-Geschäfts nicht unter den Begriff der Räumlichkeiten des Ausstellers fallen sollte. Zu den zweckbestimmten Instrumenten sollten je nach den jeweiligen vertraglichen Regelungen Karten gehören, die nur in einer bestimmten Kette von Geschäften oder in einem bestimmten Einkaufszentrum verwendet werden können, sowie Tankkarten, Mitgliedskarten, Fahrkarten für öffentliche Verkehrsmittel, Parkkarten, Essensgutscheine oder Gutscheine für bestimmte Dienstleistungen, die einem spezifischen steuer- oder arbeitsrechtlichen Rahmen zur Förderung des Einsatzes solcher Instrumente unterliegen können, um die in den Sozialvorschriften festgelegten Ziele zu erreichen, wie etwa Kinderbetreuungsgutscheine oder ökologische Gutscheine. Zweckbestimmte Instrumente sollten auch E-Geld-basierte Instrumente umfassen, sobald sie die Anforderungen dieser Ausnahme erfüllen. Zahlungsinstrumente, die für Einkäufe in den Geschäften der teilnehmenden Händler verwendet werden können, sollten nicht ausgenommen sein, da sie in der Regel für ein stetig wachsendes Netz von Dienstleistern gedacht sind.

(14) Die Ausnahme für Zahlungsvorgänge, die über ein Telekommunikations- oder IT-Gerät ausgeführt werden, sollte speziell auf Kleinstbetragszahlungen für digitale Inhalte und Sprachdienste ausgerichtet werden. Es sollte ein deutlicher Hinweis auf Zahlungsvorgänge für den Erwerb von elektronischen Tickets beibehalten werden, damit Kunden von jedem Ort aus und zu jeder Zeit einfach über ihr Mobiltelefon oder ein anderes Gerät elektronische Tickets bestellen, bezahlen, erhalten und validieren können. Elektronische Tickets ermöglichen und erleichtern die Bereitstellung von Diensten, die die Kunden andernfalls in Papierform erwerben würden, und gelten in den Bereichen Beförderung, Unterhaltung, Parken und Eintritt zu Veranstaltungen, jedoch nicht für körperliche Waren. Zahlungsvorgänge eines bestimmten Anbieters elektronischer Kommunikationsnetze, die von oder über ein elektronisches Gerät ausgeführt und auf der entsprechenden Rechnung für die Entgegennahme gemeinnütziger Spenden in Rechnung gestellt werden, sollten ebenfalls ausgenommen werden. Dies sollte nur dann gelten, wenn der Wert von Zahlungsvorgängen unter einem bestimmten Schwellenwert liegt.

[38] Europäische Bankenaufsichtsbehörde, EBA/GL/2022/02.

(15) Der einheitliche Euro-Zahlungsverkehrsraum (Single Euro Payments Area, SEPA) hat die Einrichtung unionsweiter „Zahlungs- und Inkassozentralen“ erleichtert, die die Zentralisierung der Zahlungsvorgänge derselben Gruppe ermöglicht. In diesem Zusammenhang sollten Zahlungsvorgänge zwischen einem Mutterunternehmen und seinem Tochterunternehmen oder zwischen Tochterunternehmen desselben Mutterunternehmens, die von einem Zahlungsdienstleister derselben Gruppe ausgeführt werden, vom Anwendungsbereich dieser Verordnung ausgenommen werden. Der Einzug von Zahlungsaufträgen im Namen der Gruppe durch ein Mutterunternehmen oder sein Tochterunternehmen für die Weiterleitung an einen anderen Zahlungsdienstleister sollte nicht als Zahlungsdienst gelten.

(16) Die Erbringung von Zahlungsdiensten erfordert die Unterstützung durch technische Dienste. Zu diesen technischen Diensten gehören die Verarbeitung und Speicherung von Daten, Zahlungs-Gateway-Dienste, Vertrauensdienste und Dienste zum Schutz der Privatsphäre, die Authentifizierung von Daten und Einrichtungen, die Bereitstellung von Informationstechnologie (IT) und Kommunikationsnetzen, die Bereitstellung und Wartung von verbraucherseitigen Schnittstellen zur Erfassung von Zahlungsinformationen, einschließlich der für Zahlungsdienste verwendeten Endgeräte und Geräte. Zahlungsauslösedienste und Kontoinformationsdienste sind keine technischen Dienste.

(17) Technische Dienste stellen keine Zahlungsdienste dar, da technische Dienstleister zu keinem Zeitpunkt das zu überweisende Geld in Besitz nehmen. Sie sollten daher von der Definition von Zahlungsdiensten ausgenommen werden. Für diese Dienste sollten jedoch bestimmte Anforderungen gelten, z. B. in Bezug auf die Haftung für den Fall, dass die Anwendung einer starken Kundenauthentifizierung nicht unterstützt wird, oder die Verpflichtung zum Abschluss von Auslagerungsvereinbarungen mit Zahlungsdienstleistern für den Fall, dass technische Dienstleister die Elemente einer starken Kundenauthentifizierung bereitstellen und überprüfen müssen. Es sollten auch Anforderungen für die Kündigungsgebühren von Rahmenverträgen gelten, wenn Zahlungsdienste gemeinsam mit technischen Diensten angeboten werden.

(18) Angesichts der raschen Entwicklung des Massenzahlungsmarkts und des Aufkommens neuer Zahlungsdienste und Zahlungslösungen ist es angezeigt, einige der Begriffsbestimmungen der Richtlinie (EU) 2015/2366 an die Marktgegebenheiten anzupassen, um sicherzustellen, dass die Rechtsvorschriften der Union ihren Zweck erfüllen und technologieneutral bleiben.

(19) Die Klärung des Verfahrens und der verschiedenen Schritte, die bei der Ausführung eines Zahlungsvorgangs zu befolgen sind, ist von wesentlicher Bedeutung für die Rechte und Pflichten der an einem Zahlungsvorgang beteiligten Parteien und für die Anwendung einer starken Kundenauthentifizierung. Der Vorgang, der zur Ausführung eines Zahlungsvorgangs führt, wird entweder vom Zahler oder in seinem Namen oder vom Zahlungsempfänger ausgelöst. Der Zahler leitet den Zahlungsvorgang durch Erteilung eines Zahlungsauftrags ein. Sobald der Zahlungsauftrag erteilt wurde, prüft der Zahlungsdienstleister, ob der Vorgang autorisiert und authentifiziert wurde, gegebenenfalls auch durch eine starke Kundenauthentifizierung, und der Zahlungsdienstleister validiert dann den Zahlungsauftrag. Der Zahlungsdienstleister ergreift dann die erforderlichen Schritte zur Ausführung des Zahlungsvorgangs, einschließlich des Geldtransfers.

(20) Angesichts der unterschiedlichen Auffassungen, die die Kommission in ihrer Überprüfung der Umsetzung der Richtlinie (EU) 2015/2366 festgestellt und die die

Europäische Bankenaufsichtsbehörde (EBA) in ihrer Stellungnahme vom 23. Juni 2022 zur Überprüfung der Richtlinie (EU) 2015/2366 hervorgehoben hat, muss die Definition des Begriffs „Zahlungskonto“ präzisiert werden. Das entscheidende Kriterium für die Einstufung eines Kontos als Zahlungskonto liegt in der Fähigkeit, tägliche Zahlungsvorgänge von einem solchen Konto auszuführen. Die Möglichkeit, Zahlungsvorgänge von einem Konto an einen Dritten zu tätigen oder von von einem Dritten getätigten Zahlungsvorgängen zu profitieren, ist ein charakteristisches Merkmal des Begriffs des Zahlungskontos. Ein Zahlungskonto sollte daher definiert werden als ein Konto, das verwendet wird, um Geld an Dritte zu senden und von Dritten zu empfangen. Jedes Konto, das diese Merkmale aufweist, sollte als Zahlungskonto gelten und für die Erbringung von Zahlungsauslöse- und Kontoinformationsdiensten zugänglich sein. Fälle, in denen ein anderes anderes zwischengeschaltetes Konto benötigt wird, um Zahlungsvorgänge von oder an Dritte auszuführen, sollten nicht unter die Definition eines Zahlungskontos fallen. Sparkonten werden nicht verwendet, um Geld an Dritte zu senden und von Dritten zu empfangen, sodass sie nicht unter die Definition eines Zahlungskontos fallen.

(21) Angesichts des Aufkommens neuer Arten von Zahlungsinstrumenten und der Unsicherheiten, die auf dem Markt hinsichtlich ihrer rechtlichen Qualifizierung bestehen, sollte die Definition eines „Zahlungsinstruments“ weiter präzisiert werden, indem einige Beispiele angeführt werden, um zu verdeutlichen, was ein Zahlungsinstrument darstellt und was nicht, wobei der Grundsatz der Technologieneutralität zu berücksichtigen ist.

(22) Obwohl die Nahfeldkommunikation (Near-Field Communication, NFC) die Auslösung eines Zahlungsvorgangs ermöglicht, würde die Einstufung als vollwertiges „Zahlungsinstrument“ einige Herausforderungen mit sich bringen, beispielsweise die Anwendung einer starken Kundenauthentifizierung für kontaktlose Zahlungen an der Verkaufsstelle und die Haftungsregelung des Zahlungsdienstleisters. Die Nahfeldkommunikation sollte daher eher als Funktion eines Zahlungsinstruments und nicht als Zahlungsinstrument als solches betrachtet werden.

(23) In der Richtlinie (EU) 2015/2366 wurde „Zahlungsinstrument“ als „personalisiertes Instrument“ definiert. Da es Guthabenkarten gibt, bei denen der Name des Inhabers des Instruments nicht auf der Karte aufgedruckt ist, könnte diese Formulierung der Begriffsbestimmung dazu führen, dass diese Kartenarten nicht unter die Definition des Zahlungsinstruments fallen. Die Definition des Begriffs „Zahlungsinstrument“ sollte daher dahin gehend geändert werden, dass auf „individuelle“ Instrumente und nicht auf „personalisierte“ Instrumente Bezug genommen wird, wodurch klargestellt wird, dass Guthabenkarten, bei denen der Name des Inhabers des Instruments nicht auf der Karte aufgedruckt ist, in den Anwendungsbereich dieser Verordnung fallen.

(24) Sogenannte digitale Pass-through-Brieftaschen, die die Tokenisierung eines bestehenden Zahlungsinstruments, z. B. einer Zahlungskarte, beinhalten, sind als technische Dienste anzusehen und sollten daher von der Definition des Zahlungsinstruments ausgenommen werden, da ein Token nach Ansicht der Kommission nicht selbst als Zahlungsinstrument, sondern vielmehr als „Zahlungsanwendung“ im Sinne von Artikel 2 Nummer 21 der Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates[39] angesehen werden kann.

[39] Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge (ABl. L 123 vom 19.5.2015, S. 1).

Einige andere Kategorien digitaler Brieftaschen, nämlich vorausbezahlte elektronische Brieftaschen, wie z. B. „Staged-Wallets“, bei denen Nutzer Geld für künftige Online-Transaktionen speichern können, sollten jedoch als Zahlungsinstrument und ihre Ausstellung als Zahlungsdienst betrachtet werden.

(25) Die technischen Entwicklungen seit der Annahme der Richtlinie (EU) 2015/2366 haben die Art und Weise, wie Kontoinformationsdienste bereitgestellt werden, verändert. Die Unternehmen, die diese Dienste anbieten, bieten den Zahlungsdienstnutzern aggregierte Online-Informationen zu einem oder mehreren Zahlungskonten bei einem oder mehreren Zahlungsdienstleistern, die über Online-Schnittstellen des kontoführenden Zahlungsdienstleisters zugänglich sind. Die Zahlungsdienstnutzer erhalten somit in Echtzeit und zu jedem Zeitpunkt einen umfassenden und strukturierten Überblick über ihre Zahlungskonten.

(26) Bei der Überprüfung durch die Kommission wurde hervorgehoben, dass zugelassene Kontoinformationsdienstleister mitunter Zahlungskontodaten bereitstellen, die sie nicht für den Verbraucher, von dem sie die Erlaubnis zum Zugriff auf die Daten und zur Aggregierung der Daten erhalten haben, aggregiert haben, sondern für eine andere Partei, um es dieser zu ermöglichen, dem Verbraucher, der die Daten nutzt, andere Dienste zu erbringen. Es gibt jedoch unterschiedliche Ansichten darüber, ob diese Tätigkeit unter den regulierten Kontoinformationsdienst fällt. Die Kommission ist der Auffassung, dass diese Entwicklung der „Lizenz als Dienstleistung“ des Geschäftsmodells „Open Banking“ eine Quelle innovativer, datengestützter Dienste sein kann, was letztlich den Endnutzern zugutekommt. Dieses Geschäftsmodell ermöglicht es den Endnutzern nämlich, Zugang zu ihren Zahlungskontodaten zu gewähren, um andere Dienstleistungen als Zahlungsdienste wie Kreditvergabe, Rechnungslegung und Kreditwürdigkeitsprüfung in Anspruch zu nehmen. Es ist jedoch von wesentlicher Bedeutung, dass Zahlungsdienstnutzer genau wissen, wer auf ihre Zahlungskontodaten zugreifen kann, aus welchen rechtlichen Gründen und zu welchem Zweck. Zahlungsdienstnutzer sollten umfassend auf die Übermittlung ihrer Daten an ein anderes Unternehmen aufmerksam gemacht werden und deren Übermittlung an ein anderes Unternehmen genehmigen. Dieses neue Open-Banking-basierte Geschäftsmodell erfordert eine Änderung der Definition von Kontoinformationsdiensten, um klarzustellen, dass die vom autorisierten Kontoinformationsdienstleister aggregierten Informationen an einen Dritten übermittelt werden können, damit dieser Dritte mit Erlaubnis des Endnutzers einen anderen Dienst für den Endnutzer erbringen kann. Um den Verbrauchern einen angemessenen Schutz ihrer Zahlungskontodaten und Rechtssicherheit in Bezug auf den Status von Stellen, die auf ihre Daten zugreifen, zu bieten, sollte der Dienst der Datenaggregation von Zahlungskonten stets von einem regulierten Unternehmen auf der Grundlage einer Lizenz erbracht werden, auch wenn die Daten letztlich an einen anderen Dienstleister übermittelt werden.

(27) Der Finanztransfer ist ein Zahlungsdienst, der in der Regel auf der Bereitstellung von Bargeld durch einen Zahler an einen Zahlungsdienstleister beruht, ohne dass ein Zahlungskonto auf den Namen des Zahlers oder des Zahlungsempfängers eingerichtet wird. Der Zahlungsdienstleister überweist den entsprechenden Betrag an einen Zahlungsempfänger oder an einen anderen Zahlungsdienstleister, der im Namen des Zahlungsempfängers handelt. In einigen Mitgliedstaaten bieten Supermärkte, Groß- und Einzelhändler ihren Kunden eine Dienstleistung für die Bezahlung von Rechnungen von Versorgungsunternehmen und anderen regelmäßigen

Haushaltsrechnungen. Diese Dienstleistungen für die Bezahlung von Rechnungen sollten wie Finanztransfers behandelt werden.

(28) Die Definition des Begriffs „Geld“ sollte alle Formen von Zentralbankgeld umfassen, die für die Verwendung auf der Retail-Stufe ausgegeben werden, einschließlich Banknoten und Münzen, sowie etwaige künftige digitale Zentralbankwährung, E-Geld und Geschäftsbankgeld. Zentralbankgeld, das für die Verwendung zwischen der Zentralbank und Geschäftsbanken, d. h. für die Verwendung auf der Wholesale-Stufe, ausgegeben wird, sollte nicht erfasst werden.

(29) In der Verordnung (EU) 2023/1114 vom 31. Mai 2023 über Märkte für Kryptowerte ist festgelegt, dass E-Geld-Token als E-Geld gelten. E-Geld-Token werden daher als E-Geld in die Definition des Begriffs „Geld“ in der Verordnung aufgenommen.

(30) Um das Vertrauen des E-Geld-Inhabers zu erhalten, muss E-Geld zurückgetauscht werden können. Die Rücktauschbarkeit impliziert nicht, dass das für die Ausgabe von E-Geld entgegengenommene Geld als Einlagen oder andere rückzahlbare Gelder im Sinne der Richtlinie 2013/36/EU[40] anzusehen sind. Ein Rücktausch sollte jederzeit zum Nennwert und ohne die Möglichkeit, eine Mindestgrenze für den Rücktausch zu vereinbaren, möglich sein. Für einen Rücktausch sollte grundsätzlich kein Entgelt verlangt werden. Es sollte jedoch möglich sein, ein verhältnismäßiges und kostenbasiertes Entgelt zu verlangen. Dies gilt unbeschadet der einzelstaatlichen Steuer- bzw. Sozialgesetzgebung oder von Verpflichtungen des E-Geld-Emittenten aus anderen Unionsrechtsvorschriften bzw. einzelstaatlichen Rechtsvorschriften, einschließlich Rechtsvorschriften zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung, jeglicher Maßnahmen betreffend das Einfrieren von Geldern oder jeglicher Maßnahme im Zusammenhang mit der Verbrechensvorbeugung und -aufklärung.

(31) Zahlungsdienstleister benötigen Zugang zu Zahlungssystemen, um den Nutzern Zahlungsdienste anbieten zu können. Typische Beispiele für solche Zahlungssysteme sind Vier-Parteien-Kartensysteme sowie die wichtigsten Überweisungs- und Lastschriftsysteme. Um zwischen den einzelnen Kategorien von zugelassenen Zahlungsdienstleistern eine unionsweite Gleichbehandlung sicherzustellen, sollten die Regeln für den Zugang zu Zahlungssystemen präzisiert werden. Dieser Zugang kann direkt oder indirekt über einen anderen Teilnehmer dieses Zahlungssystems erfolgen. Der Zugang sollte Anforderungen unterliegen, die die Integrität und Stabilität dieser Zahlungssysteme sicherstellen. Zu diesem Zweck sollte der Betreiber von Zahlungssystemen eine Risikobewertung eines Zahlungsdienstleisters durchführen, der eine direkte Teilnahme beantragt; bei der Risikobewertung sollten alle relevanten Risiken, gegebenenfalls einschließlich des Abwicklungsrisikos, des operationellen Risikos, des Kreditrisikos, des Liquiditätsrisikos und des Geschäftsrisikos, untersucht werden. Jeder Zahlungsdienstleister, der die Teilnahme an einem Zahlungssystem beantragt, sollte die Entscheidung für ein System auf eigenes Risiko treffen und gegenüber dem Zahlungssystem den Nachweis erbringen, dass seine internen Vorkehrungen hinreichend solide sind, um diesen Arten von Risiken standhalten zu können. Ein Antrag auf direkte Teilnahme eines Zahlungsdienstleisters sollte nur von

[40] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

einem Betreiber von Zahlungssystemen abgelehnt werden, wenn der Zahlungsdienstleister die Regeln des Systems nicht einhalten kann oder ein unannehmbar hohes Risiko darstellt.

(32) Die Betreiber von Zahlungssystemen sollten über Zugangsregeln und -verfahren verfügen, die verhältnismäßig, objektiv, nichtdiskriminierend und transparent sind. Betreiber von Zahlungssystemen sollten Zahlungsinstitute nicht in Bezug auf die Teilnahme diskriminieren, wenn die Systemregeln eingehalten werden können und kein unannehmbares Risiko für das System besteht. Zu diesen Systemen gehören unter anderem die in der Richtlinie 98/26/EG des Europäischen Parlaments und des Rates[41] genannten Systeme. In Fällen, in denen das betreffende Zahlungssystem gemäß der Verordnung (EU) Nr. 795/2014[42] der Europäischen Zentralbank bereits der Aufsicht des Europäischen Systems der Zentralbanken unterliegt, sollte(n) die Zentralbank(en) die Einhaltung dieser Vorschriften im Rahmen ihrer Aufsicht überwachen. Im Falle anderer Zahlungssysteme sollten die Mitgliedstaaten die zuständigen nationalen Behörden benennen, um sicherzustellen, dass die Betreiber von Zahlungssystemen diese Anforderungen einhalten.

(33) Um jedoch einen fairen Wettbewerb zwischen Zahlungsdienstleistern sicherzustellen, sollte einem Teilnehmer eines Zahlungssystems, das für einen zugelassenen oder registrierten Zahlungsdienstleister Dienste im Zusammenhang mit einem solchen System erbringt, der Zugang zu diesen Diensten wie jedem anderen zugelassenen oder registrierten Zahlungsdienstleister auf Antrag in objektiver, verhältnismäßiger und nichtdiskriminierender Weise gewährt werden.

(34) Die Bestimmungen über den Zugang zu den Zahlungssystemen sollten nicht für Systeme gelten, die von einem einzigen Zahlungsdienstleister eingerichtet und betrieben werden. Solche Zahlungssysteme können zwar auch in unmittelbarem Wettbewerb mit anderen Zahlungssystemen stehen, in der Regel aber besetzen sie eine Marktnische, die von diesen nicht abgedeckt wird. Zu diesen Systemen zählen Dreiparteiensysteme, einschließlich Drei-Parteien-Kartensysteme, solange diese Systeme niemals de facto als Vier-Parteien-Kartensysteme betrieben werden – auch nicht durch Rückgriff auf Lizenznehmer, Agenten oder Markenpartner („Co-Branding-Partner“). Zu ihnen zählen in der Regel auch Zahlungsdienste von Telekommunikationsdiensten, bei denen der Betreiber der Zahlungsdienstleister sowohl des Zahlers als auch des Zahlungsempfängers ist, und interne Systeme von Bankengruppen. Um den Wettbewerb zwischen solchen geschlossenen Zahlungssystemen und etablierten gängigen Zahlungssystemen zu fördern, sollte Dritten der Zugang zu diesen geschlossenen proprietären Zahlungssystemen nicht gewährt werden. Allerdings sollten auch solche geschlossenen Systeme den Wettbewerbsvorschriften der Union und der Mitgliedstaaten unterliegen, sodass es nötig sein könnte, Zugang zu diesen Zahlungssystemen zu gewähren, um einen wirksamen Wettbewerb in den Zahlungsmärkten aufrechtzuerhalten.

(35) Zahlungsinstitute müssen in der Lage sein, ein Konto bei einem Kreditinstitut zu eröffnen und zu unterhalten, um ihre Zulassungsanforderungen in Bezug auf die Sicherung der Kundengelder zu erfüllen. Wie jedoch insbesondere die EBA in ihrer

---

41 Richtlinie 98/26/EG des Europäischen Parlaments und des Rates vom 19. Mai 1998 über die Wirksamkeit von Abrechnungen in Zahlungs- sowie Wertpapierliefer- und -abrechnungssystemen (ABl. L 166 vom 11.6.1998, S. 45).

42 Verordnung (EU) Nr. 795/2014 der Europäischen Zentralbank vom 3. Juli 2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (ABl. L 217 vom 23.7.2014, S. 16).

Stellungnahme vom 5. Januar 2022[43] belegt hat, sind einige Zahlungsinstitute oder Unternehmen, die eine Zulassung für Zahlungsinstitute beantragen, trotz der in der Richtlinie (EU) 2015/2366 festgelegten Bestimmungen über Zahlungsinstitutskonten bei einer Geschäftsbank nach wie vor mit Praktiken einiger Kreditinstitute konfrontiert, die sich entweder weigern, für sie ein Konto zu eröffnen, oder ein Konto schließen, wenn ein solches besteht, da das Risiko der Geldwäsche oder Terrorismusfinanzierung als höher eingeschätzt wird. Diese sogenannten „risikomindernden“ Praktiken stellen Zahlungsinstitute vor erhebliche Wettbewerbsherausforderungen.

(36) Kreditinstitute sollten daher Zahlungsinstituten und Antragstellern, die eine Zulassung als Zahlungsinstitut beantragen, sowie deren Agenten und Vertriebsstellen ein Zahlungskonto zur Verfügung stellen, außer in Ausnahmefällen, in denen schwerwiegende Gründe für die Verweigerung des Zugangs vorliegen. Antragsteller, die eine Zulassung als Zahlungsinstitut beantragen, müssen in diese Bestimmung eingeschlossen werden, da ein Bankkonto, auf dem Kundengelder verwahrt werden können, eine Voraussetzung für den Erhalt einer Zulassung als Zahlungsinstitut ist. Die Verweigerungsgründe sollten schwerwiegende Gründe für den Verdacht umfassen, dass von oder über das Zahlungsinstitut illegale Tätigkeiten ausgeübt werden, oder ein Geschäftsmodell oder ein Risikoprofil, das dem Kreditinstitut ernsthafte Risiken oder übermäßige Befolgungskosten verursacht. Beispielsweise können Geschäftsmodelle, bei denen Zahlungsinstitute ein weitreichendes Netz von Agenten nutzen, erhebliche Befolgungskosten zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung verursachen. Ein Zahlungsinstitut sollte das Recht haben, gegen die Verweigerung durch ein Kreditinstitut bei einer von einem Mitgliedstaat benannten zuständigen Behörde Beschwerde einzulegen. Um die Ausübung dieses Beschwerderechts zu erleichtern, sollten die Kreditinstitute jede Verweigerung der Kontoführung oder eine spätere Schließung eines Kontos schriftlich und ausführlich begründen. Diese Begründung sollte sich auf spezifische Elemente in Bezug auf das betreffende Zahlungsinstitut beziehen, und nicht auf generelle oder allgemeine Erwägungen. Um den zuständigen Behörden die Bearbeitung von Beschwerden gegen die Verweigerung oder den Entzug von Konten und deren Begründung zu erleichtern, sollte die EBA technische Durchführungsstandards ausarbeiten, in denen die Darlegung dieser Gründe harmonisiert wird.

(37) Um sachkundige Entscheidungen treffen und ihren Zahlungsdienstleister innerhalb der Union problemlos auswählen zu können, sollten Zahlungsdienstnutzer vergleichbare und klare Informationen über Zahlungsdienste erhalten. Um sicherzustellen, dass Zahlungsdienstnutzer notwendige, ausreichende und verständliche Informationen über den Zahlungsdienstvertrag und die Zahlungsvorgänge erhalten, müssen die Pflichten der Zahlungsdienstleister hinsichtlich der Unterrichtung der Zahlungsdienstnutzer präzisiert und harmonisiert werden.

(38) Bei der Bereitstellung der erforderlichen Informationen für Zahlungsdienstnutzer sollten die Zahlungsdienstleister je nach dem jeweiligen Zahlungsdienstvertrag den Bedürfnissen der Zahlungsdienstnutzer sowie praktischen Aspekten und der Kosteneffizienz Rechnung tragen. Zahlungsdienstleister sollten entweder aktiv und rechtzeitig ohne Veranlassung durch den Zahlungsdienstnutzer kommunizieren oder die Informationen den Zahlungsdienstnutzern auf Anfrage zur Verfügung stellen. Im

[43] Europäische Bankenaufsichtsbehörde, EBA/Op/2022/01.

zweiten Fall sollten Zahlungsdienstnutzer selbst aktiv werden, um sich die Informationen zu verschaffen, einschließlich durch ausdrückliche Anforderung von Informationen bei den Zahlungsdienstleistern, durch Einloggen in eine bankkontospezifische Mailbox oder durch Eingabe einer Bankkarte in den Kontoauszugdrucker. Zu diesen Zwecken sollten die Zahlungsdienstleister sicherstellen, dass die Informationen zugänglich sind und Zahlungsdienstnutzern zur Verfügung stehen.

(39) Da Verbraucher und Unternehmen nicht gleichermaßen gefährdet sind, brauchen sie nicht im selben Umfang geschützt zu werden. Zwar müssen die Verbraucherrechte durch Vorschriften geschützt werden, die nicht vertraglich abbedungen werden können, doch sollte es Unternehmen und Organisationen freistehen, abweichende Vereinbarungen zu schließen, wenn es nicht um vertragliche Beziehungen zu Verbrauchern geht. Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[44] können wie Verbraucher behandelt werden. Es sollten stets bestimmte Regeln gelten, unabhängig vom Status des Nutzers.

(40) Um ein hohes Verbraucherschutzniveau aufrechtzuerhalten, sollten die Verbraucher das Recht haben, kostenlos Informationen über die Dienstleistungsbedingungen und Preise zu erhalten, bevor sie durch einen Zahlungsdienstvertrag gebunden sind. Damit die Verbraucher die von Zahlungsdienstleistern angebotenen Dienste und Bedingungen vergleichen und im Streitfall ihre vertraglichen Rechte und Pflichten überprüfen können, sollten die Verbraucher diese Informationen und den Rahmenvertrag kostenlos und jederzeit während des Vertragsverhältnisses in Papierform anfordern können.

(41) Um die Transparenz zu erhöhen, sollten Zahlungsdienstleister dem Verbraucher grundlegende Informationen über ausgeführte Zahlungsvorgänge ohne Berechnung eines zusätzlichen Entgelts zur Verfügung stellen. Bei Einzelzahlungen sollte der Zahlungsdienstleister diese Informationen nicht getrennt in Rechnung stellen. Ebenso sollten Zahlungsdienstleister anschließende Informationen über Zahlungsvorgänge im Rahmen eines Rahmenvertrags kostenlos und monatlich zur Verfügung stellen. Da die Preisbildung jedoch transparent sein muss und die Kunden unterschiedliche Bedürfnisse haben, sollten die Vertragsparteien vereinbaren können, dass für die häufigere Übermittlung von Informationen oder die Übermittlung zusätzlicher Informationen Entgelte erhoben werden.

(42) Zahlungsinstrumente für Kleinbetragszahlungen sollten bei Waren und Dienstleistungen des Niedrigpreissegments eine kostengünstige und benutzerfreundliche Alternative darstellen und nicht durch übermäßig hohe Anforderungen überfrachtet werden. Aus diesem Grund sollten die betreffenden Informationspflichten und Ausführungsvorschriften auf die unbedingt notwendigen Informationen beschränkt werden, wobei auch die technischen Möglichkeiten berücksichtigt werden sollten, die von diesen für Kleinbetragszahlungen vorgesehenen Instrumenten berechtigterweise erwartet werden können. Der weniger strengen Regelung zum Trotz sollten die Zahlungsdienstnutzer unter Berücksichtigung der mit diesen Zahlungsinstrumenten verbundenen begrenzten Risiken, insbesondere mit Blick auf Instrumente auf Guthabenbasis, angemessen geschützt sein..

(43) Bei Einzelzahlungen sollten die Zahlungsdienstleister die wichtigsten Informationen stets von sich aus zur Verfügung stellen müssen. Da Zahler in der Regel anwesend

[44] ABl. L 124 vom 20.5.2003, S. 36.

sind, wenn sie den Zahlungsauftrag erteilen, sollte es nicht notwendig sein, dass die Informationen immer auf Papier oder einem anderen dauerhaften Datenträger mitgeteilt werden. Zahlungsdienstleister sollten entweder mündlich Auskunft erteilen können oder die Informationen anderweitig leicht zugänglich machen, einschließlich des Anbringens einer Tafel mit den Vertragsbedingungen in den Geschäftsräumen. Es sollte darauf hingewiesen werden, wo weitere Informationen erhältlich sind, einschließlich der Website. Allerdings sollte der Verbraucher auf Verlangen die wichtigsten Informationen auch auf Papier oder einem anderen dauerhaften Datenträger von Zahlungsdienstleistern erhalten können.

(44) Die Informationen sollten den Bedürfnissen der Nutzer angemessen sein. Für Einzelzahlungen sollten andere Informationspflichten gelten als für Rahmenverträge, die mehrere Zahlungsvorgänge betreffen.

(45) Um eine sachkundige Entscheidung treffen zu können, sollten Zahlungsdienstnutzer die Entgelte für die Nutzung von Geldautomaten mit jenen anderer Anbieter vergleichen können. Um die Transparenz der Geldautomatenentgelte für die Zahlungsdienstleister zu erhöhen, sollten die Zahlungsdienstleister den Zahlungsdienstnutzern Informationen über alle Entgelte für inländische Geldabhebungen in unterschiedlichen Situationen zur Verfügung stellen, je nachdem, von welchem Geldautomaten die Zahlungsdienstnutzer Bargeld abheben.

(46) Rahmenverträge und unter diese Verträge fallende Zahlungsvorgänge sind weitaus häufiger und fallen wirtschaftlich mehr ins Gewicht als Einzelzahlungen. Bei Zahlungskonten oder bestimmten Zahlungsinstrumenten ist ein Rahmenvertrag erforderlich. Daher sollten die Anforderungen an Vorabinformationen zu Rahmenverträgen umfassend sein und die Informationen sollten stets auf Papier oder auf einem anderen dauerhaften Datenträger bereitgestellt werden. Zahlungsdienstleister und Zahlungsdienstnutzer sollten jedoch im Rahmenvertrag vereinbaren können, wie spätere Informationen über ausgeführte Zahlungsvorgänge zu erteilen sind.

(47) Vertragliche Bestimmungen sollten nicht zu Diskriminierung von Verbrauchern mit rechtmäßigem Wohnsitz in der Union aufgrund ihrer Staatsangehörigkeit oder ihres Wohnsitzes führen. Ist in einem Rahmenvertrag das Recht vorgesehen, ein Zahlungsinstrument aus objektiv gerechtfertigten Gründen zu sperren, sollte der Zahlungsdienstleister nicht die Möglichkeit haben, dieses Recht in Anspruch zu nehmen, nur weil der Zahlungsdienstnutzer seinen Wohnsitz innerhalb der Union geändert hat.

(48) Um ein hohes Verbraucherschutzniveau sicherzustellen, sollten die Mitgliedstaaten im Interesse des Verbrauchers Beschränkungen oder Verbote einseitiger Änderungen der Bedingungen eines Rahmenvertrags aufrechterhalten oder einführen können, beispielsweise wenn eine solche Änderung nicht gerechtfertigt ist.

(49) Um die Mobilität der Zahlungsdienstnutzer zu erleichtern, sollten die Nutzer einen Rahmenvertrag gebührenfrei kündigen können. Wird ein Vertrag weniger als sechs Monate nach Inkrafttreten vom Zahlungsdienstnutzer gekündigt, sollte es Zahlungsdienstleistern allerdings gestattet sein, entsprechend den durch die Kündigung des Rahmenvertrags durch den Nutzer entstandenen Kosten ein Entgelt zu erheben. Werden im Wege eines Rahmenvertrags Zahlungsdienste gemeinsam mit technischen Diensten angeboten, die die Erbringung von Zahlungsdiensten unterstützen, wie z. B. die Anmietung von Terminals, die für Zahlungsdienste genutzt werden, so sollten Zahlungsdienstnutzer nicht durch strengere Bedingungen in den

Vertragsklauseln für die technischen Dienste an ihren Zahlungsdienstleister gebunden werden. Um den Wettbewerb zu wahren, sollten solche Vertragsklauseln den Anforderungen des Rahmenvertrags in Bezug auf Kündigungsgebühren unterliegen. Die vertraglich festgelegte Kündigungsfrist sollte für den Verbraucher einen Monat nicht überschreiten und für den Zahlungsdienstleister mindestens zwei Monate betragen. Diese Regeln sollten unbeschadet der Verpflichtung des Zahlungsdienstleisters gelten, den Zahlungsdienstvertrag unter außergewöhnlichen Umständen im Rahmen anderer einschlägiger Rechtsvorschriften der Union oder der Mitgliedstaaten, etwa zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, im Rahmen von Maßnahmen zum Einfrieren von Geldern oder im Rahmen spezifischer Maßnahmen zur Prävention und Aufklärung von Straftaten zu kündigen.

(50) Um Vergleichbarkeit zu erreichen, sollten die geschätzten Währungsumrechnungsentgelte für Überweisungen und Finanztransfers innerhalb der Union und aus der Union in ein Drittland in derselben Weise ausgedrückt werden, nämlich als prozentualer Aufschlag auf die jüngsten verfügbaren Euro-Referenzwechselkurse der Europäischen Zentralbank (EZB). Wird in dieser Verordnung auf „Entgelte“ Bezug genommen, sollte dies gegebenenfalls auch „Währungsumrechnungsentgelte“ einschließen.

(51) Eine Teilung der Entgelte zwischen Zahler und Zahlungsempfänger ist erfahrungsgemäß am effizientesten, da sie die vollautomatisierte Abwicklung von Zahlungen erleichtert. Aus diesem Grund sollte dafür gesorgt werden, dass die jeweiligen Zahlungsdienstleister ihre Entgelte direkt beim Zahler bzw. beim Zahlungsempfänger erheben. Das Entgelt kann auch null betragen, denn die Regeln sollten die Praxis, dass Zahlungsdienstleister Kontogutschriften für Verbraucher kostenlos ausführen, nicht beeinträchtigen. Auch kann ein Zahlungsdienstleister je nach Vertragsbedingungen lediglich beim Zahlungsempfänger Entgelte für die Nutzung des Zahlungsdienstes erheben; in diesem Fall hat der Zahler keine Entgelte zu entrichten. Die Zahlungssysteme erheben möglicherweise Entgelte in Form einer Grundgebühr. Die Bestimmungen über die transferierten Beträge oder Entgelte haben keine unmittelbaren Auswirkungen auf die Preisbildung zwischen Zahlungsdienstleistern oder sonstigen zwischengeschalteten Stellen.

(52) Ein Aufschlag ist eine Gebühr, die ein Händler einem Verbraucher zusätzlich zum geforderten Preis für Waren und Dienstleistungen berechnet, wenn der Verbraucher eine bestimmte Zahlungsmethode anwendet. Einer der Gründe für die Aufschläge besteht darin, die Verbraucher zu kostengünstigeren oder effizienteren Zahlungsinstrumenten zu lenken und so den Wettbewerb zwischen verschiedenen Zahlungsmethoden zu fördern. Nach der mit der Richtlinie (EU) 2015/2366 eingeführten Regelung wurden Zahlungsempfänger daran gehindert, Entgelte für die Nutzung von Zahlungsinstrumenten zu erheben, für die die Interbankenentgelte in Kapitel II der Verordnung (EU) 2015/751 geregelt sind, d. h. für Verbraucherdebitkarten und Verbraucherkreditkarten, die im Rahmen von Vier-Parteien-Kartensystemen ausgegeben werden, sowie für Zahlungsdienste, auf die die Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates[45] Anwendung findet, d. h. Überweisungen und Lastschriften in Euro innerhalb der

[45] Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009 (ABl. L 94 vom 30.3.2012, S. 22).

Union. Die Mitgliedstaaten durften gemäß der Richtlinie (EU) 2015/2366 dem Zahlungsempfänger die Erhebung von Entgelten ferner untersagen oder dieses Recht begrenzen unter Berücksichtigung der Notwendigkeit, den Wettbewerb und die Nutzung effizienter Zahlungsinstrumente zu fördern.

(53) Die bei der Überprüfung der Richtlinie (EU) 2015/2366 gesammelten Erkenntnisse zeigen, dass die derzeitigen Bestimmungen über Entgelte angemessen sind und sich positiv ausgewirkt haben. Eine weitere Angleichung der Entgeltpraxis zwischen den Mitgliedstaaten ist nicht zwingend erforderlich, da das bestehende Verbot von Aufschlägen bereits für einen sehr großen Teil der Zahlungen in der Union gilt. Schätzungen zufolge unterliegen 95 % der Kartenzahlungen dem geltenden Verbot von Aufschlägen. Darüber hinaus wird ein Aufschlag auf die dem Händler tatsächlich entstandenen Kosten begrenzt. Bei der Überprüfung der Richtlinie (EU) 2015/2366 stellte die Kommission jedoch unterschiedliche Auslegungen in Bezug auf die Zahlungsinstrumente fest, die unter das Verbot von Aufschlägen fallen. Daher ist es notwendig, das Aufschlagsverbot ausdrücklich auf alle Überweisungen und Lastschriften auszuweiten und nicht nur auf diejenigen, die unter die Verordnung (EU) Nr. 260/2012 fallen, wie dies bei der Richtlinie (EU) 2015/2366 der Fall war.

(54) Kontoinformationsdienste und Zahlungsauslösedienste, die häufig als „Open-Banking-Dienste“ bezeichnet werden, sind Zahlungsdienste, die Zahlungsdienstleistern, die weder über das Geld des Kontoinhabers noch über ein Zahlungskonto verfügen, Zugang zu den Daten eines Zahlungsdienstnutzers verschaffen. Kontoinformationsdienste ermöglichen die Aggregation der Daten eines Nutzers auf Antrag des Zahlungsdienstnutzers mit verschiedenen kontoführenden Zahlungsdienstleistern an einem einzigen Ort. Zahlungsauslösedienste ermöglichen die Auslösung einer Zahlung vom Konto des Nutzers, wie etwa eine Überweisung oder eine Lastschrift, auf eine für den Nutzer und den Zahlungsempfänger bequeme Weise, ohne dass ein Instrument wie eine Zahlungskarte verwendet wird.

(55) Kontoführende Zahlungsdienstleister sollten Kontoinformations- und Zahlungsauslösedienstleistern Zugang zu Zahlungskontodaten gewähren, wenn der Zahlungsdienstnutzer online auf das Zahlungskonto zugreifen kann und der Zahlungsdienstnutzer die Erlaubnis für diesen Zugang erteilt hat. Die Richtlinie (EU) 2015/2366 beruhte auf dem Grundsatz des Zugangs zu Zahlungskontodaten, ohne dass es einer vertraglichen Beziehung zwischen dem kontoführenden Zahlungsdienstleister und den Kontoinformations- und Zahlungsauslösedienstleistern bedurfte, was zur Folge hatte, dass eine Entgelterhebung für den Datenzugang in der Praxis nicht möglich war. Seit der Anwendung der Richtlinie (EU) 2015/2366 erfolgt der Zugang zu Daten im Rahmen des Open Banking auf einer solchen außervertraglichen Grundlage und ohne Entgelt. Wenn regulierte Datenzugangsdienste entgeltpflichtig wären, ohne dass bisher Entgelte erhoben wurden, könnten die Auswirkungen auf die weitere Erbringung dieser Dienste und damit auf den Wettbewerb und die Innovation auf den Zahlungsverkehrsmärkten erheblich sein. Dieser Grundsatz sollte daher beibehalten werden. Die Beibehaltung dieses Ansatzes steht im Einklang mit den Kapiteln III und IV des Vorschlags für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)[46], insbesondere mit Artikel 9 Absatz 3 dieses Vorschlags über Ausgleichszahlungen, der durch die vorliegende Verordnung nicht berührt wird. Der

[46] Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz) (COM(2022) 68 final).

Vorschlag der Kommission für eine Verordnung über den Zugang zu Finanzdaten (FIDA) sieht eine mögliche Vergütung des Datenzugangs im Rahmen der FIDA vor. Eine solche Regelung würde sich somit von der in der vorliegenden Verordnung unterscheiden. Diese Ungleichbehandlung ist dadurch gerechtfertigt, dass im Gegensatz zum Zugang zu Zahlungskontodaten, der seit dem Inkrafttreten der Richtlinie (EU) 2015/2366 im Unionsrecht geregelt ist, der Zugang zu anderen Finanzdaten noch nicht den Rechtsvorschriften der Union unterliegt. Es besteht daher keine Gefahr einer Störung, da dieser Markt im Gegensatz zum Zugang zu Zahlungskontodaten neu entsteht und mit der FIDA erstmalig reguliert wird.

(56) Kontoführende Zahlungsdienstleister sowie Kontoinformations- und Zahlungsauslösedienstleister können für den Zugang zu Zahlungskontodaten und die Bereitstellung von Open-Banking-Diensten, die nicht in dieser Verordnung vorgeschrieben sind, ein Vertragsverhältnis, auch im Rahmen einer multilateralen vertraglichen Vereinbarung (z. B. eines Systems), eingehen, das eine Vergütung vorsehen kann. Ein Beispiel für solche Mehrwertdienste, die über sogenannte „Premium"-Anwendungsprogrammierschnittstellen (API) angeboten werden, ist die Möglichkeit, künftige variable wiederkehrende Zahlungen zu planen. Jede Vergütung solcher Dienste müsste nach dem Geltungsbeginn mit den Kapiteln III und IV des vorgeschlagenen Datengesetzes in Einklang stehen, insbesondere in Bezug auf Artikel 9 Absatz 1 und Artikel 9 Absatz 2 über die Vergütung. Der Zugang von Kontoinformations- und Zahlungsauslösedienstleistern zu Zahlungskontodaten, die unter diese Verordnung fallen, ohne dass ein Vertragsverhältnis verlangt wird, und für den damit kein Entgelt erhoben wird, sollte auch dann immer möglich sein, wenn eine multilaterale vertragliche Vereinbarung (z. B. ein System) besteht und dieselben Daten auch als Teil der besagten multilateralen vertraglichen Vereinbarung erhältlich sind.

(57) Um beim Datenzugang und -austausch ein hohes Maß an Sicherheit zu gewährleisten, sollte der Zugang zu Zahlungskonten und den darin enthaltenen Daten vorbehaltlich besonderer Umstände den Kontoinformations- und Zahlungsauslösedienstleistern über eine Schnittstelle, die für „Open-Banking"-Zwecke konzipiert und bestimmt ist, wie z. B. eine Anwendungsprogrammierschnittstelle, gewährt werden. Zu diesem Zweck sollte der kontoführende Zahlungsdienstleister eine sichere Kommunikation mit Kontoinformations- und Zahlungsauslösedienstleistern einrichten. Damit keinerlei Unsicherheit darüber entsteht, wer Zugang zu den Daten des Zahlungsdienstnutzers hat, sollte die dedizierte Schnittstelle Kontoinformations- und Zahlungsauslösedienstleister in die Lage versetzen, sich gegenüber dem kontoführenden Zahlungsdienstleister zu identifizieren und sich auf alle Authentifizierungsverfahren zu verlassen, die der kontoführende Zahlungsdienstleister dem Zahlungsdienstnutzer zur Verfügung stellt. Kontoinformations- und Zahlungsauslösedienstleister sollten in der Regel die für ihren Zugang vorgesehene Schnittstelle nutzen und daher die Kundenschnittstelle eines kontoführenden Zahlungsdienstleisters nicht für die Zwecke des Datenzugangs nutzen, außer bei Ausfall oder Nichtverfügbarkeit der dedizierten Schnittstelle unter den in dieser Verordnung festgelegten Bedingungen. Unter solchen Umständen würde ihre Geschäftskontinuität dadurch gefährdet, dass sie nicht auf die Daten zugreifen können, für die ihnen eine Erlaubnis erteilt wurde. Es ist unerlässlich, dass Kontoinformations- und Zahlungsauslösedienstleister jederzeit in der Lage sind, auf die Daten zuzugreifen, die sie für ihren Kundenservice benötigen.

(58) Um die reibungslose Nutzung der dedizierten Schnittstelle zu erleichtern, sollten deren technische Spezifikationen angemessen dokumentiert und sollte vom kontoführenden

Zahlungsdienstleister eine Zusammenfassung öffentlich zugänglich gemacht werden. Damit die Open-Banking-Dienstleister ihren künftigen Zugang angemessen vorbereiten und etwaige technische Probleme lösen können, sollte der kontoführende Zahlungsdienstleister Kontoinformations- und Zahlungsauslösedienstleister in die Lage versetzen, vor dem Datum, an dem die Schnittstelle aktiviert wird, eine Schnittstelle zu testen. Nur autorisierte Kontoinformations- und Zahlungsauslösedienstleister sollten über diese Schnittstelle auf Zahlungskontodaten zugreifen, auch wenn Antragsteller, die eine Zulassung als Kontoinformations- und Zahlungsauslösedienstleister beantragen, die Möglichkeit haben sollten, die technischen Spezifikationen einzusehen. Zur Sicherstellung der Interoperabilität der verschiedenen technischen Kommunikationslösungen sollte die Schnittstelle von internationalen oder europäischen Normungsorganisationen, insbesondere auch vom Europäischen Komitee für Normung (European Committee for Standardization, CEN) oder von der Internationalen Organisation für Normung (International Organization for Standardization, ISO) entwickelte Kommunikationsstandards verwenden.

(59) Damit Kontoinformations- und Zahlungsauslösedienstleister jederzeit ihre Geschäftskontinuität sicherstellen und für ihre Kunden hochwertige Dienstleistungen erbringen können, muss die von ihnen zu nutzende dedizierte Schnittstelle hohe Leistungs- und Funktionsanforderungen erfüllen. Sie sollte zumindest die „Datenparität“ mit der Kundenschnittstelle sicherstellen, die der kontoführende Zahlungsdienstleister seinen Nutzern zur Verfügung stellt, und daher auch die Zahlungskontodaten einbeziehen, die auch den Zahlungsdienstnutzern über die ihnen vom kontoführenden Zahlungsdienstleister bereitgestellte Schnittstelle zur Verfügung stehen. In Bezug auf Zahlungsauslösedienste sollte die dedizierte Schnittstelle nicht nur die Auslösung von Einzelzahlungen, sondern auch die Auslösung von Daueraufträgen und Lastschriften ermöglichen. Detailliertere Anforderungen an dedizierte Schnittstellen sollten in von der EBA entwickelten technischen Regulierungsstandards festgelegt werden.

(60) Angesichts der dramatischen Auswirkungen, die eine längere Nichtverfügbarkeit einer dedizierten Schnittstelle auf die Geschäftskontinuität der Kontoinformations- und Zahlungsauslösedienstleister hätte, sollten kontoführende Zahlungsdienstleister diese Nichtverfügbarkeit unverzüglich beheben. Kontoführende Zahlungsdienstleister sollten Kontoinformations- und Zahlungsauslösedienstleister über eine solche Nichtverfügbarkeit ihrer dedizierten Schnittstelle und die zu ihrer Behebung ergriffenen Maßnahmen unverzüglich informieren. Falls keine dedizierte Schnittstelle verfügbar ist und der kontoführende Zahlungsdienstleister keine wirksame Alternativlösung anbietet, sollten Kontoinformations- und Zahlungsauslösedienstleister in der Lage sein, ihre Geschäftskontinuität zu wahren. Sie sollten ihre zuständige nationale Behörde ersuchen können, die ihren Nutzern vom kontoführenden Zahlungsdienstleister bereitgestellte Schnittstelle zu nutzen, bis die dedizierte Schnittstelle wieder verfügbar ist. Nach Eingang des Ersuchens sollte die zuständige Behörde ihre Entscheidung unverzüglich treffen. Bis zur Entscheidung der Behörde sollte es den ersuchenden Kontoinformations- und Zahlungsauslösedienstleistern gestattet sein, die Schnittstelle, die der kontoführende Zahlungsdienstleister seinen Nutzern zur Verfügung stellt, vorübergehend zu nutzen. Die jeweils zuständige Behörde sollte dem kontoführenden Zahlungsdienstleister eine Frist setzen, um das uneingeschränkte Funktionieren der dedizierten Schnittstelle wiederherzustellen, wobei die Möglichkeit von Sanktionen besteht, falls dies nicht innerhalb der Frist geschieht. Alle Kontoinformations- und Zahlungsauslösedienstleister, nicht nur diejenigen, die das Ersuchen gestellt haben,

sollten Zugang zu den Daten haben, die sie benötigen, um ihre Geschäftskontinuität sicherzustellen.

(61) Ein solcher vorübergehender direkter Zugang sollte keine negativen Auswirkungen auf die Verbraucher haben. Kontoinformations- und Zahlungsauslösedienstleister sollten sich daher stets ordnungsgemäß identifizieren und alle ihre Verpflichtungen einhalten, wie etwa die Grenzen der ihnen erteilten Erlaubnis, und insbesondere nur auf die Daten zugreifen, die sie benötigen, um ihren vertraglichen Verpflichtungen nachzukommen und den regulierten Dienst zu erbringen. Der Zugang zu Zahlungskontodaten ohne ordnungsgemäße Identifizierung (sogenanntes „Screenscraping“) sollte in keinem Fall erfolgen.

(62) Da die Einrichtung einer dedizierten Schnittstelle für bestimmte kontoführende Zahlungsdienstleister als unverhältnismäßig aufwendig angesehen werden könnte, sollte eine zuständige nationale Behörde einen kontoführenden Zahlungsdienstleister auf Antrag von der Verpflichtung befreien können, über eine dedizierte Datenzugangsschnittstelle zu verfügen, und entweder den Zugang zu Zahlungsdaten nur über ihre „Kundenschnittstelle“ oder überhaupt keine Schnittstelle für den Zugang zu Open-Banking-Daten anzubieten. Im Falle eines sehr kleinen kontoführenden Zahlungsdienstleisters, für den eine dedizierte Schnittstelle eine erhebliche finanzielle und ressourcenbezogene Belastung darstellen würde, kann der Datenzugang über die Kundenschnittstelle (ohne dedizierte Schnittstelle) angemessen sein. Die Befreiung von der Verpflichtung, eine Schnittstelle für den Zugang zu „Open-Banking“-Daten zu unterhalten, kann gerechtfertigt sein, wenn der kontoführende Zahlungsdienstleister ein bestimmtes Geschäftsmodell hat, z. B. wenn Open-Banking-Dienste für seine Kunden nicht relevant wären. Detaillierte Kriterien für die Gewährung solcher unterschiedlicher Arten von Freistellungsentscheidungen sollten in technischen Regulierungsstandards festgelegt werden, die von der EBA ausgearbeitet werden.

(63) Um das Potenzial des Open Banking in der Union voll auszuschöpfen, ist es von entscheidender Bedeutung, jede diskriminierende Behandlung von Kontoinformations- und Zahlungsauslösedienstleistern durch kontoführende Zahlungsdienstleister zu verhindern. Hat der Zahlungsdienstnutzer beschlossen, die Dienste eines Kontoinformationsdienstleisters oder eines Zahlungsauslösedienstleisters in Anspruch zu nehmen, so sollte der kontoführende Zahlungsdienstleister diesen Auftrag genauso behandeln wie einen solchen Antrag, wenn er vom Zahlungsdienstnutzer direkt über seine „Kundenschnittstelle“ gestellt wird, es sei denn, der kontoführende Zahlungsdienstleister hat objektive Gründe, den Antrag auf Zugang zum Konto anders zu behandeln, einschließlich eines schwerwiegenden Betrugsverdachts.

(64) Für die Erbringung von Zahlungsauslösediensten sollte der kontoführende Zahlungsdienstleister dem Zahlungsauslösedienstleister unmittelbar nach Eingang des Zahlungsauftrags alle ihm zugänglichen Informationen über die Ausführung des Zahlungsvorgangs zur Verfügung stellen. Mitunter erhält der kontoführende Zahlungsdienstleister weitere Informationen, nachdem er den Zahlungsauftrag erhalten, aber den Zahlungsvorgang noch nicht ausgeführt hat. Sofern dies für den Zahlungsauftrag und die Ausführung des Zahlungsvorgangs relevant ist, sollte der kontoführende Zahlungsdienstleister diese Informationen dem Zahlungsauslösedienstleister zur Verfügung stellen. Dem Zahlungsauslösedienstleister sollten die Informationen zuteilwerden, die erforderlich sind, um das Risiko der Nichtausführung des ausgelösten Geschäfts einzuschätzen. Diese Informationen sind unerlässlich, damit der Zahlungsauslösedienstleister einem Zahlungsempfänger, in dessen Namen er den Vorgang veranlasst, einen Dienst anbieten kann, dessen Qualität

mit anderen dem Zahlungsempfänger zur Verfügung stehenden elektronischen Zahlungsmitteln, einschließlich Zahlungskarten, im Wettbewerb stehen kann.

(65) Um das Vertrauen in Open Banking zu stärken, ist es von entscheidender Bedeutung, dass Zahlungsdienstnutzer, die Kontoinformations- und Zahlungsauslösedienste nutzen, die volle Kontrolle über ihre Daten und Zugang zu klaren Informationen über die Datenzugangserlaubnisse haben, die diese Zahlungsdienstnutzer den Zahlungsdienstleistern erteilt haben, einschließlich des Zwecks der Erlaubnis und der Kategorien der betreffenden Zahlungskontodaten und auch der Identitätsdaten des Kontos, der Transaktion und des Kontosaldos. Kontoführende Zahlungsdienstleister sollten daher Zahlungsdienstnutzern, die solche Dienste in Anspruch nehmen, ein „Dashboard“ für die Überwachung und den Entzug oder die Wiederherstellung des Datenzugangs für „Open-Banking“-Dienstleister zur Verfügung stellen. Erlaubnisse zur Auslösung einmaliger Zahlungen sollten nicht auf diesem Dashboard erscheinen. Ein Dashboard erlaubt es Zahlungsdienstnutzern möglicherweise nicht, neue Datenzugangserlaubnisse mit Kontoinformations- oder Zahlungsauslösedienstleistern zu erstellen, denen zuvor noch kein Datenzugang gewährt wurde. Kontoführende Zahlungsdienstleister sollten Kontoinformations- und Zahlungsauslösedienstleister unverzüglich über jeden Entzug des Datenzugangs informieren. Kontoinformations- und Zahlungsauslösedienstleister sollten kontoführende Zahlungsdienstleister unverzüglich über neue und wiederhergestellte Datenzugangserlaubnisse informieren, die von Zahlungsdienstnutzern erteilt wurden, einschließlich der Geltungsdauer der Erlaubnis und ihres Zwecks (insbesondere, ob die Konsolidierung der Daten dem Nutzer oder der Übermittlung an Dritte dient). Ein kontoführender Zahlungsdienstleister sollte einen Zahlungsdienstnutzer in keiner Weise dazu anhalten, die Kontoinformations- und Zahlungsauslösedienstleistern erteilten Erlaubnisse zurückzuziehen. Das Dashboard sollte den Zahlungsdienstnutzer standardmäßig vor dem Risiko möglicher vertraglicher Folgen des Entzugs des Datenzugangs eines Open-Banking-Dienstleisters warnen, da das Dashboard nicht das Vertragsverhältnis zwischen dem Nutzer und einem „Open-Banking“-Anbieter regelt, sondern es Sache des Zahlungsdienstnutzers ist, dieses Risiko zu überprüfen. Ein Erlaubnis-Dashboard sollte die Kunden in die Lage versetzen, ihre Erlaubnisse in sachkundig und objektiv zu verwalten, und den Kunden ein hohes Maß an Kontrolle darüber geben, wie ihre personenbezogenen und nicht personenbezogenen Daten verwendet werden. Bei einem Erlaubnis-Dashboard sollten gegebenenfalls die Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates berücksichtigt werden.

(66) Die Überprüfung der Richtlinie (EU) 2015/2366 hat ergeben, dass Kontoinformations- und Zahlungsauslösedienstleister trotz des erreichten Harmonisierungsgrads und des Verbots von Beeinträchtigungen nach Artikel 32 Absatz 3 der Delegierten Verordnung (EU) 2018/389[47] der Kommission nach wie vor vielen ungerechtfertigten Beeinträchtigungen ausgesetzt sind. Diese Beeinträchtigungen schränken nach wie vor das volle Potenzial des Open Banking in der Union ein. Diese Beeinträchtigungen werden den Aufsichtsbehörden, den Regulierungsbehörden und der Kommission regelmäßig von Kontoinformations- und Zahlungsauslösedienstleistern gemeldet. Sie

[47] Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (ABl. L 69 vom 13.3.2018, S. 23).

wurden von der EBA in ihrer Stellungnahme vom Juni 2020 zu den „*Hindernissen für die Erbringung von Dienstleistungen von Drittanbietern gemäß der Zahlungsdiensterichtlinie*“ analysiert. Trotz Klarstellungen besteht auf dem Markt und bei den Aufsichtsbehörden nach wie vor große Unsicherheit darüber, was eine „verbotene Beeinträchtigung“ für regulierte Open-Banking-Dienste darstellt. Daher ist es unerlässlich, eine klare und nicht erschöpfende Liste solcher verbotener Beeinträchtigungen für Open Banking vorzulegen, wobei insbesondere auf die Arbeit der EBA zurückgegriffen werden sollte.

(67) Die Verpflichtung, personalisierte Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen, ist äußerst wichtig, um das Geld des Zahlungsdienstnutzers zu schützen und Betrugsrisiken und den unbefugten Zugriff auf Zahlungskonten zu begrenzen. Die Geschäftsbedingungen oder andere dem Zahlungsdienstnutzer durch Zahlungsdienstleister auferlegte Pflichten zum Schutz personalisierter Sicherheitsmerkmale vor unbefugtem Zugriff sollten jedoch nicht so abgefasst sein, dass Zahlungsdienstnutzer davon abgehalten werden, die Vorteile der durch andere Zahlungsdienstleister angebotenen Dienste, einschließlich Zahlungsauslösedienste und Kontoinformationsdienste, zu nutzen. Solche Geschäftsbedingungen sollten keine Bestimmungen enthalten, die die Nutzung von Zahlungsdiensten anderer gemäß dieser Richtlinie (EU) XXX (PSD3) zugelassener oder registrierter Zahlungsdienstleister in irgendeiner Weise erschweren. Darüber hinaus sollte festgelegt werden, dass für die Tätigkeiten von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern der Name des Kontoinhabers und die Kontonummer keine sensiblen Zahlungsdaten darstellen.

(68) Für den umfassenden Erfolg von „Open Banking“ müssen die Vorschriften, mit denen diese Tätigkeit geregelt wird, konsequent und wirksam durchgesetzt werden. Da es auf Unionsebene keine Behörde für die Durchsetzung der Rechte und Pflichten des „Open Banking“ gibt, sind die zuständigen nationalen Behörden die erste Ebene für die Durchsetzung der Vorschriften zum Open Banking. Es ist von wesentlicher Bedeutung, dass die zuständigen nationalen Behörden proaktiv und rigoros dafür sorgen, dass der Rechtsrahmen der Union für „Open Banking“ eingehalten wird. Die unzureichende Durchsetzung durch die zuständigen Behörden wird von Open-Banking-Betreibern regelmäßig als einer der Gründe für die nach wie vor begrenzte Inanspruchnahme in der Union angeführt. Die zuständigen nationalen Behörden sollten über angemessene Ressourcen verfügen, um ihre Durchsetzungsaufgaben wirksam und effizient wahrnehmen zu können. Die zuständigen nationalen Behörden sollten einen reibungslosen und regelmäßigen Dialog zwischen den verschiedenen Akteuren des „Open-Banking“-Ökosystems fördern und vermitteln. Kontoführende Zahlungsdienstleister sowie Kontoinformations- und Zahlungsauslösedienstleister, die ihren Verpflichtungen nicht nachkommen, sollten mit angemessenen Sanktionen belegt werden. Eine von der EBA koordinierte regelmäßige Überwachung des Marktes für „Open Banking“ in der Union durch die zuständigen Behörden dürfte die Durchsetzung erleichtern, und die Erhebung von Daten über den Markt für „Open Banking“ wird eine derzeit bestehende Datenlücke schließen, wodurch eine wirksame Messung der tatsächlichen Inanspruchnahme von „Open Banking“ in der Union behindert wird. Kontoführende Zahlungsdienstleister sowie Kontoinformations- und Zahlungsauslösedienstleister sollten gemäß Artikel 10 des Vorschlags zum Datengesetz Zugang zu Streitbeilegungsstellen haben, sobald die genannte Verordnung in Kraft tritt.

(69) Die parallele Verwendung des Begriffs „ausdrückliche Zustimmung“ in der Richtlinie (EU) 2015/2366 bzw. „ausdrückliche Einwilligung“ in der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[48] hat zu Fehlinterpretationen geführt. Gegenstand der ausdrücklichen Zustimmung gemäß Artikel 94 Absatz 2 der Richtlinie (EU) 2015/2366 ist die Erlaubnis, die personenbezogenen Daten, die für das Erbringen des Zahlungsdienstes notwendig sind, abzurufen, zu verarbeiten und zu speichern. Daher sollte eine Klarstellung vorgenommen werden, um die Rechtssicherheit zu erhöhen und eine klare Differenzierung gegenüber den Datenschutzvorschriften vorzunehmen. Wo in der Richtlinie (EU) 2015/2366 der Ausdruck „ausdrückliche Zustimmung“ verwendet wurde, sollte in der vorliegenden Verordnung der Ausdruck „Erlaubnis“ verwendet werden. Wird auf eine „Erlaubnis“ Bezug genommen, so sollte diese Bezugnahme die Pflichten der Zahlungsdienstleister nach Artikel 6 der Verordnung (EU) 2016/679 unberührt lassen. Daher sollte „Erlaubnis“ nicht ausschließlich als „Einwilligung“ oder „ausdrückliche Einwilligung“ im Sinne der Verordnung (EU) 2016/679 verstanden werden.

(70) Die Sicherheit von Überweisungen ist von grundlegender Bedeutung, um das Vertrauen der Zahlungsdienstnutzer in diese Dienste zu stärken und deren Nutzung sicherzustellen. Zahler, die eine Überweisung an einen bestimmten Zahlungsempfänger in Auftrag geben wollen, geben möglicherweise aufgrund von Betrug oder aufgrund eines Fehlers einen Kundenidentifikator an, der nicht dem Konto des Zahlungsempfängers zuzuordnen ist. Um zur Verringerung von Betrug und Fehlern beizutragen, sollten Zahlungsdienstnutzer einen Service in Anspruch nehmen können, mit dem überprüft wird, ob zwischen dem Kundenidentifikator des Zahlungsempfängers und dem vom Zahler angegebenen Namen des Zahlungsempfängers Abweichungen bestehen, und bei Feststellung solcher Abweichungen den Zahler davon in Kenntnis setzt. Diese Leistungen haben sich in den Ländern, in denen sie verwendet werden, sehr positiv auf das Ausmaß von Betrug und Fehlern ausgewirkt. Angesichts der Bedeutung dieses Service für die Betrugs- und Fehlerprävention sollte dieser Service den Verbrauchern kostenlos zur Verfügung stehen. Um unnötige Reibungsverluste oder Verzögerungen bei der Bearbeitung des Vorgangs zu vermeiden, sollte der Zahlungsdienstleister des Zahlers eine entsprechende Benachrichtigung innerhalb von höchstens wenigen Sekunden ab dem Zeitpunkt übermitteln, zu dem der Zahler die Angaben zum Zahlungsempfänger eingegeben hat. Damit der Zahler entscheiden kann, ob er den beabsichtigten Vorgang weiterverfolgen will, sollte der Zahlungsdienstleister des Zahlers eine solche Benachrichtigung vornehmen, bevor der Zahler den Vorgang autorisiert. Den Zahlern können bestimmte Lösungen für die Auslösung von Überweisungen zur Verfügung stehen, die es ihnen ermöglichen, einen Zahlungsauftrag zu erteilen, ohne selbst den Kundenidentifikator einzufügen. Stattdessen werden solche Datenelemente vom Anbieter dieser Auslösungslösung bereitgestellt. In solchen Fällen ist kein Service erforderlich, der die Übereinstimmung zwischen dem Kundenidentifikator und dem Namen des Zahlungsempfängers überprüft, da das Betrugs- oder Fehlerrisiko erheblich verringert wird.

[48] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

(71) Die Verordnung (EU) XXX zur Änderung der Verordnung (EU) Nr. 260/2012 sieht vor, dass den Nutzern von Sofortüberweisungen in Euro ein Service zur Überprüfung der Übereinstimmung zwischen dem Kundenidentifikator und dem Namen des Zahlungsempfängers angeboten wird. Um einen kohärenten Rahmen für alle Überweisungen zu schaffen und gleichzeitig unnötige Überschneidungen zu vermeiden, sollte der in der vorliegenden Verordnung genannte Überprüfungsservice nur für Überweisungen gelten, die nicht unter die Verordnung (EU) XXX zur Änderung der Verordnung (EU) Nr. 260/2012 fallen.

(72) Einige Attribute des Namens des Zahlungsempfängers, an dessen Konto der Zahler eine Überweisung versenden möchte, könnten die Wahrscheinlichkeit erhöhen, dass der Zahlungsdienstleister eine Unstimmigkeit feststellt, etwa das Vorhandensein diakritischer Zeichen oder unterschiedliche mögliche Transliterationen von Namen in verschiedenen Alphabeten, bei natürlichen Personen Unterschiede zwischen üblicherweise verwendeten Namen und Namen, die in formalen Identifikationsdokumenten angegeben sind, oder bei juristischen Personen Unterschiede zwischen Handels- und Firmennamen. Um unnötige Reibungsverluste bei der Bearbeitung von Überweisungen zu vermeiden und dem Zahler die Entscheidung darüber zu erleichtern, ob er einen beabsichtigten Vorgang fortsetzen will, sollten Zahlungsdienstleister anzeigen, wie deutlich sich die Angaben unterscheiden, indem sie in der Benachrichtigung angeben, ob es „keine Übereinstimmung“ oder eine „starke Übereinstimmung“ gibt.

(73) Wird ein Zahlungsvorgang autorisiert, obwohl der Abgleichservice eine Abweichung festgestellt und dem Zahlungsdienstnutzer angezeigt hat, kann dies dazu führen, dass der Geldbetrag an einen unbeabsichtigten Zahlungsempfänger überwiesen wird. Die Zahlungsdienstleister sollten die Zahlungsdienstnutzer über die möglichen Folgen ihrer Entscheidung informieren, die gemeldete Abweichung zu ignorieren und mit der Ausführung des Vorgangs fortzufahren. Zahlungsdienstnutzer sollten sich während ihres Vertragsverhältnisses mit dem Zahlungsdienstleister jederzeit gegen die Nutzung eines solchen Service entscheiden können. Nachdem sie sich dagegen entschieden haben, sollten die Zahlungsdienstnutzer weiterhin die Möglichkeit haben, den Service wieder in Anspruch zu nehmen.

(74) Der Zahlungsdienstnutzer sollte den Zahlungsdienstleister so bald wie möglich über Beanstandungen im Zusammenhang mit angeblich nicht autorisierten, fehlerhaft ausgeführten Zahlungsvorgängen oder autorisierten Überweisungen informieren, bei denen eine Fehlfunktion des Abgleichservice aufgetreten ist, sofern der Zahlungsdienstleister seinen Informationspflichten nachgekommen ist. Hat der Zahlungsdienstnutzer die Anzeigefrist eingehalten, so sollte er diese Ansprüche innerhalb der nationalen Verjährungsfristen geltend machen können. Andere Ansprüche zwischen Zahlungsdienstnutzern und Zahlungsdienstleistern sollten davon unberührt bleiben.

(75) Für den Fall von Schäden durch nicht autorisierte Zahlungen oder bestimmte autorisierte Überweisungen sollte die Verlustzuweisung geregelt werden. Für andere Zahlungsdienstnutzer als Verbraucher können andere Bestimmungen gelten, da diese in der Regel besser in der Lage sein dürften, das Betrugsrisiko einzuschätzen und Gegenmaßnahmen zu treffen. Zur Sicherstellung eines hohen Verbraucherschutzniveaus sollten Zahler stets berechtigt sein, ihren Antrag auf Erstattung an den kontoführenden Zahlungsdienstleister zu richten, auch wenn ein Zahlungsauslösedienstleister am Zahlungsvorgang beteiligt war. Die

Haftungsverteilung zwischen den Zahlungsdienstleistern sollte davon unberührt bleiben.

(76) Im Fall von Zahlungsauslösediensten sollten der kontoführende Zahlungsdienstleister und der in den Zahlungsvorgang eingebundene Zahlungsauslösedienstleister durch Haftungsverteilung gezwungen sein, für den jeweils von ihnen kontrollierten Teil des Zahlungsvorgangs die Verantwortung zu übernehmen.

(77) Im Falle eines nicht autorisierten Zahlungsvorgangs sollte der Zahlungsdienstleister dem Zahler unverzüglich den Betrag, der Gegenstand dieses Zahlungsvorgangs war, erstatten. Besteht jedoch ein dringender Verdacht, dass ein nicht autorisierter Zahlungsvorgang Folge eines betrügerischen Verhaltens des Zahlers ist, und beruht dieser Verdacht auf objektiven Gründen, die der zuständigen nationalen Behörde vom Zahlungsdienstleister mitgeteilt wurden, so sollte der Zahlungsdienstleister eine Untersuchung durchführen können, bevor er dem Zahler den entsprechenden Betrag erstattet. Der Zahlungsdienstleister sollte dem Zahler innerhalb von zehn Geschäftstagen nach Kenntnisnahme oder Benachrichtigung über den Zahlungsvorgang entweder den Betrag des nicht autorisierten Zahlungsvorgangs erstatten oder dem Zahler die Gründe und Belege für die Ablehnung der Erstattung vorlegen und die Stellen angeben, an die sich der Zahler wenden kann, wenn der Zahler die angegebenen Gründe nicht akzeptiert. Um den Zahler vor Nachteilen zu schützen, sollte das Wertstellungsdatum der Erstattung nicht nach dem Datum liegen, an dem das Konto mit dem Betrag belastet wurde. Um dem Zahlungsdienstnutzer einen Anreiz zu geben, seinem Zahlungsdienstleister jeden Diebstahl oder Verlust eines Zahlungsinstruments unverzüglich anzuzeigen und so das Risiko nicht autorisierter Zahlungsvorgänge zu verringern, sollte der Nutzer lediglich für einen begrenzten Betrag selbst haften, es sei denn, er hat in betrügerischer Absicht oder grob fahrlässig gehandelt. In diesem Zusammenhang erscheint ein Betrag von 50 EUR zur Sicherstellung eines harmonisierten und hochgradigen Schutzes der Nutzer innerhalb der Union angemessen. Keine Haftung sollte bestehen, wenn der Zahler außerstande ist, den Verlust, den Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments zu bemerken. Auch sollte ein Zahlungsdienstnutzer, sobald er seinem Zahlungsdienstleister angezeigt hat, dass sein Zahlungsinstrument missbraucht worden sein könnte, keine weiteren, durch die nicht autorisierte Nutzung dieses Instruments verursachten Schäden tragen müssen. Zahlungsdienstleister sollten für die technische Sicherheit ihrer eigenen Produkte verantwortlich sein.

(78) Haftungsbestimmungen für autorisierte Überweisungen bei fehlerhafter Anwendung oder Fehlfunktion des Service zur Feststellung von Abweichungen zwischen Namen und Kundenidentifikator eines Zahlungsempfängers würden die richtigen Anreize für Zahlungsdienstleister schaffen, einen voll funktionsfähigen Service zu erbringen, um das Risiko schlecht informierter Zahlungsautorisierungen zu verringern. Beschließt der Zahler, einen solchen Service in Anspruch zu nehmen, so sollte der Zahlungsdienstleister des Zahlers für den vollen Betrag der Überweisung haftbar gemacht werden, wenn der Zahlungsdienstleister es unterlassen hat, den Zahler über eine Abweichung zwischen dem Kundenidentifikator und dem vom Zahler angegebenen Namen des Zahlungsempfängers zu unterrichten, obwohl er dies bei ordnungsgemäßem Funktionieren hätte tun müssen, und dieser Fehler dem Zahler einen finanziellen Schaden verursacht hat. Ist die Haftung des Zahlungsdienstleisters des Zahlers dem Zahlungsdienstleister des Zahlungsempfängers zuzurechnen, so sollte der Zahlungsdienstleister des Zahlungsempfängers dem Zahlungsdienstleister des Zahlers den entstandenen finanziellen Schaden ersetzen.

(79) Verbraucher sollten im Zusammenhang mit bestimmten betrügerischen Zahlungsvorgängen, die sie autorisiert haben, ohne zu wissen, dass es sich um betrügerische Zahlungsvorgänge handelte, angemessen geschützt werden. Die Zahl der Fälle von „Social Engineering“, in denen Verbraucher bei der Autorisierung eines Zahlungsvorgangs an einen Betrüger irregeführt werden, hat in den letzten Jahren erheblich zugenommen. Leider werden Fälle, in denen Betrüger vorgeben, Mitarbeiter des Zahlungsdienstleisters eines Kunden zu sein („Spoofing“), und den Namen, die Postanschrift oder die Telefonnummer des Zahlungsdienstleisters missbrauchen, um das Vertrauen der Kunden zu gewinnen und sie dazu zu bewegen, bestimmte Handlungen durchzuführen, in der Union immer häufiger. Diese neuen Arten des „Spoofing“-Betrugs verwischen die in der Richtlinie (EU) 2015/2366 getroffene Unterscheidung zwischen autorisierten und nicht autorisierten Transaktionen. Auch die Mittel, bei denen davon ausgegangen werden kann, dass die Zustimmung erteilt wurde, werden immer schwieriger zu identifizieren, da Betrüger die Kontrolle über den gesamten Zustimmungs- und Authentifizierungsprozess, einschließlich des Abschlusses einer starken Kundenauthentifizierung, übernehmen können. Die Bedingungen, unter denen der Kunde eine Transaktion autorisiert hat, indem er seine Erlaubnis dazu erteilt hat, sollten – auch von Gerichten – gebührend berücksichtigt werden, um eine Transaktion als autorisiert oder nicht autorisiert einzustufen. So könnte eine Transaktion in einer Situation autorisiert worden sein, in der die Autorisierung in manipulierten Räumlichkeiten erteilt wurde, die die Integrität der Erlaubnis beeinträchtigten. Es ist daher nicht mehr möglich, wie in der Richtlinie (EU) 2015/2366, Erstattungen auf nicht autorisierte Transaktionen zu beschränken. Es wäre jedoch für die Zahlungsdienstleister unverhältnismäßig und finanziell sehr kostspielig, bei allen betrügerischen Transaktionen, unabhängig davon, ob sie autorisiert wurden oder nicht, einen systematischen Erstattungsanspruch einzuräumen. Dies könnte auch zu einem moralischem Risiko und einer geringeren Wachsamkeit des Kunden führen.

(80) Zahlungsdienstleister könnten ebenfalls als Opfer von Datenmanipulation („Spoofing“) angesehen werden, weil ihre Daten missbraucht wurden. Zahlungsdienstleister haben jedoch mehr Möglichkeiten als Verbraucher, solche Betrugsfälle zu unterbinden, und zwar durch angemessene Prävention und robuste technische Schutzmaßnahmen, die gemeinsam mit den Anbietern elektronischer Kommunikationsdienste wie Mobilfunkbetreibern, Internetplattformen usw. entwickelt werden. Fälle, in denen sich Betrüger als Bankmitarbeiter ausgeben, beeinträchtigen den guten Ruf der Bank und des gesamten Bankensektors und können den Verbrauchern in der Union erheblichen finanziellen Schaden zufügen, indem sie ihr Vertrauen in den elektronischen Zahlungsverkehr und in das Bankensystem beeinträchtigen. Ein gutgläubiger Verbraucher, der Opfer eines solchen „Spoofing“-Betrugs geworden ist, bei dem Betrüger vorgeben, Mitarbeiter des Zahlungsdienstleisters eines Kunden zu sein, und den Namen, die Postanschrift oder die Telefonnummer des Zahlungsdienstleisters missbräuchlich verwenden, sollte daher Anspruch auf Erstattung des vollen Betrags des betrügerischen Zahlungsvorgangs durch den Zahlungsdienstleister haben, es sei denn, der Zahler hat in betrügerischer Absicht oder grob fahrlässig gehandelt. Sobald der Verbraucher Kenntnis davon erhält, dass er Opfer dieser Art von Spoofing-Betrug geworden ist, sollte er den Vorfall unverzüglich der Polizei, vorzugsweise über Online-Beschwerdeverfahren, sofern sie von der Polizei zur Verfügung gestellt werden, und seinem Zahlungsdienstleister unter Vorlage aller erforderlichen Belege melden. Eine Erstattung sollte nicht gewährt werden, wenn diese Verfahrensvoraussetzungen nicht erfüllt sind.

(81) Aufgrund ihrer Verpflichtung, die Sicherheit ihrer Dienste gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[49] zu gewährleisten, sind die Anbieter elektronischer Kommunikationsdienste in der Lage, einen Beitrag zur gemeinsamen Bekämpfung von „Spoofing"-Betrug zu leisten. Unbeschadet der in den nationalen Rechtsvorschriften zur Umsetzung dieser Richtlinie festgelegten Verpflichtungen sollten die Anbieter elektronischer Kommunikationsdienste daher mit den Zahlungsdienstleistern zusammenarbeiten, um weitere Betrugsfälle dieser Art zu verhindern, indem sie unter anderem unverzüglich tätig werden, um sicherzustellen, dass geeignete organisatorische und technische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit der Kommunikation gemäß der Richtlinie 2002/58/EG getroffen werden. Ansprüche eines Zahlungsdienstleisters gegen andere Anbieter, z. B. Anbieter elektronischer Kommunikationsdienste, wegen eines im Zusammenhang mit dieser Art von Betrug entstandenen finanziellen Schadens sollten im Einklang mit dem nationalen Recht geltend gemacht werden.

(82) Zur Feststellung einer möglichen Fahrlässigkeit oder einer groben Fahrlässigkeit des Zahlungsdienstnutzers sollten alle Umstände berücksichtigt werden. Ob und in welchem Maße fahrlässig gehandelt wurde, sollte nach nationalem Recht beurteilt werden. Während der Begriff der Fahrlässigkeit einen Verstoß gegen die Sorgfaltspflicht impliziert, sollte der Begriff „grobe Fahrlässigkeit" mehr als reine Fahrlässigkeit bedeuten, wenn es sich um ein Verhalten handelt, das ein erhebliches Maß an mangelnder Sorgfalt aufwies; beispielsweise die Aufbewahrung der zur Autorisierung eines Zahlungsvorgangs verwendeten Sicherheitsmerkmale neben dem Zahlungsinstrument in einem Format, das für Dritte offen und leicht auffindbar ist. Die Tatsache, dass ein Verbraucher bereits eine Erstattung von einem Zahlungsdienstleister erhalten hat, nachdem er Opfer von sich als Bankmitarbeiter ausgebenden Betrügern geworden ist, und einen weiteren Erstattungsantrag bei demselben Zahlungsdienstleister einreicht, nachdem er erneut Opfer derselben Art von Betrug geworden ist, könnte als „grobe Fahrlässigkeit" angesehen werden, da dies auf ein hohes Maß an mangelnder Sorgfalt seitens des Nutzers hindeuten könnte, der wachsamer hätte sein müssen, nachdem er bereits Opfer derselben betrügerischen Vorgehensweise gewesen ist.

(83) Klauseln und Bedingungen in einem Vertrag über die Bereitstellung und Nutzung eines Zahlungsinstruments, die eine Erschwerung der Beweislast für den Verbraucher oder eine Verringerung der Beweislast für die kartenausgebende Stelle zur Folge hätten, sollten nichtig sein. Darüber hinaus ist es angemessen, dass in bestimmten Situationen und insbesondere dann, wenn das Zahlungsinstrument bei der Verkaufsstelle nicht vorliegt, wie im Falle von Online-Zahlungen, die Beweislast für eine angebliche Fahrlässigkeit beim Zahlungsdienstleister liegt, da die entsprechenden Möglichkeiten des Zahlers in solchen Fällen sehr begrenzt sind.

(84) Verbraucher sind besonders gefährdet in Fällen von kartengebundenen Zahlungsvorgängen, bei denen der genaue Betrag zum Zeitpunkt, an dem der Zahler seine Erlaubnis zur Ausführung des Zahlungsvorgangs erteilt, noch nicht bekannt ist, beispielsweise an automatisierten Tankstellen, bei Mietwagenverträgen oder bei Hotelbuchungen. Der Zahlungsdienstleister des Zahlers sollte in der Lage sein, einen Geldbetrag auf dem Zahlungskonto des Zahlers zu sperren, der zu dem Betrag des

[49] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ABl. L 201 vom 31.7.2002, S. 37).

Zahlungsvorgangs im Verhältnis steht, der vom Zahler vernünftigerweise erwartet werden kann, und nur dann, wenn der Zahler dem Blockieren dieses genauen Betrags zugestimmt hat. Diese Gelder sollten unmittelbar nach Erhalt der Informationen über den genauen endgültigen Betrag des Zahlungsvorgangs und spätestens unmittelbar nach Eingang des Zahlungsauftrags freigegeben werden. Um eine rasche Freigabe der Differenz zwischen dem blockierten Betrag und dem genauen Betrag des Zahlungsvorgangs sicherzustellen, sollte der Zahlungsempfänger den Zahlungsdienstleister unverzüglich nach der Erbringung der Dienstleistung oder der Lieferung der Waren an den Zahler informieren.

(85) Es bestehen in Mitgliedstaaten, deren Währung nicht der Euro ist, weiterhin herkömmliche Lastschriftverfahren für andere Währungen als den Euro. Diese Verfahren haben sich als effizient erwiesen und gewährleisten dem Zahler das gleiche hohe Schutzniveau durch andere Formen des Schutzes, der nicht immer auf einem bedingungslosen Erstattungsanspruch beruht. In diesem Fall sollte der Zahler durch den allgemeinen Grundsatz der Erstattung geschützt werden, wenn der ausgeführte Zahlungsvorgang den Betrag übersteigt, den der Zahler vernünftigerweise hätte erwarten können. Darüber hinaus sollten die Mitgliedstaaten Vorschriften für das Recht auf Erstattung festlegen können, die für den Zahler günstiger sind als die in der vorliegenden Verordnung festgelegten. Es wäre verhältnismäßig, es dem Zahler und dem Zahlungsdienstleister des Zahlers zu gestatten, in einem Rahmenvertrag zu vereinbaren, dass der Zahler in Fällen, in denen der Zahler geschützt ist, keinen Erstattungsanspruch hat. Ein Grund dafür könnte entweder sein, dass er die Erlaubnis zur Ausführung des Zahlungsvorgangs seinem Zahlungsdienstleister direkt erteilt hat – auch wenn der Zahlungsdienstleister im Auftrag des Zahlungsempfängers handelt – oder dass die Informationen über den anstehenden Zahlungsvorgang dem Zahler in einer vereinbarten Form mindestens vier Wochen vor dem Fälligkeitstermin vom Zahlungsdienstleister oder vom Zahlungsempfänger mitgeteilt oder zugänglich gemacht wurden. In jedem Fall sollte der Zahler im Falle von nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorgängen oder im Falle von autorisierten Überweisungen, bei denen der Abgleichservice fehlerhaft angewandt wurde oder sich Betrüger als Mitarbeiter des Zahlungsdienstleisters ausgegeben haben, durch die allgemeine Erstattungsregel geschützt sein.

(86) Für ihre Finanzplanung und die fristgerechte Erfüllung ihrer Zahlungsverpflichtungen müssen Verbraucher und Unternehmen genau wissen, wie lange es dauert, bis ein Zahlungsauftrag ausgeführt ist. Daher muss festgelegt werden, wann Rechte und Pflichten wirksam werden, d. h. wann der Zahlungsdienstleister den Zahlungsauftrag erhält, und auch wann der Zahlungsdienstleister die Möglichkeit hatte, ihn über die im Zahlungsdienstvertrag vereinbarten Kommunikationsmittel zu erhalten. Dies gilt ungeachtet einer vorherigen Beteiligung an dem Prozess, der zur Erstellung und Übermittlung des Zahlungsauftrags führt, einschließlich der Sicherheit und Verfügbarkeit von Mitteln, Informationen über die Verwendung der persönlichen Identifikationsnummer oder der Erteilung eines Zahlungsversprechens. Darüber hinaus sollte als Eingang eines Zahlungsauftrags der Zeitpunkt gelten, zu dem der Zahlungsauftrag, mit dem das Konto des Zahlers belastet werden soll, beim Zahlungsdienstleister des Zahlers eingeht. Der Zeitpunkt, an dem ein Zahlungsempfänger seinem Zahlungsdienstleister Zahlungsaufträge z. B. für das Inkasso von Kartenzahlungen oder Lastschriften übermittelt oder an dem er von seinem Zahlungsdienstleister eine Vorfinanzierung der entsprechenden Beträge (Gutschrift unter Vorbehalt) erhält, sollte hingegen unerheblich sein. Die Nutzer sollten sich darauf verlassen können, dass ihr vollständig ausgefüllter und gültiger

Zahlungsauftrag ordnungsgemäß ausgeführt wird, wenn der Zahlungsdienstleister keinen vertraglichen oder gesetzlichen Grund hat, ihn abzulehnen. Lehnt der Zahlungsdienstleister es ab, einen Zahlungsauftrag auszuführen, sollte der Zahlungsdienstnutzer von der Ablehnung und den Gründen dafür vorbehaltlich des Unionsrechts und des nationalen Rechts so rasch wie möglich in Kenntnis gesetzt werden. Bestimmt der Rahmenvertrag, dass der Zahlungsdienstleister ein Entgelt für die Ablehnung erheben kann, sollte ein derartiges Entgelt objektiv begründet und so niedrig wie möglich sein.

(87) Da vollautomatisierte Zahlungssysteme Zahlungen mit hoher Geschwindigkeit abwickeln und Zahlungsaufträge ab einem bestimmten Zeitpunkt nicht ohne kostspieligen manuellen Eingriff widerrufen werden können, muss eine Widerrufsfrist festgelegt werden. Allerdings sollten die Parteien je nach Art des Zahlungsdienstes und des Zahlungsauftrags unterschiedliche Zeitpunkte vereinbaren können. Der Widerruf sollte dabei nur zwischen einem Zahlungsdienstnutzer und einem Zahlungsdienstleister gelten und nicht die Unwiderrufbarkeit und Endgültigkeit der Zahlungsvorgänge in Zahlungssystemen berühren.

(88) Die Unwiderrufbarkeit eines Zahlungsauftrags sollte nicht die Rechte oder Pflichten eines Zahlungsdienstleisters nach dem Recht der Mitgliedstaaten – soweit sie sich aus dem Rahmenvertrag des Zahlers, innerstaatlichen Rechts- und Verwaltungsvorschriften oder Leitlinien ergeben – berühren, im Falle einer Streitigkeit zwischen dem Zahler und dem Zahlungsempfänger dem Zahler den Betrag, der Gegenstand des ausgeführten Zahlungsvorgangs war, zu erstatten. Eine solche Erstattung sollte als neuer Zahlungsauftrag gelten. In allen anderen Fällen sollten Rechtsstreitigkeiten, die sich aus der dem Zahlungsauftrag zugrunde liegenden Vertragsbeziehung ergeben, ausschließlich zwischen Zahler und Zahlungsempfänger geregelt werden.

(89) Im Interesse einer voll integrierten und vollautomatisierten Abwicklung von Zahlungen und im Interesse der Rechtssicherheit im Hinblick auf sämtliche Verpflichtungen der Zahlungsdienstnutzer untereinander sollte der vom Zahler transferierte Betrag dem Konto des Zahlungsempfängers in voller Höhe gutgeschrieben werden. Aus diesem Grund sollte keine der an der Ausführung eines Zahlungsauftrags beteiligten zwischengeschalteten Stellen Abzüge vom transferierten Betrag vornehmen dürfen. Zahlungsempfänger sollten jedoch mit ihrem Zahlungsdienstleister eine ausdrückliche Vereinbarung treffen dürfen, die Letztere zum Abzug ihrer eigenen Entgelte berechtigt. Damit der Zahlungsempfänger jedoch überprüfen kann, ob der geschuldete Betrag ordnungsgemäß bezahlt wurde, sollten in den Informationen über die Ausführung des Zahlungsvorgangs nicht nur die transferierten Beträge in voller Höhe, sondern auch die abgezogenen Entgelte aufgeführt werden.

(90) Im Interesse einer unionsweit effizienteren Abwicklung von Zahlungen sollte für alle vom Zahler ausgelösten Zahlungsaufträge, die auf den Euro oder die Währung eines Mitgliedstaats, dessen Währung nicht der Euro ist, lauten, einschließlich für andere Überweisungen als Sofortüberweisungen und für Finanztransfers, eine Ausführungsfrist von maximal einem Tag festgelegt werden. Für alle anderen Zahlungen, z. B. solche, die vom oder über den Zahlungsempfänger ausgelöst werden (einschließlich Lastschriften oder Kartenzahlungen), sollte ebenfalls eine Eintagesfrist gelten, sofern Zahlungsdienstleister und Zahler nicht ausdrücklich eine längere Ausführungsfrist vereinbart haben. Diese Fristen sollten um einen zusätzlichen Geschäftstag verlängert werden können, wenn ein Zahlungsauftrag beleghaft erteilt

wird, damit auch weiterhin Zahlungsdienste für Verbraucher erbracht werden können, die nur mit der Papierform vertraut sind. Wenn ein Lastschriftverfahren genutzt wird, sollte der Zahlungsdienstleister des Zahlungsempfängers den Inkassoauftrag so rechtzeitig innerhalb der zwischen ihm und dem Zahlungsempfänger vereinbarten Frist übermitteln, dass eine Verrechnung zu dem vereinbarten Fälligkeitstermin möglich ist. Es sollte möglich sein, Vorschriften beizubehalten oder festzulegen, in denen eine Ausführungsfrist von weniger als einem Geschäftstag festgelegt wird.

(91) Ist einer der Zahlungsdienstleister nicht in der Union ansässig, sollten die Regeln über die Gutschrift des vollen Betrags und die Ausführungsfrist als gute Praxis gelten. Bei Überweisungen oder Finanztransfers an einen außerhalb der Union ansässigen Zahlungsempfänger sollte der Zahlungsdienstleister des Zahlers dem Zahler eine Schätzung des Zeitraums vorlegen, der für die Gutschrift der Überweisung oder des Finanztransfers an den Zahlungsdienstleister des Zahlungsempfängers außerhalb der Union benötigt wird. Von Zahlungsdienstleistern in der Union kann nicht erwartet werden, dass sie den Zeitraum schätzen, den ein Zahlungsdienstleister außerhalb der Union benötigt, um das Geld nach dessen Erhalt dem Konto des Zahlungsempfängers gutzuschreiben.

(92) Um ihr Vertrauen in die Zahlungsmärkte zu stärken, ist es von entscheidender Bedeutung, dass die Zahlungsdienstnutzer die tatsächlichen Entgelte für Zahlungsdienste kennen. Eine intransparente Preisgestaltung sollte deshalb untersagt werden, da diese es den Nutzern anerkanntermaßen extrem erschwert, den tatsächlichen Preis eines Zahlungsdienstes zu ermitteln. Insbesondere eine für den Nutzer ungünstige Wertstellungspraxis sollte unzulässig sein.

(93) Der Zahlungsdienstleister sollte unmissverständlich angeben können, welche Angaben für die ordnungsgemäße Ausführung eines Zahlungsauftrags erforderlich sind. Der Zahlungsdienstleister des Zahlers sollte die gebührende Sorgfalt („Due Diligence“) walten lassen und – soweit technisch und ohne manuellen Eingriff möglich – überprüfen, ob der Kundenidentifikator kohärent ist, und wenn das nicht der Fall ist, den Zahlungsauftrag zurückweisen und den Zahler davon unterrichten.

(94) Reibungslos und zügig funktionierende Zahlungssysteme setzen 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. Daher ist es außer im Falle ungewöhnlicher und unvorhersehbarer Umstände gerechtfertigt, dem Zahlungsdienstleister die Haftung für die Ausführung eines vom Nutzer entgegengenommenen Zahlungsauftrags zu übertragen, außer für Handlungen und Unterlassungen des Zahlungsdienstleisters des Zahlungsempfängers, für dessen Auswahl allein der Zahlungsempfänger verantwortlich ist. Um jedoch den Zahler im unwahrscheinlichen Fall, dass unklar bleibt, ob der Zahlungsbetrag tatsächlich beim Zahlungsdienstleister des Zahlungsempfängers eingegangen ist oder nicht, nicht ungeschützt zu lassen, sollte die entsprechende Beweislast in diesem Fall beim Zahlungsdienstleister des Zahlers liegen. Im Regelfall kann davon ausgegangen werden, dass das zwischengeschaltete Institut (üblicherweise eine unparteiische Stelle wie eine Zentralbank oder eine Clearingstelle), das den Zahlungsbetrag vom sendenden zum empfangenden Zahlungsdienstleister transferiert, die Kontodaten

speichert und in der Lage ist, sie erforderlichenfalls mitzuteilen. Ist der Zahlungsbetrag dem Konto des empfangenden Zahlungsdienstleisters gutgeschrieben worden, so sollte der Zahlungsempfänger einen unmittelbaren Anspruch gegen seinen Zahlungsdienstleister auf Gutschrift des Betrags auf seinem Konto haben.

(95) Der Zahlungsdienstleister des Zahlers, also der kontoführende Zahlungsdienstleister oder gegebenenfalls der Zahlungsauslösedienstleister, sollte für die ordnungsgemäße Ausführung des Zahlungsvorgangs haften, einschließlich dafür, dass die Zahlung in voller Höhe und fristgerecht ausgeführt wird, und für Fehler anderer Parteien in der Zahlungskette bis zum Zahlungskonto des Zahlungsempfängers vollverantwortlich sein. Im Zuge dieser Haftung sollte der Zahlungsdienstleister des Zahlers dann, wenn dem Zahlungsdienstleister des Zahlungsempfängers der vollständige Betrag nicht oder zu spät gutgeschrieben wird, den Zahlungsvorgang korrigieren oder dem Zahler den betreffenden Betrag des Zahlungsvorgangs unbeschadet etwaiger anderer nach nationalem Recht angemeldeter Ansprüche unverzüglich erstatten. Wegen der Haftung des Zahlungsdienstleisters sollten Zahler oder Zahlungsempfänger im Zusammenhang mit einer fehlerhaften Zahlung keine Kosten tragen. Für den Fall der nicht erfolgten, fehlerhaften oder verspäteten Ausführung von Zahlungsvorgängen sollte das Wertstellungsdatum korrigierender Zahlungen durch Zahlungsdienstleister stets dem Datum der Wertstellung bei korrekter Ausführung entsprechen.

(96) Das ordnungsgemäße Funktionieren von Überweisungen und anderen Zahlungsdiensten setzt voraus, dass die Zahlungsdienstleister und ihre zwischengeschalteten Stellen, einschließlich Verarbeiter, an Verträge gebunden sind, die ihre wechselseitigen Rechte und Pflichten festlegen. Haftungsfragen bilden einen wesentlichen Teil dieser Verträge. Um das gegenseitige Vertrauen unter den an einem Zahlungsvorgang beteiligten Zahlungsdienstleistern und zwischengeschalteten Stellen sicherzustellen, muss Rechtssicherheit dahin gehend geschaffen werden, dass ein Zahlungsdienstleister bei Nichtverschulden für Verluste oder gemäß der Haftungsregeln gezahlte Beträge entschädigt wird. Weitere Ansprüche und Einzelheiten der Ausgestaltung des Regressanspruchs sowie die Frage der praktischen Abwicklung von Ansprüchen gegenüber dem Zahlungsdienstleister oder der zwischengeschalteten Stelle aufgrund eines fehlerhaft ausgeführten Zahlungsvorgangs sollten Gegenstand einer Vereinbarung sein.

(97) Das Erbringen von Zahlungsdiensten durch den Zahlungsdienstleister kann mit der Verarbeitung personenbezogener Daten einhergehen. Die Bereitstellung von Kontoinformationsdiensten kann die Verarbeitung personenbezogener Daten einer betroffenen Person umfassen, die nicht Nutzer eines bestimmten Zahlungsdienstleisters ist, deren personenbezogene Daten jedoch für die Erfüllung eines Vertrags zwischen diesem Zahlungsdienstleister und dem Zahlungsdienstnutzer durch den Zahlungsdienstleister verarbeitet werden müssen. Werden personenbezogene Daten verarbeitet, sollte die Verarbeitung im Einklang mit der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[50], einschließlich der Grundsätze der Zweckbindung, der Datenminimierung und der Speicherbegrenzung, erfolgen. In allen im Rahmen dieser

[50] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

Verordnung entwickelten und eingesetzten Datenverarbeitungssystemen sollte der Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen eingebaut sein. Daher sollten die Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725 für die Überwachung der Verarbeitung personenbezogener Daten im Rahmen der vorliegenden Verordnung zuständig sein.

(98) Wie in der Mitteilung der Kommission über eine EU-Strategie für den Massenzahlungsverkehr anerkannt, ist das reibungslose Funktionieren der EU-Zahlungsmärkte von erheblichem öffentlichen Interesse. Wenn dies im Zusammenhang mit dieser Verordnung für die Erbringung von Zahlungsdiensten und die Einhaltung dieser Verordnung erforderlich ist, sollten Zahlungsdienstleister und Betreiber von Zahlungssystemen daher in der Lage sein, besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 und des Artikels 10 Absatz 1 der Verordnung (EU) 2018/1725 zu verarbeiten. Werden besondere Kategorien personenbezogener Daten verarbeitet, sollten Zahlungsdienstleister und Betreiber von Zahlungssystemen geeignete technische und organisatorische Maßnahmen ergreifen, um die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen. Diese Maßnahmen sollten technische Beschränkungen für die Weiterverwendung von Daten und die Anwendung modernster Sicherheits- und Datenschutzmaßnahmen, einschließlich Pseudonymisierung oder Verschlüsselung, umfassen, um die Einhaltung der Grundsätze der Zweckbindung, der Datenminimierung und der Speicherbegrenzung gemäß der Verordnung (EU) 2016/679 sicherzustellen. Die Zahlungsdienstleister und Zahlungssysteme sollten auch spezifische organisatorische Maßnahmen umsetzen, darunter Schulungen zur Verarbeitung solcher Daten, die Beschränkung des Zugangs zu besonderen Datenkategorien und die Aufzeichnung eines solchen Zugangs.

(99) Die Unterrichtung natürlicher Personen über die Verarbeitung personenbezogener Daten sollte im Einklang mit der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725 erfolgen.

(100) Betrüger richten sich häufig gegen die schutzbedürftigsten Personen unserer Gesellschaft. Die rechtzeitige Aufdeckung betrügerischer Zahlungsvorgänge ist von wesentlicher Bedeutung, und die Überwachung von Transaktionen spielt bei dieser Aufdeckung eine wichtige Rolle. Es ist daher angezeigt, den Zahlungsdienstleistern vorzuschreiben, dass sie über Mechanismen zur Überwachung von Transaktionen verfügen müssen, die dem entscheidenden Beitrag dieser Mechanismen zur Betrugsprävention Rechnung tragen und über den Schutz hinausgehen, den eine starke Kundenauthentifizierung in Bezug auf Zahlungsvorgänge, einschließlich Zahlungsauslösediensten, bietet.

(101) Die EBA sollte Entwürfe technischer Regulierungsstandards zu den spezifischen technischen Anforderungen im Zusammenhang mit Mechanismen zur Überwachung von Transaktionen ausarbeiten. Diese Anforderungen sollten auf dem Mehrwert aufbauen, der sich aus umgebungs- und verhaltensbezogenen Merkmalen im Zusammenhang mit den Zahlungsgewohnheiten des Zahlungsdienstnutzers ergibt.

(102) Um sicherzustellen, dass die Mechanismen zur Überwachung von Transaktionen wirksam funktionieren und die Zahlungsdienstleister so in die Lage versetzen, Betrug aufzudecken und zu verhindern, insbesondere durch Aufdeckung einer atypischen Nutzung von Zahlungsdiensten, die auf einen potenziell betrügerischen Vorgang hindeuten könnte, sollten die Zahlungsdienstleister in der Lage sein, Informationen über die Zahlungsvorgänge ihrer Kunden und ihre Zahlungskonten zu verarbeiten. Die

Zahlungsdienstleister sollten jedoch angemessene Aufbewahrungsfristen für verschiedene Datentypen festlegen, die zur Betrugsprävention verwendet werden. Diese Aufbewahrungsfristen sollten strikt auf den Zeitraum beschränkt sein, der für die Aufdeckung atypischer, potenziell betrügerischer Verhaltensweisen erforderlich ist, und die Zahlungsdienstleister sollten die Daten, die für die Aufdeckung und Prävention von Betrug nicht mehr erforderlich sind, regelmäßig löschen. Daten, die für die Zwecke der Transaktionsüberwachung verarbeitet werden, sollten nicht mehr verwendet werden, nachdem der Zahlungsdienstnutzer nicht mehr Kunde des Zahlungsdienstleisters ist.

(103) Überweisungsbetrug ist naturgemäß wandelbar und umfasst eine unerschöpfliche Vielfalt an Verfahren und Techniken, einschließlich des Diebstahls von Authentifizierungsdaten, Manipulation von Rechnungen und sozialer Manipulation. Um immer neue Arten von Betrug verhindern zu können, sollte die Überwachung von Transaktionen daher unter umfassender Nutzung von Technologien wie künstlicher Intelligenz kontinuierlich verbessert werden. Häufig ist ein Zahlungsdienstleister nicht über alle Elemente im Bilde, die zu einer zeitnahen Aufdeckung von Betrug führen könnten. Diese kann jedoch wirksamer gestaltet werden, wenn mehr Informationen über potenziell betrügerische Tätigkeiten anderer Zahlungsdienstleister bereitgestellt werden. Daher sollte der Austausch aller relevanten Informationen zwischen den Zahlungsdienstleistern möglich sein. Um betrügerische Zahlungsvorgänge besser aufdecken und ihre Kunden besser schützen zu können, sollten Zahlungsdienstleister für die Zwecke der Transaktionsüberwachung die von anderen Zahlungsdienstleistern auf multilateraler Basis ausgetauschten Daten zum Betrug nutzen, z. B. spezielle IT-Plattformen auf der Grundlage von Vereinbarungen über den Informationsaustausch. Um den Schutz der Zahler vor Überweisungsbetrug zu verbessern, sollten sich die Zahlungsdienstleister auf möglichst umfassende und aktuelle Informationen stützen können, insbesondere indem sie gemeinsam Informationen über Kundenidentifikatoren, Manipulationstechniken und andere Umstände im Zusammenhang mit betrügerischen Überweisungen verwenden, die von den einzelnen Zahlungsdienstleistern identifiziert werden. Bevor Zahlungsdienstleister eine Vereinbarung über den Informationsaustausch schließen, sollten sie eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der Verordnung (EU) 2016/679 durchführen. Geht aus der Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ohne Garantien, Sicherheitsmaßnahmen und Mechanismen zur Minderung des Risikos zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen würde, sollten Zahlungsdienstleister die zuständige Datenschutzbehörde gemäß Artikel 36 der Verordnung (EU) 2016/679 konsultieren. Eine neue Folgenabschätzung sollte nicht erforderlich sein, wenn ein Zahlungsdienstleister einer bestehenden Vereinbarung über den Informationsaustausch beitritt, für die bereits eine Datenschutz-Folgenabschätzung durchgeführt wurde. In der Vereinbarung über den Informationsaustausch sollten technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festgelegt werden. Sie sollte die datenschutzrechtlichen Rollen und Zuständigkeiten aller Zahlungsdienstleister, auch im Falle gemeinsam Verantwortlicher, festlegen.

(104) Für die Zwecke des Austauschs personenbezogener Daten mit anderen Zahlungsdienstleistern, die Vereinbarungen über den Informationsaustausch unterliegen, sollte der Begriff „Kundenidentifikator“ so verstanden werden, dass er sich auf „IBAN“ im Sinne von Artikel 2 Nummer 15 der Verordnung (EU) Nr. 260/2012 bezieht.

(105) Um zu verhindern, dass ein rechtmäßiger Informationsaustausch über potenziell betrügerische Aktivitäten zu einer ungerechtfertigten Risikominderung oder einem ungerechtfertigten Entzug von Zahlungskontodiensten für Zahlungsdienstnutzer führt, ohne dass eine Erklärung gegeben oder ein Rechtsbehelf eingelegt wird, sollten Schutzmaßnahmen vorgesehen werden. Im Rahmen einer multilateralen Vereinbarung über den Informationsaustausch ausgetauschte Daten über Zahlungsbetrug, die die Offenlegung personenbezogener Daten, einschließlich Kundenidentifikatoren von Zahlungsempfängern, die möglicherweise an Betrug bei Überweisungen beteiligt sind, nach sich ziehen können, sollten von Zahlungsdienstleistern nur zur Verbesserung der Transaktionsüberwachung verwendet werden. Zahlungsdienstleister sollten zusätzliche Schutzvorkehrungen treffen, wie z. B. die Kontaktaufnahme mit dem Kunden, wenn er der Auftraggeber einer Überweisung ist, die als betrügerisch angesehen werden kann, und die weitere Überwachung eines Kontos, wenn der als potenziell betrügerisch ausgetauschte Kundenidentifikator einen Kunden dieses Zahlungsdienstleisters benennt. Daten über Zahlungsbetrug, die im Rahmen solcher Vereinbarungen zwischen Zahlungsdienstleistern ausgetauscht werden, sollten ohne eingehende Untersuchung keinen Grund für den Entzug von Bankdienstleistungen darstellen.

(106) Zahlungsbetrug wird immer raffinierter, wobei Betrüger manipulative und personenbezogene Techniken einsetzen, die für Zahlungsdienstnutzer ohne ausreichende Sensibilisierung und Information über Betrug nur schwer aufzudecken sind. Zahlungsdienstleister können eine wichtige Rolle bei der Verstärkung der Betrugsprävention spielen, indem sie regelmäßig alle erforderlichen Initiativen ergreifen, um das Verständnis und das Bewusstsein ihrer Zahlungsdienstnutzer für die Risiken und Trends bei Zahlungsbetrug zu verbessern. Insbesondere sollten Zahlungsdienstleister angemessene Sensibilisierungsprogramme und -kampagnen für Betrugstrends und -risiken durchführen, die sich an Kunden und Mitarbeiter von Zahlungsdienstleistern richten, um den Kunden erkennen zu helfen, dass sie Opfer eines Betrugsversuchs sind. Zahlungsdienstleister sollten ihren Verbrauchern über verschiedene Medien angepasste Informationen über Betrug zur Verfügung stellen, ihnen klare Botschaften und Warnungen geben und ihnen dabei helfen, angemessen zu reagieren, wenn sie potenziell betrügerischen Situationen ausgesetzt sind. Die EBA sollte Leitlinien zu den verschiedenen Arten von Programmen entwickeln, die von Zahlungsdienstleistern zu Zahlungsbetrugsrisiken zu entwickeln sind, wobei dem sich ständig wandelnden Charakter von Betrugsrisiken Rechnung zu tragen ist.

(107) Die Sicherheit elektronischer Zahlungen ist von grundlegender Bedeutung für die Gewährleistung des Schutzes der Nutzer und die Entwicklung einer gesunden E-Commerce-Umgebung. Alle elektronisch angebotenen Zahlungsdienste sollten sicher abgewickelt werden, wobei Technologien einzusetzen sind, die eine sichere Authentifizierung des Nutzers sicherstellen und das Betrugsrisiko möglichst weitgehend einschränken können. Im Bereich Betrug bestand die wichtigste Neuerung der Richtlinie (EU) 2015/2366 in der Einführung der starken Kundenauthentifizierung. Die Kommission kam in ihrer Bewertung der Umsetzung der Richtlinie (EU) 2015/2366 zu dem Schluss, dass die starke Kundenauthentifizierung bei der Eindämmung von Betrug bereits sehr erfolgreich war.

(108) Die starke Kundenauthentifizierung sollte insbesondere nicht durch eine ungerechtfertigte Berufung auf Ausnahmen von der starken Kundenauthentifizierung umgangen werden. Es sollten klare Definitionen der Begriffe „von Händlern ausgelöste Zahlungsvorgänge“ und „Bestellungen per Post oder Telefon“ eingeführt werden, da diese Begriffe, die herangezogen werden können, um die Nichtanwendung

der starken Kundenauthentifizierung zu rechtfertigen, unterschiedlich verstanden und angewandt werden und missbräuchlich verwendet werden können. In Bezug auf von Händlern ausgelöste Zahlungsvorgänge sollte bei der Festlegung des ursprünglichen Mandats eine starke Kundenauthentifizierung angewandt werden, ohne dass für nachfolgende von Händlern ausgelöste Zahlungsvorgänge eine starke Kundenauthentifizierung erforderlich ist. In Bezug auf Bestellungen per Post oder Telefon sollte nur die Auslösung von Zahlungsvorgängen – nicht ihre Ausführung – nicht digital sein müssen, damit eine Transaktion als Bestellung per Post oder Telefon betrachtet werden kann und daher nicht unter die Verpflichtung zur Anwendung der starken Kundenauthentifizierung fällt. Zahlungsvorgänge auf der Grundlage von beleghaften Zahlungsaufträgen oder Bestellungen per Post oder Telefon, die vom Zahler erteilt werden, sollten jedoch nach wie vor Sicherheitsanforderungen und Kontrollen durch den Zahlungsdienstleister des Zahlers zur Authentifizierung des Zahlungsvorgangs beinhalten. Die starke Kundenauthentifizierung sollte auch nicht durch Praktiken umgangen werden, einschließlich des Rückgriffs auf einen außerhalb der Union niedergelassenen Erwerber, um sich den Anforderungen an die starke Kundenauthentifizierung zu entziehen.

(109) Da der Zahlungsdienstleister, der eine starke Kundenauthentifizierung anwenden sollte, der Zahlungsdienstleister ist, der die personalisierten Sicherheitsmerkmale ausgibt, sollten Zahlungsvorgänge, die nicht vom Zahler, sondern nur vom Zahlungsempfänger ausgelöst werden, keiner starken Kundenauthentifizierung unterliegen, sofern diese Transaktionen ohne jegliche Interaktion oder Beteiligung des Zahlers ausgelöst werden. Der Regulierungsansatz für von Händlern ausgelöste Zahlungsvorgänge und Lastschriften, die beide vom Zahlungsempfänger ausgelöst werden, sollte angeglichen werden und dieselben Verbraucherschutzmaßnahmen, einschließlich Erstattungen, beinhalten.

(110) Um die finanzielle Inklusion zu verbessern und im Einklang mit der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates[51] über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen sollten alle Zahlungsdienstnutzer, einschließlich Menschen mit Behinderungen, ältere Menschen, Menschen mit geringen digitalen Kompetenzen und Personen, die keinen Zugang zu digitalen Geräten wie Smartphones haben, von dem von der starken Kundenauthentifizierung bereitgestellten Schutz vor Betrug profitieren, insbesondere wenn es um die Nutzung digitaler Fernzahlungsvorgänge und den Online-Zugang zu Zahlungskonten als grundlegende Finanzdienstleistungen geht. Mit der Einführung der starken Kundenauthentifizierung war es einigen Verbrauchern in der Union nicht möglich, Online-Transaktionen durchzuführen, weil sie materiell nicht in der Lage waren, die starke Kundenauthentifizierung durchzuführen. Daher sollten Zahlungsdienstleister sicherstellen, dass ihre Kunden von verschiedenen Methoden zur Durchführung der starken Kundenauthentifizierung profitieren können, die an ihre Bedürfnisse und Situationen angepasst sind. Diese Methoden sollten nicht von einer einzigen Technologie, einem Gerät oder Mechanismus oder vom Besitz eines Smartphones abhängen.

[51] Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (ABl. L 151 vom 7.6.2019, S. 70).

(111) EUid-Brieftaschen, die gemäß der Verordnung (EU) Nr. 910/2014[52] des Europäischen Parlaments und des Rates, geändert durch die Verordnung [XXX], umgesetzt werden, sind elektronische Identifizierungsmittel, die Identifizierungs- und Authentifizierungsinstrumente für den grenzüberschreitenden Zugang zu Finanzdienstleistungen, einschließlich Zahlungsdiensten, bieten. Die Einführung der EUid-Brieftasche würde die grenzüberschreitende digitale Identifizierung und Authentifizierung für sichere digitale Zahlungen weiter erleichtern und die Entwicklung einer gesamteuropäischen digitalen Zahlungslandschaft erleichtern.

(112) Die Zunahme des E-Commerce und der mobilen Zahlungen sollte mit einer allgemeinen Verbesserung der Sicherheitsmaßnahmen einhergehen. Im Falle der Fernauslösung eines Zahlungsvorgangs, d. h. wenn ein Zahlungsauftrag über das Internet erteilt wird, sollte sich die Authentifizierung von Transaktionen auf dynamische Codes stützen, um den Nutzer jederzeit über den Betrag und den Zahlungsempfänger des Zahlungsvorgangs zu informieren, den der Nutzer autorisiert.

(113) Die Anforderung, bei Fernzahlungsvorgängen die starke Kundenauthentifizierung über Codes anzuwenden, die die Transaktion dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen, sollte dem Wachstum mobiler Zahlungen und der Entstehung einer Vielzahl von Modellen Rechnung tragen, über die mobile Zahlungen ausgeführt werden.

(114) Da die dynamische Verknüpfung das Risiko einer Manipulation des Namens des Zahlungsempfängers und des konkreten Betrags der Transaktion zwischen dem Zeitpunkt der Erteilung eines Zahlungsauftrags und der Authentifizierung von Zahlungen, aber auch das Betrugsrisiko im Allgemeinen adressiert, sollten die Zahlungsdienstleister bei mobilen Zahlungen, bei denen die Durchführung einer starken Kundenauthentifizierung die Nutzung des Internets auf dem Gerät des Zahlers erfordert, auch Elemente anwenden, die die Transaktion dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen, oder harmonisierte Sicherheitsmaßnahmen mit gleicher Wirkung, die die Vertraulichkeit, Authentizität und Integrität der Transaktion in allen Phasen der Auslösung sicherstellen.

(115) Gemäß der Ausnahme von der starken Kundenauthentifizierung nach Artikel 18 der Delegierten Verordnung (EU) 2018/389 durften Zahlungsdienstleister von der Anwendung der starken Kundenauthentifizierung absehen, wenn der Zahler einen elektronischen Fernzahlungsvorgang ausgelöst hat, der vom Zahlungsdienstleister als mit einem geringen Risiko behaftet eingestuft wurde, das auf der Grundlage von Transaktionsüberwachungsmechanismen bewertet wurde. Die Rückmeldungen aus dem Markt haben jedoch gezeigt, dass es, damit mehr Zahlungsdienstleister eine Transaktionsrisikoanalyse durchführen, erforderlich ist, geeignete Vorschriften über den Umfang der Transaktionsrisikoanalyse zu erlassen, klare Prüfungsanforderungen einzuführen, detailliertere und bessere Definitionen der Anforderungen an die Risikoüberwachung und die auszutauschenden Daten bereitzustellen und die potenziellen Vorteile zu bewerten, die sich daraus ergäben, dass Zahlungsdienstleister betrügerische Zahlungsvorgänge, für die sie allein haften, melden könnten. Die EBA

[52] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

sollte Entwürfe technischer Regulierungsstandards mit Vorschriften für die Transaktionsrisikoanalyse ausarbeiten.

(116) Die Sicherheitsmaßnahmen sollten dem Risikoniveau der Zahlungsdienste angemessen sein. Um die Entwicklung benutzerfreundlicher und leicht zugänglicher Zahlungsmittel für Zahlungen mit einem niedrigen Risiko wie kontaktlose Kleinbetragszahlungen an der Verkaufsstelle, unabhängig davon, ob diese Zahlungen an ein Mobiltelefon gebunden sind, zu ermöglichen, sollten in den technischen Regulierungsstandards die Ausnahmen von der Anwendung der Sicherheitsanforderungen dargelegt sein. Die sichere Nutzung personalisierter Sicherheitsmerkmale ist notwendig, um die Risiken im Zusammenhang mit Spoofing, Phishing und anderen Betrugspraktiken einzuschränken. Der Nutzer sollte sich darauf verlassen können, dass Vorkehrungen getroffen werden, die die Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale schützen.

(117) Zahlungsdienstleister sollten die starke Kundenauthentifizierung unter anderem dann anwenden, wenn der Zahlungsdienstnutzer über einen Fernkanal Maßnahmen durchführt, die das Risiko von Zahlungsbetrug oder anderem Missbrauch bergen können. Die Zahlungsdienstleister sollten über angemessene Sicherheitsmaßnahmen verfügen, um die Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale des Zahlungsdienstnutzers zu schützen.

(118) Es gibt kein einheitliches Verständnis der Marktakteure in allen Mitgliedstaaten über die Anforderungen an die starke Kundenauthentifizierung, die für die Registrierung von Zahlungsinstrumenten, insbesondere Zahlungskarten, in digitalen Brieftaschen gelten. Die Schaffung eines Tokens oder dessen Ersatzvorgangs kann die Gefahr von Zahlungsbetrug oder anderen Formen des Missbrauchs bergen. Die Erstellung oder der Austausch eines Tokens eines Zahlungsinstruments, die über einen Fernkanal unter Beteiligung des Zahlungsdienstnutzers erfolgt, sollte daher die Anwendung einer starken Kundenauthentifizierung durch den Zahlungsdienstleister des Zahlungsdienstnutzers zum Zeitpunkt der Ausgabe oder des Ersatzes des Tokens erfordern. Durch die Anwendung der starken Kundenauthentifizierung in der Phase der Erstellung oder Ersetzung eines Tokens sollte der Zahlungsdienstleister aus der Ferne überprüfen, ob der Zahlungsdienstnutzer der rechtmäßige Nutzer des Zahlungsinstruments ist, und den Nutzer und die digitalisierte Version des Zahlungsinstruments mit dem jeweiligen Gerät in Verbindung bringen.

(119) Betreiber digitaler Pass-through-Brieftaschen, die die Elemente der starken Kundenauthentifizierung überprüfen, wenn in den digitalen Brieftaschen gespeicherte tokenisierte Instrumente für Zahlungen verwendet werden, sollten verpflichtet werden, Auslagerungsvereinbarungen mit den Zahlungsdienstleistern des Zahlers zu schließen, damit diese diese Überprüfungen fortsetzen können, aber auch dazu verpflichtet werden, die wesentlichen Sicherheitsanforderungen zu erfüllen. Die Zahlungsdienstleister des Zahlers sollten im Rahmen solcher Vereinbarungen die volle Haftung für den Fall behalten, dass Betreiber digitaler Pass-through-Brieftaschen die starke Kundenauthentifizierung nicht anwenden, und das Recht haben, die Sicherheitsbestimmungen des Betreibers der Brieftasche zu prüfen und zu kontrollieren.

(120) Wenn technische Dienstleister oder Betreiber von Zahlungssystemen für Zahlungsempfänger oder Zahlungsdienstleister von Zahlungsempfängern oder Zahlern Dienstleistungen erbringen, sollten sie die Anwendung einer starken Kundenauthentifizierung im Rahmen ihrer Rolle bei der Auslösung oder Ausführung

von Zahlungsvorgängen unterstützen. Angesichts der Rolle, die sie dabei spielen, sicherzustellen, dass die zentralen Sicherheitsanforderungen für Massenzahlungen ordnungsgemäß umgesetzt werden, unter anderem durch die Bereitstellung geeigneter IT-Lösungen, sollten technische Dienstleister und Betreiber von Zahlungssystemen für finanzielle Schäden haftbar gemacht werden, die Zahlungsempfängern oder Zahlungsdienstleistern von Zahlungsempfängern oder Zahlern entstehen, falls sie die Anwendung der starken Kundenauthentifizierung nicht unterstützen.

(121) Die Mitgliedstaaten sollten die zuständigen Behörden für die Zulassung von Zahlungsinstituten sowie für die Akkreditierung und Überwachung von Verfahren zur alternativen Streitbeilegung benennen.

(122) Unbeschadet des Rechts der Kunden, Gerichte anzurufen, sollten die Mitgliedstaaten sicherstellen, dass leicht zugängliche, adäquate, unabhängige, unparteiische, transparente und wirksame Verfahren zur alternativen Streitbeilegung zwischen Zahlungsdienstleistern und Zahlungsdienstnutzern bestehen. Die Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates[53] sieht vor, dass der Schutz, der einem Verbraucher nach den zwingenden Rechtsvorschriften des Landes gewährt wird, in dem er seinen gewöhnlichen Aufenthalt hat, nicht durch vertragliche Bestimmungen über das auf den Vertrag anzuwendende Recht ausgehöhlt werden darf. Im Hinblick auf die Einführung eines effizienten und wirksamen Streitbeilegungsverfahrens sollten die Mitgliedstaaten sicherstellen, dass sich Zahlungsdienstleister einem Verfahren zur alternativen Streitbeilegung im Einklang mit den Qualitätsanforderungen der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates[54] unterwerfen, um Streitigkeiten beizulegen, bevor sie ein Gericht anrufen. Die benannten zuständigen Behörden sollten der Kommission eine oder mehrere zuständige Stellen zur alternativen Streitbeilegung in ihrem Hoheitsgebiet mitteilen, die für die Beilegung nationaler und grenzüberschreitender Streitigkeiten zuständig sind und bei Streitigkeiten über Rechte und Pflichten gemäß dieser Verordnung zusammenarbeiten.

(123) Die Verbraucher sollten berechtigt sein, ihre Rechte in Bezug auf die Pflichten, die Zahlungsdienstleistern und E-Geld-Dienstleistern gemäß dieser Verordnung auferlegt werden, durch Verbandsklagen gemäß der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates[55] durchzusetzen.

(124) Es sollten geeignete Verfahren eingeführt werden, um gegen Zahlungsdienstleister, die ihren Pflichten nicht nachkommen, Beschwerde zu erheben, und sicherzustellen, dass gegebenenfalls verhältnismäßige, wirksame und abschreckende Sanktionen verhängt werden. Um die Einhaltung dieser Verordnung sicherzustellen, sollten die Mitgliedstaaten zuständige Behörden benennen, die die Bedingungen der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates[56] erfüllen und

---

53 ABl. L 177 vom 4.7.2008, S. 6.

54 Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (ABl. L 165 vom 18.6.2013, S. 63).

55 Richtlinie (EU) 2020/1828 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG (ABl. L 409, 4.12.2020, S. 1).

56 Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

unabhängig von den Zahlungsdienstleistern handeln. Die Mitgliedstaaten sollten der Kommission mitteilen, welche Behörden benannt wurden, und eine genaue Beschreibung ihrer Aufgaben vorlegen.

(125) Unbeschadet des Rechts, vor Gericht zu klagen, um die Einhaltung dieser Verordnung sicherzustellen, sollten die zuständigen Behörden die notwendigen Befugnisse nach dieser Verordnung ausüben, einschließlich der Befugnis, mutmaßliche Verstöße zu untersuchen und verwaltungsrechtliche Sanktionen und Verwaltungsmaßnahmen aufzuerlegen, wenn der Zahlungsdienstleister die Rechte und Pflichten gemäß dieser Verordnung nicht einhält, insbesondere wenn die Gefahr eines erneuten Verstoßes oder andere Bedenken im Hinblick auf die kollektiven Verbraucherinteressen bestehen. Die zuständigen Behörden sollten wirksame Mechanismen einrichten, um die Meldung potenzieller oder tatsächlicher Verstöße zu fördern. Die Verteidigungsrechte eines Angeklagten sollten von diesen Mechanismen unberührt bleiben.

(126) Die Mitgliedstaaten sollten verpflichtet werden, wirksame, verhältnismäßige und abschreckende verwaltungsrechtliche Sanktionen und Verwaltungsmaßnahmen im Zusammenhang mit Verstößen gegen die Bestimmungen dieser Verordnung vorzusehen. Diese verwaltungsrechtlichen Sanktionen, Zwangsgelder und Verwaltungsmaßnahmen sollten bestimmten Mindestanforderungen genügen, einschließlich der Mindestbefugnisse, die den zuständigen Behörden übertragen werden sollten, um sie verhängen zu können, der Kriterien, die die zuständigen Behörden bei ihrer Anwendung, bei ihrer Veröffentlichung und bei der Berichterstattung über sie berücksichtigen sollten. Die Mitgliedstaaten sollten spezifische Vorschriften und wirksame Mechanismen für die Verhängung von Zwangsgeldern festlegen.

(127) Die zuständigen Behörden sollten befugt sein, Verwaltungsgeldstrafen zu verhängen, die so hoch sind, dass sie den zu erwartenden Nutzen aufwiegen und selbst auf größere Institute abschreckend wirken.

(128) Bei der Verhängung von verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen sollten die zuständigen Behörden bei der Festlegung der Art der verwaltungsrechtlichen Sanktionen oder anderen Verwaltungsmaßnahmen und der Höhe der Verwaltungsgeldstrafen etwaige frühere strafrechtliche Sanktionen berücksichtigen, die gegen dieselbe natürliche oder juristische Person verhängt wurden, die für denselben Verstoß verantwortlich ist. Damit soll sichergestellt werden, dass die Schwere aller Sanktionen und anderen Verwaltungsmaßnahmen, die im Falle einer Kumulierung von Verwaltungs- und Strafverfahren zu Strafzwecken verhängt werden, auf das Maß beschränkt ist, das angesichts der Schwere des betreffenden Verstoßes erforderlich ist.

(129) Ein wirksames Aufsichtssystem setzt voraus, dass die Aufsichtsbehörden sich der Schwächen bei der Einhaltung der Vorschriften dieser Verordnung durch die Zahlungsdienstleister bewusst sind. Daher ist es wichtig, dass Aufseher sich gegenseitig über verwaltungsrechtliche Sanktionen und Verwaltungsmaßnahmen informieren können, die gegen Zahlungsdienstleister verhängt werden, sofern diese Informationen auch für andere Aufseher relevant sind.

(130) Die Wirksamkeit des Unionsrahmens für Zahlungsdienste hängt von der Zusammenarbeit zwischen einem breiten Spektrum zuständiger Behörden ab, darunter nationale Behörden für Steuern, Datenschutz, Wettbewerb, Verbraucherschutz, Audit, Polizei und andere Durchsetzungsbehörden. Die Mitgliedstaaten sollten sicherstellen,

dass ihr Rechtsrahmen die erforderliche Zusammenarbeit ermöglicht und erleichtert, um die Ziele des Unionsrahmens für Zahlungsdienste auch durch die ordnungsgemäße Durchsetzung seiner Vorschriften zu erreichen. Diese Zusammenarbeit sollte den Informationsaustausch sowie die Amtshilfe bei der wirksamen Durchsetzung von verwaltungsrechtlichen Sanktionen, insbesondere bei der grenzüberschreitenden Beitreibung von Geldstrafen, umfassen.

(131) Unabhängig von ihrer Bezeichnung nach nationalem Recht gibt es in vielen Mitgliedstaaten Formen von beschleunigten Durchsetzungsverfahren oder Vergleichsvereinbarungen, die als Alternative zu förmlichen Verfahren genutzt werden, um eine schnellere Annahme einer Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion oder einer Verwaltungsmaßnahme oder zur Beendigung des mutmaßlichen Verstoßes und seiner Folgen zu erreichen, bevor ein förmliches Sanktionsverfahren eingeleitet wird. Auch wenn es aufgrund der sehr unterschiedlichen rechtlichen Ansätze auf nationaler Ebene nicht angebracht erscheint, auf Unionsebene solche Durchsetzungsmethoden zu harmonisieren, die von vielen Mitgliedstaaten eingeführt wurden, sollte anerkannt werden, dass solche Methoden es den zuständigen Behörden, die sie anwenden können, ermöglichen, Verfahren wegen Regelverstößen unter Umständen schneller, kostengünstiger und insgesamt effizienter zu bearbeiten. Diese Methoden sollten daher gefördert werden. Die Mitgliedstaaten sollten jedoch nicht verpflichtet sein, solche Durchsetzungsmethoden in ihren Rechtsrahmen aufzunehmen oder die zuständigen Behörden zur Anwendung dieser Methoden zu zwingen, wenn sie dies nicht für angemessen halten.

(132) Die Mitgliedstaaten haben eine Vielzahl von verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen für Verstöße gegen die wichtigsten Bestimmungen zur Regelung der Zahlungsdienste eingeführt und sehen derzeit uneinheitliche Ansätze für die Untersuchung und Ahndung von Verstößen gegen diese Bestimmungen vor. Wenn nicht genauer festgelegt würde, welche Kernbestimmungen eine hinreichend abschreckende Durchsetzung überall in der Union auslösen müssen, würde dies die Verwirklichung des Binnenmarkts für Zahlungsdienste behindern und die Gefahr bergen, Anreize für die Wahl des günstigsten Gerichtsstands zu schaffen, da die zuständigen Behörden in den Mitgliedstaaten nicht über dieselbe Handhabe verfügen, um diese Verstöße rasch und mit derselben Abschreckungswirkung ahnden zu können.

(133) Da der Zweck der Zwangsgelder darin besteht, natürliche oder juristische Personen, die als für einen andauernden Verstoß verantwortlich identifiziert wurden oder einer Anordnung der untersuchenden zuständigen Behörde nachkommen müssen, zu zwingen, dieser Anordnung nachzukommen oder den andauernden Verstoß zu beenden, sollte die Verhängung von Zwangsgeldern die zuständigen Behörden nicht daran hindern, spätere verwaltungsrechtliche Sanktionen für denselben Verstoß zu verhängen.

(134) Sofern die Mitgliedstaaten nichts anderes vorsehen, sollten Zwangsgelder tageweise berechnet werden.

(135) Die zuständigen Behörden sollten von den Mitgliedstaaten ermächtigt werden, solche verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen gegen Zahlungsdienstleister oder gegebenenfalls andere natürliche oder juristische Personen zu verhängen, um im Falle eines Verstoßes Abhilfe zu schaffen. Die Sanktionen und Maßnahmen sollten ausreichend breit gefächert sein, damit die Mitgliedstaaten und die zuständigen Behörden den Unterschieden zwischen Zahlungsdienstleistern,

insbesondere zwischen Kreditinstituten und anderen Zahlungsinstituten und in Bezug auf ihre Größe, Merkmale und Art der Geschäftstätigkeit Rechnung tragen können.

(136) Die Veröffentlichung einer verwaltungsrechtlichen Sanktion oder einer Verwaltungsmaßnahme bei Verstößen gegen die Bestimmungen dieser Verordnung kann eine starke abschreckende Wirkung gegen die Wiederholung eines solchen Verstoßes haben. Die Veröffentlichung informiert auch andere Stellen über die Risiken, die mit dem sanktionierten Zahlungsdienstleister verbunden sind, bevor sie eine Geschäftsbeziehung eingehen, und unterstützt die zuständigen Behörden in anderen Mitgliedstaaten in Bezug auf die Risiken, die mit einem Zahlungsdienstleister verbunden sind, wenn dieser in ihrem Mitgliedstaat grenzüberschreitend tätig ist. Aus diesen Gründen sollte die Veröffentlichung von Entscheidungen über verwaltungsrechtliche Sanktionen und Verwaltungsmaßnahmen zulässig sein, solange sie juristische Personen betrifft. Bei der Entscheidung über die Veröffentlichung einer verwaltungsrechtlichen Sanktion oder Verwaltungsmaßnahme sollten die zuständigen Behörden die Schwere des Verstoßes und die abschreckende Wirkung, die die Veröffentlichung voraussichtlich haben wird, berücksichtigen. Eine solche Veröffentlichung, die sich auf natürliche Personen bezieht, kann jedoch in unverhältnismäßiger Weise in deren Rechte eingreifen, die sich aus der Charta der Grundrechte und den geltenden Datenschutzvorschriften der Union ergeben. Daher sollte die Veröffentlichung anonymisiert erfolgen, es sei denn, die zuständige Behörde hält es für erforderlich, Entscheidungen, die personenbezogene Daten enthalten, für die wirksame Durchsetzung dieser Verordnung zu veröffentlichen, auch im Falle öffentlicher Erklärungen oder vorübergehender Verbote. In solchen Fällen sollte die zuständige Behörde ihre Entscheidung begründen.

(137) Um genauere Informationen über den Grad der Einhaltung des Unionsrechts vor Ort zu erlangen und gleichzeitig die Durchsetzungstätigkeit der zuständigen Behörden sichtbarer zu machen, ist es notwendig, den Anwendungsbereich auszuweiten und die Qualität der Daten, die die zuständigen Behörden der EBA melden, zu verbessern. Die zu meldenden Informationen sollten anonymisiert werden, um den geltenden Datenschutzvorschriften zu entsprechen, und in aggregierter Form bereitgestellt werden, um den Vorschriften über die Wahrung des Berufsgeheimnisses und der Vertraulichkeit von Verfahren Rechnung zu tragen. Die EBA sollte der Kommission regelmäßig über die Fortschritte bei den Durchsetzungsmaßnahmen in den Mitgliedstaaten Bericht erstatten.

(138) Der Kommission sollte die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte zu erlassen, um unter Berücksichtigung der Inflation die Beträge zu aktualisieren, bis zu denen ein Zahler verpflichtet sein kann, die Verluste im Zusammenhang mit nicht autorisierten Zahlungsvorgängen zu tragen, die sich aus der Nutzung eines verlorenen oder gestohlenen Zahlungsinstruments oder aus der missbräuchlichen Verwendung eines Zahlungsinstruments ergeben. Bei der Ausarbeitung delegierter Rechtsakte sollte die Kommission sicherstellen, dass die einschlägigen Dokumente dem Europäischen Parlament und dem Rat zeitgleich, rechtzeitig und in geeigneter Weise übermittelt werden.

(139) Um eine kohärente Anwendung dieser Verordnung sicherzustellen, sollte sich die Kommission auf das Fachwissen und die Unterstützung der EBA verlassen können, die die Aufgabe haben sollte, Leitlinien auszuarbeiten und Entwürfe für die technischen Regulierungs- und Durchführungsstandards auszuarbeiten. Der Kommission sollte die Befugnis übertragen werden, diese Entwürfe technischer

Regulierungsstandards zu erlassen. Die EBA sollte bei der Ausarbeitung von Leitlinien, Entwürfen technischer Regulierungsstandards und Entwürfen technischer Durchführungsstandards gemäß dieser Verordnung und im Einklang mit der Verordnung (EU) Nr. 1093/2010 alle einschlägigen Interessenträger, einschließlich derer des Zahlungsdienstmarktes, anhören und den Interessen aller Beteiligten Rechnung tragen.

(140) Die EBA sollte im Einklang mit Artikel 9 Absatz 5 der Verordnung (EU) Nr. 1093/2010 mit Produktinterventionsbefugnissen ausgestattet werden, um in der Union bestimmte Arten oder Merkmale eines Zahlungsdienstes oder eines E-Geld-Dienstes, bei denen festgestellt wird, dass sie den Verbrauchern schaden und das ordnungsgemäße Funktionieren und die Integrität der Finanzmärkte gefährden könnten, vorübergehend verbieten oder beschränken zu können. Die Verordnung (EU) Nr. 1093/2010 sollte daher entsprechend geändert werden.

(141) Der Anhang der Verordnung (EU) 2017/2394 des Europäischen Parlaments und des Rates[57] sollte durch Aufnahme eines Verweises auf die vorliegende Verordnung geändert werden, damit die grenzübergreifende Zusammenarbeit bei der Durchsetzung der vorliegenden Verordnung erleichtert wird.

(142) Da das Ziel dieser Verordnung, nämlich die weitere Integration eines Binnenmarktes für Zahlungsdienste, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, da es die Harmonisierung einer Reihe von unterschiedlichen Vorschriften des Unionsrechts und des nationalen Rechts erfordert, sondern vielmehr wegen seines Umfangs und seiner Wirkungen auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(143) Da mit dieser Verordnung und der Richtlinie (EU) XXX (PSD3) der Rechtsrahmen für die Erbringung von Massenzahlungsdiensten und E-Geld-Diensten in der Union festgelegt wird, um Rechtssicherheit und die Kohärenz des Rechtsrahmens der Union sicherzustellen, sollte die vorliegende Verordnung ab demselben Zeitpunkt gelten wie die Rechts- und Verwaltungsvorschriften, die die Mitgliedstaaten erlassen müssen, um der Richtlinie (EU) XXX (PSD3) nachzukommen. Die Bestimmungen, nach denen Zahlungsdienstleister bei Überweisungen Abweichungen zwischen dem Namen und dem Kundenidentifikator eines Zahlungsempfängers überprüfen müssen, und die jeweilige Haftungsregelung sollten jedoch 24 Monate nach Inkrafttreten dieser Verordnung gelten, sodass die Zahlungsdienstleister genügend Zeit haben, um die erforderlichen Schritte zur Anpassung ihrer internen Systeme zu unternehmen, um diesen Anforderungen nachzukommen.

(144) Im Einklang mit den Grundsätzen der besseren Rechtsetzung sollte diese Verordnung auf ihre Wirksamkeit und Effizienz bei der Erreichung ihrer Ziele überprüft werden. Die Überprüfung sollte so lange nach dem Geltungsbeginn dieser Verordnung erfolgen, dass ausreichende Nachweise vorliegen, auf die sich die Überprüfung stützen kann. Fünf Jahre gelten als angemessener Zeitraum. Während bei der Überprüfung die

[57] Verordnung (EU) 2017/2394 des Europäischen Parlaments und des Rates vom 12. Dezember 2017 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden und zur Aufhebung der Verordnung (EG) Nr. 2006/200 (ABl. L 345 vom 27.12.2017, S. 1).

vorliegende Verordnung als Ganzes berücksichtigt werden sollte, sollte bestimmten Themen besondere Aufmerksamkeit gewidmet werden, nämlich dem Funktionieren des Open Banking, der Erhebung von Gebühren für Zahlungsdienste und weiteren Lösungen zur Betrugsbekämpfung. In Bezug auf den Anwendungsbereich dieser Verordnung ist es jedoch angesichts der Bedeutung, die diesem Gegenstand in Artikel 58 Absatz 2 der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates[58] beigemessen wird, angezeigt, eine Überprüfung zu einem früheren Zeitpunkt, nämlich drei Jahre nach ihrem Geltungsbeginn, vorzunehmen. Bei dieser Überprüfung des Anwendungsbereichs sollte sowohl die mögliche Ausweitung der Liste der erfassten Zahlungsdienste auf Dienste wie solche, die von Zahlungssystemen und Zahlverfahren erbracht werden, als auch die mögliche Aufnahme einiger derzeit ausgeschlossener technischer Dienste in den Anwendungsbereich geprüft werden.

(145) Diese Verordnung steht im Einklang mit den Grundrechten und den mit der Charta der Grundrechte der Europäischen Union anerkannten Grundsätzen, einschließlich des Rechts auf Achtung des Privat- und Familienlebens, des Rechts auf Schutz personenbezogener Daten, der unternehmerischen Freiheit, des Rechts auf einen wirksamen Rechtsbehelf und des Rechts, wegen derselben Straftat nicht zweimal strafrechtlich verfolgt oder bestraft zu werden. Diese Verordnung sollte unter Wahrung dieser Rechte und Grundsätze angewandt werden.

(146) Verweise auf Beträge in Euro sind als Verweise auf den entsprechenden Gegenwert in der nationalen Währung der Mitgliedstaaten zu verstehen, deren Währung nicht der Euro ist.

(147) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[59] konsultiert und hat am [XX XX 2023][60] eine Stellungnahme abgegeben —

---

58 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Betriebsstabilität digitaler Systeme im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1).

59 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

60 ABl. C […] vom […], S. […].

HABEN FOLGENDE VERORDNUNG ERLASSEN:

TITEL I

GEGENSTAND, GELTUNGSBEREICH UND BEGRIFFSBESTIMMUNGEN

Artikel 1

Gegenstand

(1) Mit dieser Verordnung werden für die Erbringung von Zahlungsdiensten und E-Geld-Diensten einheitliche Anforderungen in Bezug auf Folgendes festgelegt:

a) die Transparenz der Vertragsbedingungen und die Informationspflichten bei Zahlungsdiensten und E-Geld-Diensten,

b) die Rechte und Pflichten von Zahlungsdienstnutzern und E-Geld-Dienstnutzern sowie von Zahlungs- und E-Geld-Dienstleistern im Zusammenhang mit der Erbringung von Zahlungs- und E-Geld-Diensten.

(2) Sofern nicht anders angegeben, sind Bezugnahmen auf Zahlungsdienste in dieser Verordnung als Bezugnahmen auf Zahlungs- und E-Geld-Dienste zu verstehen.

(3) Sofern nicht anders angegeben, sind Bezugnahmen auf Zahlungsdienstleister in dieser Verordnung als Bezugnahmen auf Zahlungs- und E-Geld-Dienstleister zu verstehen.

Artikel 2

Geltungsbereich

(1) Diese Verordnung gilt für Zahlungsdienste, die innerhalb der Union von folgenden Kategorien von Zahlungsdienstleistern erbracht werden:

a) Kreditinstituten im Sinne von Artikel 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates[61], einschließlich deren Zweigniederlassungen, sofern diese sich in der Union befinden, unabhängig davon, ob sich der Hauptsitz innerhalb oder außerhalb der Union befindet,

b) Postscheckämtern, die nach nationalem Recht zur Erbringung von Zahlungsdiensten berechtigt sind,

c) Zahlungsinstituten,

[61] Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).

d) der Europäischen Zentralbank (EZB) und den nationalen Zentralbanken, wenn diese nicht in ihrer Eigenschaft als Währungsbehörden oder andere Behörden handeln,

e) den Mitgliedstaaten oder ihren regionalen oder lokalen Gebietskörperschaften, wenn diese nicht in ihrer Eigenschaft als Behörden handeln.

(2) Diese Verordnung gilt nicht für

a) Zahlungsvorgänge, die ohne zwischengeschaltete Stellen ausschließlich als direkte Bargeldzahlung vom Zahler an den Zahlungsempfänger erfolgen,

b) Zahlungsvorgänge, die über einen Handelsvertreter im Sinne von Artikel 1 Absatz 2 der Richtlinie 86/653/EWG zwischen dem Zahler und dem Zahlungsempfänger abgewickelt werden, sofern alle folgenden Bedingungen erfüllt sind: i) der Handelsvertreter ist aufgrund einer Vereinbarung befugt, den Verkauf oder Erwerb von Waren oder Dienstleistungen nur im Namen des Zahlers oder nur im Namen des Zahlungsempfängers, nicht aber beider, auszuhandeln oder abzuschließen, unabhängig davon, ob er im Besitz des Kundengeldes ist oder nicht, und ii) eine solche Vereinbarung verschafft dem Zahler oder Zahlungsempfänger eine echte Marge, um mit dem Handelsvertreter zu verhandeln oder den Verkauf oder Erwerb von Waren oder Dienstleistungen abzuschließen,

c) die nicht gewerbsmäßige Entgegennahme und Übergabe von Bargeld im Rahmen einer gemeinnützigen Tätigkeit oder einer Tätigkeit ohne Erwerbszweck,

d) Dienste, bei denen der Zahlungsempfänger dem Zahler im Rahmen eines Zahlungsvorgangs zum Erwerb von Waren und Dienstleistungen Bargeld aushändigt, nachdem ihn der Zahlungsdienstnutzer kurz vor Ausführung des Zahlungsvorgangs ausdrücklich darum gebeten hat,

e) Dienste, bei denen unabhängig von der Ausführung eines Zahlungsvorgangs und ohne jede Verpflichtung zum Erwerb von Waren und Dienstleistungen in Einzelhandelsgeschäften auf ausdrücklichen Wunsch des Zahlungsdienstnutzers Bargeld ausgehändigt wird. Der Zahlungsdienstnutzer ist vor Aushändigung des verlangten Bargelds über alle etwaigen Entgelte für diesen Dienst zu informieren,

f) Zahlungsvorgänge, denen eines der folgenden Dokumente zugrunde liegt, das auf den Zahlungsdienstleister gezogen ist und die Bereitstellung von Geld an einen Zahlungsempfänger vorsieht:

i) ein Papierscheck im Sinne des Genfer Abkommens vom 19. März 1931 über das Einheitliche Scheckgesetz,

ii) ein Papierscheck, der dem unter Ziffer i genannten ähnlich ist und dem Recht von Mitgliedstaaten unterliegt, die nicht Vertragspartei des Genfer Abkommens vom 19. März 1931 über das Einheitliche Scheckgesetz sind,

iii) ein im Genfer Abkommens vom 7. Juni 1930 über das Einheitliche Wechselgesetz genannter Wechsel in Papierform,

iv) ein Wechsel in Papierform, der dem in Ziffer iii genannten ähnlich ist und dem Recht von Mitgliedstaaten unterliegt, die nicht Vertragspartei

des Genfer Abkommens vom 7. Juni 1930 über das Einheitliche Wechselgesetz sind,

v) ein Gutschein in Papierform,

vi) ein Reisescheck in Papierform,

vii) eine Postanweisung in Papierform im Sinne der Definition des Weltpostvereins,

g) Zahlungsvorgänge, die innerhalb eines Zahlungs- oder Wertpapierabwicklungssystems zwischen Zahlungsausgleichsagenten, zentralen Gegenparteien, Clearingstellen oder Zentralbanken und anderen Teilnehmern des Systems und Zahlungsdienstleistern abgewickelt werden; Artikel 31 bleibt hiervon unberührt,

h) Zahlungsvorgänge im Zusammenhang mit der Bedienung von Wertpapieranlagen, wie z. B. Dividenden, Erträge oder sonstige Ausschüttungen oder deren Einlösung oder Veräußerung, die von den unter Buchstabe g genannten Personen oder von Wertpapierdienstleistungen erbringenden Wertpapierfirmen, Kreditinstituten, Organismen für gemeinsame Anlagen oder Vermögensverwaltungsgesellschaften und jeder anderen Einrichtung, die für die Verwahrung von Finanzinstrumenten zugelassen ist, durchgeführt werden,

i) unbeschadet des Artikels 23 Absatz 2 und der Artikel 58 und 87 Dienste, die von technischen Dienstleistern erbracht werden,

j) Dienste, die auf bestimmten Zahlungsinstrumenten beruhen, die eine der folgenden Bedingungen erfüllen:

i) die Instrumente gestatten ihrem Inhaber, Waren oder Dienstleistungen lediglich in den Geschäftsräumen des Emittenten oder innerhalb eines einzigen begrenzten Netzes von Dienstleistern im Rahmen einer Geschäftsvereinbarung mit einem professionellen Emittenten zu erwerben,

ii) die Instrumente können nur zum Erwerb eines sehr begrenzten Waren- oder Dienstleistungsspektrums verwendet werden,

iii) die Instrumente sind nur in einem Mitgliedstaat gültig, werden auf Ersuchen eines Unternehmens oder einer öffentlichen Stelle bereitgestellt, unterliegen zu bestimmten sozialen oder steuerlichen Zwecken den Vorschriften einer nationalen oder regionalen öffentlichen Stelle und dienen dem Erwerb bestimmter Waren oder Dienstleistungen von Anbietern, die eine gewerbliche Vereinbarung mit dem Emittenten geschlossen haben,

k) Zahlungsvorgänge eines Anbieters elektronischer Kommunikationsnetze im Sinne von Artikel 2 Nummer 1 der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates[62] oder Dienste, die zusätzlich zu elektronischen Kommunikationsdiensten im Sinne von Artikel 2 Nummer 4 der

[62] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36).

genannten Richtlinie für einen Teilnehmer des Netzes oder Dienstes zu folgendem Zweck bereitgestellt werden:

i) zum Erwerb von digitalen Inhalten und Sprachdiensten, ungeachtet des für den Erwerb oder Konsum des digitalen Inhalts verwendeten Geräts, und die über die entsprechende Rechnung abgerechnet werden, oder

ii) die von einem elektronischen Gerät aus oder über dieses ausgeführt und über die entsprechende Rechnung im Rahmen einer gemeinnützigen Tätigkeit oder für den Erwerb von Tickets abgerechnet werden,

sofern der Wert jeder Einzelzahlung 50 EUR nicht überschreitet und

– die Zahlungsvorgänge eines einzelnen Teilnehmers kumuliert 300 EUR monatlich nicht überschreiten oder

– bei Teilnehmern, die auf ihr Konto bei einem Anbieter elektronischer Kommunikationsnetze oder -dienste Vorauszahlungen leisten, die Zahlungsvorgänge kumuliert 300 EUR monatlich nicht überschreiten,

l) Zahlungsvorgänge, die zwischen Zahlungsdienstleistern, ihren Agenten oder Zweigniederlassungen auf eigene Rechnung ausgeführt werden,

m) Zahlungsvorgänge zwischen einem Mutterunternehmen und seinem Tochterunternehmen oder zwischen Tochterunternehmen desselben Mutterunternehmens und damit verbundene Dienste ohne Mitwirkung eines Zahlungsdienstleisters, es sei denn, es handelt sich bei diesem um ein Unternehmen derselben Gruppe, und der Einzug von Zahlungsaufträgen im Namen der Gruppe durch ein Mutterunternehmen oder dessen Tochterunternehmen zur Weiterleitung an einen Zahlungsdienstleister.

(3) Die Titel II und III gelten für Zahlungsvorgänge in der Währung eines Mitgliedstaats, wenn sowohl der Zahlungsdienstleister des Zahlers als auch der des Zahlungsempfängers oder — falls nur ein einziger Zahlungsdienstleister an dem Zahlungsvorgang beteiligt ist — dieser in der Union ansässig ist.

(4) Titel II, mit Ausnahme von Artikel 13 Absatz 1 Buchstabe b, Artikel 20 Nummer 2 Buchstabe e und Artikel 24 Buchstabe a und Titel III, mit Ausnahme der Artikel 67 bis 72, gelten für Zahlungsvorgänge in einer Währung, die nicht die Währung eines Mitgliedstaats ist, wenn sowohl der Zahlungsdienstleister des Zahlers als auch der des Zahlungsempfängers in der Union ansässig ist oder — falls nur ein einziger Zahlungsdienstleister an dem Zahlungsvorgang beteiligt ist — dieser in der Union ansässig ist, und zwar für die Bestandteile der Zahlungsvorgänge, die in der Union getätigt werden.

(5) Titel II, mit Ausnahme von Artikel 13 Absatz 1 Buchstabe b, Artikel 20 Nummer 2 Buchstabe e und Nummer 5 Buchstabe h und Artikel 24 Buchstabe a sowie Titel III, mit Ausnahme von Artikel 28 Absätze 2 und 3, Artikel 62, 63 und 67, Artikel 69 Absatz 1 und Artikel 75 und 78 gelten für Zahlungsvorgänge in allen Währungen, bei denen lediglich einer der beteiligten Zahlungsdienstleister in der Union ansässig ist, und zwar für die Bestandteile der Zahlungsvorgänge, die in der Union getätigt werden.

(6) Die Mitgliedstaaten können in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU genannte Institute ganz oder teilweise von der Anwendung dieser Verordnung ausnehmen.

(7) Zum Ausschluss der in Absatz 2 Buchstabe b des vorliegenden Artikels genannten, über einen Handelsvertreter abgewickelten Zahlungsvorgänge zwischen einem Zahler und einem Zahlungsempfänger gibt die EBA gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = ein Jahr nach Inkrafttreten dieser Verordnung] Leitlinien an die im Rahmen dieser Verordnung benannten zuständigen Behörden aus.

(8) Die EBA arbeitet Entwürfe technischer Regulierungsstandards aus, in denen die Bedingungen für die in Absatz 2 Buchstabe j genannten Ausschlüsse präzisiert werden. Dabei berücksichtigt sie die Erfahrungen, die bei der Anwendung der EBA-Leitlinien vom 24. Februar 2022 über die Ausnahme für begrenzte Netze gemäß der Richtlinie (EU) 2015/2366 gesammelt wurden.

Die EBA übermittelt der Kommission die in Unterabsatz 1 genannten technischen Regulierungsstandards bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = ein Jahr nach Inkrafttreten dieser Verordnung]. Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010 zu erlassen.

(9) Jeder Mitgliedstaat teilt der Kommission bis zum Geltungsbeginn dieser Verordnung die Rechtsvorschriften, die er aufgrund von Absatz 6 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Herkunftsmitgliedstaat“

   a) den Mitgliedstaat, in dem der Zahlungsdienstleister seinen Sitz hat, 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, eine Vertriebsstelle 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 13 der Richtlinie (EU) [PSD3] eine Zulassung für die unionsweite Erbringung von Zahlungsdiensten oder E-Geld-Diensten erteilt wurde;

5. „Zahlungsvorgang“ die Bereitstellung, den Transfer oder die Abhebung von Geld auf der Grundlage eines Zahlungsauftrags, der unabhängig von etwaigen zugrunde liegenden Verpflichtungen zwischen Zahler und Zahlungsempfänger vom Zahler oder in dessen Namen oder vom Zahlungsempfänger oder in dessen Namen erteilt wurde;

6. „Auslösung eines Zahlungsvorgangs“ die zur Vorbereitung der Ausführung eines Zahlungsvorgangs erforderlichen Schritte, einschließlich der Erteilung eines Zahlungsauftrags und der vollständigen Durchführung des Authentifizierungsverfahrens;

7. „Fernauslösung eines Zahlungsvorgangs“ einen Zahlungsvorgang, für den ein Zahlungsauftrag über das Internet erteilt wird;

8. „Ausführung eines Zahlungsvorgangs“ den Vorgang, der unmittelbar nach Auslösung eines Zahlungsvorgangs beginnt und endet, sobald das bereitgestellte, abgehobene oder transferierte Geld dem Zahlungsempfänger zur Verfügung steht;

9. „Zahlungssystem“ ein System zum Geldtransfer mit formalen und standardisierten Regeln und einheitlichen Vorschriften für die Verarbeitung, das Clearing oder die Abwicklung von Zahlungen;

10. „Zahlungssystembetreiber“ eine juristische Person, die für den Betrieb eines Zahlungssystems rechtlich verantwortlich ist;

11. „Zahler“ eine natürliche oder juristische Person, die Inhaber eines Zahlungskontos ist und von diesem Zahlungskonto aus einen Zahlungsauftrag erteilt oder — falls kein Zahlungskonto vorhanden ist — eine natürliche oder juristische Person, die einen Zahlungsauftrag erteilt;

12. „Zahlungsempfänger“ eine natürliche oder juristische Person, die das bei einem Zahlungsvorgang transferierte Geld als Empfänger erhalten soll;

13. „Zahlungsdienstnutzer“ eine natürliche oder juristische Person, die einen Zahlungsdienst oder einen E-Geld-Dienst als Zahler oder Zahlungsempfänger oder in beiden Eigenschaften in Anspruch nimmt;

14. „Zahlungsdienstleister“ eine Stelle im Sinne von Artikel 2 Absatz 1 oder eine natürliche oder juristische Personen, für die eine Ausnahme gemäß den Artikeln 34, 36 und 38 der Richtlinie (EU) [PSD3] gilt;

15. „Zahlungskonto“ ein von einem Zahlungsdienstleister im Namen eines oder mehrerer Zahlungsdienstnutzer geführtes Konto, das für die Ausführung eines oder mehrerer Zahlungsvorgänge genutzt wird und es ermöglicht, Geld an Dritte zu senden und von Dritten zu erhalten;

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

17. „Mandat“ die Autorisierung des Zahlungsempfängers und (direkt oder indirekt über den Zahlungsempfänger) des Zahlungsdienstleisters durch den Zahler, aufgrund deren der Zahlungsempfänger einen Zahlungsvorgang zur Belastung des angegebenen Zahlungskontos des Zahlers auslösen und der Zahlungsdienstleister einen solchen Auftrag ausführen kann;

18. „Zahlungsinstrument“ jedes individualisierte Instrument und/oder jeden individualisierten Verfahrensablauf, das bzw. der zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister vereinbart wurde und die Auslösung eines Zahlungsvorgangs ermöglicht;

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

20. „Zahlungsauslösedienst“ einen Dienst, der auf Antrag des Zahlers oder des Zahlungsempfängers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto erteilt;

21. „Kontoinformationsdienst“ einen Online-Dienst, der entweder direkt oder über einen technischen Dienstleister Informationen zu einem oder mehreren Zahlungskonten

eines Zahlungsdienstnutzers bei einem oder mehreren kontoführenden Zahlungsdienstleistern sammelt und konsolidiert;

22. „Zahlungsauslösedienstleister“ einen Zahlungsdienstleister, der Zahlungsauslösedienste erbringt;

23. „Kontoinformationsdienstleister“ einen Zahlungsdienstleister, der Kontoinformationsdienste erbringt;

24. „Verbraucher“ eine natürliche Person, die bei den unter dieser Verordnung fallenden Zahlungsdienstverträgen nicht für die Zwecke ihrer Handels-, gewerblichen oder beruflichen Tätigkeit handelt;

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

26. „Finanztransfer“ einen Zahlungsdienst, bei dem ohne Einrichtung eines Zahlungskontos auf den Namen des Zahlers oder des Zahlungsempfängers Geld des Zahlers zum alleinigen Zweck des Transfers des entsprechenden Betrags an einen Zahlungsempfänger oder an einen anderen, im Namen des Zahlungsempfängers handelnden Zahlungsdienstleister entgegengenommen wird oder bei dem das Geld im Namen des Zahlungsempfängers entgegengenommen und diesem verfügbar gemacht wird;

27. „Lastschrift“ einen Zahlungsdienst zur Belastung des Zahlungskontos eines Zahlers, wenn ein Zahlungsvorgang vom Zahlungsempfänger aufgrund eines Mandats des Zahlers an den Zahlungsempfänger, dessen Zahlungsdienstleister oder seinen eigenen Zahlungsdienstleister ausgelöst wird;

28. „Überweisung“ einen Zahlungsdienst, der auch Sofortüberweisungen einschließt, bei dem dem Zahlungskonto des Zahlungsempfängers auf Anweisung des Zahlers zulasten von dessen Zahlungskonto in einem Zahlungsvorgang oder in einer Serie von Zahlungsvorgängen, die vom Zahlungsdienstleister, der das Zahlungskonto des Zahlers führt, ausgeführt werden, ein Betrag gutgeschrieben wird;

29. „Sofortüberweisung“ eine Überweisung, die unabhängig von Tag oder Uhrzeit unverzüglich ausgeführt wird;

30. „Geld“ für den Massenzahlungsverkehr ausgegebenes Zentralbankgeld, Giralgeld und E-Geld;

31. „Wertstellungsdatum“ den Zeitpunkt, den ein Zahlungsdienstleister für die Berechnung der Zinsen für das von einem Zahlungskonto abgebuchte oder diesem gutgeschriebene Geld zugrunde legt;

32. „Referenzwechselkurs“ den Wechselkurs, der als Grundlage für die Berechnung von Währungsumrechnungskosten zugrunde gelegt und vom Zahlungsdienstleister angegeben wird oder aus einer öffentlich zugänglichen Quelle stammt;

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

34. „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;

35. „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 sichergestellt ist;

36. „technischer Dienstleister“ einen Dienstleister, der die Erbringung von Zahlungsdiensten unterstützt, aber zu keinem Zeitpunkt in den Besitz des zu transferierenden Geldes gelangt;

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

38. „sensible Zahlungsdaten“ Daten, die für Betrugszwecke genutzt werden können, einschließlich personalisierter Sicherheitsmerkmale;

39. „Kundenidentifikator“ eine Kombination aus Buchstaben, Zahlen oder Symbolen, die der Zahlungsdienstleister dem Zahlungsdienstnutzer mitteilt und die der Zahlungsdienstnutzer angeben muss, damit ein anderer am Zahlungsvorgang beteiligter Zahlungsdienstnutzer oder das Zahlungskonto dieses anderen Zahlungsdienstnutzers bei einem Zahlungsvorgang zweifelsfrei ermittelt werden kann;

40. „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;

41. „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;

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

43. „Geschäftstag“ einen Tag, an dem der an der Ausführung eines Zahlungsvorgangs beteiligte Zahlungsdienstleister des Zahlers bzw. des Zahlungsempfängers geöffnet hat und einen Zahlungsvorgang ausführen kann;

44. „Agent“ eine natürliche oder juristische Person, die im Namen eines Zahlungsinstituts Zahlungsdienste außer E-Geld-Diensten ausführt;

45. „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;

46. „Gruppe“ eine Gruppe von Unternehmen, die durch eine in Artikel 22 Absätze 1, 2 oder 7 der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates[63] genannte Beziehung miteinander verbunden sind, oder in den Artikeln 4, 5, 6 und 7 der delegierten Verordnung (EU) Nr. 241/2014 der Kommission[64] genannte Unternehmen, die durch eine in Artikel 10 Absatz 1, in Artikel 113 Absatz 6 Unterabsatz 1 oder in Artikel 113 Absatz 7 Unterabsatz 1 der Verordnung (EU) Nr. 575/2013 genannte Beziehung miteinander verbunden sind;

47. „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;

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

49. „Ausgabe von Zahlungsinstrumenten“ einen Zahlungsdienst, bei dem sich ein Zahlungsdienstleister vertraglich dazu verpflichtet, einem Zahler ein Zahlungsinstrument zur Auslösung und Verarbeitung seiner Zahlungsvorgänge zur Verfügung zu stellen;

50. „E-Geld“ einen elektronisch, darunter auch magnetisch, gespeicherten monetären Wert in Form einer Forderung gegenüber dem Emittenten, der gegen eine Geldzahlung ausgestellt wird, um damit Zahlungsvorgänge durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem Emittenten angenommen wird;

51. „Vertriebsstelle“ eine natürliche oder juristische Person, die im Namen eines Zahlungsinstituts E-Geld vertreibt oder zurücktauscht;

52. „E-Geld-Dienste“ die Ausgabe von E-Geld, die Führung von Zahlungskonten für E-Geld-Einheiten und den Transfer von E-Geld-Einheiten;

53. „Handelsname“ den Namen, der vom Zahlungsempfänger im Allgemeinen verwendet wird, um sich gegenüber dem Zahler zu identifizieren;

54. „Geldautomatenbetreiber“ die Betreiber von Geldautomaten, die keine Zahlungskonten führen.

55. „Zahlungsinstitut, das E-Geld-Dienste anbietet“ ein Zahlungsinstitut, das E-Geld ausgibt, Zahlungskonten für E-Geld-Einheiten führt und E-Geld-Einheiten transferiert, unabhängig davon, ob es darüber hinaus auch einen der in Anhang I genannten Dienste erbringt.

---

63 Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates (ABl. L 182 vom 29.6.2013, S. 19).

64 Delegierte Verordnung (EU) Nr. 241/2014 der Kommission vom 7. Januar 2014 zur Ergänzung der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates im Hinblick auf technische Regulierungsstandards für die Eigenmittelanforderungen an Institute (ABl. L 74 vom 14.3.2014, S. 8).

TITEL II

TRANSPARENZ DER VERTRAGSBEDINGUNGEN UND INFORMATIONSPFLICHTEN BEI ZAHLUNGSDIENSTEN

KAPITEL 1

Allgemeine Vorschriften

Artikel 4

Geltungsbereich

(1) Dieser Titel gilt für Einzelzahlungen, für Rahmenverträge und für die unter solche Verträge fallenden Zahlungsvorgänge. Die an solchen Einzelzahlungen, Rahmenverträgen und unter solche Verträge fallenden Zahlungsvorgängen beteiligten Parteien können vereinbaren, dass Teile oder die Gesamtheit dieses Titels nicht gelten, wenn es sich bei dem Zahlungsdienstnutzer nicht um einen Verbraucher handelt.

(2) Die Mitgliedstaaten können diesen Titel in gleicher Weise auf Kleinstunternehmen anwenden wie auf Verbraucher.

(3) Jeder Mitgliedstaat teilt der Kommission bis zum Geltungsbeginn dieser Verordnung die Rechtsvorschriften, die er aufgrund von Absatz 2 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

Artikel 5

Währung und Währungsumrechnung

(1) Zahlungen sind in der zwischen den Parteien vereinbarten Währung zu leisten.

(2) Wird vor Auslösung eines Zahlungsvorgangs an einem Geldautomaten, an der Verkaufsstelle oder vom Zahlungsempfänger eine Währungsumrechnung angeboten, muss der Anbieter dieser Währungsumrechnung den Zahler über alle damit verbundenen Entgelte und den der Währungsumrechnung zugrunde gelegten Wechselkurs informieren.

(3) Dem Zahler muss die Möglichkeit gegeben werden, der auf dieser Grundlage angebotenen Währungsumrechnung zuzustimmen.

Artikel 6

Informationen über zusätzliche Entgelte oder Ermäßigungen

(1) Verlangt der Zahlungsempfänger für die Nutzung eines bestimmten Zahlungsinstruments ein Entgelt oder bietet er eine Ermäßigung an, so teilt er dies dem Zahler vor Auslösung des Zahlungsvorgangs mit.

(2) Verlangt der Zahlungsdienstleister oder eine andere, an dem Zahlungsvorgang beteiligte Partei für die Nutzung eines bestimmten Zahlungsinstruments ein Entgelt,

so teilt der Zahlungsdienstleister oder die andere Partei dies dem Zahlungsdienstnutzer vor der Auslösung des Zahlungsvorgangs mit.

(3) Der Zahler ist nur dann zur Zahlung der in den Absätzen 1 und 2 genannten Entgelte verpflichtet, wenn deren volle Höhe vor der Auslösung des Zahlungsvorgangs bekannt gemacht wurde.

Artikel 7

Informationspflichten bei Bargeldabhebungsdiensten

Natürliche oder juristische Personen, die die in Artikel 38 der Richtlinie (EU) [PSD3] genannten Bargeldabhebungsdienste erbringen, informieren ihre Kunden über sämtliche Entgelte oder machen diese Informationen für ihre Kunden zugänglich, und zwar sowohl bevor der Kunde die Abhebung vornimmt, als auch bei Empfang des Bargelds, wenn der Vorgang abgeschlossen ist.

Artikel 8

Entgelte für Informationen

(1) Zahlungsdienstleister dürfen Zahlungsdienstnutzern die Bereitstellung von Informationen nach diesem Titel nicht in Rechnung stellen.

(2) Zahlungsdienstleister und Zahlungsdienstnutzer können Entgelte für darüber hinausgehende Informationen, für deren häufigere Bereitstellung oder für deren Übermittlung über andere als die im Rahmenvertrag vorgesehenen Kommunikationsmittel vereinbaren, sofern die betreffenden Leistungen auf Verlangen des Zahlungsdienstnutzers erbracht werden.

(3) Die in Absatz 2 genannten Entgelte für Informationen müssen angemessen und an den tatsächlichen Kosten des Zahlungsdienstleisters ausgerichtet sein.

Artikel 9

Beweislast bei den Informationspflichten

Die Beweislast, dass die in diesem Titel festgelegten Informationspflichten erfüllt sind, liegt bei den Zahlungsdienstleistern.

Artikel 10

Ausnahme von Kleinbetragszahlungsinstrumenten und E-Geld von den Informationspflichten

Bei Zahlungsinstrumenten, die dem betreffenden Rahmenvertrag zufolge nur einzelne Zahlungsvorgänge bis höchstens 50 EUR betreffen oder die entweder eine Ausgabenobergrenze von 200 EUR haben oder zu keiner Zeit mehr als 200 EUR speichern,

a) teilt der Zahlungsdienstleister dem Zahler abweichend von den Artikeln 19, 20 und 24 nur die wesentlichen Merkmale des Zahlungsdienstes mit, darunter die Nutzungsmöglichkeiten des Zahlungsinstruments, Haftungshinweise sowie die anfallenden Entgelte und andere wesentliche Informationen, die der Zahler für

eine fundierte Entscheidung benötigt; ferner gibt er an, wo die weiteren in Artikel 20 genannten Informationen und Vertragsbedingungen in leicht zugänglicher Form verfügbar sind;

b) können die Parteien des Rahmenvertrags vereinbaren, dass der Zahlungsdienstleister abweichend von Artikel 22 Änderungen der Bedingungen des Rahmenvertrags nicht in der in Artikel 19 Absatz 1 vorgesehenen Weise vorschlagen muss;

c) können die Parteien des Rahmenvertrags vereinbaren, dass der Zahlungsdienstleister abweichend von den Artikeln 25 und 26 nach Ausführung eines Zahlungsvorgangs

i) dem Zahlungsdienstnutzer nur eine Referenz mitteilt oder zugänglich macht, die diesem die Identifizierung des betreffenden Zahlungsvorgangs, des Betrags des Zahlungsvorgangs und der entsprechenden Entgelte ermöglicht oder im Falle mehrerer gleichartiger Zahlungsvorgänge an den gleichen Zahlungsempfänger nur Informationen über den Gesamtbetrag und die entsprechenden Entgelte für diese Zahlungsvorgänge zur Verfügung stellt;

ii) die unter Ziffer i genannten Informationen nicht erteilen bzw. zugänglich machen muss, wenn das Zahlungsinstrument anonym genutzt wird oder der Zahlungsdienstleister ansonsten technisch nicht zur Erteilung dieser Informationen in der Lage ist. Der Zahlungsdienstleister muss dem Zahler die Möglichkeit zur Überprüfung der Höhe der gespeicherten Geldbeträge bieten.

KAPITEL 2

Einzelzahlungen

Artikel 11

Geltungsbereich

(1) Dieses Kapitel gilt für Einzelzahlungen, die nicht unter einen Rahmenvertrag fallen.

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

Artikel 12

Allgemeine vorvertragliche Informationen

(1) Bevor der Zahlungsdienstnutzer durch einen Vertrag oder ein Angebot für einen Einzelzahlungsdienst gebunden ist, stellt der Zahlungsdienstleister dem Zahlungsdienstnutzer die in Artikel 13 genannten Informationen und Vertragsbedingungen für seine eigenen Dienste in leicht zugänglicher Form zur

Verfügung. Auf Verlangen des Zahlungsdienstnutzers werden die Informationen und Vertragsbedingungen vom Zahlungsdienstleister in Papierform oder auf einem anderen dauerhaften Datenträger geliefert. 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 leicht verständlich abzufassen.

(2) Wurde der Vertrag über den Einzelzahlungsdienst auf Verlangen des Zahlungsdienstnutzers über ein Fernkommunikationsmittel geschlossen, das es dem Zahlungsdienstleister nicht erlaubt, seinen in Absatz 1 genannten Pflichten nachzukommen, kommt er diesen Pflichten unverzüglich nach Ausführung des Zahlungsvorgangs nach.

(3) Zahlungsdienstleister können ihren in Absatz 1 genannten Pflichten auch nachkommen, indem sie Zahlungsdienstnutzern eine Kopie des Entwurfs des Vertrags über den Einzelzahlungsdienst oder des Entwurfs des Zahlungsauftrags samt der in Artikel 13 genannten Informationen und Vertragsbedingungen zur Verfügung stellen.

Artikel 13

Informationen und Vertragsbedingungen

(1) Folgende Informationen und Vertragsbedingungen werden den Zahlungsdienstnutzern von den Zahlungsdienstleistern geliefert oder zugänglich gemacht:

a) die Informationen oder der Kundenidentifikator, die vom Zahlungsdienstnutzer mitzuteilen sind, damit ein Zahlungsauftrag ordnungsgemäß erteilt oder ausgeführt werden kann,

b) die maximale Ausführungsfrist für den zu erbringenden Zahlungsdienst,

c) die geschätzte Dauer bis zum Eingang der Überweisungen und Finanztransfers bei einem außerhalb der Union ansässigen Zahlungsdienstleister des Zahlers,

d) alle Entgelte, die der Zahlungsdienstnutzer an den Zahlungsdienstleister zu entrichten hat, sowie gegebenenfalls eine Aufschlüsselung dieser Entgelte,

e) falls zutreffend, der dem Zahlungsvorgang zugrunde zu legende tatsächliche Wechselkurs oder Referenzwechselkurs,

f) falls zutreffend, die geschätzten Entgelte für die Währungsumrechnung bei Überweisungen und Finanztransfers, ausgedrückt als prozentualer Aufschlag auf den letzten verfügbaren, von der betreffenden Zentralbank ausgegebenen anwendbaren Referenzwechselkurs,

g) ein Hinweis auf die alternativen Streitbeilegungsverfahren, die dem Zahlungsdienstnutzer gemäß den Artikeln 90, 94 und 95 zur Verfügung stehen.

(2) Zudem erteilen Zahlungsauslösedienstleister dem Zahler vor der Auslösung die folgenden klaren und umfassenden Informationen oder machen diese für den Zahler zugänglich:

a) den Namen des Zahlungsauslösedienstleisters, die Anschrift seiner Hauptverwaltung und gegebenenfalls die Anschrift seines Agenten oder seiner Zweigniederlassung in dem Mitgliedstaat, in dem der Zahlungsdienst

angeboten wird, sowie alle anderen Kontaktdaten einschließlich der E-Mail-Adresse, die für die Kommunikation mit dem Zahlungsauslösedienstleister von Belang sind, und

b) die Kontaktdaten der im Rahmen dieser Verordnung benannten zuständigen Behörde.

(3) Alle anderen in Artikel 20 genannten einschlägigen Informationen und Vertragsbedingungen sind dem Zahlungsdienstnutzer – falls zutreffend – in leicht zugänglicher Form zugänglich zu machen.

Artikel 14

Informationen für Zahler und Zahlungsempfänger nach Erteilung eines Zahlungsauftrags

Wird ein Zahlungsauftrag über einen Zahlungsauslösedienstleister erteilt, so liefert dieser dem Zahler sowie gegebenenfalls dem Zahlungsempfänger unmittelbar nach der Auslösung alle nachstehenden Daten oder macht sie für sie zugänglich:

a) eine Bestätigung, dass der Zahlungsauftrag dem kontoführenden Zahlungsdienstleister des Zahlers erfolgreich erteilt wurde,

b) eine Referenz, die dem Zahler und dem Zahlungsempfänger die Identifizierung des Zahlungsvorgangs und dem Zahlungsempfänger gegebenenfalls die Identifizierung des Zahlers ermöglicht, sowie jede weitere mit dem Zahlungsvorgang übermittelte Angabe,

c) den Betrag des Zahlungsvorgangs,

d) falls zutreffend, die Höhe aller an den Zahlungsauslösedienstleister für den Zahlungsvorgang zu entrichtenden Entgelte und falls zutreffend, eine betragsmäßige Aufschlüsselung dieser Entgelte.

Artikel 15

Informationen für den kontoführenden Zahlungsdienstleister des Zahlers, wenn ein Zahlungsauftrag über einen Zahlungsauslösedienst erteilt wird

Wird ein Zahlungsauftrag über einen Zahlungsauslösedienstleister erteilt, so stellt dieser dem kontoführenden Zahlungsdienstleister des Zahlers die Referenz des Zahlungsvorgangs zur Verfügung.

Artikel 16

Informationen für den Zahler nach Eingang des Zahlungsauftrags

Unmittelbar nach Eingang des Zahlungsauftrags liefert der Zahlungsdienstleister des Zahlers dem Zahler bezüglich seiner eigenen Dienste in der in Artikel 12 Absatz 1 vorgesehenen Weise alle nachstehenden Daten oder macht sie für den Zahler zugänglich:

a) eine Referenz, die dem Zahler die Identifizierung des Zahlungsvorgangs ermöglicht, und die Angaben, die der Zahler zur zweifelsfreien Identifizierung des Zahlungsempfängers benötigt, einschließlich des Handelsnamens des Zahlungsempfängers,

b) den Betrag des Zahlungsvorgangs in der im Zahlungsauftrag verwendeten Währung,

c) die Höhe der vom Zahler für den Zahlungsvorgang zu entrichtenden Entgelte und falls zutreffend, eine betragsmäßige Aufschlüsselung dieser Entgelte,

d) falls zutreffend, den Wechselkurs, den der Zahlungsdienstleister des Zahlers dem Zahlungsvorgang zugrunde gelegt hat, oder einen Verweis darauf, sofern dieser Kurs von dem in Artikel 13 Absatz 1 Buchstabe e genannten Kurs abweicht, und den Betrag des Zahlungsvorgangs nach dieser Währungsumrechnung,

e) das Datum des Eingangs des Zahlungsauftrags.

Artikel 17

Informationen für den Zahlungsempfänger nach Ausführung des Zahlungsvorgangs

Unmittelbar nach Ausführung des Zahlungsvorgangs liefert der Zahlungsdienstleister des Zahlungsempfängers dem Zahlungsempfänger bezüglich seiner eigenen Dienste in der in Artikel 12 Absatz 1 vorgesehenen Weise alle nachstehenden Daten oder macht sie für den Zahlungsempfänger zugänglich:

a) eine Referenz, die dem Zahlungsempfänger die Identifizierung des Zahlungsvorgangs und gegebenenfalls des Zahlers ermöglicht, sowie jede weitere mit dem Zahlungsvorgang übermittelte Angabe,

b) den Betrag des Zahlungsvorgangs in der Währung, in der der Zahlungsempfänger über das Geld verfügen kann,

c) die Höhe der vom Zahlungsempfänger für den Zahlungsvorgang zu entrichtenden Entgelte und – falls zutreffend – eine betragsmäßige Aufschlüsselung dieser Entgelte,

d) falls zutreffend, den Wechselkurs, den der Zahlungsdienstleister des Zahlungsempfängers dem Zahlungsvorgang zugrunde gelegt hat, und den Betrag des Zahlungsvorgangs vor dieser Währungsumrechnung,

e) das Wertstellungsdatum.

KAPITEL 3

Rahmenverträge

Artikel 18

Geltungsbereich

Dieses Kapitel gilt für Zahlungsvorgänge, die unter einen Rahmenvertrag fallen.

Artikel 19

Allgemeine vorvertragliche Informationen

(1) Der Zahlungsdienstleister liefert dem Zahlungsdienstnutzer rechtzeitig bevor dieser durch einen Rahmenvertrag oder ein Vertragsangebot gebunden ist, in Papierform oder auf einem anderen dauerhaften Datenträger die in Artikel 20 genannten Informationen und Vertragsbedingungen. 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 leicht verständlich abzufassen.

(2) Wurde der Rahmenvertrag auf Verlangen des Zahlungsdienstnutzers über ein Fernkommunikationsmittel geschlossen, das es dem Zahlungsdienstleister nicht erlaubt, seinen in Absatz 1 genannten Pflichten nachzukommen, kommt er diesen Pflichten unverzüglich nach Abschluss des Rahmenvertrags nach.

(3) Zahlungsdienstleister können ihren in Absatz 1 genannten Pflichten auch nachkommen, indem sie Zahlungsdienstnutzern eine Kopie des Rahmenvertragsentwurfs samt der in Artikel 20 genannten Informationen und Vertragsbedingungen zur Verfügung stellen.

Artikel 20

Informationen und Vertragsbedingungen

Der Zahlungsdienstleister liefert dem Zahlungsdienstnutzer folgende Informationen und Vertragsbedingungen:

a) Zum Zahlungsdienstleister selbst:

   i) den Namen des Zahlungsdienstleisters, die Anschrift seiner Hauptverwaltung und gegebenenfalls die Anschrift seines Agenten, seiner Vertriebsstelle oder seiner Zweigniederlassung in dem Mitgliedstaat, in dem der Zahlungsdienst angeboten wird, sowie alle anderen Anschriften einschließlich der E-Mail-Adresse, die für die Kommunikation mit dem Zahlungsdienstleister von Belang sind;

   ii) Angaben über die im Rahmen der Richtlinie (EU) [PSD3] benannten zuständigen Aufsichtsbehörden und das in den Artikeln 17 und 18 dieser Richtlinie vorgesehene Register oder über jedes andere relevante öffentliche Register, in das der Zahlungsdienstleister als zugelassen eingetragen ist, sowie seine Registernummer oder eine gleichwertige in dem betreffenden Register verwendete Kennung;

b) Zur Nutzung des Zahlungsdiensts:

   i) eine Beschreibung der wesentlichen Merkmale des zu erbringenden Zahlungsdienstes;

   ii) die vom Zahlungsdienstnutzer zu liefernden Informationen oder Kundenidentifikatoren, die für die ordnungsgemäße Erteilung oder Ausführung eines Zahlungsauftrags erforderlich sind;

   iii) die Form und das Verfahren für die Erteilung eines Zahlungsauftrags oder die Erteilung der Erlaubnis zur Ausführung eines Zahlungsvorgangs

und für den Entzug einer solchen Erlaubnis gemäß den Artikeln 49 und 66;

iv) den Zeitpunkt des Eingangs eines Zahlungsauftrags gemäß Artikel 64 und gegebenenfalls den vom Zahlungsdienstleister festgelegten Annahmeschluss;

v) die maximale Ausführungsfrist für die zu erbringenden Zahlungsdienste;

vi) die geschätzte Dauer bis zum Eingang der Überweisungen bei einem außerhalb der Union ansässigen Zahlungsdienstleister des Zahlers;

vii) die Angabe, ob die Möglichkeit besteht, gemäß Artikel 51 Absatz 1 Ausgabenobergrenzen für die Nutzung des Zahlungsinstruments zu vereinbaren;

viii) bei kartengebundenen Zahlungsinstrumenten, die durch Co-Badging mehrere Zahlungsmarken tragen, die Rechte des Zahlungsdienstnutzers gemäß Artikel 8 der Verordnung (EU) 2015/751;

c) Zu Entgelten, Zinsen und Wechselkursen:

i) alle Entgelte, die der Zahlungsdienstnutzer an den Zahlungsdienstleister zu entrichten hat, einschließlich derjenigen, die damit zusammenhängen, wie und wie oft die in dieser Verordnung verlangten Informationen erteilt oder zugänglich gemacht werden, sowie – falls zutreffend – eine betragsmäßige Aufschlüsselung dieser Entgelte;

ii) soweit zutreffend, alle etwaigen Entgelte für Abhebungen an Geldautomaten im Inland, die Zahlungsdienstnutzer an ihren Zahlungsdienstleister entrichten müssen, wenn es sich handelt um:

1. einen Geldautomaten ihres Zahlungsdienstleisters,

2. einen Geldautomaten eines Zahlungsdienstleisters, der demselben Geldautomatennetz angehört wie der Zahlungsdienstleister des Nutzers,

3. einen Geldautomaten eines Zahlungsdienstleisters, der einem Geldautomatennetz angehört, mit dem der Zahlungsdienstleister des Nutzers eine vertragliche Beziehung unterhält,

4. einen Geldautomaten eines Betreibers, der Bargeldabhebungsdienste anbietet, aber keine Zahlungskonten führt;

iii) falls zutreffend, die zugrunde gelegten Zinssätze und Wechselkurse oder — bei Anwendung von Referenzzinssätzen und -wechselkursen — die Methode für die Berechnung der tatsächlichen Zinsen sowie den maßgeblichen Stichtag und den maßgeblichen Index oder die maßgebliche Grundlage für die Bestimmung des Referenzzinssatzes oder -wechselkurses;

iv) soweit vereinbart, die unmittelbare Anwendung von Änderungen des Referenzzinssatzes oder -wechselkurses und die Benachrichtigungspflichten in Bezug auf diese Änderungen gemäß Artikel 22 Absatz 3;

v) falls zutreffend, die geschätzten Entgelte für Währungsumrechnungsdienste bei Überweisungen, ausgedrückt als prozentualer Aufschlag auf den letzten verfügbaren, von der betreffenden Zentralbank ausgegebenen anwendbaren Referenzwechselkurs;

d) Zur Kommunikation:

i) falls zutreffend, die Kommunikationsmittel, die zwischen den Parteien für die Übermittlung von Informationen oder Anzeigen nach Maßgabe dieser Verordnung vereinbart werden, einschließlich der technischen Anforderungen an die Ausstattung und die Software des Zahlungsdienstnutzers;

ii) Angaben dazu, wie und wie oft die in dieser Verordnung verlangten Informationen zu erteilen oder zugänglich zu machen sind;

iii) die Sprache oder Sprachen, in der bzw. denen der Rahmenvertrag geschlossen wird und in der bzw. denen die Kommunikation für die Dauer dieses Vertragsverhältnisses stattfinden soll;

iv) ein Hinweis auf das Recht des Zahlungsdienstnutzers, Informationen und die Vertragsbedingungen des Rahmenvertrags gemäß Artikel 21 zu erhalten;

e) Zu den Schutz- und Abhilfemaßnahmen:

i) falls zutreffend, eine Beschreibung der Vorkehrungen, die der Zahlungsdienstnutzer für die sichere Aufbewahrung eines Zahlungsinstruments zu treffen hat, und wie der Zahlungsdienstnutzer seiner Anzeigepflicht gegenüber dem Zahlungsdienstleister nach Artikel 52 Buchstabe b nachzukommen hat;

ii) eine Beschreibung des sicheren Verfahrens, mit dem der Zahlungsdienstleister den Zahlungsdienstnutzer im Falle vermuteten oder tatsächlichen Betrugs oder bei Sicherheitsrisiken unterrichtet;

iii) sofern vereinbart, die Bedingungen, unter denen sich der Zahlungsdienstleister das Recht vorbehält, ein Zahlungsinstrument gemäß Artikel 51 zu sperren;

iv) Informationen zur Haftung des Zahlers gemäß Artikel 57 Absatz 5, Artikel 59 Absatz 3 und Artikel 60 einschließlich Angaben zum relevanten Betrag;

v) Angaben dazu, wie und innerhalb welcher Frist der Zahlungsdienstnutzer dem Zahlungsdienstleister – und bei einem in Artikel 59 genannten Identitätsbetrug auch der Polizei – jeden nicht autorisierten oder fehlerhaft ausgelösten oder ausgeführten Zahlungsvorgang oder jede nach einer fehlerhaften Anwendung des Abgleichservice für Namen und Kundenidentifikator oder nach einem Identitätsbetrug autorisierte Überweisung gemäß Artikel 54 anzeigen muss;

vi) Informationen über die Haftung des Zahlungsdienstleisters bei nicht autorisierten Zahlungsvorgängen gemäß Artikel 56, bei fehlerhafter Anwendung des Abgleichservice für Namen und Kundenidentifikator gemäß Artikel 57 und bei Identitätsbetrug gemäß Artikel 59;

vii) Informationen über die Haftung des Zahlungsdienstleisters bei der Auslösung oder Ausführung von Zahlungsvorgängen gemäß den Artikeln 75 und 76;

viii) die Bedingungen für Erstattungen gemäß den Artikeln 62 und 63;

f) Zu Änderungen und zur Kündigung des Rahmenvertrags:

i) soweit vereinbart, die Angabe, dass die Zustimmung des Zahlungsdienstnutzers zu einer Änderung der Vertragsbedingungen nach Artikel 22 als erteilt gilt, sofern der Zahlungsdienstnutzer dem Zahlungsdienstleister nicht vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens der geänderten Bedingungen anzeigt, dass er diese Änderung ablehnt;

ii) die Laufzeit des Rahmenvertrags;

iii) ein Hinweis auf das Recht des Zahlungsdienstnutzers, den Rahmenvertrag zu kündigen, sowie auf sonstige kündigungsrelevante Vereinbarungen nach Artikel 22 Absatz 1 und Artikel 23;

g) Zum Rechtsbehelf:

i) die Vertragsklauseln über das für den Rahmenvertrag geltende Recht und/oder die zuständigen Gerichte;

ii) ein Hinweis auf die alternativen Streitbeilegungsverfahren, die dem Zahlungsdienstnutzer gemäß den Artikeln 90, 94 und 95 zur Verfügung stehen.

Artikel 21

Verfügbarkeit der Informationen und der Rahmenvertragsbedingungen

Während der vertraglichen Beziehung hat der Zahlungsdienstnutzer jederzeit das Recht, auf Verlangen die Bedingungen des Rahmenvertrags sowie die in Artikel 20 genannten Informationen und Vertragsbedingungen auf Papier oder auf einem anderen dauerhaften Datenträger zu erhalten.

Artikel 22

Änderungen der Rahmenvertragsbedingungen

(1) Der Zahlungsdienstleister schlägt jede Änderung am Rahmenvertrag oder an den in Artikel 20 genannten Informationen und Vertragsbedingungen in der in Artikel 19 Absatz 1 vorgesehenen Weise vor, spätestens jedoch zwei Monate vor dem vorgeschlagenen Geltungsbeginn. Der Zahlungsdienstnutzer kann den Änderungen vor dem vorgeschlagenen Zeitpunkt ihres Inkrafttretens entweder zustimmen oder sie ablehnen.

(2) Falls zutreffend unterrichtet der Zahlungsdienstleister den Zahlungsdienstnutzer gemäß Artikel 20 Buchstabe f Ziffer i, dass dessen Zustimmung zu den Änderungen als erteilt gilt, wenn er dem Zahlungsdienstleister nicht vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens der geänderten Bedingungen seine Ablehnung angezeigt hat. Der Zahlungsdienstleister klärt den Zahlungsdienstnutzer ferner über sein Recht

auf, den Rahmenvertrag jederzeit bis zum Geltungsbeginn der Änderungen kostenlos zu kündigen, sollte er diese Änderungen ablehnen.

(3) Änderungen der Zinssätze oder Wechselkurse können vom Zahlungsdienstleister unmittelbar und ohne vorherige Benachrichtigung angewandt werden, sofern dieses Recht im Rahmenvertrag vereinbart wurde und die Zinssatz- oder Wechselkursänderungen auf den gemäß Artikel 20 Buchstabe c Ziffern iii und iv vereinbarten Referenzzinssätzen oder -wechselkursen beruhen. Der Zahlungsdienstleister unterrichtet den Zahlungsdienstnutzer so rasch wie möglich in der in Artikel 19 Absatz 1 vorgesehenen Weise über jede Zinssatzänderung, es sei denn, die Parteien haben eine Vereinbarung darüber getroffen, wie oft und wie die Informationen zu erteilen oder zugänglich zu machen sind. Für den Zahlungsdienstnutzer vorteilhafte Zinssatz- oder Wechselkursänderungen können vom Zahlungsdienstleister jedoch ohne Benachrichtigung angewandt werden.

(4) Änderungen an den bei Zahlungsvorgängen zugrunde gelegten Zinssätzen oder Wechselkursen sind vom Zahlungsdienstleister neutral anzuwenden und zu berechnen, sodass Zahlungsdienstnutzer nicht benachteiligt werden.

Artikel 23

Kündigung

(1) Sofern die Parteien keine Kündigungsfrist vereinbart haben, kann der Zahlungsdienstnutzer den Rahmenvertrag jederzeit kündigen. Eine solche Kündigungsfrist darf einen Monat nicht überschreiten.

(2) Die Kündigung des Rahmenvertrags muss für den Zahlungsdienstnutzer kostenlos sein, es sei denn, der Vertrag war weniger als sechs Monate in Kraft. Sofern für die Kündigung des Rahmenvertrags Entgelte anfallen, müssen diese angemessen und an den Kosten ausgerichtet sein. Werden Zahlungsdienste dem Rahmenvertrag zufolge gemeinsam mit technischen Diensten angeboten, die die Erbringung von Zahlungsdiensten unterstützen sollen und vom Zahlungsdienstleister oder einem Dritten erbracht werden, mit dem der Zahlungsdienstleister eine Partnerschaft eingegangen ist, so gelten für diese technischen Dienste in Bezug auf Kündigungsentgelte die Anforderungen des Rahmenvertrags.

(3) Sofern im Rahmenvertrag vereinbart, kann der Zahlungsdienstleister einen auf unbestimmte Zeit geschlossenen Rahmenvertrag unter Einhaltung einer mindestens zweimonatigen Kündigungsfrist in der in Artikel 19 Absatz 1 vorgesehenen Weise kündigen.

(4) Regelmäßig erhobene Zahlungsdienstentgelte sind vom Zahlungsdienstnutzer nur anteilsmäßig bis zur Kündigung des Vertrags zu entrichten. Werden solche Entgelte im Voraus entrichtet, sind sie vom Zahlungsdienstleister anteilsmäßig zu erstatten.

(5) Die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über das Recht der Parteien, den Rahmenvertrag für aufgehoben oder nichtig zu erklären, bleiben von diesem Artikel unberührt.

(6) Die Mitgliedstaaten können für die Kündigung von Verträgen Vorschriften erlassen, die für die Zahlungsdienstnutzer vorteilhafter sind.

(7) Die Mitgliedstaaten teilen der Kommission bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = Geltungsbeginn dieser Verordnung] ihre nach Absatz 6

erlassenen gesetzlichen Bestimmungen mit. Alle nachfolgenden Änderungen dieser Bestimmungen teilen sie umgehend mit.

Artikel 24

Informationen vor Ausführung einzelner Zahlungsvorgänge

Bei einem einzelnen Zahlungsvorgang, der innerhalb eines Rahmenvertrags vom Zahler ausgelöst wird, teilt der Zahlungsdienstleister auf Verlangen des Zahlers für diesen bestimmten Zahlungsvorgang alles Folgende ausdrücklich mit:

a) die maximale Ausführungsfrist,

b) die vom Zahler zu entrichtenden Entgelte,

c) falls zutreffend, eine betragsmäßige Aufschlüsselung aller Entgelte.

Artikel 25

Informationen für den Zahler zu einzelnen Zahlungsvorgängen

(1) Nach Belastung des Kontos des Zahlers mit dem Betrag eines einzelnen Zahlungsvorgangs oder — falls der Zahler kein Zahlungskonto verwendet — nach Eingang des Zahlungsauftrags teilt der Zahlungsdienstleister des Zahlers dem Zahler unverzüglich in der in Artikel 19 Absatz 1 vorgesehenen Weise alles Folgende mit:

a) eine Referenz, die dem Zahler die Identifizierung jedes Zahlungsvorgangs ermöglicht, und die Angaben, die zur zweifelsfreien Identifizierung des Zahlungsempfängers erforderlich sind, einschließlich des Handelsnamens des Zahlungsempfängers,

b) den Betrag des Zahlungsvorgangs in der Währung, in der das Zahlungskonto des Zahlers belastet wird, oder in der Währung, die im Zahlungsauftrag verwendet wird,

c) die für den Zahlungsvorgang zu entrichtenden Entgelte und – falls zutreffend – eine betragsmäßige Aufschlüsselung dieser Entgelte oder die vom Zahler zu entrichtenden Zinsen,

d) falls zutreffend, den Wechselkurs, den der Zahlungsdienstleister des Zahlers dem Zahlungsvorgang zugrunde gelegt hat, und den Betrag des Zahlungsvorgangs nach dieser Währungsumrechnung,

e) das Wertstellungsdatum der Belastung oder das Datum des Eingangs des Zahlungsauftrags.

(2) Ein Rahmenvertrag muss eine Klausel enthalten, wonach der Zahler verlangen kann, dass die in Absatz 1 genannten Informationen mindestens einmal monatlich kostenlos und nach einem vereinbarten Verfahren so erteilt oder zugänglich gemacht werden, dass der Zahler sie unverändert aufbewahren und reproduzieren kann.

(3) Die Mitgliedstaaten können Zahlungsdienstleistern jedoch vorschreiben, dass die Informationen mindestens einmal monatlich in Papierform oder auf einem anderen dauerhaften Datenträger kostenlos zu erteilen sind.

(4) Die Mitgliedstaaten teilen der Kommission bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = Geltungsbeginn dieser Verordnung] ihre nach Absatz 3

erlassenen gesetzlichen Bestimmungen mit. Alle nachfolgenden Änderungen dieser Bestimmungen teilen sie umgehend mit.

Artikel 26

Informationen für den Zahlungsempfänger zu einzelnen Zahlungsvorgängen

(1) Nach Ausführung eines einzelnen Zahlungsvorgangs teilt der Zahlungsdienstleister des Zahlungsempfängers dem Zahlungsempfänger unverzüglich in der in Artikel 19 Absatz 1 vorgesehenen Weise alles Folgende mit:

a) eine Referenz, die dem Zahlungsempfänger die Identifizierung des Zahlungsvorgangs und des Zahlers ermöglicht, sowie alle weiteren mit dem Zahlungsvorgang übermittelten Angaben,

b) den Betrag des Zahlungsvorgangs, in der Währung, in der der Betrag dem Zahlungskonto des Zahlungsempfängers gutgeschrieben wird,

c) die für den Zahlungsvorgang zu entrichtenden Entgelte und gegebenenfalls eine betragsmäßige Aufschlüsselung dieser Entgelte oder die vom Zahlungsempfänger zu entrichtenden Zinsen,

d) falls zutreffend, den Wechselkurs, den der Zahlungsdienstleister des Zahlungsempfängers dem Zahlungsvorgang zugrunde gelegt hat, und den Betrag des Zahlungsvorgangs vor dieser Währungsumrechnung,

e) das Wertstellungsdatum.

(2) Ein Rahmenvertrag kann eine Klausel enthalten, wonach die in Absatz 1 genannten Informationen mindestens einmal monatlich nach einem vereinbarten Verfahren so erteilt oder zugänglich gemacht werden, dass der Zahlungsempfänger sie unverändert aufbewahren und reproduzieren kann.

(3) Die Mitgliedstaaten können Zahlungsdienstleistern jedoch vorschreiben, dass die Informationen mindestens einmal monatlich in Papierform oder auf einem anderen dauerhaften Datenträger kostenlos zu erteilen sind.

(4) Die Mitgliedstaaten teilen der Kommission bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = Geltungsbeginn dieser Verordnung] ihre nach Absatz 3 erlassenen gesetzlichen Bestimmungen mit. Alle nachfolgenden Änderungen dieser Bestimmungen teilen sie umgehend mit.

TITEL III

RECHTE UND PFLICHTEN BEI DER ERBRINGUNG UND NUTZUNG VON ZAHLUNGSDIENSTEN

KAPITEL 1

Allgemeine Bestimmungen

Artikel 27

Geltungsbereich

(1) Handelt es sich bei dem Zahlungsdienstnutzer nicht um einen Verbraucher, können der Zahlungsdienstnutzer und der Zahlungsdienstleister vereinbaren, dass Artikel 28 Absatz 1, Artikel 49 Absatz 7 sowie die Artikel 55, 60, 62, 63, 66, 75 und 76 ganz oder teilweise keine Anwendung finden. Zahlungsdienstnutzer und Zahlungsdienstleister können auch andere als die in Artikel 54 festgelegten Fristen vereinbaren.

(2) Die Mitgliedstaaten können vorsehen, dass Artikel 95 keine Anwendung findet, wenn es sich bei dem Zahlungsdienstnutzer nicht um einen Verbraucher handelt.

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

(4) Die Mitgliedstaaten teilen der Kommission bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = Geltungsbeginn dieser Verordnung] ihre nach den Absätzen 2 und 3 erlassenen gesetzlichen Bestimmungen mit. Alle nachfolgenden Änderungen dieser Bestimmungen teilen sie umgehend mit.

Artikel 28

Entgelte

(1) Der Zahlungsdienstleister darf dem Zahlungsdienstnutzer für die Erfüllung seiner Informationspflichten oder für Berichtigungs- und Schutzmaßnahmen nach diesem Titel nur dann Entgelte in Rechnung stellen, wenn dies in Artikel 65 Absatz 1, Artikel 66 Absatz 5 und Artikel 74 Absatz 4 ausdrücklich vorgesehen ist. Diese Entgelte müssen zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister vereinbart werden; sie müssen angemessen und an den tatsächlichen Kosten des Zahlungsdienstleisters ausgerichtet sein.

(2) Bei Zahlungsvorgängen innerhalb der Union, bei denen sowohl der Zahlungsdienstleister des Zahlers als auch der Zahlungsdienstleister des Zahlungsempfängers in der Union ansässig ist oder — falls nur ein einziger Zahlungsdienstleister an dem Zahlungsvorgang beteiligt ist — dieser in der Union ansässig ist, tragen Zahlungsempfänger und Zahler die von ihrem jeweiligen Zahlungsdienstleister erhobenen Entgelte.

(3) Für die Nutzung von Zahlungsinstrumenten, bei denen die Interbankenentgelte in Kapitel II der Verordnung (EU) 2015/751 festgelegt sind, sowie für Überweisungen,

einschließlich Sofortüberweisungen, und Lastschriften innerhalb der Union darf der Zahlungsempfänger keine Entgelte verlangen.

(4) Unter Berücksichtigung der Notwendigkeit, den Wettbewerb und die Nutzung effizienter Zahlungsinstrumente zu fördern, können die Mitgliedstaaten das Verbot, für die Nutzung anderer Zahlungsinstrumente als der in Absatz 3 genannten Instrumente Entgelte zu verlangen, verlängern oder ein entsprechendes Recht des Zahlungsempfängers einschränken.

(5) Unbeschadet der Absätze 3 und 4 darf der Zahlungsdienstleister es dem Zahlungsempfänger bei nicht unter diese Absätze fallenden Instrumenten nicht verwehren, vom Zahler für die Nutzung eines bestimmten Zahlungsinstruments ein Entgelt zu verlangen, ihm eine Ermäßigung anzubieten oder dem Zahler anderweitig einen Anreiz zur Nutzung dieses Instruments zu geben. Entgelte dürfen nicht höher sein als die direkten Kosten, die dem Zahlungsempfänger für die Nutzung des betreffenden Zahlungsinstruments entstehen.

(6) Die Mitgliedstaaten teilen der Kommission bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = Geltungsbeginn dieser Verordnung] ihre nach Absatz 4 erlassenen gesetzlichen Bestimmungen mit. Alle nachfolgenden Änderungen dieser Bestimmungen teilen sie umgehend mit.

Artikel 29

Ausnahmeregelung für Kleinbetragszahlungsinstrumente und elektronisches Geld

(1) Bei Zahlungsinstrumenten, die dem Rahmenvertrag zufolge nur einzelne Zahlungsvorgänge bis höchstens 50 EUR betreffen oder die entweder eine Ausgabenobergrenze von 200 EUR haben oder Geldbeträge speichern, die zu keiner Zeit 200 EUR übersteigen, können die Zahlungsdienstleister mit ihren Zahlungsdienstnutzern vereinbaren, dass

a) Artikel 52 Buchstabe b, Artikel 53 Absatz 1 Buchstaben c und d und Artikel 60 Absatz 4 keine Anwendung finden, wenn das Zahlungsinstrument nicht gesperrt werden oder seine weitere Nutzung nicht verhindert werden kann,

b) die Artikel 55 und 56 sowie Artikel 60 Absätze 1 und 4 keine Anwendung finden, wenn das Zahlungsinstrument anonym genutzt wird oder der Zahlungsdienstleister aus anderen Gründen, die dem Zahlungsinstrument immanent sind, nicht nachweisen kann, dass ein Zahlungsvorgang autorisiert war,

c) abweichend von Artikel 65 Absatz 1 der Zahlungsdienstleister nicht verpflichtet ist, den Zahlungsdienstnutzer von einer Ablehnung des Zahlungsauftrags zu unterrichten, wenn die Nichtausführung aus dem Zusammenhang hervorgeht,

d) abweichend von Artikel 66 der Zahler den Zahlungsauftrag nach dessen Übermittlung oder nach Autorisierung des Zahlungsvorgangs an den Zahlungsempfänger nicht widerrufen kann,

e) abweichend von den Artikeln 69 und 70 andere Ausführungsfristen gelten.

(2) Die Artikel 56 und 60 gelten auch für E-Geld, außer in Fällen, in denen der Zahlungsdienstleister des Zahlers nicht die Möglichkeit hat, das Zahlungskonto, auf dem das E-Geld gespeichert ist, oder das Zahlungsinstrument zu sperren. Die Mitgliedstaaten können diese Ausnahmeregelung auf Zahlungskonten, auf denen das E-Geld gespeichert ist, oder auf Zahlungsinstrumente mit einem gewissen Wert beschränken.

(3) Die Mitgliedstaaten teilen der Kommission bis zum Geltungsbeginn dieser Verordnung ihre nach Absatz 2 erlassenen gesetzlichen Bestimmungen mit. Alle nachfolgenden Änderungen dieser Bestimmungen teilen sie umgehend mit.

Artikel 30

Ausgabe und Rücktauschbarkeit von E-Geld

(1) E-Geld-Emittenten geben E-Geld zum Nennwert des entgegengenommenen Geldes aus.

(2) Auf Verlangen des E-Geld-Inhabers tauscht der E-Geld-Emittent den monetären Wert des gehaltenen E-Geldes jederzeit zum Nennwert zurück.

(3) Im Vertrag zwischen dem E-Geld-Emittenten und dem E-Geld-Inhaber sind die Rücktauschbedingungen, einschließlich etwaiger diesbezüglicher Entgelte, eindeutig und an gut erkennbarer Stelle anzugeben; der E-Geld-Inhaber ist über diese Bedingungen zu informieren, bevor er durch einen Vertrag oder ein Angebot gebunden ist.

(4) Beim Rücktausch von E-Geld darf nur dann ein Entgelt erhoben werden, wenn dies gemäß Absatz 3 im Vertrag festgelegt wurde und einer der folgenden Fälle vorliegt:

a) der E-Geld-Inhaber verlangt den Rücktausch vor Ablauf des Vertrags,

b) der Vertrag sieht ein Ablaufdatum vor und der E-Geld-Inhaber kündigt den Vertrag vor diesem Termin,

c) der Rücktausch wird mehr als ein Jahr nach Vertragsablauf verlangt.

Ein solches Entgelt muss in einem angemessenen Verhältnis zu den tatsächlich entstandenen Kosten des E-Geld-Emittenten stehen.

(5) Verlangt der E-Geld-Inhaber den Rücktausch vor Vertragsablauf, so kann er entweder einen Teil oder den gesamten E-Geld-Betrag verlangen.

(6) Verlangt der E-Geld-Inhaber den Rücktausch am Tag des Vertragsablaufs oder bis zu einem Jahr nach Ablauf des Vertrags, so

a) tauscht der E-Geld-Emittent den vollen monetären Wert des E-Gelds zurück oder

b) tauscht der E-Geld-Emittent alle vom E-Geld-Inhaber verlangten Gelder zurück, falls das Zahlungsinstitut eine oder mehrere der in Artikel 10 Absatz 1 Buchstabe c der Richtlinie XXX [PSD3] genannten Tätigkeiten ausübt und im Voraus nicht bekannt ist, welcher Anteil der Gelder von den E-Geld-Inhabern als E-Geld verwendet werden soll.

(7) Unbeschadet der Absätze 4, 5 und 6 unterliegen die Rücktauschrechte von Personen, die E-Geld akzeptieren und bei denen es sich nicht um Verbraucher handelt, der vertraglichen Vereinbarung zwischen dem E-Geld-Emittenten und diesen Personen.

(8) Ein Zahlungsinstitut, das E-Geld-Dienste anbietet, darf einem E-Geld-Inhaber keine Zinsen oder sonstigen Leistungen gewähren, die im Zusammenhang mit dem Zeitraum stehen, in dem der E-Geld-Inhaber das E-Geld hält.

KAPITEL 2

Zugang zu Zahlungssystemen und zu Konten bei Kreditinstituten

Artikel 31

Zugang zu Zahlungssystemen

(1) Zahlungssystembetreiber verfügen über objektive, nicht diskriminierende, transparente und verhältnismäßige Regeln, nach denen zugelassene oder registrierte Zahlungsdienstleister, bei denen es sich um juristische Personen handelt, Zugang zu einem Zahlungssystem erhalten können. Zahlungssystembetreiber dürfen den Zugang zu einem Zahlungssystem nur so weit einschränken, wie es für den Schutz gegen spezifische Risiken, wie gegebenenfalls das Abwicklungsrisiko, das operationelle Risiko, das Kreditrisiko, das Liquiditätsrisiko und das Geschäftsrisiko oder für den Schutz der finanziellen und operativen Stabilität des Zahlungssystems erforderlich ist.

(2) Ein Zahlungssystembetreiber stellt seine Regeln und Verfahren, nach denen er die Zulassung für die Teilnahme an diesem Zahlungssystem erteilt, sowie die Kriterien und Methoden, nach denen er die Risikobewertung für Antragsteller vornimmt, öffentlich zur Verfügung.

(3) Wenn ein Zahlungssystembetreiber von einem Zahlungsdienstleister einen Antrag auf Teilnahme erhält, bewertet er, mit welchen Risiken es im jeweiligen Fall verbunden ist, dem antragstellenden Zahlungsdienstleister Zugang zum System zu gewähren. Ein Zahlungssystembetreiber verweigert einem antragstellenden Zahlungsdienstleister die Teilnahme nur dann, wenn der Antragsteller für das System gemäß Absatz 1 mit Risiken verbunden ist. Der Zahlungssystembetreiber teilt dem antragstellenden Zahlungsdienstleister schriftlich mit, ob seinem Teilnahmeantrag stattgegeben wird oder nicht und begründet jede Ablehnung umfassend.

(4) Die Absätze 1, 2 und 3 gelten nicht für Zahlungssysteme, die ausschließlich aus Zahlungsdienstleistern derselben Unternehmensgruppe bestehen.

(5) Zahlungssystembetreiber dürfen keine der folgenden Beschränkungen auferlegen:

a) restriktive Regeln hinsichtlich der effektiven Mitgliedschaft in anderen Zahlungssystemen,

b) Regeln, die zugelassene Zahlungsdienstleister oder registrierte Zahlungsdienstleister untereinander in Bezug auf Rechte, Pflichten und Ansprüche von Mitgliedern diskriminieren,

c) Beschränkungen, die auf den Status als Institut abstellen.

(6) Gestattet ein Zahlungssystemteilnehmer einem zugelassenen oder registrierten Zahlungsdienstleister, der kein Teilnehmer des Zahlungssystems ist, Zahlungs- bzw. Übertragungsaufträge über dieses Zahlungssystem zu erteilen, muss er anderen zugelassenen oder registrierten Zahlungsdienstleistern auf Antrag in objektiver,

verhältnismäßiger und nichtdiskriminierender Weise dieselbe Möglichkeit einräumen. Wird ein solcher Antrag abgelehnt, ist diese Ablehnung vom Zahlungssystemteilnehmer gegenüber jedem antragstellenden Zahlungsdienstleister umfassend zu begründen.

(7) Für Zahlungssysteme, die nach der Verordnung (EU) Nr. 795/2014 nicht vom Eurosystem überwacht werden, benennen die Mitgliedstaaten eine für die Zahlungssystemüberwachung zuständige Behörde, um die Durchsetzung der Absätze 1, 2, 3, 5 und 6 durch die ihrem nationalen Recht unterliegenden Zahlungssysteme sicherzustellen.

Artikel 32

Zahlungskonten, die von Kreditinstituten für Zahlungsinstitute bereitgestellt werden

(1) Ein Kreditinstitut darf die Eröffnung eines Zahlungskontos für ein Zahlungsinstitut oder dessen Agenten oder Vertriebsstellen oder für einen Antragsteller, der eine Zulassung als Zahlungsinstitut erhalten möchte, nur in nachstehend genannten Fällen verweigern oder ein solches Konto nur in nachstehend genannten Fällen schließen:

a) das Kreditinstitut hat schwerwiegende Gründe für den Verdacht, dass die Kontrollen des Antragstellers auf Geldwäsche oder Terrorismusfinanzierung mangelhaft sind, oder dass der Antragsteller oder dessen Kunden rechtswidrige Handlungen begehen,

b) der Antragsteller hat einen Vertrag verletzt oder ist dabei, dies zu tun,

c) der Antragsteller hat unzureichende Informationen und Unterlagen vorgelegt,

d) das Risikoprofil des Antragstellers oder seines Geschäftsmodells ist übermäßig hoch,

e) der Antragsteller brächte für das Kreditinstitut unverhältnismäßig hohe Befolgungskosten mit sich.

(2) Rechte, die Agenten oder Vertriebsstellen nach Absatz 1 gewährt werden, gelten ausschließlich für die Erbringung von Zahlungsdiensten im Namen des Zahlungsinstituts.

(3) Ein Kreditinstitut setzt das Zahlungsinstitut oder dessen Agenten oder Vertriebsstellen oder den Antragsteller, der eine Zulassung als Zahlungsinstitut erhalten möchte, über jede Entscheidung in Kenntnis, dem Zahlungsinstitut, seinen Agenten oder Vertriebsstellen oder dem Antragsteller, der eine Zulassung als Zahlungsinstitut erhalten möchte, die Eröffnung eines Zahlungskontos zu verweigern oder ein solches Konto zu schließen; jede derartige Entscheidung ist gebührend zu begründen. Eine solche Begründung muss speziell auf die Risiken abstellen, mit denen die Tätigkeit oder geplante Tätigkeit dieses Zahlungsinstituts oder seiner Agenten oder Vertriebsstellen nach Einschätzung des Kreditinstituts verbunden ist, und darf nicht allgemeiner Natur sein.

(4) Zahlungsinstitute, deren Agenten oder Vertriebsstellen oder Antragsteller, die eine Zulassung als Zahlungsinstitut erhalten möchten, die von einem Kreditinstitut über dessen Entscheidung in Kenntnis gesetzt wurden, den Zugang zu

Zahlungskontodiensten zu verweigern oder solche Konten zu schließen, können bei einer zuständigen Behörde Beschwerde einlegen.

(5) Die EBA arbeitet Entwürfe technischer Regulierungsstandards aus, in denen das harmonisierte Format und die Informationen, die in der in Absatz 3 genannten Mitteilung und der dort genannten Begründung enthalten sein müssen, festgelegt werden.

Die EBA übermittelt der Kommission den Entwurf der in Unterabsatz 1 genannten technischen Regulierungsstandards bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = ein Jahr nach Inkrafttreten dieser Verordnung]. Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010 zu erlassen.

Kapitel 3

Kontoinformationsdienste und Zahlungsauslösedienste

ABSCHNITT 1

ALLGEMEINE GRUNDSÄTZE

Artikel 33

Rechte der Zahlungsdienstnutzer

(1) Zahlungsdienstleister hindern Zahlungsdienstnutzer nicht daran, für die in Anhang I Nummer 6 genannten Zahlungsauslösedienste einen Zahlungsauslösedienstleister in Anspruch zu nehmen. Diese Verpflichtung gilt für alle online zugänglichen Zahlungskonten des Zahlungsdienstnutzers.

(2) Zahlungsdienstleister hindern Zahlungsdienstnutzer nicht daran, die in Anhang I Nummer 7 genannten Kontoinformationsdienste in Anspruch zu nehmen. Diese Verpflichtung gilt für alle online zugänglichen Zahlungskonten des Zahlungsdienstnutzers.

Artikel 34

Vertragliche Beziehungen

(1) Die Bereitstellung von Kontoinformations- und Zahlungsauslösediensten darf von keiner Partei davon abhängig gemacht werden, dass zwischen den Anbietern solcher Dienste und einem kontoführenden Zahlungsdienstleister eine entsprechende vertragliche Beziehung besteht.

(2) Besteht eine mehrseitige vertragliche Vereinbarung und stehen die unter diese Verordnung fallenden Zahlungskontodaten auch im Rahmen dieser mehrseitigen vertraglichen Vereinbarung zur Verfügung, so müssen Kontoinformations- und Zahlungsauslösedienstleister stets auf die unter diese Verordnung fallenden

Zahlungskontodaten zugreifen können, ohne Partei der mehrseitigen vertraglichen Vereinbarung sein zu müssen.

ABSCHNITT 2

DATENZUGANGSSCHNITTSTELLEN FÜR KONTOINFORMATIONS- UND ZAHLUNGSAUSLÖSEDIENSTE

Artikel 35

Bereitstellung dedizierter Zugangsschnittstellen

(1) Kontoführende Zahlungsdienstleister, die einem Zahler ein online zugängliches Zahlungskonto bereitstellen, haben für den Datenaustausch mit Kontoinformations- und Zahlungsauslösedienstleistern mindestens eine dedizierte Schnittstelle eingerichtet.

(2) Unbeschadet der Artikel 38 und 39 dürfen kontoführende Zahlungsdienstleister, die einem Zahler ein online zugängliches Zahlungskonto bereitstellen und gemäß Absatz 1 eine dedizierte Schnittstelle eingerichtet haben, nicht dazu verpflichtet werden, für den Datenaustausch mit Kontoinformations- und Zahlungsauslösedienstleistern zur Sicherheit dauerhaft eine weitere Schnittstelle zu unterhalten.

(3) Kontoführende Zahlungsdienstleister gewährleisten, dass ihre in Absatz 1 genannten dedizierten Schnittstellen den von europäischen oder internationalen Normungsorganisationen, einschließlich des Europäischen Komitees für Normung (CEN) oder der Internationalen Organisation für Normung (ISO), herausgegeben Standards für die Kommunikation entsprechen. Kontoführende Zahlungsdienstleister gewährleisten zudem, dass die technischen Spezifikationen einer jeden in Absatz 1 genannten dedizierten Schnittstelle dokumentiert sind und die Routinen, Protokolle und Tools enthalten, die von Zahlungsauslöse- und Kontoinformationsdienstleistern benötigt werden, damit die Interoperabilität ihrer Software und ihrer Anwendungen mit den Systemen des kontoführenden Zahlungsdienstleisters gegeben ist. Kontoführende Zahlungsdienstleister machen die Dokumentation der technischen Spezifikationen für ihre in Absatz 1 genannten dedizierten Schnittstellen auf Verlangen der zugelassenen Zahlungsauslösedienstleister, Kontoinformationsdienstleister oder Zahlungsdienstleister, die ihre entsprechende Zulassung bei den zuständigen Behörden beantragt haben, kostenfrei zugänglich und veröffentlichen eine Zusammenfassung dieser Dokumentation auf ihrer Website.

(4) Kontoführende Zahlungsdienstleister gewährleisten, dass jegliche Änderung der technischen Spezifikation für ihre in Absatz 1 genannte dedizierte Schnittstelle den zugelassenen Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern oder Zahlungsdienstleistern, die kartengebundene Zahlungsinstrumente ausstellen, oder Zahlungsdienstleistern, die ihre entsprechende Zulassung bei den zuständigen Behörden beantragt haben, so bald wie möglich und nicht später als drei Monate vor Implementierung der Änderung im Voraus zur Verfügung gestellt wird, es sei denn, sie werden durch eine Notfallsituation daran gehindert. Kontoführende Zahlungsdienstleister dokumentieren Notfallsituationen, in denen Änderungen ohne

vorherige Ankündigung implementiert wurden, und machen die Dokumentation den zuständigen Behörden auf Verlangen zugänglich.

(5) Kontoführende Zahlungsdienstleister veröffentlichen auf ihrer Website vierteljährliche Statistiken über die Verfügbarkeit und die Leistung ihrer dedizierten Schnittstelle. Bewertet wird die Leistung der dedizierten Schnittstellen anhand der Zahl der erfolgreichen Kontoinformationsabfragen im Verhältnis zur Gesamtanzahl der Kontoinformationsabfragen und anhand der Zahl und des Transaktionsvolumens der erfolgreichen Zahlungsauslöseanfragen im Verhältnis zur Gesamtanzahl und zum Gesamttransaktionsvolumen der Zahlungsauslöseanfragen.

(6) Kontoführende Zahlungsdienstleister stellen eine Testumgebung, einschließlich Unterstützung, für den Verbindungsaufbau zu den dedizierten Schnittstellen und für Funktionstests zur Verfügung, damit die zugelassenen Zahlungsauslösedienstleister und Kontoinformationsdienstleister oder Zahlungsdienstleister, die eine entsprechende Zulassung beantragt haben, ihre Software und ihre Anwendungen testen können, die sie verwenden, um Benutzern einen Zahlungsdienst anzubieten. Über die Testumgebung dürfen keine sensiblen Zahlungsdaten oder andere personenbezogene Daten weitergegeben werden.

(7) Der kontoführende Zahlungsdienstleister sieht für den Fall, dass während der Identifizierung, der Authentifizierung oder des Austauschs von Datenelementen über die dedizierte Schnittstelle ein unvorhergesehenes Ereignis oder ein unvorhergesehener Fehler auftritt, vor, dass Benachrichtigungen an den Zahlungsauslösedienstleister oder den Kontoinformationsdienstleister geschickt werden, in denen der Grund für das unvorhergesehene Ereignis oder den unvorhergesehenen Fehler erläutert wird.

Artikel 36

Anforderungen an dedizierte Datenzugangsschnittstellen

(1) Kontoführende Zahlungsdienstleister gewährleisten, dass die in Artikel 35 Absatz 1 genannte dedizierte Schnittstelle die folgenden Sicherheits- und Leistungsanforderungen erfüllt:

a) während der Authentifizierung des Zahlungsdienstnutzers werden über die dedizierte Schnittstelle Kommunikationssitzungen zwischen dem kontoführenden Zahlungsdienstleister, dem Kontoinformationsdienstleister, dem Zahlungsauslösedienstleister und dem betreffenden Zahlungsdienstnutzer aufgebaut und aufrechterhalten,

b) die dedizierte Schnittstelle gewährleistet die Integrität und Vertraulichkeit der personalisierten Sicherheitsmerkmale und der Authentifizierungscodes, die durch oder über den Zahlungsauslösedienstleister oder den Kontoinformationsdienstleister übertragen werden,

c) die Antwortzeit der dedizierten Schnittstelle bei Zugangsanfragen von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern ist nicht länger als die Antwortzeit der Schnittstelle, die der kontoführende Zahlungsdienstleister seinen Zahlungsdienstnutzern für den direkten Online-Zugriff auf ihr Zahlungskonto zur Verfügung stellt.

(2) Kontoführende Zahlungsdienstleister gewährleisten, dass die in Artikel 35 Absatz 1 genannte dedizierte Schnittstelle es sowohl Kontoinformationsdienstleistern als auch Zahlungsauslösedienstleistern ermöglicht,

a) sich gegenüber dem kontoführenden Zahlungsdienstleister zu identifizieren,

b) den kontoführenden Zahlungsdienstleister anzuweisen, ausgehend von der Erlaubnis, die der Zahlungsdienstnutzer dem Kontoinformationsdienstleister oder den Zahlungsauslösedienstleistern gemäß Artikel 49 Absatz 2 erteilt hat, mit der Authentifizierung zu beginnen,

c) auf nichtdiskriminierende Weise von etwaigen Authentifizierungsausnahmen des kontoführenden Zahlungsdienstleisters Gebrauch zu machen,

d) vor Auslösung der Zahlung – wenn es sich um einen Zahlungsauslösedienstleister handelt – den Kundenidentifikator für das Konto, die zugehörigen Namen des Kontoinhabers und die dem Zahlungsdienstnutzer zur Verfügung stehenden Währungen einzusehen.

(3) Kontoführende Zahlungsdienstleister müssen es Kontoinformationsdienstleistern ermöglichen, über die dedizierte Schnittstelle auf sichere Weise zu kommunizieren, um Informationen über ein oder mehrere bezeichnete Zahlungskonten und damit in Zusammenhang stehende Zahlungsvorgänge anzufordern und zu empfangen.

(4) Kontoführende Zahlungsdienstleister gewährleisten, dass die dedizierte Schnittstelle es Zahlungsauslösedienstleistern zumindest ermöglicht,

a) einen Dauerauftrag oder eine Lastschrift zu erteilen oder zu widerrufen,

b) eine Einzelzahlung auszulösen,

c) eine auf einen Termin in der Zukunft datierte Zahlung auszulösen oder zu widerrufen,

d) Zahlungen an mehrere Begünstigte auszulösen,

e) Zahlungen auszulösen, unabhängig davon, ob der Zahlungsempfänger auf der Liste der Begünstigten des Zahlers steht,

f) auf sichere Weise zu kommunizieren, um vom Zahlungskonto des Zahlers einen Zahlungsauftrag zu erteilen, und alle Informationen über die Auslösung des Zahlungsvorgangs sowie alle dem kontoführenden Zahlungsdienstleister zugänglichen Informationen in Bezug auf die Ausführung des Zahlungsvorgangs zu empfangen,

g) vor Auslösung der Zahlung und unabhängig davon, ob der Name des Kontoinhabers über die direkte Schnittstelle verfügbar ist, den Namen des Kontoinhabers zu überprüfen,

h) eine Zahlung mit einer einzigen starken Kundenauthentifizierung auszulösen, sofern der Zahlungsauslösedienstleister dem kontoführenden Zahlungsdienstleister alle folgenden Informationen zur Verfügung gestellt hat:

i) den Kundenidentifikator des Zahlers,

ii) den eingetragenen Namen und den Handelsnamen sowie den „Kundenidentifikator“ des Zahlungsempfängers,

iii) eine Transaktionsreferenz,

iv) den Zahlungsbetrag und die Währung der Zahlung, aufgrund deren die einzige starke Kundenauthentifizierung ausgelöst wird.

(5) Kontoführende Zahlungsdienstleister gewährleisten, dass die dedizierte Schnittstelle Zahlungsauslösedienstleistern

a) auf Verlangen die sofortige Bestätigung in Form eines einfachen „Ja“ oder „Nein“ übermittelt, ob der für die Ausführung eines Zahlungsvorgangs erforderliche Betrag auf dem Zahlungskonto des Zahlers verfügbar ist,

b) die Bestätigung des kontoführenden Zahlungsdienstleisters übermittelt, dass die Zahlung ausgehend von den ihm vorliegenden Informationen ausgeführt wird, wobei etwaige bereits erteilte Zahlungsaufträge, die die vollständige Ausführung des erteilten Zahlungsauftrags beeinflussen könnten, berücksichtigt werden.

Die unter Buchstabe b genannten Angaben dürfen nicht an den Zahlungsauslösedienstleister weitergegeben werden, können vom kontoführenden Zahlungsdienstleister aber dafür verwendet werden, die Ausführung des Vorgangs zu bestätigen.

Artikel 37

Gleicher Datenzugang bei dedizierter Zugangsschnittstelle und Kundenschnittstelle

(1) Unbeschadet des Artikels 36 gewährleisten kontoführende Zahlungsdienstleister, dass ihre in Artikel 35Absatz 1 genannte dedizierte Schnittstelle jederzeit zumindest denselben Grad an Verfügbarkeit und Leistung, einschließlich technischer und IT-bezogener Unterstützung, aufweist wie die Schnittstellen, die kontoführende Zahlungsdienstleister dem Zahlungsdienstnutzer für den direkten Online-Zugriff auf sein Zahlungskonto zur Verfügung stellen.

(2) Kontoführende Zahlungsdienstleister erteilen Kontoinformationsdienstleistern zumindest dieselben Informationen von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen, die auch dem Zahlungsdienstnutzer erteilt werden, wenn er den Zugang zu Kontoinformationen direkt anfordert, sofern diese Informationen keine sensiblen Zahlungsdaten enthalten.

(3) Kontoführende Zahlungsdienstleister erteilen Zahlungsauslösedienstleistern zumindest dieselben Informationen über die Auslösung und Ausführung des Zahlungsvorgangs, die auch dem Zahlungsdienstnutzer erteilt oder zugänglich gemacht werden, wenn dieser den Zahlungsvorgang direkt auslöst. Diese Informationen werden unmittelbar nach Eingang des Zahlungsauftrags und bis zur endgültigen Zahlung laufend erteilt.

Artikel 38

Notfallmaßnahmen bei Nichtverfügbarkeit einer dedizierten Schnittstelle

(1) Kontoführende Zahlungsdienstleister treffen alle in ihrer Macht stehenden Maßnahmen, um eine Nichtverfügbarkeit der dedizierten Schnittstelle zu verhindern. Nichtverfügbarkeit gilt als gegeben, wenn fünf aufeinanderfolgende Informationsanfragen für die Erbringung von Zahlungsauslöse- oder

Kontoinformationsdiensten nicht innerhalb von 30 Sekunden von der dedizierten Schnittstelle des kontoführenden Zahlungsdienstleisters beantwortet werden.

(2) Bei Nichtverfügbarkeit der dedizierten Schnittstelle teilen die kontoführenden Zahlungsdienstleister den die die dedizierte Schnittstelle nutzenden Zahlungsdienstleistern mit, welche Maßnahmen zur Wiederherstellung der Schnittstelle getroffen werden, und wie lange die Lösung des Problems schätzungsweise in Anspruch nehmen wird. Solange die Schnittstelle nicht verfügbar ist, bieten die kontoführenden Zahlungsdienstleister den Kontoinformations- und Zahlungsauslösedienstleistern unverzüglich eine wirksame alternative Lösung an, wie die Nutzung der Schnittstelle, die der jeweilige kontoführende Zahlungsdienstleister für die Authentifizierung und die Kommunikation mit seinen Nutzern für den Zugriff auf Zahlungskontodaten verwendet.

(3) Ist die dedizierte Schnittstelle nicht verfügbar und hat der kontoführende Zahlungsdienstleister nicht gemäß Absatz 2 eine schnelle und wirksame alternative Lösung angeboten, können Zahlungsauslöse- oder Kontoinformationsdienstleister bei der für sie zuständigen Behörde unter Vorlage aller notwendigen Informationen und Nachweise die Erlaubnis zur Nutzung der Schnittstelle beantragen, die der kontoführende Zahlungsdienstleister für die Authentifizierung und Kommunikation mit seinen Nutzern für den Zugriff auf Zahlungskontodaten verwendet.

(4) Ausgehend von dem in Absatz 3 genannten Antrag kann die zuständige Behörde für begrenzte Zeit, bis die dedizierte Schnittstelle wieder verfügbar ist, allen Zahlungsauslöse- und Kontoinformationsdienstleistern die Erlaubnis erteilen, über eine Schnittstelle, die der kontoführende Zahlungsdienstleister für die Authentifizierung und die Kommunikation mit seinen Nutzern verwendet, auf Zahlungskontodaten zuzugreifen. Die zuständige Behörde teilt dem antragstellenden Kontoinformations- oder Zahlungsauslösedienstleiser ihre Entscheidung mit und macht sie auf ihrer Website öffentlich bekannt. Die zuständige Behörde weist den kontoführenden Zahlungsdienstleister an, die uneingeschränkte Funktionsfähigkeit der dedizierten Schnittstelle bis zum Ablauf der befristeten Erlaubnis wiederherzustellen.

(5) Die zuständige Behörde entscheidet über jeden nach Absatz 3 gestellten Antrag unverzüglich. Solange die zuständige Behörde nicht über den Antrag entschieden hat, darf der antragstellende Zahlungsauslöse- oder Kontoinformationsdienstleister ausnahmsweise über eine Schnittstelle, die der kontoführende Zahlungsdienstleister für die Authentifizierung und die Kommunikation mit seinen Nutzern nutzt, auf Zahlungskontodaten zugreifen. Der antragstellende Zahlungsauslöse- oder Kontoinformationsdienstleister stellt diese Nutzung wieder ein, wenn die dedizierte Schnittstelle wieder verfügbar ist oder – sollte dies früher der Fall sein – die zuständige Behörde entscheidet, dass die Erlaubnis für eine solche Nutzung nicht erteilt wird.

(6) In Fällen, in denen der kontoführende Zahlungsdienstleister dazu verpflichtet wird, Kontoinformations- oder Zahlungsauslösedienstleistern den Zugang zu der Schnittstelle zu gestatten, die er für die Authentifizierung und Kommunikation mit seinen Nutzern verwendet, stellt der kontoführende Zahlungsdienstleister umgehend alle technischen Spezifikationen zur Verfügung, die Kontoinformations- oder Zahlungsauslösedienstleister benötigen, um eine angemessene Verbindung zu der Schnittstelle herzustellen, die der kontoführende Zahlungsdienstleister für die Authentifizierung und Kommunikation mit seinen Nutzern verwendet.

(7) Beim Zugriff auf die Schnittstelle, die der kontoführende Zahlungsdienstleister für die Authentifizierung und Kommunikation mit seinen Nutzern verwendet, müssen die Kontoinformations- oder Zahlungsauslösedienstleister alle in Artikel 45 Absatz 2 festgelegten Anforderungen erfüllen. Insbesondere müssen sich die Kontoinformations- oder Zahlungsauslösedienstleister stets ordnungsgemäß bei dem kontoführenden Zahlungsdienstleister identifizieren.

Artikel 39

Ausnahme von der Pflicht zur Bereitstellung einer dedizierten Datenzugangsschnittstelle

(1) Abweichend von Artikel 35 Absatz 1 kann die zuständige Behörde einen kontoführenden Zahlungsdienstleister auf dessen Antrag hin von der Pflicht, über eine dedizierte Schnittstelle zu verfügen, befreien und ihm gestatten, entweder als Schnittstelle für den sicheren Datenaustausch eine der Schnittstellen anzubieten, die er für die Authentifizierung und Kommunikation mit seinen Zahlungsdienstnutzern verwendet, oder, wenn dies gerechtfertigt ist, überhaupt keine Schnittstelle für den sicheren Datenaustausch anzubieten.

(2) Die EBA arbeitet Entwürfe technischer Regulierungsstandards aus, in denen die Kriterien festgelegt werden, nach denen ein kontoführender Zahlungsdienstleister gemäß Absatz 1 von der Pflicht, über eine dedizierte Schnittstelle zu verfügen, befreit werden und die Erlaubnis erhalten kann, entweder als Schnittstelle für den sicheren Datenaustausch mit Kontoinformations- und Zahlungsauslösedienstleistern die Schnittstelle bereitzustellen, die er seinen Zahlungsdienstnutzern für den Online-Zugriff auf deren Zahlungskonten zur Verfügung stellt, oder gegebenenfalls ganz auf eine Schnittstelle für den sicheren Datenaustausch zu verzichten.

Die EBA übermittelt der Kommission den Entwurf der in Unterabsatz 1 genannten technischen Regulierungsstandards bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = ein Jahr nach Inkrafttreten dieser Verordnung]. Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010 zu erlassen.

ABSCHNITT 3

RECHTE UND PFLICHTEN KONTOFÜHRENDER ZAHLUNGSDIENSTLEISTER

Artikel 40

Pflichten kontoführender Zahlungsdienstleister in Bezug auf Zahlungsauslösedienste

Um das Recht des Zahlers auf Nutzung des Zahlungsauslösedienstes sicherzustellen, unternimmt der kontoführende Zahlungsdienstleister Folgendes:

a) er kommuniziert auf sichere Weise mit Zahlungsauslösedienstleistern,

b) unmittelbar nach Eingang des Zahlungsauftrags eines Zahlungsauslösedienstleisters erteilt er diesem alle Informationen über die Auslösung des Zahlungsvorgangs und alle Informationen, über die er selbst

hinsichtlich der Ausführung des Zahlungsvorgangs verfügt, oder macht diese dem Zahlungsauslösedienstleister zugänglich,

c) er behandelt Zahlungsaufträge, die über die Dienste eines Zahlungsauslösedienstleisters übermittelt werden, insbesondere in Bezug auf zeitliche Abwicklung, Prioritäten oder Entgelte wie Zahlungsaufträge, die direkt vom Zahler oder Zahlungsempfänger übermittelt werden.

Für die Zwecke des Buchstaben b gewährleistet der kontoführende Zahlungsdienstleister für den Fall, dass die Gesamtheit oder ein Teil der dort genannten Informationen bei Eingang des Zahlungsauftrags nicht verfügbar ist, dass dem Zahlungsauslösedienstleister sämtliche Informationen über die Ausführung des Zahlungsauftrags umgehend zur Verfügung gestellt werden, sobald sie dem kontoführenden Zahlungsdienstleister selbst zur Verfügung stehen.

Artikel 41

Pflichten kontoführender Zahlungsdienstleister in Bezug auf Kontoinformationsdienste

(1) Um das Recht des Zahlungsdienstnutzers auf Nutzung des Kontoinformationsdienstes sicherzustellen, unternimmt der kontoführende Zahlungsdienstleister Folgendes:

a) er kommuniziert auf sichere Weise mit dem Kontoinformationsdienstleister,

b) er behandelt Anfragen, die über die Dienste eines Kontoinformationsdienstleisters übermittelt werden, als wären die Daten vom Zahlungsdienstnutzer über die Schnittstelle angefordert worden, die der kontoführende Zahlungsdienstleister seinen Zahlungsdienstnutzern für den direkten Zugriff auf ihr Zahlungskonto zur Verfügung stellt.

(2) Kontoführende Zahlungsdienstleister gestatten Kontoinformationsdienstleistern den Zugriff auf Informationen von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen, die von kontoführenden Zahlungsdienstleistern für Kontoinformationsdienstzwecke gespeichert werden, gleich ob der Zahlungsdienstnutzer diese Informationen aktiv anfragt oder nicht.

Artikel 42

Beschränkung des Zugangs zu Zahlungskonten für Kontoinformations- und Zahlungsauslösedienstleister

(1) Ein kontoführender Zahlungsdienstleister kann einem Kontoinformationsdienstleister oder einem Zahlungsauslösedienstleister aus objektiv gerechtfertigten und hinreichend nachgewiesenen Gründen den Zugang zu einem Zahlungskonto verweigern. Diese Gründe müssen mit einem nicht autorisierten (im Sinne von Artikel 49 Absatz 3) oder betrügerischen Zugriff auf das Zahlungskonto durch diesen Kontoinformationsdienstleister oder diesen Zahlungsauslösedienstleister, worunter auch die nicht autorisierte oder betrügerische Auslösung eines Zahlungsvorgangs fällt, in Zusammenhang stehen. In solchen Fällen informiert der kontoführende Zahlungsdienstleister den Zahlungsdienstnutzer unter Angabe von Gründen darüber, dass der Zugang zum Zahlungskonto verweigert wird. Diese Information ist dem Zahlungsdienstnutzer möglichst vor Verweigerung des Zugangs, spätestens jedoch sofort danach zu erteilen, es sei denn, eine solche Information würde objektiv

gerechtfertigten Sicherheitserwägungen zuwiderlaufen oder gegen sonstiges einschlägiges Recht der Union oder der Mitgliedstaaten verstoßen.

(2) In den in Absatz 1 genannten Fällen setzt der kontoführende Zahlungsdienstleister die zuständige Behörde unverzüglich über den Vorfall im Zusammenhang mit dem Kontoinformationsdienstleister oder dem Zahlungsauslösedienstleister in Kenntnis. Diese Mitteilung umfasst auch die maßgeblichen Einzelheiten des Vorfalls und die Gründe für das Tätigwerden. Die zuständige Behörde bewertet den Fall und ergreift erforderlichenfalls geeignete Maßnahmen.

Artikel 43

Datenzugangsmanagement durch die Zahlungsdienstnutzer

(1) Der kontoführende Zahlungsdienstleister stellt dem Zahlungsdienstnutzer ein in seine Nutzerschnittstelle integriertes Dashboard für Überwachung und Management der Erlaubnisse zur Verfügung, die der Zahlungsdienstnutzer für die Zwecke von Kontoinformationsdiensten oder Zahlungsauslösediensten für mehrere oder wiederkehrende Zahlungen erteilt hat.

(2) Dieses Dashboard muss

a) dem Zahlungsdienstnutzer einen Überblick über jede aktive Erlaubnis geben, die für die Zwecke von Kontoinformations- oder Zahlungsauslösediensten erteilt wurde, und alle folgenden Angaben umfassen:

i) den Namen des Kontoinformationsdienstleisters oder Zahlungsauslösedienstleisters, dem der Zugriff gestattet wurde,

ii) das Kundenkonto, für das der Zugriff gestattet wurde,

iii) den Zweck der Erlaubnis,

iv) die Geltungsdauer der Erlaubnis,

v) die Kategorien der weitergegebenen Daten.

b) es dem Zahlungsdienstnutzer ermöglichen, einem bestimmten Kontoinformations- oder Zahlungsauslösedienstleister das Recht auf Datenzugriff zu entziehen,

c) es dem Zahlungsdienstnutzer ermöglichen, den Datenzugriff nach einem solchen Entzug wiederherzustellen,

d) eine zwei Jahre umfassende Aufstellung der entzogenen oder abgelaufenen Datenzugriffserlaubnisse umfassen.

(3) Der kontoführende Zahlungsdienstleister gewährleistet, dass das Dashboard in seiner Nutzerschnittstelle leicht auffindbar ist und dass die im Dashboard enthaltenen Informationen klar, richtig und für den Zahlungsdienstnutzer leicht verständlich sind.

(4) Der kontoführende Zahlungsdienstleister und der Kontoinformations- oder Zahlungsauslösedienstleister, dem die Erlaubnis erteilt wurde, arbeiten zusammen, um dem Zahlungsdienstnutzer über das Dashboard Informationen in Echtzeit zur Verfügung zu stellen. Für die Zwecke von Absatz 2 Buchstaben a, b, c und e

a) unterrichtet der kontoführende Zahlungsdienstleister den Kontoinformationsdienstleister oder den Zahlungsauslösedienstleister in

Echtzeit über Änderungen, die ein Zahlungsdienstnutzer über das Dashboard an einer Erlaubnis für den betreffenden Dienstleister vorgenommen hat;

b) unterrichtet ein Kontoinformations- oder Zahlungsauslösedienstleister den kontoführenden Zahlungsdienstleister in Echtzeit über eine neue Erlaubnis, die ein Zahlungsdienstnutzer für ein von diesem kontoführenden Zahlungsdienstleister bereitgestelltes Zahlungskonto erteilt hat, und nennt dabei u. a. Folgendes:

i) den Zweck der vom Zahlungsdienstnutzer erteilten Erlaubnis,

ii) die Geltungsdauer der Erlaubnis,

iii) die davon betroffenen Datenkategorien.

Artikel 44

Unzulässige Hindernisse für den Datenzugriff

(1) Kontoführende Zahlungsdienstleister gewährleisten, dass ihre dedizierte Schnittstelle die Bereitstellung von Zahlungsauslöse- und Kontoinformationsdiensten nicht behindert.

Ein unzulässiges Hindernis liegt u. a. vor, wenn

a) Zahlungsauslöse- oder Kontoinformationsdienstleister daran gehindert werden, die von kontoführenden Zahlungsdienstleistern für ihre Zahlungsdienstnutzer ausgestellten Sicherheitsmerkmale zu nutzen,

b) Zahlungsdienstnutzer für die Nutzung von Kontoinformations- oder Zahlungsauslösediensten ihren Kundenidentifikator manuell in der Domäne des kontoführenden Zahlungsdienstleisters eingeben müssen,

c) die Erlaubnis, die der Zahlungsdienstnutzer einem Zahlungsauslöse- oder Kontoinformationsdienstleister erteilt hat, zusätzlich überprüft werden muss,

d) Zahlungsauslöse- und Kontoinformationsdienstleister sich zusätzlich registrieren müssen, um auf das Zahlungskonto des Zahlungsdienstnutzers oder auf die dedizierte Schnittstelle zugreifen zu können,

e) Zahlungsauslöse- und Kontoinformationsdienstleister ihre Kontaktdaten vorab beim kontoführenden Zahlungsdienstleister registrieren müssen, es sei denn, dies ist unerlässlich, um den Informationsaustausch zwischen kontoführenden Zahlungsdienstleistern und Zahlungsauslöse- und Kontoinformationsdienstleistern insbesondere bezüglich der Aktualisierung des in Artikel 43 genannten Dashboards zu erleichtern,

f) ein Zahlungsdienstnutzer Zahlungen über einen Zahlungsauslösedienstleister nur auslösen kann, wenn der Zahlungsempfänger auf der Liste der Begünstigten des Zahlers steht,

g) die Auslösung eingehender oder ausgehender Zahlungen auf inländische Kundenidentifikatoren beschränkt ist,

h) im Vergleich zur starken Kundenauthentifizierung bei einem direkten Zugriff des Zahlungsdienstnutzers auf sein Zahlungskonto oder bei der Auslösung einer Zahlung direkt beim kontoführenden Zahlungsdienstleister eine häufigere starke Kundenauthentifizierung verlangt wird,

i) die bereitgestellte dedizierte Schnittstelle nicht alle Authentifizierungsverfahren unterstützt, die der kontoführende Zahlungsdienstleister seinem Zahlungsdienstnutzer zur Verfügung stellt,

j) für Kontoinformationen oder Zahlungsauslösungen ein Verlauf vorgeschrieben wird, der mit einer Umleitung oder Entkopplung einhergeht und bei dem die Authentifizierung des Zahlungsdienstnutzers beim kontoführenden Zahlungsdienstleister im Vergleich zum entsprechenden Authentifizierungsverfahren, das Zahlungsdienstnutzern beim direkten Zugriff auf ihre Zahlungskonten oder bei der Auslösung einer Zahlung direkt beim kontoführenden Zahlungsdienstleister angeboten wird, zusätzliche Schritte oder Maßnahmen erfordert,

k) der Nutzer bei der Authentifizierung automatisch zur Adresse der Website des kontoführenden Zahlungsdienstleisters weitergeleitet wird, wenn dies die einzige vom kontoführenden Zahlungsdienstleister unterstützte Authentifizierungsmethode für den Zahlungsdienstnutzer ist,

l) bei einem Verlauf, der ausschließlich in der Auslösung einer Zahlung besteht, zwei starke Kundenauthentifizierungen verlangt werden, bei denen der Zahlungsauslösedienstleister dem kontoführenden Zahlungsdienstleister alle für die Auslösung der Zahlung erforderlichen Informationen übermittelt, d. h. einer starken Kundenauthentifizierung für die Bestätigung durch „ja“ oder „nein“ und einer zweiten starken Kundenauthentifizierung für die Auslösung der Zahlung.

(2) Bei Zahlungsauslöse- und Kontoinformationsdiensten stellen der Name des Kontoinhabers und dessen Kontonummer keine sensiblen Zahlungsdaten dar.

ABSCHNITT 4

RECHTE UND PFLICHTEN VON KONTOINFORMATIONSDIENSTLEISTERN UND ZAHLUNGSAUSLÖSEDIENSTLEISTERN

Artikel 45

Nutzung der Kundenschnittstelle durch Kontoinformations- und Zahlungsauslösedienstleister

(1) Kontoinformations- und Zahlungsauslösedienstleister dürfen außer in den in Artikel 38 Absätze 4 und 5 und Artikel 39 genannten Fällen nur über die in Artikel 35 genannte dedizierte Schnittstelle auf Zahlungskontodaten zugreifen.

(2) Greift ein Kontoinformationsdienstleister oder ein Zahlungsauslösedienstleister gemäß Artikel 38 Absätze 4 und 5 auf Zahlungskontodaten über eine Schnittstelle zu, die der kontoführende Zahlungsdienstleister seinen Zahlungsdienstnutzern für einen direkten Zugriff auf ihr Zahlungskonto zur Verfügung stellt, oder handelt es dabei gemäß Artikel 39 um die einzige verfügbare Schnittstelle, muss der Kontoinformationsdienstleister oder der Zahlungsauslösedienstleister

a) sich stets gegenüber dem kontoführenden Zahlungsdienstleister identifizieren,

b) sich stets auf die Authentifizierungsverfahren verlassen, die der kontoführende Zahlungsdienstleister dem Zahlungsdienstnutzer zur Verfügung stellt,

c) stets die notwendigen Maßnahmen treffen, um sicherzustellen, dass er Daten nicht für andere Zwecke als die Bereitstellung des vom Zahlungsdienstnutzer angeforderten Dienstes verarbeitet (worunter auch Datenzugriff und Datenspeicherung fallen),

d) stets die Daten protokollieren, die über die vom kontoführenden Zahlungsdienstleister für seine Zahlungsdienstnutzer betriebene Schnittstelle abgerufen werden, und der zuständigen Behörde auf Verlangen die Protokolldateien unverzüglich zur Verfügung stellen. Die Protokolle werden drei Jahre nach ihrer Erstellung gelöscht. Protokolle können auch länger aufbewahrt werden, wenn sie für bereits laufende Überwachungsverfahren benötigt werden.

Für die Zwecke des Buchstaben d werden Protokolle drei Jahre nach ihrer Erstellung gelöscht. Protokolle können auch länger aufbewahrt werden, wenn sie für bereits laufende Überwachungsverfahren benötigt werden.

Artikel 46

Spezielle Pflichten von Zahlungsauslösedienstleistern

(1) Zahlungsauslösedienstleister

a) müssen kontoführenden Zahlungsdienstleistern dieselben Informationen erteilen, wie sie vom Zahlungsdienstnutzer beim direkten Auslösen des Zahlungsvorgangs angefordert werden,

b) dürfen ihre Dienste gemäß Artikel 49 nur mit Erlaubnis des Zahlungsdienstnutzers erbringen,

c) dürfen in Verbindung mit der Erbringung des Zahlungsauslösedienstes zu keiner Zeit Gelder des Zahlers halten,

d) müssen gewährleisten, dass die personalisierten Sicherheitsmerkmale des Zahlungsdienstenutzers außer für den Zahler und den Emittenten der personalisierten Sicherheitsmerkmale für keine andere Partei zugänglich sind und über sichere und effiziente Kanäle übermittelt werden,

e) müssen sicherstellen, dass alle sonstigen Informationen über den Zahlungsdienstenutzer, die sie bei der Erbringung von Zahlungsauslösediensten erhalten, nur an den Zahlungsempfänger und nur mit Erlaubnis des Zahlungsdienstenutzers weitergegeben werden,

f) müssen sich bei jeder Zahlungsauslösung gegenüber dem kontoführenden Zahlungsdienstleister identifizieren und mit dem kontoführenden Zahlungsdienstleister, dem Zahler und dem Zahlungsempfänger auf sichere Weise kommunizieren.

(2) Zahlungsauslösedienstleister dürfen

a) sensible Zahlungsdaten des Zahlungsdienstnutzers nicht speichern,

b) vom Zahlungsdienstnutzer keine anderen als die für die Erbringung des Zahlungsauslösedienstes erforderlichen Daten verlangen,

c) personenbezogene oder nicht personenbezogene Daten nicht für andere Zwecke als die vom Zahlungsdienstenutzer erlaubte Erbringung des Zahlungsauslösedienstes verarbeiten (worunter auch die Datennutzung, der Datenzugriff oder die Datenspeicherung fällt),

d) den Betrag, den Zahlungsempfänger oder ein sonstiges Merkmal des Zahlungsvorgangs nicht ändern.

Artikel 47

Spezielle Pflichten von Kontoinformationsdienstleistern und sonstige Bestimmungen für Kontoinformationsdienstleister

(1) Der Kontoinformationsdienstleister

a) darf seine Dienste gemäß Artikel 49 nur mit Erlaubnis des Zahlungsdienstnutzers erbringen,

b) muss gewährleisten, dass die personalisierten Sicherheitsmerkmale des Zahlungsdienstnutzers außer für den Nutzer und den Emittenten der personalisierten Sicherheitsmerkmale für keine andere Partei zugänglich sind, und dass für den Fall, dass diese Sicherheitsmerkmale vom Kontoinformationsdienstleister übermittelt werden, diese Übermittlung über sichere und effiziente Kanäle erfolgt,

c) muss sich für jede Kommunikationssitzung gegenüber dem kontoführenden Zahlungsdienstleister des Zahlungsdienstnutzers identifizieren und mit dem kontoführenden Zahlungsdienstleister und dem Zahlungsdienstnutzer auf sichere Weise kommunizieren,

d) darf nur auf Informationen von bezeichneten Zahlungskonten und zugehörigen Zahlungsvorgängen zugreifen,

e) muss über geeignete und wirksame Mechanismen verfügen, damit der Zugriff auf andere Informationen als die von bezeichneten Zahlungskonten und zugehörigen Zahlungsvorgängen gemäß der Erlaubnis des Zahlungsdienstnutzers verhindert wird.

(2) Der Kontoinformationsdienstleister darf

a) keine sensiblen Zahlungsdaten anfordern, die mit den Zahlungskonten in Verbindung stehen,

b) gemäß der Verordnung (EU) 2016/679 Daten nicht für andere Zwecke als für den vom Zahlungsdienstnutzer erlaubten Kontoinformationsdienst verwenden, abrufen oder speichern.

(3) Die Artikel 4 bis 8, die Artikel 10 bis 12, die Artikel 14 bis 19, die Artikel 21 bis 29, die Artikel 50 und 51, die Artikel 53 bis 79 und die Artikel 83 und 84 gelten nicht für Kontoinformationsdienstleister.

ABSCHNITT 5

UMSETZUNG

Artikel 48

Rolle der zuständigen Behörden

(1) Die zuständigen Behörden gewährleisten, dass kontoführende Zahlungsdienstleister ihren Pflichten bezüglich der in Artikel 35 Absatz 1 genannten Schnittstelle jederzeit nachkommen und dass jedes in Artikel 44 aufgeführte festgestellte unzulässige Hindernis vom betreffenden kontoführenden Zahlungsdienstleister unverzüglich beseitigt wird. Wird – u. a. durch Informationen von Zahlungsauslöse- und Kontoinformationsdienstleistern – festgestellt, dass dedizierte Schnittstellen nicht den Anforderungen dieser Verordnung genügen oder Hindernisse bestehen, ergreifen die zuständigen Behörden unverzüglich die notwendigen Durchsetzungsmaßnahmen und verhängen angemessene Sanktionen oder gewähren gegebenenfalls gemäß Artikel 38 Absatz 4 die Zugriffsrechte.

(2) Die zuständigen Behörden ergreifen unverzüglich jede Durchsetzungsmaßnahme, die erforderlich ist, um die Zugangsrechte von Zahlungsauslöse- und Kontoinformationsdienstleistern zu erhalten. Solche Durchsetzungsmaßnahmen können angemessene Sanktionen umfassen.

(3) Die zuständigen Behörden gewährleisten, dass Zahlungsauslöse- und Kontoinformationsdienstleister ihren Pflichten bezüglich der Nutzung von Datenzugangsschnittstellen jederzeit nachkommen.

(4) Die zuständigen Behörden müssen über die notwendigen Ressourcen, insbesondere das entsprechende Personal verfügen, um ihre Aufgaben jederzeit erfüllen zu können.

(5) Wenn es um die Verarbeitung personenbezogener Daten geht, arbeiten die zuständigen Behörden gemäß der Verordnung (EU) 2016/679 mit den Aufsichtsbehörden zusammen.

(6) Die zuständigen Behörden halten auf eigene Initiative regelmäßig gemeinsame Sitzungen mit kontoführenden Zahlungsdienstleistern, Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern ab und bemühen sich nach Kräften sicherzustellen, dass mögliche Probleme zwischen kontoführenden Zahlungsdienstleistern, Zahlungsauslöse- und Kontoinformationsdienstleistern, die sich aus der Nutzung von Schnittstellen für den Datenaustausch und dem Zugang zu solchen Schnittstellen ergeben, rasch und dauerhaft gelöst werden.

(7) Kontoführende Zahlungsdienstleister stellen den zuständigen Behörden Daten über den Zugriff von Kontoinformations- und Zahlungsauslösedienstleistern auf die von ihnen geführten Zahlungskonten zur Verfügung. Die zuständigen Behörden dürfen von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern gegebenenfalls auch die Vorlage aller relevanten Daten über ihre Tätigkeiten verlangen. Die EBA koordiniert diese Überwachungstätigkeit der zuständigen Behörden gemäß ihren Befugnissen nach Artikel 29 Buchstabe b, Artikel 31 und

Artikel 35 Absatz 2 der Verordnung (EU) Nr. 1093/2010, um doppelte Datenmeldungen zu vermeiden. Die EBA erstattet der Kommission alle zwei Jahre Bericht über die Größe und Funktionsweise der Märkte für Kontoinformations- und Zahlungsauslösedienste in der Union. Diese regelmäßigen Berichte können gegebenenfalls Empfehlungen enthalten.

(8) Die EBA arbeitet Entwürfe technischer Regulierungsstandards aus, in denen festgelegt wird, welche Daten den zuständigen Behörden nach Absatz 7 zu übermitteln sind, und nach welcher Methodik und in welchen Abständen die Daten zu übermitteln sind.

Die EBA legt der Kommission diese Entwürfe technischer Regulierungsstandards bis zum [Amt für Veröffentlichungen: Bitte Datum einfügen = 18 Monate nach Inkrafttreten dieser Verordnung] vor.

Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010 zu erlassen.

KAPITEL 4

Autorisierung von Zahlungsvorgängen

Artikel 49

Autorisierung

(1) Ein Zahlungsvorgang oder eine Serie von Zahlungsvorgängen wird nur dann autorisiert, wenn der Zahler seine Erlaubnis zur Ausführung des Zahlungsvorgangs erteilt hat. Ein Zahlungsvorgang kann vom Zahler autorisiert werden, bevor oder – falls zwischen dem Zahler und dem kontoführenden Zahlungsdienstleister so vereinbart – nachdem der Zahlungsvorgang ausgeführt wurde.

(2) Der Zugriff von Zahlungsdienstleistern auf ein Zahlungskonto für die Zwecke von Kontoinformationsdiensten oder Zahlungsauslösediensten wird nur dann autorisiert, wenn der Zahlungsdienstnutzer dem Kontoinformationsdienstleister bzw. dem Zahlungsauslösedienstleister die Erlaubnis erteilt hat, auf das Zahlungskonto und auf die einschlägigen Daten auf diesem Konto zuzugreifen.

(3) Liegt keine Erlaubnis vor, gelten ein Zahlungsvorgang oder der Zugriff eines Kontoinformationsdienstleisters oder eines Zahlungsauslösedienstleisters auf ein Zahlungskonto als nicht autorisiert.

(4) Die Erlaubnis, die der Zahlungsdienstnutzer dem Kontoinformationsdienstleister oder dem Zahlungsauslösedienstleister erteilt hat, wird vom kontoführenden Zahlungsdienstleister nicht überprüft.

(5) Die in den Absätzen 1 und 2 genannte Erlaubnis wird in der zwischen dem Zahler und dem betroffenen Zahlungsdienstleister vereinbarten Form erteilt. Die Erlaubnis zur Ausführung eines Zahlungsvorgangs kann auch über den Zahlungsempfänger oder den Zahlungsauslösedienstleister erteilt werden.

(6) Das Verfahren für die Erteilung der Erlaubnis wird zwischen dem Zahler und dem betroffenen Zahlungsdienstleister vereinbart.

(7) Der Zahlungsdienstnutzer kann die Erlaubnis, einen Zahlungsvorgang auszuführen oder für die Zwecke von Zahlungsauslösediensten oder Kontoinformationsdiensten auf ein Zahlungskonto zuzugreifen, jederzeit widerrufen. Der Zahlungsdienstnutzer kann auch die Erlaubnis, eine Serie von Zahlungsvorgängen auszuführen, widerrufen, woraufhin jeder darauffolgende Zahlungsvorgang als nicht autorisiert gilt.

Artikel 50

Unstimmigkeiten zwischen Namen und Kundenidentifikator des Zahlungsempfängers bei Überweisungen

(1) Bei Überweisungen überprüft der Zahlungsdienstleister des Zahlungsempfängers auf Verlangen des Zahlungsdienstleisters des Zahlers kostenlos, ob der Kundenidentifikator und der Name des Zahlungsempfängers, wie sie vom Zahler angegeben wurden, übereinstimmen, und teilt dem Zahlungsdienstleister des Zahlers das Ergebnis dieser Überprüfung mit. Stimmen Kundenidentifikator und Name des Zahlungsempfängers nicht überein, benachrichtigt der Zahlungsdienstleister des Zahlers den Zahler über jede festgestellte Unstimmigkeit dieser Art und unterrichtet den Zahler über den Grad dieser Unstimmigkeit.

(2) Die Zahlungsdienstleister erbringen die in Absatz 1 genannten Leistung sofort, nachdem der Zahler seinem Zahlungsdienstleister den Kundenidentifikator und den Namen des Zahlungsempfängers übermittelt und bevor der Zahler die Möglichkeit erhält, die Überweisung zu autorisieren.

(3) Die Zahlungsdienstleister stellen sicher, dass die Feststellung einer in Absatz 1 genannten Unstimmigkeit und die entsprechende Benachrichtigung des Zahlers diesen nicht daran hindern, die Überweisung zu autorisieren. Autorisiert der Zahler die Überweisung, nachdem er über eine festgestellte Unstimmigkeit benachrichtigt wurde, und wird der Vorgang gemäß dem vom Zahler angegebenen Kundenidentifikator ausgeführt, so gilt der Vorgang als korrekt ausgeführt.

(4) Die Zahlungsdienstleister stellen sicher, dass die Zahlungsdienstnutzer das Recht haben, auf das in Absatz 1 genannte Leistungsangebot zu verzichten, und teilen den Nutzern ihrer Zahlungsdienste mit, wie sie diesen Verzicht zum Ausdruck bringen können. Die Zahlungsdienstleister stellen sicher, dass Zahlungsdienstnutzer, die anfänglich auf die in Absatz 1 genannte Leistung verzichtet haben, das Recht haben, diese Leistung auf Wunsch wieder in Anspruch zu nehmen.

(5) Die Zahlungsdienstleister informieren die Nutzer ihrer Zahlungsdienste darüber, dass die Autorisierung eines Vorgangs trotz festgestellter Unstimmigkeit und trotz entsprechender Benachrichtigung oder der Verzicht auf die in Absatz 1 genannte Leistung dazu führen können, dass das Geld auf ein Zahlungskonto überwiesen wird, dessen Inhaber nicht der vom Zahler angegebene Zahlungsempfänger ist. Die Zahlungsdienstleister erteilen diese Information zeitgleich mit der Benachrichtigung über Unstimmigkeiten oder zu dem Zeitpunkt, zu dem der Zahlungsdienstnutzer seinen Verzicht auf die in Absatz 1 genannte Leistung erklärt.

(6) Die in Absatz 1 genannte Leistung wird bei Zahlungsaufträgen, die über elektronische Wege der Zahlungsauslösung erteilt werden, und bei nicht-elektronischen Zahlungsaufträgen erbracht, die eine Echtzeit-Interaktion zwischen dem Zahler und seinem Zahlungsdienstleister beinhalten.

(7) Der in Absatz 1 genannte Abgleichservice ist nicht vorgeschrieben, wenn der Zahler den Kundenidentifikator und den Namen des Zahlungsempfängers nicht selbst eingegeben hat.

(8) Dieser Artikel gilt nicht für Sofortüberweisungen in Euro, die unter die Verordnung XXX (IPR) fallen.

Artikel 51

Begrenzung und Sperrung der Nutzung des Zahlungsinstruments

(1) Wird eine Erlaubnis mittels eines bestimmten Zahlungsinstruments erteilt, können der Zahler und sein Zahlungsdienstleister Ausgabenobergrenzen für Zahlungsvorgänge vereinbaren, die mit diesem Zahlungsinstrument ausgeführt werden. Zahlungsdienstleister dürfen die mit ihren Zahlungsdienstnutzern vereinbarten Ausgabenobergrenzen nicht einseitig anheben.

(2) Bei einer entsprechenden Vereinbarung im Rahmenvertrag kann der Zahlungsdienstleister sich das Recht vorbehalten, ein Zahlungsinstrument zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit des Zahlungsinstruments dies rechtfertigen, wenn der Verdacht einer nicht autorisierten oder betrügerischen Nutzung des Zahlungsinstruments besteht oder wenn im Falle eines Zahlungsinstruments mit einer Kreditlinie ein erheblich erhöhtes Risiko besteht, dass der Zahler seiner Zahlungspflicht nicht nachkommen kann.

(3) In diesen Fällen unterrichtet der Zahlungsdienstleister den Zahler möglichst vor, spätestens jedoch sofort nach der Sperrung des Zahlungsinstruments in einer vereinbarten Form über die Sperrung und die Gründe hierfür, es sei denn, diese Unterrichtung würde objektiv berechtigten Sicherheitserwägungen zuwiderlaufen oder gegen sonstiges einschlägiges Recht der Union oder der Mitgliedstaaten verstoßen.

(4) Der Zahlungsdienstleister hebt die Sperrung des Zahlungsinstruments auf oder ersetzt es durch ein neues Zahlungsinstrument, wenn die Gründe für die Sperrung nicht mehr gegeben sind.

Artikel 52

Pflichten des Zahlungsdienstnutzers in Bezug auf Zahlungsinstrumente und personalisierte Sicherheitsmerkmale

Der zur Nutzung eines Zahlungsinstruments berechtigte Zahlungsdienstnutzer

a) hält bei der Nutzung des Zahlungsinstruments die Bedingungen für dessen Ausgabe und Nutzung ein, die objektiv, nichtdiskriminierend und verhältnismäßig sein müssen;

b) zeigt dem Zahlungsdienstleister oder der vom Zahlungsdienstleister benannten Stelle den Verlust, den Diebstahl, die missbräuchliche Verwendung oder die nicht autorisierte Nutzung des Zahlungsinstruments unverzüglich nach deren Feststellung an.

Für die Zwecke des Buchstabens a trifft der Zahlungsdienstnutzer unmittelbar nach Erhalt eines Zahlungsinstruments alle zumutbaren Vorkehrungen, um seine personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen.

Artikel 53

Pflichten des Zahlungsdienstleisters in Bezug auf Zahlungsinstrumente

(1) Der Zahlungsdienstleister, der ein Zahlungsinstrument ausgibt,

a) muss unbeschadet der Pflichten des Zahlungsdienstnutzers nach Artikel 52 sicherstellen, dass die personalisierten Sicherheitsmerkmale keiner anderen Person als dem zur Nutzung des Zahlungsinstruments berechtigten Zahlungsdienstnutzer zugänglich sind;

b) darf dem Zahlungsdienstnutzer nicht unaufgefordert ein Zahlungsinstrument zusenden, es sei denn, ein bereits an den Zahlungsdienstnutzer ausgegebenes Zahlungsinstrument muss ersetzt werden;

c) muss sicherstellen, dass der Zahlungsdienstnutzer durch geeignete Mittel jederzeit die Möglichkeit hat, eine Anzeige gemäß Artikel 52 Buchstabe b vorzunehmen oder die Aufhebung der Sperrung des Zahlungsinstruments gemäß Artikel 51 Absatz 4 zu verlangen;

d) muss dem Zahlungsdienstnutzer die Möglichkeit bieten, eine Anzeige gemäß Artikel 52 Buchstabe b kostenlos vorzunehmen, und darf nur etwaige direkt mit dem Zahlungsinstrument verbundene Ersatzkosten in Rechnung stellen;

e) muss jedwede Nutzung des Zahlungsinstruments verhindern, sobald eine Anzeige nach Artikel 52 Buchstabe b erfolgt ist.

f) Für die Zwecke von Buchstabe c stellt der Zahlungsdienstleister dem Zahlungsdienstnutzer auf Verlangen Beweismittel zur Verfügung, mit denen dieser bis zu 18 Monate nach der Anzeige den Beweis erbringen kann, dass der Zahlungsdienstnutzer seiner Anzeigepflicht nachgekommen ist.

(2) Der Zahlungsdienstleister trägt das Risiko der Versendung eines Zahlungsinstruments oder personalisierter Sicherheitsmerkmale des Zahlungsinstruments an den Zahlungsdienstnutzer.

Artikel 54

Anzeige und Korrektur nicht autorisierter, autorisierter oder fehlerhaft ausgeführter Zahlungsvorgänge

(1) Der Zahlungsdienstleister korrigiert einen nicht autorisierten, einen fehlerhaft ausgeführten oder einen autorisierten Zahlungsvorgang nur dann, wenn der Zahlungsdienstnutzer dem Zahlungsdienstleister gemäß den Artikeln 57 und 59 den betreffenden Zahlungsvorgang, der einen Anspruch, einschließlich eines Anspruchs nach Artikel 75, begründet, unverzüglich nach dessen Feststellung, spätestens jedoch 13 Monate nach dem Tag der Belastung, anzeigt.

Die in Unterabsatz 1 festgelegten Anzeigefristen gelten nicht, wenn der Zahlungsdienstleister die Informationen über den Zahlungsvorgang nach Maßgabe von Titel II nicht erteilt oder nicht zugänglich gemacht hat.

(2) Ist ein Zahlungsauslösedienstleister beteiligt, erwirkt der Zahlungsdienstnutzer die Korrektur gemäß Absatz 1 unbeschadet des Artikels 56 Absatz 4 und des Artikels 75 Absatz 1 durch den kontoführenden Zahlungsdienstleister.

Artikel 55

Nachweis der Autorisierung und der Ausführung von Zahlungsvorgängen

(1) Bestreitet ein Zahlungsdienstnutzer, einen ausgeführten Zahlungsvorgang autorisiert zu haben, oder macht ein Zahlungsdienstnutzer geltend, dass der Zahlungsvorgang nicht korrekt ausgeführt wurde, so trägt der Zahlungsdienstleister die Beweislast, dass der Zahlungsvorgang autorisiert war, korrekt aufgezeichnet und verbucht wurde und nicht durch eine technische Störung oder einen anderen Mangel des von dem Zahlungsdienstleister erbrachten Dienstes beeinträchtigt wurde.

Wird der Zahlungsvorgang über einen Zahlungsauslösedienstleister ausgelöst, so trägt der Zahlungsauslösedienstleister die Beweislast, dass der Zahlungsvorgang — innerhalb seines Zuständigkeitsbereichs — autorisiert, korrekt aufgezeichnet und nicht durch eine technische Störung 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 allein nicht als Beweis dafür aus, dass der Zahler den Zahlungsvorgang autorisiert hat oder dass der Zahler in betrügerischer Absicht gehandelt oder eine oder mehrere seiner Pflichten nach Artikel 52 vorsätzlich oder grob fahrlässig verletzt hat. Der Zahlungsdienstleister, gegebenenfalls einschließlich des Zahlungsauslösedienstleisters, muss unterstützende Beweismittel vorlegen, um Betrug oder grobe Fahrlässigkeit des Zahlungsdienstnutzers zu beweisen.

Artikel 56

Haftung des Zahlungsdienstleisters für nicht autorisierte Zahlungsvorgänge

(1) Unbeschadet des Artikels 54 erstattet der Zahlungsdienstleister des Zahlers im Falle eines nicht autorisierten Zahlungsvorgangs dem Zahler den Betrag des nicht autorisierten Zahlungsvorgangs sofort, in jeden Fall jedoch spätestens bis zum Ende des folgenden Geschäftstags, nachdem er den nicht autorisierten Zahlungsvorgang festgestellt hat oder dieser ihm angezeigt wurde, es sei denn, der Zahlungsdienstleister des Zahlers hat berechtigte Gründe für den Verdacht, dass der Zahler Betrug begangen hat, und teilt der zuständigen nationalen Behörde diese Gründe schriftlich mit.

(2) Hatte der Zahlungsdienstleister des Zahlers berechtigte Gründe für den Verdacht, dass der Zahler Betrug begangen hat, so unternimmt der Zahlungsdienstleister des Zahlers innerhalb von zehn Geschäftstagen nach Feststellung oder Erhalt der Anzeige dieses Vorgangs einen der folgenden beiden Schritte:

a) Er erstattet dem Zahler den Betrag des nicht autorisierten Zahlungsvorgangs, wenn der Zahlungsdienstleister des Zahlers nach weiteren Untersuchungen zu dem Schluss gelangt ist, dass der Zahler keinen Betrug begangen hat.

b) Er liefert eine Begründung, warum er die Erstattung ablehnt, und nennt die Stellen, an die sich der Zahler gemäß den Artikeln 90, 91, 93, 94 und 95 wenden kann, falls der Zahler die angegebenen Gründe nicht akzeptiert.

(3) Der Zahlungsdienstleister des Zahlers bringt gegebenenfalls das belastete Zahlungskonto wieder auf den Stand, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte. Der Zahlungsdienstleister des Zahlers stellt außerdem sicher, dass die Wertstellung der Gutschrift auf dem Zahlungskonto des Zahlers nicht später erfolgt als zu dem Datum, an dem der Betrag belastet wurde.

(4) Wird der Zahlungsvorgang über einen Zahlungsauslösedienstleister ausgelöst, so erstattet der kontoführende Zahlungsdienstleister den Betrag des nicht autorisierten Zahlungsvorgangs sofort, in jedem Fall jedoch spätestens bis zum Ende des folgenden Geschäftstags und bringt das belastete Zahlungskonto gegebenenfalls wieder auf den Stand, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte.

(5) Ist der Zahlungsauslösedienstleister für den nicht autorisierten Zahlungsvorgang haftbar, so entschädigt der Zahlungsauslösedienstleister den kontoführenden Zahlungsdienstleister auf dessen Verlangen sofort für die infolge der Erstattung an den Zahler erlittenen Verluste oder gezahlten Beträge, einschließlich des Betrags des nicht autorisierten Zahlungsvorgangs. Im Einklang mit Artikel 55 Absatz 1 trägt der Zahlungsauslösedienstleister die Beweislast, dass der Zahlungsvorgang innerhalb seines Zuständigkeitsbereichs autorisiert, korrekt aufgezeichnet und nicht durch eine technische Störung oder einen anderen Mangel im Zusammenhang mit dem von ihm verantworteten Zahlungsdienst beeinträchtigt wurde.

(6) Gegebenenfalls kann der Zahler nach dem auf den Vertrag zwischen dem Zahler und dem Zahlungsdienstleister oder auf den Vertrag zwischen dem Zahler und dem Zahlungsauslösedienstleister anwendbaren Recht Anspruch auf eine darüber hinausgehende finanzielle Entschädigung durch den Zahlungsdienstleister haben.

Artikel 57

Haftung des Zahlungsdienstleisters für fehlerhafte Anwendung des Abgleichservice

(1) Dem Zahler werden keine durch autorisierte Überweisungen entstandenen finanziellen Verluste angelastet, wenn es der Zahlungsdienstleister des Zahlers unter Verstoß gegen Artikel 50 Absatz 1 versäumt hat, den Zahler bei einer festgestellten Unstimmigkeit zwischen dem vom Zahler angegebenen Kundenidentifikator und dem vom Zahler angegebenen Namen des Begünstigten zu benachrichtigen.

(2) Innerhalb von zehn Geschäftstagen nach Feststellung oder Erhalt der Anzeige eines unter den in Absatz 1 genannten Umständen ausgeführten Überweisungsvorgangs unternimmt der Zahlungsdienstleister einen der folgenden beiden Schritte:

a) Er erstattet dem Zahler die autorisierte Überweisung in voller Höhe.

b) Er liefert eine Begründung, warum er die Erstattung ablehnt, und nennt die Stellen, an die sich der Zahler gemäß den Artikeln 90, 91, 93, 94 und 95 wenden kann, falls der Zahler die angegebenen Gründe nicht akzeptiert.

(3) Ist der Zahlungsdienstleister des Zahlungsempfängers für den vom Zahlungsdienstleister des Zahlers begangenen Verstoß gegen Artikel 50 Absatz 1

verantwortlich, so erstattet der Zahlungsdienstleister des Zahlungsempfängers den finanziellen Schaden, der dem Zahlungsdienstleister des Zahlers entstanden ist.

(4) Der Zahlungsdienstleister des Zahlers oder in dem in Absatz 3 genannten Fall des Zahlungsempfängers trägt die Beweislast, dass nicht gegen Artikel 50 Absatz 1 verstoßen wurde.

(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn der Zahler betrügerisch gehandelt hat oder wenn der Zahler gemäß Artikel 50 Absatz 4 auf die Inanspruchnahme des Abgleichservice verzichtet hat.

(6) Dieser Artikel gilt nicht für Sofortüberweisungen in Euro, die unter die Verordnung XXX (IPR) fallen.

Artikel 58

Haftung von technischen Dienstleistern und Betreibern von Zahlverfahren für fehlende Unterstützung der Durchführung der starken Kundenauthentifizierung

Technische Dienstleister und Betreiber von Zahlverfahren, die entweder für den Zahlungsempfänger oder für den Zahlungsdienstleister des Zahlungsempfängers oder den Zahlungsdienstleister des Zahlers Dienstleistungen erbringen, haften für jeden finanziellen Schaden, der dem Zahlungsempfänger, dem Zahlungsdienstleister des Zahlungsempfängers oder dem Zahlungsdienstleister des Zahlers dadurch entsteht, dass sie im Rahmen ihrer Vertragsbeziehung nicht die Leistungen erbringen, die erforderlich sind, um die Durchführung einer starken Kundenauthentifizierung zu ermöglichen.

Artikel 59

Haftung des Zahlungsdienstleisters für Identitätsbetrug

(1) Wurde ein Zahlungsdienstnutzer, bei dem es sich um einen Verbraucher handelt, von einem Dritten manipuliert, der sich unter Verwendung des Namens oder der E-Mail-Adresse oder der Telefonnummer des Zahlungsdienstleisters des Verbrauchers als Mitarbeiter dieses Zahlungsdienstleisters ausgab, und hatte diese Manipulation anschließend autorisierte betrügerische Zahlungsvorgänge zur Folge, so erstattet der Zahlungsdienstleister dem Verbraucher den autorisierten betrügerischen Zahlungsvorgang unter der Bedingung in voller Höhe, dass der Verbraucher den Betrug unverzüglich polizeilich gemeldet und seinem Zahlungsdienstleister angezeigt hat.

(2) Innerhalb von zehn Geschäftstagen nach Feststellung oder Erhalt der Anzeige des autorisierten betrügerischen Zahlungsvorgangs unternimmt der Zahlungsdienstleister einen der folgenden beiden Schritte:

a) Er erstattet dem Verbraucher den Betrag des autorisierten betrügerischen Zahlungsvorgangs.

b) Hat der Zahlungsdienstleister berechtigte Gründe für den Verdacht, dass der Verbraucher betrügerisch oder grob fahrlässig gehandelt hat, liefert er eine Begründung, warum er die Erstattung ablehnt, und nennt dem Verbraucher die Stellen, an die er sich gemäß den Artikeln 90, 91, 93, 94 und 95 wenden kann, falls er die angegebenen Gründe nicht akzeptiert.

(3) Absatz 1 findet keine Anwendung, wenn der Verbraucher betrügerisch oder grob fahrlässig gehandelt hat.

(4) Der Zahlungsdienstleister des Verbrauchers trägt die Beweislast, dass der Verbraucher betrügerisch oder grob fahrlässig gehandelt hat.

(5) Werden Anbieter elektronischer Kommunikationsdienste von einem Zahlungsdienstleister darüber unterrichtet, dass es zu einem in Absatz 1 genannten Betrugsfall gekommen ist, arbeiten diese Anbieter elektronischer Kommunikationsdienste eng mit den Zahlungsdienstleistern zusammen und handeln umgehend, um sicherzustellen, dass angemessene organisatorische und technische Maßnahmen getroffen werden, um die Sicherheit und Vertraulichkeit der Kommunikation gemäß der Richtlinie 2002/58/EG, insbesondere auch in Bezug auf die Rufnummeranzeige und die E-Mail-Adresse, sicherzustellen.

Artikel 60

Haftung des Zahlers für nicht autorisierte Zahlungsvorgänge

(1) Abweichend von Artikel 56 kann der Zahler dazu verpflichtet werden, Verluste, 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 gilt nicht, wenn

a) der Verlust, der Diebstahl oder die missbräuchliche Verwendung eines Zahlungsinstruments für den Zahler vor einer Zahlung nicht zu erkennen war, es sei denn, der Zahler hat betrügerisch gehandelt, oder

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

Der Zahler trägt alle mit nicht autorisierten Zahlungsvorgängen zusammenhängenden Verluste, wenn diese Verluste durch betrügerisches Handeln des Zahlers oder durch vorsätzliche oder grob fahrlässige Verletzung einer oder mehrerer seiner in Artikel 52 festgelegten Pflichten entstehen. In diesen Fällen findet der Höchstbetrag nach Unterabsatz 1 keine Anwendung.

Hat der Zahler weder betrügerisch gehandelt noch seine Pflichten nach Artikel 52 vorsätzlich verletzt, können die zuständigen nationalen Behörden oder die Zahlungsdienstleister die in diesem Absatz genannte Haftung 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) Verletzt der Zahlungsdienstleister seine in Artikel 85 niedergelegte Pflicht, eine starke Kundenauthentifizierung zu verlangen, trägt der Zahler finanzielle Verluste nur im Falle eigenen betrügerischen Handelns. Gleiches gilt, wenn der Zahlungsdienstleister des Zahlers oder der Zahlungsdienstleister des Zahlungsempfängers eine Ausnahme von der Durchführung der starken Kundenauthentifizierung anwendet. Versäumt es der Zahlungsempfänger oder der Zahlungsdienstleister des Zahlungsempfängers, die Systeme, die Hardware und die Software, die für die Durchführung der starken Kundenauthentifizierung notwendig

sind, anzupassen oder weiterzuentwickeln, erstattet der Zahlungsempfänger oder der Zahlungsdienstleister des Zahlungsempfängers den finanziellen Schaden, der dem Zahlungsdienstleister des Zahlers entstanden ist.

(3) Wendet der Zahlungsdienstleister des Zahlungsempfängers eine Ausnahme von der Durchführung der starken Kundenauthentifizierung an, haftet der Zahlungsdienstleister des Zahlungsempfängers gegenüber dem Zahlungsdienstleister des Zahlers für alle finanziellen Verluste, die dem Zahlungsdienstleister des Zahlers entstehen.

(4) Nach der Anzeige gemäß Artikel 52 Buchstabe b trägt der Zahler keine finanziellen Folgen aus der Nutzung des verlorenen, gestohlenen oder missbräuchlich verwendeten Zahlungsinstruments, es sei denn, der Zahler hat betrügerisch gehandelt.

Kommt der Zahlungsdienstleister seiner Pflicht nach Artikel 53 Absatz 1 Buchstabe c nicht nach, jederzeit geeignete Mittel für die Anzeige des Verlusts, des Diebstahls oder der missbräuchlichen Verwendung eines Zahlungsinstruments bereitzustellen, haftet der Zahler nicht für die finanziellen Folgen der Nutzung dieses Zahlungsinstruments, es sei denn, der Zahler hat betrügerisch gehandelt.

Artikel 61

Zahlungsvorgänge, bei denen der Betrag nicht im Voraus bekannt ist

(1) Wird im Zusammenhang mit einem kartengebundenen Zahlungsvorgang ein Zahlungsvorgang vom oder über den Zahlungsempfänger ausgelöst und ist der genaue künftige Betrag zu dem Zeitpunkt, zu dem der Zahler die Ausführung des Zahlungsvorgangs autorisiert, noch nicht bekannt, so darf der Zahlungsdienstleister des Zahlers Geld auf dem Zahlungskonto des Zahlers nur dann blockieren, wenn der Zahler seine Erlaubnis für die genaue Höhe des zu blockierenden Geldbetrags erteilt hat.

(2) Der vom Zahlungsdienstleister des Zahlers blockierte Geldbetrag muss im Verhältnis zu dem Betrag des Zahlungsvorgangs stehen, den der Zahler nach vernünftigem Ermessen erwarten kann.

(3) Der Zahlungsempfänger teilt seinem Zahlungsdienstleister den genauen Betrag des Zahlungsvorgangs sofort mit, nachdem die Dienstleistung erbracht oder die Ware geliefert wurde.

(4) Der Zahlungsdienstleister des Zahlers gibt das auf dem Zahlungskonto des Zahlers blockierte Geld sofort nach Erhalt der Information über den genauen Betrag des Zahlungsvorgangs frei.

Artikel 62

Erstattung eines von einem oder über einen Zahlungsempfänger ausgelösten Zahlungsvorgangs

(1) Ein Zahler hat gegenüber dem Zahlungsdienstleister Anspruch auf Erstattung eines autorisierten, von einem oder über einen Zahlungsempfänger ausgelösten und bereits ausgeführten Zahlungsvorgangs, wenn die beiden folgenden Bedingungen erfüllt sind:

a) Bei der Autorisierung wurde der genaue Betrag des Zahlungsvorgangs nicht angegeben.

b) Der Betrag des Zahlungsvorgangs übersteigt den Betrag, den der Zahler angesichts des bisherigen Ausgabenmusters, der Bedingungen des Rahmenvertrags und der jeweiligen Umstände des Einzelfalls nach vernünftigem Ermessen hätte erwarten können.

Auf Verlangen des Zahlungsdienstleisters erbringt der Zahler den Beweis, dass diese Bedingungen erfüllt sind.

Erstattet wird der volle Betrag des ausgeführten Zahlungsvorgangs. Die Wertstellung der Gutschrift auf dem Zahlungskonto des Zahlers erfolgt nicht später als zu dem Datum, an dem der Betrag belastet wurde.

Unbeschadet des Absatzes 3 hat der Zahler bei autorisierten, von einem Zahlungsempfänger ausgelösten Zahlungsvorgängen einschließlich Lastschriften nach Artikel 1 der Verordnung (EU) Nr. 260/2012 zusätzlich zu dem in Unterabsatz 1 genannten Anspruch einen bedingungslosen Anspruch auf Erstattung innerhalb der in Artikel 63 der vorliegenden Verordnung festgelegten Fristen.

(2) Für die Zwecke von Absatz 1 Unterabsatz 1 Buchstabe b darf der Zahler keine mit möglichen Währungsumtauschkosten zusammenhängenden Gründe geltend machen, wenn der mit seinem Zahlungsdienstleister gemäß Artikel 13 Absatz 1 Buchstabe e und Artikel 20 Buchstabe c Ziffer iii vereinbarte Referenzwechselkurs angewandt wurde.

(3) Der Zahler und der Zahlungsdienstleister können in einem Rahmenvertrag vereinbaren, dass der Zahler keinen Erstattungsanspruch hat, wenn

a) der Zahler die Ausführung des Zahlungsvorgangs direkt beim Zahlungsdienstleister autorisiert hat,

b) dem Zahler, soweit anwendbar, die Informationen über den anstehenden Zahlungsvorgang in einer vereinbarten Form mindestens vier Wochen vor dem Fälligkeitstermin vom Zahlungsdienstleister oder vom Zahlungsempfänger mitgeteilt oder zugänglich gemacht wurden.

(4) Für Lastschriften in anderen Währungen als dem Euro dürfen Zahlungsdienstleister im Rahmen ihrer Lastschriftverfahren günstigere Erstattungsansprüche anbieten, sofern diese für den Zahler vorteilhafter sind.

Artikel 63

Erstattungsanträge für Zahlungsvorgänge, die von einem oder über einen Zahlungsempfänger ausgelöst wurden

(1) Der Zahler kann die in Artikel 62 genannte Erstattung eines autorisierten Zahlungsvorgangs, der von einem oder über einen Zahlungsempfänger ausgelöst wurde, innerhalb von acht Wochen ab dem Zeitpunkt der Belastung des betreffenden Geldbetrags beantragen.

(2) Innerhalb von zehn Geschäftstagen nach Erhalt eines Erstattungsantrags unternimmt der Zahlungsdienstleister einen der folgenden beiden Schritte:

a) Er erstattet den vollen Betrag des Zahlungsvorgangs.

b) Er liefert eine Begründung, warum er die Erstattung ablehnt, und nennt die Stellen, an die sich der Zahler gemäß den Artikeln 90, 91, 93, 94 und 95 wenden kann, falls der Zahler die angegebenen Gründe nicht akzeptiert.

Das Recht des Zahlungsdienstleisters nach Unterabsatz 1 auf Ablehnung einer Erstattung gilt nicht in dem in Artikel 62 Absatz 1 Unterabsatz 4 festgelegten Fall.

KAPITEL 5

Ausführung von Zahlungsvorgängen

ABSCHNITT 1

ZAHLUNGSAUFTRÄGE UND TRANSFERIERTE BETRÄGE

Artikel 64

Eingang von Zahlungsaufträgen

(1) Als Zeitpunkt des Eingangs eines Zahlungsauftrags gilt der Zeitpunkt, zu dem der Zahlungsauftrag beim Zahlungsdienstleister des Zahlers eingeht.

Das Konto des Zahlers darf nicht vor Eingang des Zahlungsauftrags belastet werden. Fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag des Zahlungsdienstleisters des Zahlers, so gilt der Zahlungsauftrag als am darauf folgenden Geschäftstag eingegangen. Der Zahlungsdienstleister kann als Annahmeschluss einen Zeitpunkt gegen Ende des Geschäftstages festlegen, nach dem Zahlungsaufträge als am darauf folgenden Geschäftstag eingegangen gelten.

(2) Vereinbaren der Zahlungsdienstnutzer, der einen Zahlungsauftrag erteilt, und der Zahlungsdienstleister, dass die Ausführung des Zahlungsauftrags an einem bestimmten Tag oder am Ende eines bestimmten Zeitraums oder an dem Tag, an dem der Zahler dem Zahlungsdienstleister das Geld zur Verfügung gestellt hat, beginnen soll, so gilt der vereinbarte Termin für die Zwecke des Artikels 69 als Zeitpunkt des Eingangs. Fällt der vereinbarte Termin nicht auf einen Geschäftstag des Zahlungsdienstleisters, gilt der eingegangene Zahlungsauftrag als am darauf folgenden Geschäftstag eingegangen.

(3) Dieser Artikel gilt nicht für Sofortüberweisungen in Euro, die unter die Verordnung XXX (IPR) fallen.

Artikel 65

Ablehnung von Zahlungsaufträgen

(1) Lehnt der Zahlungsdienstleister die Ausführung eines Zahlungsauftrags oder die Auslösung eines Zahlungsvorgangs ab, teilt er dem Zahlungsdienstnutzer die Ablehnung und, sofern möglich, die Gründe dafür sowie das Verfahren mit, mit dem sachliche Fehler, die zur Ablehnung des Auftrags geführt haben, berichtigt werden können, es sei denn, dies ist nach sonstigem einschlägigem Recht der Union oder der Mitgliedstaaten untersagt.

Der Zahlungsdienstleister hat diese Mitteilung so rasch wie möglich, auf jeden Fall aber innerhalb der in Artikel 69 festgelegten Fristen zu übermitteln oder in einer vereinbarten Form zugänglich zu machen.

Der Rahmenvertrag kann vorsehen, dass der Zahlungsdienstleister für eine solche Ablehnung ein angemessenes Entgelt in Rechnung stellen darf, sofern die Ablehnung sachlich gerechtfertigt ist.

(2) Sind alle im Rahmenvertrag des Zahlers festgelegten Bedingungen erfüllt, darf der kontoführende Zahlungsdienstleister des Zahlers die Ausführung eines autorisierten Zahlungsvorgangs, unabhängig davon, ob der Zahlungsauftrag von einem Zahler, einschließlich eines Zahlungsauslösedienstleisters, erteilt oder von einem oder über einen Zahlungsempfänger ausgelöst wurde, nicht ablehnen, es sei denn, er ist durch sonstiges einschlägiges Recht der Union oder der Mitgliedstaaten untersagt.

(3) Für die Zwecke der Artikel 69 und 75a gilt ein Zahlungsauftrag, dessen Ausführung abgelehnt wurde, als nicht eingegangen.

Artikel 66

Unwiderruflichkeit eines Zahlungsauftrags

(1) Der Zahlungsdienstnutzer kann einen Zahlungsauftrag nach dessen Eingang beim Zahlungsdienstleister des Zahlers nicht mehr widerrufen, sofern dieser Artikel nichts anderes vorsieht.

(2) Wird der Zahlungsvorgang von einem Zahlungsauslösedienstleister oder vom oder über den Zahlungsempfänger ausgelöst, kann der Zahler den Zahlungsauftrag nicht mehr widerrufen, nachdem er dem Zahlungsauslösedienstleister die Erlaubnis erteilt hat, den Zahlungsvorgang auszulösen, oder nachdem er dem Zahlungsempfänger die Erlaubnis erteilt hat, den Zahlungsvorgang auszuführen.

(3) Im Falle einer Lastschrift kann der Zahler den Zahlungsauftrag unbeschadet etwaiger Erstattungsansprüche spätestens bis zum Ende des Geschäftstages, der dem vereinbarten Belastungstag vorausgeht, widerrufen.

(4) In dem in Artikel 64 Absatz 2 genannten Fall kann der Zahlungsdienstnutzer einen Zahlungsauftrag spätestens bis zum Ende des Geschäftstages, der dem vereinbarten Tag vorausgeht, widerrufen.

(5) Nach Ablauf der in den Absätzen 1 bis 4 festgelegten Fristen kann der Zahlungsauftrag nur dann widerrufen werden, wenn der Zahlungsdienstnutzer und die betreffenden Zahlungsdienstleister dies vereinbart haben. In den in den Absätzen 2 und 3 genannten Fällen ist auch die Zustimmung des Zahlungsempfängers erforderlich. Falls im Rahmenvertrag vereinbart, kann der betreffende Zahlungsdienstleister für den Widerruf ein Entgelt in Rechnung stellen.

Artikel 67

Transferierte und erhaltene Beträge

(1) Der Zahlungsdienstleister des Zahlers, der oder die Zahlungsdienstleister des Zahlungsempfängers und alle etwaigen zwischengeschalteten Stellen der

Zahlungsdienstleister transferieren den vollen Betrag des Zahlungsvorgangs und ziehen keine Entgelte vom transferierten Betrag ab.

(2) Der Zahlungsempfänger und der Zahlungsdienstleister können vereinbaren, dass der betreffende Zahlungsdienstleister seine Entgelte von dem transferierten Betrag abziehen darf, bevor er diesen dem Zahlungsempfänger gutschreibt. In diesem Fall werden der volle Betrag des Zahlungsvorgangs und die Entgelte in den Informationen für den Zahlungsempfänger getrennt ausgewiesen.

(3) Werden von dem transferierten Betrag andere als die in Absatz 2 genannten Entgelte abgezogen, stellt der Zahlungsdienstleister des Zahlers sicher, dass der Zahlungsempfänger den vollen Betrag des vom Zahler ausgelösten Zahlungsvorgangs erhält. Wird der Zahlungsvorgang vom oder über den Zahlungsempfänger ausgelöst, stellt der Zahlungsdienstleister des Zahlungsempfängers sicher, dass der Zahlungsempfänger den vollen Betrag des Zahlungsvorgangs erhält.

ABSCHNITT 2

AUSFÜHRUNGSFRIST UND WERTSTELLUNGSDATUM

Artikel 68

Geltungsbereich

(1) Dieser Abschnitt gilt für

a) Zahlungsvorgänge in Euro,

b) inländische Zahlungsvorgänge in der Währung des Mitgliedstaats, der nicht dem Euro-Währungsgebiet angehört,

c) Zahlungsvorgänge, bei denen nur eine Währungsumrechnung zwischen dem Euro und der Währung eines nicht dem Euro-Währungsgebiet angehörenden Mitgliedstaats stattfindet, sofern die erforderliche Währungsumrechnung in dem nicht dem Euro-Währungsgebiet angehörenden Mitgliedstaat durchgeführt wird und – im Falle von grenzüberschreitenden Zahlungsvorgängen – der grenzüberschreitende Transfer in Euro stattfindet.

(2) Dieser Abschnitt findet auf in Absatz 1 nicht genannte Zahlungsvorgänge Anwendung, sofern zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister nichts anderes vereinbart wurde; hiervon ausgenommen ist Artikel 73, den die Parteien nicht vertraglich abbedingen können. Vereinbaren der Zahlungsdienstnutzer und der Zahlungsdienstleister jedoch für Zahlungsvorgänge innerhalb der Union eine längere als die in Artikel 69 festgelegte Frist, so darf diese längere Frist vier Geschäftstage ab dem in Artikel 64 genannten Zeitpunkt des Eingangs nicht überschreiten.

Artikel 69

Zahlungsvorgänge mit Übertragung auf ein Zahlungskonto

(1) Unbeschadet des Artikels 2 Absatz 1 Buchstabe c der Verordnung (EU) Nr. 260/2012 stellt der Zahlungsdienstleister des Zahlers sicher, dass nach dem in Artikel 64 genannten Zeitpunkt des Eingangs der Betrag des Zahlungsvorgangs dem Konto des Zahlungsdienstleisters des Zahlungsempfängers bis zum Ende des darauffolgenden Geschäftstags gutgeschrieben wird. Diese Frist kann für in Papierform ausgelöste Zahlungsvorgänge um einen weiteren Geschäftstag verlängert werden.

(2) Der Zahlungsdienstleister des Zahlungsempfängers nimmt die Wertstellung und die Verfügbarmachung des Betrags des Zahlungsvorgangs auf dem Zahlungskonto des Zahlungsempfängers gemäß Artikel 73 vor, nachdem er seinerseits das Geld erhalten hat.

(3) Der Zahlungsdienstleister des Zahlungsempfängers übermittelt dem Zahlungsdienstleister des Zahlers einen vom oder über den Zahlungsempfänger erteilten Zahlungsauftrag innerhalb der zwischen dem Zahlungsempfänger und dem Zahlungsdienstleister vereinbarten Fristen und ermöglicht so im Falle von Lastschriften die Abwicklung zum vereinbarten Fälligkeitstermin.

Artikel 70

Fehlen eines Zahlungskontos des Zahlungsempfängers beim Zahlungsdienstleister

Unterhält der Zahlungsempfänger beim Zahlungsdienstleister kein Zahlungskonto, macht der Zahlungsdienstleister, der das Geld für den Zahlungsempfänger erhält, das Geld für den Zahlungsempfänger innerhalb der in Artikel 69 Absatz 1 genannten Frist verfügbar.

Artikel 71

Auf ein Zahlungskonto eingezahltes Bargeld

Zahlt ein Verbraucher Bargeld auf ein Zahlungskonto bei einem Zahlungsdienstleister in der Währung des betreffenden Zahlungskontos ein, so stellt dieser Zahlungsdienstleister sicher, dass der Betrag sofort nach Eingang des Geldes verfügbar gemacht und wertgestellt wird. Ist der Zahlungsdienstnutzer kein Verbraucher, muss der Betrag spätestens an dem auf den Eingang folgenden Geschäftstag auf dem Konto des Zahlungsempfängers verfügbar gemacht und wertgestellt sein.

Artikel 72

Inländische Zahlungsvorgänge

Bei inländischen Zahlungsvorgängen können die Mitgliedstaaten kürzere als die in diesem Abschnitt vorgesehenen Ausführungsfristen vorsehen.

Artikel 73

Wertstellung und Verfügbarkeit der Gelder

(1) Die Wertstellung einer Gutschrift auf dem Zahlungskonto des Zahlungsempfängers erfolgt nicht später als an dem Geschäftstag, an dem der Betrag des Zahlungsvorgangs dem Konto des Zahlungsdienstleisters des Zahlungsempfängers gutgeschrieben wird.

(2) Der Zahlungsdienstleister des Zahlungsempfängers stellt sicher, dass der Betrag des Zahlungsvorgangs dem Zahlungsempfänger sofort zur Verfügung steht, nachdem der Betrag dem Konto des Zahlungsdienstleisters des Zahlungsempfängers gutgeschrieben wurde, wenn aufseiten des Zahlungsdienstleisters des Zahlungsempfängers

a) entweder keine Währungsumrechnung erfolgt

b) oder eine Währungsumrechnung zwischen dem Euro und einer Währung eines Mitgliedstaats oder zwischen den Währungen zweier Mitgliedstaaten erfolgt.

Die in diesem Absatz festgelegte Verpflichtung gilt auch für Zahlungen innerhalb eines Zahlungsdienstleisters.

(3) Die Wertstellung einer Lastschrift auf dem Zahlungskonto des Zahlers erfolgt nicht früher als zu dem Zeitpunkt, zu dem das betreffende Zahlungskonto mit dem Betrag des Zahlungsvorgangs belastet wird.

Artikel 74

Fehlerhafte Kundenidentifikatoren

(1) Wird ein Zahlungsvorgang gemäß Kundenidentifikator ausgeführt, gilt der Zahlungsvorgang im Hinblick auf den mittels Kundenidentifikator angegebenen Zahlungsempfänger als korrekt ausgeführt.

(2) Ist der vom Zahlungsdienstnutzer angegebene Kundenidentifikator fehlerhaft, so haftet der Zahlungsdienstleister nicht im Rahmen von Artikel 75 für die nicht erfolgte oder fehlerhafte Ausführung des Zahlungsvorgangs.

(3) Der Zahlungsdienstleister des Zahlers bemüht sich im Rahmen des Zumutbaren, das Geld, das Gegenstand des Zahlungsvorgangs war, wiederzuerlangen. Der Zahlungsdienstleister des Zahlungsempfängers beteiligt sich an diesen Bemühungen auch dadurch, dass er dem Zahlungsdienstleister des Zahlers alle für die Einziehung des Geldbetrags maßgeblichen Informationen übermittelt.

Ist die Einziehung des Geldbetrags nach Unterabsatz 1 nicht möglich, übermittelt der Zahlungsdienstleister des Zahlers dem Zahler auf schriftlichen Antrag hin alle Informationen, über die der Zahlungsdienstleister des Zahlers verfügt und die für den Zahler relevant sind, damit der Zahler seinen Anspruch auf Rückerstattung des Betrags auf dem Rechtsweg geltend machen kann.

(4) Falls im Rahmenvertrag vereinbart, kann der Zahlungsdienstleister dem Zahlungsdienstnutzer für die Wiedererlangung ein Entgelt in Rechnung stellen.

(5) Übermittelt der Zahlungsdienstnutzer zusätzlich zu den in Artikel 13 Absatz 1 Buchstabe a oder Artikel 20 Buchstabe b Ziffer ii genannten Angaben weitere

Informationen, haftet der Zahlungsdienstleister nur für die Ausführung von Zahlungsvorgängen gemäß dem vom Zahlungsdienstnutzer angegebenen Kundenidentifikator.

(6) Ist der vom Zahlungsauslösedienstleister angegebene Kundenidentifikator fehlerhaft, haften die Zahlungsdienstleister gemäß Artikel 76.

Artikel 75

Haftung der Zahlungsdienstleister für nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen

(1) Wird ein Zahlungsauftrag vom Zahler direkt erteilt, haftet der Zahlungsdienstleister des Zahlers unbeschadet des Artikels 54, des Artikels 74 Absätze 2 und 3 sowie des Artikels 79 gegenüber dem Zahler für die korrekte Ausführung des Zahlungsvorgangs, es sei denn, er kann gegenüber dem Zahler und gegebenenfalls gegenüber dem Zahlungsdienstleister des Zahlungsempfängers nachweisen, dass der Zahlungsdienstleister des Zahlungsempfängers den Betrag des Zahlungsvorgangs gemäß Artikel 69 Absatz 1 erhalten hat. In diesem Fall haftet der Zahlungsdienstleister des Zahlungsempfängers gegenüber dem Zahlungsempfänger für die korrekte Ausführung des Zahlungsvorgangs.

Haftet der Zahlungsdienstleister des Zahlers nach Unterabsatz 1, so erstattet er dem Zahler den Betrag des nicht ausgeführten oder fehlerhaft ausgeführten Zahlungsvorgangs sofort und bringt das belastete Zahlungskonto gegebenenfalls wieder auf den Stand, auf dem es sich ohne den fehlerhaft ausgeführten Zahlungsvorgang befunden hätte.

Die Wertstellung der Gutschrift auf dem Zahlungskonto des Zahlers erfolgt nicht später als zu dem Datum, an dem der Betrag belastet wurde.

Haftet der Zahlungsdienstleister des Zahlungsempfängers nach Unterabsatz 1, stellt er dem Zahlungsempfänger den Betrag des Zahlungsvorgangs sofort zur Verfügung und schreibt den entsprechenden Betrag gegebenenfalls dem Zahlungskonto des Zahlungsempfängers gut.

Die Wertstellung der Gutschrift auf dem Zahlungskonto des Zahlungsempfängers erfolgt nicht später als zu dem Datum, an dem der Betrag bei korrekter Ausführung gemäß Artikel 73 wertgestellt worden wäre.

Wird ein Zahlungsvorgang verspätet ausgeführt, stellt der Zahlungsdienstleister des Zahlungsempfängers auf Verlangen des für den Zahler auftretenden Zahlungsdienstleisters des Zahlers sicher, dass die Wertstellung der Gutschrift auf dem Zahlungskonto des Zahlungsempfängers nicht später erfolgt als zu dem Datum, an dem der Betrag bei korrekter Ausführung wertgestellt worden wäre.

Im Falle eines nicht ausgeführten oder fehlerhaft ausgeführten Zahlungsvorgangs, bei dem der Zahlungsauftrag durch den Zahler erteilt wurde, unternimmt der Zahlungsdienstleister des Zahlers ungeachtet der Haftung nach diesem Absatz auf Verlangen und ohne dem Zahler ein Entgelt dafür in Rechnung zu stellen, sofortige Bemühungen zur Rückverfolgung des Zahlungsvorgangs und unterrichtet den Zahler über das Ergebnis.

(2) Wird ein Zahlungsauftrag vom oder über den Zahlungsempfänger erteilt, haftet der Zahlungsdienstleister des Zahlungsempfängers unbeschadet des Artikels 54, des

Artikels 74 Absätze 2 und 3 sowie des Artikels 79 gegenüber dem Zahlungsempfänger für die korrekte Übermittlung des Zahlungsauftrags an den Zahlungsdienstleister des Zahlers gemäß Artikel 69 Absatz 3. Haftet der Zahlungsdienstleister des Zahlungsempfängers nach diesem Unterabsatz, übermittelt er den fraglichen Zahlungsauftrag sofort erneut an den Zahlungsdienstleister des Zahlers.

Bei verspäteter Übermittlung des Zahlungsauftrags erfolgt die Wertstellung des Betrags auf dem Zahlungskonto des Zahlungsempfängers nicht später als zu dem Datum, an dem der Betrag bei korrekter Ausführung wertgestellt worden wäre.

Unbeschadet des Artikels 54, des Artikels 74 Absätze 2 und 3 und des Artikels 79 haftet der Zahlungsdienstleister des Zahlungsempfängers gegenüber dem Zahlungsempfänger für die Bearbeitung des Zahlungsvorgangs gemäß seinen Verpflichtungen nach Artikel 73. Haftet der Zahlungsdienstleister des Zahlungsempfängers nach diesem Unterabsatz, stellt er sicher, dass der Betrag des Zahlungsvorgangs dem Zahlungsempfänger sofort, nachdem der Betrag dem Konto des Zahlungsdienstleisters des Zahlungsempfängers gutgeschrieben wurde, zur Verfügung steht. Die Wertstellung des Betrags auf dem Zahlungskonto des Zahlungsempfängers erfolgt nicht später als zu dem Datum, an dem der Betrag bei korrekter Ausführung wertgestellt worden wäre.

Im Falle eines nicht ausgeführten oder fehlerhaft ausgeführten Zahlungsvorgangs, für den der Zahlungsdienstleister des Zahlungsempfängers nicht nach den Unterabsätzen 1 und 3 haftet, haftet der Zahlungsdienstleister des Zahlers gegenüber dem Zahler. Haftet der Zahlungsdienstleister des Zahlers in dieser Weise, erstattet er dem Zahler gegebenenfalls unverzüglich den Betrag des nicht ausgeführten oder fehlerhaft ausgeführten Zahlungsvorgangs und bringt das belastete Zahlungskonto wieder auf den Stand, auf dem es sich ohne den fehlerhaft ausgeführten Zahlungsvorgang befunden hätte. Die Wertstellung der Gutschrift auf dem Zahlungskonto des Zahlers erfolgt nicht später als zu dem Datum, an dem der Betrag belastet wurde.

Die Verpflichtung des Zahlungsdienstleisters des Zahlers gemäß Unterabsatz 4 besteht nicht, wenn der Zahlungsdienstleister des Zahlers nachweist, dass der Zahlungsdienstleister des Zahlungsempfängers den Betrag des Zahlungsvorgangs erhalten hat, auch wenn bei der Ausführung des Zahlungsvorgangs lediglich eine Verzögerung aufgetreten ist. In diesem Fall nimmt der Zahlungsdienstleister des Zahlungsempfängers die Wertstellung auf dem Zahlungskonto des Zahlungsempfängers nicht später vor als zu dem Datum, an dem der Betrag bei korrekter Ausführung wertgestellt worden wäre.

Im Falle eines nicht ausgeführten oder fehlerhaft ausgeführten Zahlungsvorgangs, bei dem der Zahlungsauftrag durch oder über den Zahlungsempfänger erteilt wurde, unternimmt der Zahlungsdienstleister des Zahlungsempfängers ungeachtet der Haftung nach diesem Absatz auf Verlangen und ohne dem Zahler ein Entgelt dafür in Rechnung zu stellen, sofortige Bemühungen zur Rückverfolgung des Zahlungsvorgangs und unterrichtet den Zahler über das Ergebnis.

(3) Zahlungsdienstleister haften gegenüber ihren jeweiligen Zahlungsdienstnutzern für alle von ihnen zu verantwortenden Entgelte und für Zinsen, die dem Zahlungsdienstnutzer infolge einer nicht erfolgten oder fehlerhaften, einschließlich verspäteten Ausführung des Zahlungsvorgangs in Rechnung gestellt werden.

Artikel 76

Haftung im Falle von Zahlungsauslösediensten für nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen

(1) Wird ein Zahlungsauftrag vom Zahler oder vom Zahlungsempfänger über einen Zahlungsauslösedienstleister erteilt, so erstattet der kontoführende Zahlungsdienstleister unbeschadet des Artikels 54 und des Artikels 74 Absätze 2 und 3 dem Zahler den Betrag des nicht ausgeführten oder fehlerhaft ausgeführten Zahlungsvorgangs und bringt das belastete Zahlungskonto gegebenenfalls wieder auf den Stand, auf dem es sich ohne den fehlerhaft ausgeführten Zahlungsvorgang befunden hätte.

Der Zahlungsauslösedienstleister trägt die Beweislast, dass der Zahlungsauftrag gemäß Artikel 64 beim kontoführenden Zahlungsdienstleister des Zahlers eingegangen ist und dass der Zahlungsvorgang innerhalb seines Zuständigkeitsbereichs authentifiziert, korrekt aufgezeichnet und nicht durch eine technische Störung oder einen anderen Mangel im Zusammenhang mit der nicht erfolgten, fehlerhaften oder verspäteten Ausführung des Vorgangs beeinträchtigt wurde.

(2) Haftet der Zahlungsauslösedienstleister für die nicht erfolgte, fehlerhafte oder verspätete Ausführung des Zahlungsvorgangs, so entschädigt er den kontoführenden Zahlungsdienstleister auf dessen Verlangen sofort für die infolge der Erstattung an den Zahler erlittenen Verluste oder gezahlten Beträge.

Artikel 77

Zusätzliche finanzielle Entschädigung

Eine etwaige über die Bestimmungen dieses Abschnitts hinausgehende finanzielle Entschädigung kann nach dem auf den Vertrag zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister anwendbaren Recht festgelegt werden.

Artikel 78

Regressanspruch

(1) Kann in Bezug auf die Haftung eines Zahlungsdienstleisters nach den Artikeln 56, 57, 59, 75 und 76 ein anderer Zahlungsdienstleister oder eine zwischengeschaltete Stelle in Regress genommen werden, entschädigt dieser andere Zahlungsdienstleister oder diese zwischengeschaltete Stelle den erstgenannten Zahlungsdienstleister für alle nach den Artikeln 56, 57, 59, 75 und 76 erlittenen Verluste oder gezahlten Beträge. Dies beinhaltet auch eine Entschädigung in dem Fall, dass einer der Zahlungsdienstleister keine starke Kundenauthentifizierung durchführt.

(2) Eine darüber hinausgehende finanzielle Entschädigung kann nach den Vereinbarungen zwischen den Zahlungsdienstleistern oder zwischengeschalteten Stellen und dem auf diese Vereinbarungen anwendbaren Recht festgelegt werden.

Artikel 79

Ungewöhnliche und unvorhersehbare Umstände

Die Haftung nach den Kapiteln 4 oder 5 besteht nicht im Falle ungewöhnlicher und unvorhersehbarer Umstände, auf die die Partei, die sich darauf beruft, keinen Einfluss hat und deren Folgen trotz aller Gegenbemühungen nicht abwendbar gewesen wären, oder falls ein Zahlungsdienstleister durch andere rechtliche Verpflichtungen nach dem Recht der Union oder nach nationalem Recht gebunden ist.

KAPITEL 6

Datenschutz

Artikel 80

Datenschutz

Zahlungssysteme und Zahlungsdienstleister dürfen die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 und Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 genannten besonderen Kategorien personenbezogener Daten im öffentlichen Interesse eines gut funktionierenden Zahlungsdienstebinnenmarkts verarbeiten, soweit dies für die Erbringung von Zahlungsdiensten und für die Erfüllung der Verpflichtungen im Rahmen dieser Verordnung notwendig ist, wobei sie für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen angemessene Vorkehrungen zu treffen haben, die Folgendes einschließen müssen:

a) technische Maßnahmen, um sicherzustellen, dass die in der Verordnung (EU) 2016/679 niedergelegten Grundsätze der Zweckbindung, der Datenminimierung und der Speicherbegrenzung eingehalten werden, was auch technische Beschränkungen für die Weiterverwendung von Daten und die Anwendung modernster Sicherheits- und Datenschutzvorkehrungen, wie Pseudonymisierung oder Verschlüsselung, einschließen muss;

b) organisatorische Maßnahmen, einschließlich Schulungen in Sachen Verarbeitung besonderer Datenkategorien, Beschränkung des Zugangs zu besonderen Datenkategorien und Aufzeichnung eines solchen Zugangs.

KAPITEL 7

Operationelle und sicherheitsrelevante Risiken und Authentifizierung

Artikel 81

Management operationeller und sicherheitsrelevanter Risiken

(1) Die Zahlungsdienstleister schaffen einen Rahmen mit angemessenen Risikominderungsmaßnahmen und Kontrollmechanismen für das Management der

operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit den von ihnen erbrachten Zahlungsdiensten. Als Teil dieses Rahmens müssen die Zahlungsdienstleister wirksame Verfahren für das Management von Vorfällen – auch zur Aufdeckung und Klassifizierung schwerer Betriebs- und Sicherheitsvorfälle — festlegen und anwenden.

Unterabsatz 1 berührt nicht die Anwendung von Kapitel II der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates[65] auf

a) die in Artikel 2 Absatz 1 Buchstaben a, b und d der vorliegenden Verordnung genannten Zahlungsdienstleister,

b) die in Artikel 36 Absatz 1 der Richtlinie (EU) (PSD3) genannten Kontoinformationsdienstleister und

c) Zahlungsinstitute, die gemäß Artikel 34 Absatz 1 der Richtlinie (EU) (PSD3) ausgenommen sind.

Die Zahlungsdienstleister übermitteln der gemäß der Richtlinie (EU) XXX (PSD3) benannten zuständigen Behörde jährlich oder in den von den zuständigen Behörden festgelegten kürzeren Abständen eine aktualisierte und umfassende Bewertung der operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit den von ihnen erbrachten Zahlungsdiensten und der Angemessenheit der zur Beherrschung dieser Risiken ergriffenen Risikominderungsmaßnahmen und Kontrollmechanismen.

(2) Die EBA fördert die Zusammenarbeit, einschließlich des Austauschs von Informationen, unter den zuständigen Behörden, zwischen den zuständigen Behörden und der EZB sowie gegebenenfalls der Agentur der Europäischen Union für Netz- und Informationssicherheit im Bereich der operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit Zahlungsdiensten.

Artikel 82

Berichterstattung über Betrug

(1) Die Zahlungsdienstleister stellen den für sie zuständigen Behörden mindestens jährlich statistische Daten zu Betrug im Zusammenhang mit den verschiedenen Zahlungsmitteln bereit. Die betreffenden zuständigen Behörden stellen der EBA und der EZB diese Daten in aggregierter Form bereit.

(2) Die EBA arbeitet in enger Zusammenarbeit mit der EZB Entwürfe technischer Regulierungsstandards aus, in denen festgelegt wird, welche statistischen Daten nach Absatz 1 für die in Absatz 1 genannte Berichterstattung über Betrug bereitzustellen sind.

Die EBA übermittelt der Kommission die in Unterabsatz 1 genannten technischen Regulierungsstandards bis zum [OP, bitte Datum einfügen: ein Jahr nach dem Datum

[65] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Betriebsstabilität digitaler Systeme im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1).

des Inkrafttretens dieser Verordnung]. Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Regulierungsstandards nach den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010 zu erlassen.

(3) Die EBA arbeitet Entwürfe technischer Durchführungsstandards aus, in denen die Standardformulare und -meldebögen für die in Absatz 1 genannte Übermittlung von Zahlungsbetrugsdaten durch die zuständigen Behörden an die EBA festgelegt werden.

Die EBA übermittelt der Kommission die in Unterabsatz 1 genannten technischen Durchführungsstandards bis zum [OP, bitte Datum einfügen: ein Jahr nach dem Datum des Inkrafttretens dieser Verordnung]. Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Regulierungsstandards nach Artikel 15 der Verordnung (EU) Nr. 1093/2010 zu erlassen.

Artikel 83

Transaktionsüberwachungsmechanismen und Betrugsdatenaustausch

(1) Die Zahlungsdienstleister müssen über Transaktionsüberwachungsmechanismen verfügen, die

a) die Durchführung der starken Kundenauthentifizierung gemäß Artikel 85 unterstützen,

b) Ausnahmen von der Durchführung der starken Kundenauthentifizierung auf Basis der in Artikel 85 Absatz 11 genannten Kriterien unter genau festgelegten und eingeschränkten Bedingungen vorsehen, die auf dem jeweiligen Risiko sowie der Art und den Einzelheiten der vom Zahlungsdienstleister bewerteten Daten beruhen;

c) den Zahlungsdienstleistern die Möglichkeit geben, potenziell betrügerische Zahlungsvorgänge, einschließlich Zahlungsvorgänge unter Beteiligung von Zahlungsauslösediensten, zu verhindern und aufzudecken.

(2) Die Transaktionsüberwachungsmechanismen stützen sich auf die Analyse früherer Zahlungsvorgänge und Online-Zugriffe auf Zahlungskonten. Die Verarbeitung beschränkt sich auf die folgenden Daten, die für die in Absatz 1 genannten Zwecke benötigt werden:

a) Informationen über den Zahlungsdienstnutzer, einschließlich umgebungs- und verhaltensbezogener Merkmale, die für den Zahlungsdienstnutzer im Rahmen einer normalen Verwendung der personalisierten Sicherheitsmerkmale typisch sind;

b) Informationen über das Zahlungskonto, einschließlich Zahlungsvorgangshistorie;

c) Informationen über den Vorgang, einschließlich Betrag des Vorgangs und Kundenidentifikator des Zahlungsempfängers;

d) Sitzungsdaten, einschließlich Internetprotokoll-Adressbereich, von dem aus mit einem Gerät auf das Zahlungskonto zugegriffen wurde.

Die Zahlungsdienstleister speichern die in diesem Absatz genannten Daten nicht länger, als es für die in Absatz 1 festgelegten Zwecke erforderlich ist, auf keinen Fall aber nach Beendigung der Kundenbeziehung. Die Zahlungsdienstleister stellen sicher, dass die Transaktionsüberwachungsmechanismen zumindest alle nachstehend genannten risikobasierten Faktoren einbeziehen:

a) Liste der missbräuchlich verwendeten oder gestohlenen Authentifizierungselemente,

b) Betrag eines jeden Zahlungsvorgangs,

c) bekannte Betrugsszenarien bei der Erbringung von Zahlungsdienstleistungen,

d) Anzeichen für eine Malware-Infektion in einer Phase des Authentifizierungsverfahrens,

e) falls das Zugangsgerät oder die Zugangssoftware vom Zahlungsdienstleister bereitgestellt wird, ein Protokoll über die Nutzung des Zugangsgeräts oder der Zugangssoftware, die dem Zahlungsdienstnutzer zur Verfügung gestellt werden, sowie über die ungewöhnliche Nutzung dieses Geräts oder der Software.

(3) Soweit dies zur Erfüllung von Absatz 1 Buchstabe c erforderlich ist, können die Zahlungsdienstleister den Kundenidentifikator eines Zahlungsempfängers mit anderen, den in Absatz 5 genannten Vereinbarungen über den Informationsaustausch unterliegenden Zahlungsdienstleistern austauschen, wenn der Zahlungsdienstleister ausreichende Beweise für die Annahme hat, dass ein betrügerischer Zahlungsvorgang stattgefunden hat. Von ausreichenden Beweisen für den Austausch von Kundenidentifikatoren wird ausgegangen, wenn mindestens zwei unterschiedliche Zahlungsdienstnutzer, die Kunden ein und desselben Zahlungsdienstleisters sind, mitgeteilt haben, dass ein Kundenidentifikator eines Zahlungsempfängers für eine betrügerische Überweisung verwendet wurde. Die Zahlungsdienstleister bewahren Kundenidentifikatoren, die sie im Zuge des in diesem Absatz und in Absatz 5 genannten Informationsaustauschs erhalten, nicht länger auf als für die in Absatz 1 Buchstabe c genannten Zwecke erforderlich.

(4) Die Vereinbarungen über den Austausch von Informationen regeln die Einzelheiten der Beteiligung sowie die Einzelheiten der operativen Elemente, einschließlich der Nutzung dedizierter IT-Plattformen. Vor Abschluss derartiger Vereinbarungen führen die Zahlungsdienstleister gemeinsam eine Datenschutz-Folgenabschätzung im Sinne von Artikel 35 der Verordnung (EU) 2016/679 und gegebenenfalls eine vorherige Konsultation der Aufsichtsbehörde im Sinne von Artikel 36 jener Verordnung durch.

(5) Die Zahlungsdienstleister zeigen den zuständigen Behörden ihre Beteiligung an den in Absatz 5 genannten Vereinbarungen über den Austausch von Informationen an, sobald ihre Mitgliedschaft von den Beteiligten an der Vereinbarung über den Austausch von Informationen bestätigt wurde, bzw. zeigen den zuständigen Behörden die Beendigung ihrer Mitgliedschaft an, sobald diese Beendigung wirksam wird.

(6) Die Verarbeitung personenbezogener Daten gemäß Absatz 4 darf weder die Beendigung des Vertragsverhältnisses mit dem Kunden durch den Zahlungsdienstleister zur Folge haben noch das künftige Onboarding durch einen anderen Zahlungsdienstleister beeinträchtigen.

Artikel 84

Zahlungsbetrugsrisiken und -trends

(1) Die Zahlungsdienstleister warnen ihre Kunden über alle geeigneten Wege und Medien, wenn neue Formen von Zahlungsbetrug aufkommen, wobei sie den Bedürfnissen ihrer schutzbedürftigsten Kundengruppen Rechnung tragen. Die Zahlungsdienstleister geben ihren Kunden klare Hinweise, wie sie Betrugsversuche erkennen können, und machen sie darauf aufmerksam, welche Maßnahmen und Vorkehrungen sie treffen müssen, um keinen betrügerischen Handlungen zum Opfer zu fallen. Die Zahlungsdienstleister informieren ihre Kunden darüber, wo sie betrügerische Handlungen melden und in Sachen Betrug schnell Informationen erhalten können.

(2) Die Zahlungsdienstleister organisieren für ihre Mitarbeiter mindestens jährlich Schulungsprogramme zu den Risiken und Trends in Sachen Zahlungsbetrug und stellen sicher, dass ihre Mitarbeiter angemessen ausgebildet sind, um ihre Aufgaben und Verantwortlichkeiten gemäß den einschlägigen Sicherheitsrichtlinien und -verfahren zur Minderung und Steuerung von Zahlungsbetrugsrisiken wahrnehmen zu können.

(3) Bis zum [Amt für Veröffentlichungen, bitte Datum einfügen: 18 Monate nach dem Datum des Inkrafttretens dieser Verordnung] gibt die EBA gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 Leitlinien für die in den Absätzen 1 und 2 genannten Programme zu Zahlungsbetrugsrisiken heraus.

Artikel 85

Starke Kundenauthentifizierung

(1) Ein Zahlungsdienstleister führt eine starke Kundenauthentifizierung durch, wenn der Zahler

a) online auf sein Zahlungskonto zugreift,

b) auf Zahlungskontoinformationen zugreift,

c) einen Zahlungsauftrag für einen elektronischen Zahlungsvorgang erteilt,

d) über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Zahlungsbetrugs oder anderen Missbrauchs birgt.

(2) Zahlungsvorgänge, die nicht vom Zahler, sondern nur vom Zahlungsempfänger ausgelöst werden, unterliegen keiner starken Kundenauthentifizierung, sofern die betreffenden Vorgänge ohne jegliche Interaktion oder Beteiligung des Zahlers ausgelöst werden.

(3) Hat der Zahler ein Mandat erteilt, das den Zahlungsempfänger zur Erteilung eines Zahlungsauftrags für einen Zahlungsvorgang oder eine Serie von Zahlungsvorgängen mittels eines bestimmten Zahlungsinstruments ermächtigt, das dafür ausgegeben wird, dass der Zahler damit Zahlungsaufträge für die Zahlungsvorgänge erteilen kann, und beruht das Mandat auf einer Vereinbarung zwischen dem Zahler und dem Zahlungsempfänger über die Bereitstellung von Waren oder Dienstleistungen, so

können die anschließend vom Zahlungsempfänger auf der Grundlage eines solchen Mandats ausgelösten Zahlungsvorgänge als vom Zahlungsempfänger ausgelöste Zahlungsvorgänge gelten, sofern diesen Vorgängen keine bestimmte Handlung des Zahlers vorausgehen muss, damit ihre Auslösung durch den Zahlungsempfänger erfolgen kann.

(4) Die Zahlungsvorgänge, für die der Zahlungsempfänger auf der Grundlage des vom Zahler erteilten Mandats Zahlungsaufträge erteilt, unterliegen den für vom Zahlungsempfänger ausgelöste Zahlungsvorgänge im Sinne der Artikel 61, 62 und 63 geltenden allgemeinen Bestimmungen.

(5) Wird das Mandat des Zahlers an den Zahlungsempfänger zur Erteilung von Zahlungsaufträgen für Zahlungsvorgänge im Sinne von Absatz 3 über einen Fernzugang unter Beteiligung des Zahlungsdienstleisters erteilt, so unterliegt die Einrichtung eines solchen Mandats einer starken Kundenauthentifizierung.

(6) Wird bei Lastschriften das Mandat, das der Zahler dem Zahlungsempfänger für die Auslösung einer oder mehrerer Lastschriften erteilt, über einen Fernzugang unter direkter Beteiligung eines Zahlungsdienstleisters an der Einrichtung des betreffenden Mandats erteilt, so ist eine starke Kundenauthentifizierung durchzuführen.

(7) Zahlungsvorgänge, bei denen der Zahler Zahlungsaufträge auf anderem Wege als durch Nutzung elektronischer Plattformen oder Geräte erteilt, etwa mittels beleghafter Zahlungsaufträge, oder Bestellungen per Post oder Telefon, dürfen unabhängig davon, ob der Zahlungsvorgang elektronisch ausgeführt wird, keiner starken Kundenauthentifizierung unterliegen, sofern der Zahlungsdienstleister des Zahlers Sicherheitsanforderungen und -kontrollen anwendet, die eine Form der Authentifizierung des Zahlungsvorgangs ermöglichen.

(8) Für die Erteilung eines in Absatz 1 Buchstabe c genannten Zahlungsauftrags über einen Fernzugang verlangen die Zahlungsdienstleister eine starke Kundenauthentifizierung, die Elemente umfasst, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen.

(9) Für die Erteilung eines in Absatz 1 Buchstabe c genannten Zahlungsauftrags über ein Gerät des Zahlers, das für den Informationsaustausch mit der Infrastruktur des Zahlungsempfängers Nahbereichstechnik nutzt, deren Authentifizierung die Nutzung des Internets auf dem Gerät des Zahlers erfordert, wenden die Zahlungsdienstleister eine starke Kundenauthentifizierung mit Elementen, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen, oder harmonisierte Sicherheitsmaßnahmen mit gleicher Wirkung an, die die Vertraulichkeit, die Authentizität und die Integrität des Betrags des Zahlungsvorgangs und des Zahlungsempfängers in allen Phasen der Auslösung gewährleisten.

(10) Für die Zwecke des Absatzes 1 müssen die Zahlungsdienstleister angemessene Sicherheitsmaßnahmen treffen, um die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer zu schützen.

(11) Für etwaige Ausnahmen von der Durchführung der starken Kundenauthentifizierung, die nach Artikel 89 von der EBA auszuarbeiten sind, werden eines oder mehrere der folgenden Kriterien herangezogen:

a) mit der Dienstleistung verbundenes Risikoniveau,

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

c) für die Ausführung des Zahlungsvorgangs genutzter Zahlungsweg.

(12) Die in Artikel 3 Nummer 35 genannten mindestens zwei Elemente, die bei der starken Kundenauthentifizierung heranzuziehen sind, müssen nicht zwingend verschiedenen Kategorien angehören, solange ihre Unabhängigkeit voneinander uneingeschränkt gewahrt bleibt.

Artikel 86

Starke Kundenauthentifizierung bei Zahlungsauslöse- und Kontoinformationsdiensten

(1) Artikel 85 Absatz 9 gilt auch, wenn Zahlungen über einen Zahlungsauslösedienstleister ausgelöst werden. Artikel 85 Absatz 10 gilt auch, wenn Zahlungen über einen Zahlungsauslösedienstleister ausgelöst werden und wenn die Informationen über einen Kontoinformationsdienstleister angefordert werden.

(2) Die kontoführenden Zahlungsdienstleister gestatten den Zahlungsauslösedienstleistern und den Kontoinformationsdienstleistern, sich auf die Authentifizierungsverfahren zu stützen, die der kontoführende Zahlungsdienstleister dem Zahlungsdienstnutzer gemäß Artikel 85 Absätze 1 und 10 sowie in Fällen, in denen der Zahlungsauslösedienstleister beteiligt ist, gemäß Artikel 85 Absätze 1, 8, 9, 10 und 11 bereitstellt.

(3) Unbeschadet des Absatzes 2 darf der kontoführende Zahlungsdienstleister in dem Falle, dass ein Kontoinformationsdienstleister auf Zahlungskontoinformationen zugreift, eine starke Kundenauthentifizierung nur beim Erstzugriff des betreffenden Kontoinformationsdienstleisters auf Zahlungskontoinformationen durchführen, sofern der kontoführende Zahlungsdienstleister keine berechtigte Gründe für einen Betrugsverdacht hat, jedoch nicht bei weiteren Zugriffen dieses Kontoinformationsdienstleisters auf dieses Zahlungskonto.

(4) Hat der kontoführende Zahlungsdienstleister keine berechtigten Gründe für einen Betrugsverdacht, führen die Kontoinformationsdienstleister ihre eigene starke Kundenauthentifizierung durch, wenn die letzte starke Kundenauthentifizierung beim Zugriff des Zahlungsdienstnutzers auf die vom betreffenden Kontoinformationsdienstleister abgerufenen Zahlungskontoinformationen 180 Tage oder länger zurückliegt.

Artikel 87

Auslagerungsvereinbarungen für die Durchführung der starken Kundenauthentifizierung

Ein Zahler-Zahlungsdienstleister schließt mit seinem technischen Dienstleister für den Fall, dass dieser die Elemente der starken Kundenauthentifizierung bereitstellt und überprüft, eine Auslagerungsvereinbarung. Ein Zahler-Zahlungsdienstleister bleibt im Rahmen einer solchen Vereinbarung für jegliches Versäumnis, eine starke Kundenauthentifizierung durchzuführen, in vollem Umfang haftbar und hat das Recht, die Sicherheitsbestimmungen einer Prüfung und Kontrolle zu unterziehen.

Artikel 88

Barrierefreiheitsanforderungen für die starke Kundenauthentifizierung

(1) Unbeschadet der Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 stellen die Zahlungsdienstleister sicher, dass allen ihren Kunden, einschließlich Menschen mit Behinderungen, Älteren, Menschen mit geringen digitalen Kompetenzen und Menschen, die keinen Zugang zu digitalen Wegen oder Zahlungsinstrumenten haben, mindestens ein auf ihre besondere Situation abgestimmtes Mittel zur Verfügung steht, um eine starke Kundenauthentifizierung durchführen zu können.

(2) Die Zahlungsdienstleister dürfen die Leistungsfähigkeit der starken Kundenauthentifizierung nicht von der ausschließlichen Verwendung eines einzigen Authentifizierungsverfahrens abhängig machen und dürfen die Leistungsfähigkeit der starken Kundenauthentifizierung weder explizit noch implizit vom Besitz eines Smartphones abhängig machen. Die Zahlungsdienstleister entwickeln eine Vielfalt an Verfahren für die Durchführung der starken Kundenauthentifizierung, um der besonderen Situation all ihrer Kunden gerecht zu werden.

Artikel 89

Technische Regulierungsstandards für Authentifizierung, Kommunikation und Transaktionsüberwachungsmechanismen

(1) Die EBA arbeitet Entwürfe technischer Regulierungsstandards aus, in denen Folgendes festgelegt wird:

a) die Anforderungen für die in Artikel 85 genannte starke Kundenauthentifizierung,

b) die Ausnahmen von der Anwendung des Artikels 85 Absätze 1, 8 und 9 nach den in Artikel 85 Absatz 11 niedergelegten Kriterien,

c) die Anforderungen, die Sicherheitsmaßnahmen gemäß Artikel 85 Absatz 10 erfüllen müssen, um die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer zu schützen,

d) die gemäß Artikel 87 geltenden Anforderungen für die Auslagerungsvereinbarungen zwischen den Zahlungsdienstleistern der Zahler und den technischen Dienstleistern hinsichtlich der Bereitstellung und Überprüfung der Elemente der starken Kundenauthentifizierung durch die technischen Dienstleister,

e) die Anforderungen nach Titel III Kapitel 3 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,

f) ergänzende Bestimmungen über sichere offene Standards für die Kommunikation über dedizierte Schnittstellen;

g) die technischen Anforderungen an die in Artikel 83 genannten Transaktionsüberwachungsmechanismen.

Für die Zwecke von Buchstabe b wird mit Blick auf die Ausnahme von der Durchführung einer starken Kundenauthentifizierung bei Zahlungsvorgängen auf Basis einer Transaktionsrisikoanalyse in den Entwürfen technischer Regulierungsstandards unter anderem Folgendes festgelegt:

i) die Bedingungen, die erfüllt sein müssen, damit ein elektronischer Fernzahlungsvorgang als risikoarm gilt;

ii) die Methoden und Modelle für die Durchführung der Transaktionsrisikoanalyse;

iii) die Kriterien für die Berechnung der Betrugsraten, einschließlich der Verteilung der Betrugsraten zwischen den Zahlungsdienstleistern, die Ausgabe- und Acquiring-Dienstleistungen erbringen, oder innerhalb von Zahlungsdienstleistern, die über eine einzige juristische Person Ausgabe- und Acquiring-Dienstleistungen erbringen;

iv) detaillierte und verhältnismäßige Melde- und Prüfungsanforderungen.

(2) Bei der Ausarbeitung der in Absatz 1 genannten Entwürfe technischer Regulierungsstandards trägt die EBA Folgendem Rechnung:

a) der Notwendigkeit, ein angemessenes Sicherheitsniveau für die Zahlungsdienstnutzer und Zahlungsdienstleister sicherzustellen, indem wirksame und risikobasierte Anforderungen festgelegt werden;

b) der Notwendigkeit, die Sicherheit des Geldes und der personenbezogenen Daten der Zahlungsdienstnutzer zu gewährleisten;

c) der Notwendigkeit, fairen Wettbewerb unter allen Zahlungsdienstleistern sicherzustellen und zu erhalten;

d) der Notwendigkeit, Technologie- und Geschäftsmodellneutralität zu gewährleisten;

e) der Notwendigkeit, die Entwicklung benutzerfreundlicher, barrierefreier und innovativer Zahlungsmittel zu ermöglichen.

Die EBA übermittelt der Kommission die in Absatz 1 genannten Entwürfe technischer Regulierungsstandards bis zum [OP, bitte Datum einfügen: ein Jahr nach dem Datum des Inkrafttretens dieser Verordnung]. Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Regulierungsstandards nach den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010 zu erlassen.

(3) Gemäß Artikel 10 der Verordnung (EU) Nr. 1093/2010 überprüft die EBA die technischen Regulierungsstandards regelmäßig und aktualisiert sie gegebenenfalls, unter anderem um Innovationen und technologischen Entwicklungen sowie den Bestimmungen des Kapitels II der Verordnung (EU) 2022/2554 und den im Rahmen der Verordnung (EU) Nr. 910/2014 eingeführten EUid-Brieftaschen Rechnung zu tragen.

KAPITEL 8

Durchsetzungsverfahren, zuständige Behörden und Sanktionen

ABSCHNITT 1

BESCHWERDEVERFAHREN

Artikel 90

Beschwerden

(1) Die Mitgliedstaaten richten Verfahren ein, nach denen Zahlungsdienstnutzer und andere interessierte Parteien einschließlich Verbraucherverbänden im Falle mutmaßlicher Verstöße der Zahlungsdienstleister gegen diese Verordnung bei den für die Durchsetzung dieser Verordnung als zuständig benannten Behörden Beschwerde einlegen können.

(2) Gegebenenfalls und unbeschadet des Rechts, nach dem nationalen Verfahrensrecht die Gerichte anzurufen, informieren die zuständigen Behörden den Beschwerdeführer in ihrer Antwort auf die in Absatz 1 genannten Beschwerden über die nach Artikel 95 eingerichteten alternativen Streitbeilegungsverfahren.

Artikel 91

Zuständige Behörden und Untersuchungsbefugnisse

(1) Die zuständigen Behörden üben ihre Befugnisse zur Untersuchung potenzieller Verstöße gegen diese Verordnung und zur Verhängung von in ihrem nationalen Rechtsrahmen vorgesehenen verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen im Einklang mit dieser Verordnung auf eine der folgenden Arten aus:

a) unmittelbar,

b) in Zusammenarbeit mit anderen Behörden,

c) durch Übertragung von Befugnissen auf andere Behörden oder Stellen, wobei sie für die Überwachung der beauftragten Behörde oder Stelle verantwortlich bleiben,

d) durch Antragstellung bei den zuständigen Justizbehörden.

Übertragen die zuständigen Behörden die Ausübung ihrer Befugnisse gemäß Buchstabe c auf andere Behörden oder Stellen, so werden in der Befugnisübertragung die übertragenen Aufgaben, die Bedingungen, unter denen sie auszuführen sind, und die Bedingungen festgelegt, unter denen die Befugnisübertragung widerrufen werden kann. Die Behörden oder Stellen, auf die Befugnisse übertragen werden, müssen so organisiert sein, dass Interessenkonflikte vermieden werden. Die zuständigen Behörden überwachen die Tätigkeit der Behörden oder Stellen, denen die Befugnisse übertragen werden.

(2) Die Mitgliedstaaten benennen die für die Gewährleistung und Überwachung der tatsächlichen Einhaltung dieser Verordnung zuständigen Behörden. Diese Behörden ergreifen alle geeigneten Maßnahmen, um die Einhaltung sicherzustellen.

Die zuständigen Behörden sind entweder

a) Behörden

b) oder Stellen, die nach nationalem Recht oder durch Behörden, die nach nationalem Recht ausdrücklich hierzu befugt sind, insbesondere auch durch nationale Zentralbanken, anerkannt wurden.

Die zuständigen Behörden müssen von Wirtschaftsgremien unabhängig sein und Interessenkonflikte vermeiden. Unbeschadet des Absatzes 2 Buchstabe b dürfen Zahlungsinstitute, Kreditinstitute oder Postscheckämter nicht als zuständige Behörden benannt werden.

(3) Die in Absatz 2 genannten Behörden werden mit allen Untersuchungsbefugnissen und mit angemessenen Mitteln ausgestattet, die sie für die Wahrnehmung ihrer Aufgaben benötigen.

Zu diesen Befugnissen gehören:

a) die Befugnis, im Laufe von Verfahren zur Untersuchung potenzieller Verstöße gegen diese Verordnung alle für die Durchführung der betreffenden Untersuchung erforderlichen Informationen unter anderem von den folgenden natürlichen oder juristischen Personen einzuholen:

i) Zahlungsdienstleistern,

ii) technischen Dienstleistern und Zahlungssystembetreibern,

iii) Geldautomatenbetreibern, die keine Zahlungskonten führen,

iv) Anbietern elektronischer Kommunikationsdienste,

v) natürlichen Personen, die den unter den Ziffern i, ii und iii genannten Unternehmen angehören,

vi) Dritten, an die die unter den Ziffern i, ii und iii genannten Unternehmen betriebliche Funktionen oder Tätigkeiten ausgelagert haben,

vii) Agenten und Vertriebsstellen der unter den Ziffern i, ii und iii genannten Unternehmen und ihrer im betreffenden Mitgliedstaat niedergelassenen Zweigniederlassungen;

b) die Befugnis, alle erforderlichen Untersuchungen im Hinblick auf jede unter Buchstabe a Ziffer i bis vii genannte Person durchzuführen, die im Mitgliedstaat der zuständigen Behörde niedergelassen oder ansässig ist, sofern dies zur Wahrnehmung der Aufgaben der zuständigen Behörden erforderlich ist, einschließlich der Befugnis,

i) die Vorlage von Dokumenten zu verlangen,

ii) die Bücher und Aufzeichnungen der unter Buchstabe a Ziffer i bis vii genannten Personen zu prüfen und Kopien oder Auszüge dieser Bücher und Aufzeichnungen anzufertigen,

iii) von einer unter Buchstabe a Ziffer i bis vii genannten Person oder, sofern anwendbar, deren Vertretern oder Mitarbeitern schriftliche oder mündliche Erklärungen einzuholen,

iv) jede andere natürliche Person zu befragen, die dieser Befragung zwecks Einholung von Informationen über den Gegenstand einer Untersuchung zustimmt;

c) die Befugnis, vorbehaltlich der vorherigen Unterrichtung der betroffenen zuständigen Behörden alle erforderlichen Prüfungen in den Geschäftsräumen der unter Buchstabe a Ziffer i bis vii genannten juristischen oder natürlichen Personen durchzuführen.

(4) Sieht das Recht eines Mitgliedstaats gemäß Artikel 96 Absatz 2 strafrechtliche Sanktionen für Verstöße gegen diese Verordnung vor, so muss der betreffende Mitgliedstaat über die erforderlichen Rechts- und Verwaltungsvorschriften verfügen, die den zuständigen Behörden die Möglichkeit geben,

a) mit den zuständigen Justizbehörden in Verbindung zu treten, um spezifische Informationen über strafrechtliche Ermittlungen in Bezug auf mutmaßliche Verstöße gegen diese Verordnung, über eingeleitete Strafverfahren wegen derlei mutmaßlicher Verstöße und über das Ergebnis solcher Verfahren, einschließlich des rechtskräftigen Urteils, einzuholen;

b) diese Informationen anderen zuständigen Behörden und der EBA bereitzustellen, damit diese ihre Verpflichtung erfüllen können, für die Zwecke dieser Verordnung miteinander und mit der EBA zusammenzuarbeiten.

(5) Die Durchführung und Ausübung der in diesem Artikel festgelegten Befugnisse muss verhältnismäßig sein und im Einklang mit dem Unionsrecht und dem nationalen Recht, einschließlich der geltenden Verfahrensgarantien und der Grundsätze der Charta der Grundrechte der Europäischen Union, stehen. Die in Anwendung dieser Verordnung ergriffenen Ermittlungs- und Durchsetzungsmaßnahmen müssen der Art und dem tatsächlichen oder potenziellen Gesamtschaden des Verstoßes angemessen sein.

(6) Bis zum [OP, bitte Datum einfügen: Datum des Inkrafttretens dieser Verordnung] gibt die EBA gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 Leitlinien zu den Beschwerdeverfahren, insbesondere auch zu den Wegen für die Einreichung von Beschwerden, den von den Beschwerdeführern erbetenen Informationen und der Bekanntmachung der Gesamtanalyse der in Artikel 90 Absatz 1 genannten Beschwerden heraus.

Artikel 92

Geheimhaltungspflicht

(1) Unbeschadet der unter das nationale Strafrecht fallenden Fälle unterliegen alle Personen, die für die zuständigen Behörden tätig sind oder waren, sowie die von diesen Behörden beauftragten Sachverständigen in Bezug auf die Informationen, die mit den von den zuständigen Behörden durchgeführten Untersuchungen zusammenhängen, der beruflichen Geheimhaltungspflicht.

(2) Die gemäß Artikel 93 ausgetauschten Informationen unterliegen sowohl aufseiten der Behörde, die die Informationen weitergibt, als auch der Behörde, die sie empfängt, der beruflichen Geheimhaltungspflicht.

Artikel 93

Gerichtsbarkeit und Zusammenarbeit der zuständigen Behörden

(1) Bei Verstößen oder mutmaßlichen Verstößen gegen die Titel II und III sind die Behörden des Herkunftsmitgliedstaats des Zahlungsdienstleisters zuständig, es sei denn, es handelt sich um Agenten und Zweigniederlassungen, die auf Grundlage des Niederlassungsrechts tätig sind, in welchem Falle die Behörden des Aufnahmemitgliedstaats zuständig sind.

(2) Bei Verstößen oder mutmaßlichen Verstößen gegen die Titel II und III durch technische Dienstleister, Zahlungssystembetreiber, Geldautomatenbetreiber, die keine Zahlungskonten führen, Anbieter elektronischer Kommunikationsdienste oder deren Agenten oder Zweigniederlassungen sind die Behörden desjenigen Mitgliedstaats zuständig, in dem die betreffende Dienstleistung erbracht wird.

(3) Bei der Ausübung ihrer Untersuchungs- und Sanktionsbefugnisse, insbesondere auch in grenzüberschreitenden Fällen, arbeiten die zuständigen Behörden miteinander und mit anderen Behörden etwaiger betroffener Sektoren gemäß dem Unionsrecht und dem nationalen Recht zusammen, indem sie Informationen miteinander austauschen und die gegenseitige Amtshilfe für andere betroffene zuständige Behörden sicherstellen, soweit dies für die wirksame Durchsetzung von verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen erforderlich ist.

(4) Die in Absatz 3 genannten Behörden anderer betroffener Sektoren arbeiten mit den zuständigen Behörden zusammen, damit verwaltungsrechtliche Sanktionen und Verwaltungsmaßnahmen effektiv durchgesetzt werden.

ABSCHNITT 2

STREITBEILEGUNGSVERFAHREN UND SANKTIONEN

Artikel 94

Streitbeilegung

(1) Die Zahlungsdienstleister richten angemessene und wirksame Verfahren ein und wenden diese an, um Beschwerden von Zahlungsdienstnutzern in Bezug auf deren Rechte und Pflichten aus den Titeln II und III beizulegen. Die zuständigen Behörden wachen über die Leistungsfähigkeit dieser Verfahren.

Diese Verfahren gelten in jedem Mitgliedstaat, in dem der Zahlungsdienstleister die Zahlungsdienste anbietet, und stehen in einer Amtssprache des betreffenden Mitgliedstaats oder in einer anderen zwischen dem Zahlungsdienstleister und dem Zahlungsdienstnutzer vereinbarten Sprache zur Verfügung.

(2) Die Zahlungsdienstleister unternehmen alle erdenklichen Anstrengungen, um Beschwerden der Zahlungsdienstnutzer in Papierform oder bei entsprechender Vereinbarung zwischen Zahlungsdienstleister und Zahlungsdienstnutzer auf einem

anderen dauerhaften Datenträger zu beantworten. In dieser Antwort, die innerhalb einer angemessenen Frist, spätestens aber innerhalb von 15 Geschäftstagen nach Erhalt der Beschwerde zu erfolgen hat, ist auf alle angesprochenen Fragen einzugehen. Kann der Zahlungsdienstleister in Ausnahmefällen aus Gründen, auf die er keinen Einfluss hat, nicht innerhalb von 15 Geschäftstagen antworten, so versendet er ein vorläufiges Antwortschreiben mit klaren Angaben dazu, warum sich die Beantwortung der Beschwerde verzögert und innerhalb welcher Frist der Zahlungsdienstnutzer die endgültige Antwort erhalten wird. Die Frist für den Erhalt der endgültigen Antwort darf 35 Geschäftstage keinesfalls überschreiten.

Die Mitgliedstaaten können Vorschriften über Streitbeilegungsverfahren einführen oder beibehalten, die für den Zahlungsdienstnutzer vorteilhafter sind als die in Unterabsatz 1 genannten. Machen die Mitgliedstaaten von dieser Möglichkeit Gebrauch, gelten jene Vorschriften.

(3) Der Zahlungsdienstleister informiert den Zahlungsdienstnutzer über mindestens eine Stelle zur alternativen Streitbeilegung (im Folgenden „AS-Stelle“), die für die Beilegung von Streitigkeiten in Bezug auf die Rechte und Pflichten aus Titel II und III zuständig ist.

(4) Die in Absatz 3 genannte Information muss klar, umfassend und leicht zugänglich auf der Website des Zahlungsdienstleisters und in der betreffenden mobilen Anwendung, sofern vorhanden, in der Zweigniederlassung sowie in den Allgemeinen Bedingungen des Vertrags zwischen dem Zahlungsdienstleister und dem Zahlungsdienstnutzer angegeben werden. Der Zahlungsdienstleister gibt auch an, wo weitere Informationen über die betreffende AS-Stelle und über die Bedingungen für deren Anrufung erhältlich sind.

Artikel 95

Alternative Streitbeilegungsverfahren

(1) Die Mitgliedstaaten schaffen entsprechend den in der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates[66] festgelegten Qualitätsanforderungen nach Maßgabe der einschlägigen Vorschriften des nationalen Rechts und des Unionsrechts angemessene, unabhängige, unparteiische, transparente und wirksame alternative Streitbeilegungsverfahren für die Beilegung von Streitigkeiten zwischen Zahlungsdienstnutzern und Zahlungsdienstleistern über aus den Titeln II und III erwachsende Rechte und Pflichten, wobei gegebenenfalls auf bestehende zuständige Einrichtungen zurückgegriffen wird. Alternative Streitbeilegungsverfahren sind auf Zahlungsdienstleister anwendbar.

(2) Die in Absatz 1 genannten Einrichtungen arbeiten bei der Beilegung grenzüberschreitender Streitigkeiten über die Rechte und Pflichten aus den Titeln II und III wirksam zusammen.

---

66 Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) (ABl. L 165 vom 18.6.2013, S. 63).

(3) Die Mitgliedstaaten benennen gemäß Artikel 18 der Richtlinie 2013/11/EU eine zuständige Behörde für die Akkreditierung, die Überwachung und die öffentliche Bekanntgabe des Qualitätsniveaus der AS-Stelle(n), die in ihrem Hoheitsgebiet mit der Beilegung von Streitigkeiten über die Rechte und Pflichten aus den Titeln II und III betraut ist bzw. sind.

(4) Die in Absatz 3 genannten zuständigen Behörden melden der Kommission gemäß Artikel 20 der Richtlinie 2013/11/EU die AS-Stelle(n), die in ihrem Hoheitsgebiet mit der Beilegung von Streitigkeiten über die Rechte und Pflichten aus den Titeln II und III betraut ist bzw. sind.

(5) Die Kommission macht eine Liste der ihr gemäß Absatz 4 gemeldeten AS-Stellen öffentlich zugänglich und aktualisiert diese Liste jedes Mal, wenn Änderungen mitgeteilt werden.

Artikel 96

Verwaltungsrechtliche Sanktionen und Verwaltungsmaßnahmen

(1) Unbeschadet der Aufsichtsbefugnisse der gemäß der Richtlinie (EU) XXX (PSD3) benannten zuständigen Behörden nach Maßgabe von Titel II Kapitel 1 Abschnitt 3 jener Richtlinie und unbeschadet des Rechts der Mitgliedstaaten, strafrechtliche Sanktionen festzulegen, erlassen die Mitgliedstaaten Vorschriften über verwaltungsrechtliche Sanktionen und Verwaltungsmaßnahmen, die bei Verstößen gegen diese Verordnung anwendbar sind, und stellen sicher, dass diese umgesetzt werden. Die verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Die Mitgliedstaaten können beschließen, für Verstöße gegen diese Verordnung, die Sanktionen nach ihrem nationalen Strafrecht unterliegen, keine Vorschriften über verwaltungsrechtliche Sanktionen oder Maßnahmen zu erlassen. In diesem Fall teilen die Mitgliedstaaten der Kommission die einschlägigen strafrechtlichen Bestimmungen und alle späteren Änderungen dieser Bestimmungen gemäß Artikel 103 mit.

(3) Gelten die in Absatz 1 genannten nationalen Vorschriften für Zahlungsdienstleister und andere juristische Personen, so sind bei Verstößen und vorbehaltlich der im nationalen Recht festgelegten Bedingungen die verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen auf die Mitglieder des Leitungsorgans der betreffenden Zahlungsdienstleister sowie auf die juristischen Personen und anderen natürlichen Personen anwendbar, die für einen Verstoß gegen diese Verordnung für verantwortlich befunden werden.

(4) Die Mitgliedstaaten können im Einklang mit ihrem nationalen Recht Vorschriften erlassen, die es ihren zuständigen Behörden ermöglichen, die Untersuchung eines mutmaßlichen Verstoßes gegen diese Verordnung im Anschluss an eine Vergleichsvereinbarung oder ein beschleunigtes Durchsetzungsverfahren einzustellen.

Die Ermächtigung der zuständigen Behörden zu Vergleichsvereinbarungen oder beschleunigten Durchsetzungsverfahren lässt die Verpflichtungen der Mitgliedstaaten nach Absatz 1 unberührt.

Artikel 97

Verwaltungsrechtliche Sanktionen und andere Verwaltungsmaßnahmen für bestimmte Verstöße

(1) Unbeschadet des Artikels 96 Absatz 2 regeln die nationalen Rechts- und Verwaltungsvorschriften die in Absatz 2 des vorliegenden Artikels genannten verwaltungsrechtlichen Sanktionen und anderen Verwaltungsmaßnahmen für den Fall, dass die folgenden Bestimmungen verletzt oder umgangen werden:

a) die in Artikel 32 festgelegten Vorschriften für den Zugang zu Konten bei einem Kreditinstitut;

b) die in Titel III Kapitel 3, unbeschadet des Artikels 45, festgelegten Vorschriften für den sicheren Datenzugang entweder durch kontoführende Zahlungsdienstleister oder durch Kontoinformationsdienstleister und Zahlungsauslösedienstleister;

c) die Verpflichtung zur Organisation oder Anwendung von Mechanismen für die Betrugsprävention, einschließlich der starken Kundenauthentifizierung gemäß den Artikeln 85, 86 und 87;

d) die Pflicht zur Erfüllung der Anforderungen für die Gebührentransparenz durch Geldautomatenbetreiber oder andere Bargeldvertriebsstellen gemäß Artikel 20 Buchstabe c Ziffer ii;

e) Nichteinhaltung der Frist für die Entschädigung der Zahlungsdienstnutzer gemäß Artikel 56 Absatz 2, Artikel 57 Absatz 2 und Artikel 59 Absatz 2 durch die Zahlungsdienstleister.

(2) In den in Absatz 1 genannten Fällen müssen die anwendbaren verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen Folgendes beinhalten:

a) Geldstrafen;

i) bei juristischen Personen eine Höchstgeldstrafe von mindestens 10 % des jährlichen Gesamtumsatzes im Sinne von Absatz 3;

ii) bei natürlichen Personen eine Höchstgeldstrafe von mindestens 5 000 000 EUR oder in den Mitgliedstaaten, deren Währung nicht der Euro ist, dem Gegenwert in der Landeswährung am Tag des Inkrafttretens dieser Verordnung;

iii) eine Höchstgeldstrafe von mindestens dem Zweifachen des durch den Verstoß erzielten Gewinns, sofern sich dieser Gewinn bestimmen lässt.

b) die öffentliche Bekanntgabe der für den Verstoß verantwortlichen juristischen oder natürlichen Person und der Art des Verstoßes;

c) eine Anordnung, wonach die für den Verstoß verantwortliche juristische oder natürliche Person das rechtswidrige Verhalten einzustellen und künftig davon abzusehen hat;

d) ein vorübergehendes Verbot für die Mitglieder des Leitungsorgans der juristischen Person oder für jede andere natürliche Person, die für den Verstoß verantwortlich gemacht wird, Leitungsaufgaben wahrzunehmen.

(3) Der in Absatz 2 Buchstabe a Ziffer i dieses Artikels und in Artikel 98 Absatz 1 dieser Verordnung genannte jährliche Gesamtumsatz entspricht den Nettoumsatzerlösen im Sinne von Artikel 2 Nummer 5 der Richtlinie 2013/34/EU laut dem zum letzten Bilanzstichtag verfügbaren Jahresabschluss, für den die Mitglieder des Verwaltungs-, Leitungs- und Aufsichtsorgans der juristischen Person verantwortlich zeichnen.

Handelt es sich bei der juristischen Person um eine Muttergesellschaft oder eine Tochtergesellschaft einer Muttergesellschaft, die nach Artikel 22 der Richtlinie 2013/34/EU einen konsolidierten Abschluss zu erstellen hat, so entspricht der relevante jährliche Gesamtumsatz den Nettoumsatzerlösen oder den gemäß den einschlägigen Rechnungslegungsstandards zu bestimmenden Nettoeinnahmen laut dem zum letzten Bilanzstichtag verfügbaren konsolidierten Abschluss des obersten Mutterunternehmens, für den die Mitglieder des Verwaltungs-, Leitungs- und Aufsichtsorgans des obersten Unternehmens verantwortlich zeichnen.

(4) Die Mitgliedstaaten können die zuständigen Behörden im Einklang mit ihrem nationalen Recht ermächtigen, andere Arten von Sanktionen und andere Arten von Sanktionsbefugnissen zusätzlich zu den in Absatz 2 dieses Artikels und in Artikel 98 über Zwangsgelder genannten vorzusehen.

Artikel 98

Zwangsgelder

(1) Die zuständigen Behörden sind befugt, Zwangsgelder gegen juristische oder natürliche Personen zu verhängen, wenn diese einem Beschluss, einer Anordnung, einer vorläufigen Maßnahme, einer Aufforderung, einer Verpflichtung oder einer anderen gemäß dieser Verordnung beschlossenen Maßnahme nicht nachkommen.

Die in Unterabsatz 1 genannten Zwangsgelder müssen wirksam und verhältnismäßig sein und einen Betrag beinhalten, der täglich zu entrichten ist, bis die Regeltreue wiederhergestellt ist. Sie werden für einen Zeitraum von höchstens sechs Monaten ab dem im Beschluss über das Zwangsgeld genannten Zeitpunkt verhängt.

Die zuständigen Behörden sind befugt, als Höchststrafe Zwangsgelder in mindestens folgender Höhe zu verhängen:

a) bei juristischen Personen 3 % des durchschnittlichen Tagesumsatzes;

b) bei natürlichen Personen 30 000 EUR.

Der durchschnittliche Tagesumsatz entspricht dem in Artikel 97 Absatz 3 genannten jährlichen Gesamtumsatz, geteilt durch 365.

(2) Die Mitgliedstaaten können höhere als die in Absatz 1 festgelegten Zwangsgelder vorsehen.

Artikel 99

Faktoren, die bei der Festlegung verwaltungsrechtlicher Sanktionen und anderer Verwaltungsmaßnahmen zu berücksichtigen sind

(1) Die zuständigen Behörden berücksichtigen bei der Festlegung von Art und Höhe der verwaltungsrechtlichen Sanktionen und anderen verwaltungsrechtlichen Maßnahmen alle relevanten Faktoren und Umstände, damit die angewandten Sanktionen verhältnismäßig sind, insbesondere auch

a) die Schwere und Dauer des Verstoßes;

b) den Grad an Verantwortung der für den Verstoß verantwortlichen natürlichen oder juristischen Person;

c) die Finanzkraft der für den Verstoß verantwortlichen natürlichen oder juristischen Person, wie sie sich unter anderem am jährlichen Gesamtumsatz der juristischen Person oder den Jahreseinkünften der natürlichen Person, die für den für den Verstoß verantwortlich ist, ablesen lässt;

d) die Größenordnung der durch den Verstoß von der für den Verstoß verantwortlichen natürlichen oder juristischen Person erzielten Gewinne oder vermiedenen Verluste, sofern sie sich bestimmen lassen;

e) die Verluste, die Dritten durch den Verstoß verursacht wurden, sofern sie sich bestimmen lassen,

f) den Nachteil, der der für den Verstoß verantwortlichen juristischen oder natürlichen Person dadurch entsteht, dass für ein und dasselbe Verhalten sowohl strafrechtliche als auch verwaltungsrechtliche Verfahren und Sanktionen greifen;

g) die Auswirkungen des Verstoßes auf die Interessen von Verbrauchern und anderen Zahlungsdienstnutzern;

h) alle tatsächlichen oder potenziellen nachteiligen Auswirkungen des Verstoßes auf das Finanzsystem;

i) die Mittäterschaft oder Beteiligung von mehr als einer natürlichen oder juristischen Person an dem Verstoß;

j) frühere Verstöße durch die für den Verstoß verantwortlichen natürlichen oder juristischen Person;

k) die Bereitschaft der für den Verstoß verantwortlichen natürlichen oder juristischen Person zur Zusammenarbeit mit der zuständigen Behörde;

l) Abhilfemaßnahmen oder Handlungen der für den Verstoß verantwortlichen juristischen oder natürlichen Person mit dem Ziel, eine Wiederholung des Verstoßes zu verhindern.

(2) Zuständige Behörden, die nach Artikel 96 Absatz 4 Vergleichsvereinbarungen oder beschleunigte Durchsetzungsverfahren nutzen, passen die in den Artikeln 96, 97 und 98 festgelegten einschlägigen verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen an den betreffenden Fall an, um die Verhältnismäßigkeit der Sanktionen und Verwaltungsmaßnahmen sicherzustellen.

Artikel 100

Rechtsmittel

(1) Die gemäß dieser Verordnung ergangenen Beschlüsse der zuständigen Behörden können gerichtlich angefochten werden.

(2) Absatz 1 findet auch bei Untätigkeit Anwendung.

Artikel 101

Öffentliche Bekanntmachung von verwaltungsrechtlichen Sanktionen und Verwaltungsmaßnahmen

(1) Die zuständigen Behörden veröffentlichen auf ihrer Website alle Beschlüsse zur Verhängung von verwaltungsrechtlichen Sanktionen oder Verwaltungsmaßnahmen gegen juristische und natürliche Personen wegen Verstößen gegen diese Verordnung sowie gegebenenfalls alle Vergleichsvereinbarungen. Die öffentliche Bekanntmachung beinhaltet eine kurze Beschreibung des Verstoßes, der verhängten verwaltungsrechtlichen Sanktion oder anderen Verwaltungsmaßnahme oder gegebenenfalls eine Erklärung über die Vergleichsvereinbarung. Die Identität der natürlichen Person, die Gegenstand des Beschlusses zur Verhängung einer verwaltungsrechtlichen Sanktion oder Verwaltungsmaßnahme ist, wird nicht veröffentlicht.

Die zuständigen Behörden veröffentlichen den in Unterabsatz 1 genannten Beschluss und die in Unterabsatz 1 genannte Erklärung sofort, nachdem die juristische oder natürliche Person, die Gegenstand des Beschlusses ist, von dem betreffenden Beschluss in Kenntnis gesetzt oder die Vergleichsvereinbarung unterzeichnet wurde.

(2) Abweichend von Absatz 1 kann die zuständige nationale Behörde in Fällen, in denen die zuständige nationale Behörde die öffentliche Bekanntmachung der Identität oder anderer personenbezogener Daten natürlicher Personen für erforderlich hält, um die Stabilität der Finanzmärkte zu schützen oder die wirksame Durchsetzung dieser Verordnung zu gewährleisten, auch im Falle von in Artikel 97 Absatz 2 Buchstabe b genannten öffentlichen Bekanntgaben oder in Artikel 97 Absatz 2 Buchstabe d genannten vorübergehenden Verboten die Identität der Personen oder personenbezogenen Daten veröffentlichen, sofern sie diesen Beschluss begründet und sich die öffentliche Bekanntmachung auf die personenbezogenen Daten beschränkt, die zwingend erforderlich sind, um die Stabilität der Finanzmärkte zu schützen oder die wirksamen Durchsetzung dieser Verordnung sicherzustellen.

(3) Wird der Beschluss zur Verhängung einer verwaltungsrechtlichen Sanktion oder anderen Verwaltungsmaßnahme vor der einschlägigen Justiz- oder einer sonstigen Behörde angefochten, veröffentlichen die zuständigen Behörden auch diesen Sachverhalt und alle weiteren Informationen über das Ergebnis der Anfechtung auf ihrer offiziellen Website unverzüglich, sofern juristische Personen davon betroffen sind. Betrifft der angefochtene Beschluss eine natürliche Person und kommt nicht die abweichende Regelung nach Absatz 2 zur Anwendung, veröffentlichen die zuständigen Behörden die Informationen über die Anfechtung nur in anonymisierter Form.

(4) Die zuständigen Behörden stellen sicher, dass öffentliche Bekanntmachungen nach diesem Artikel bis zu fünf Jahre lang auf ihrer offiziellen Website bleiben. Enthält die öffentliche Bekanntmachung personenbezogene Daten, so bleiben diese nur dann auf der offiziellen Website der zuständigen Behörde einsehbar, wenn eine jährliche Überprüfung ergibt, dass diese Daten öffentlich einsehbar bleiben müssen, um die Stabilität der Finanzmärkte zu schützen oder die wirksame Durchsetzung dieser Verordnung sicherzustellen, auf keinen Fall aber länger als fünf Jahre.

Artikel 102

Überwachung von Verfahren, Sanktionen und Maßnahmen

(1) Die zuständigen Behörden melden der EBA anonymisiert und aggregierter Form regelmäßig

a) die eingeleiteten, ausgesetzten oder abgeschlossenen Verwaltungsverfahren, die zur Verhängung von verwaltungsrechtlichen Sanktionen oder Verwaltungsmaßnahmen geführt haben;

b) die Zwangsgelder, die nach Artikel 98 wegen laufender Verstöße gegen diese Verordnung verhängt worden sind;

c) falls anwendbar, die Vergleichsvereinbarungen und beschleunigten Durchsetzungsverfahren sowie deren Ergebnis, unabhängig von ihrer öffentlichen Bekanntmachung, nach Artikel 96 Absatz 4;

d) die von den Justizbehörden gemäß Artikel 91 Absatz 4 Buchstabe a gemeldeten strafrechtlichen Verfahren, die zu einer Verurteilung und damit verbundenen Sanktionen geführt haben;

e) etwaige Anfechtungen von Beschlüssen zur Verhängung von strafrechtlichen oder verwaltungsrechtlichen Sanktionen oder Verwaltungsmaßnahmen und das Ergebnis einer solchen Anfechtung.

(2) Macht die zuständige Behörde eine verwaltungsrechtliche Sanktion oder eine Verwaltungsmaßnahme öffentlich bekannt, meldet sie diese gleichzeitig der EBA.

(3) Innerhalb von zwei Jahren nach dem Geltungsbeginn dieser Verordnung und sodann alle zwei Jahre übermittelt die EBA der Kommission einen Bericht über die Anwendung von Sanktionen durch die zuständigen Behörden zur Gewährleistung der Einhaltung dieser Verordnung.

Artikel 103

Mitteilung der Durchführungsmaßnahmen

Die Mitgliedstaaten teilen der Kommission bis zum [OP, bitte Datum einfügen = Datum des Inkrafttretens dieser Verordnung] die Rechts- und Verwaltungsvorschriften, einschließlich aller einschlägigen strafrechtlichen Bestimmungen, mit, die sie gemäß diesem Kapitel erlassen haben. Die Mitgliedstaaten teilen der Kommission jede spätere Änderung dieser Rechts- und Verwaltungsvorschriften unverzüglich mit.

KAPITEL 9

Produktinterventionsbefugnisse der EBA

Artikel 104

Befugnisse der EBA zur vorübergehenden Intervention

(1) Gemäß Artikel 9 Absatz 5 der Verordnung (EU) Nr. 1093/2010 kann die EBA, wenn die in den Absätzen 2 und 3 des vorliegenden Artikels genannten Bedingungen erfüllt sind, eine bestimmte Art von Zahlungsdienst oder -instrument oder E-Geld-Dienst oder -Instrument oder ein bestimmtes Merkmal eines solchen Dienstes oder Instruments in der Union vorübergehend verbieten oder beschränken. Ein Verbot oder eine Beschränkung kann in Fällen oder vorbehaltlich von Ausnahmen zur Anwendung kommen, die von der EBA festgelegt werden.

(2) Die EBA fasst einen Beschluss nach Absatz 1 nur dann, wenn die folgenden Bedingungen erfüllt sind:

a) die vorgeschlagene Maßnahme richtet sich an eine signifikante Zahl von Zahlungsdienstnutzern oder E-Geld-Dienstnutzern oder gegen eine Bedrohung für die geordnete Funktionsweise der Zahlungs- oder E-Geld-Märkte und für die Integrität dieser Märkte oder die Stabilität der Gesamtheit oder eines Teils dieser Märkte in der Union;

b) die nach dem Unionsrecht auf den jeweiligen Zahlungsdienst oder E-Geld-Dienst anwendbaren Regulierungsanforderungen werden der Bedrohung nicht gerecht;

c) eine oder mehrere zuständige Behörden haben keine Maßnahmen ergriffen, um der Bedrohung zu begegnen, oder die ergriffenen Maßnahmen werden der Bedrohung nicht ausreichend gerecht.

Sind die in Unterabsatz 1 genannten Bedingungen erfüllt, kann die EBA das in Absatz 1 genannte Verbot oder die in Absatz 1 genannte Beschränkung vorsorglich verhängen, bevor ein Zahlungsdienst oder ein E-Geld-Dienst angeboten oder an Zahlungsdienstnutzer vertrieben wird.

(3) Bei Maßnahmen gemäß diesem Artikel hat die EBA alles Folgende sicherzustellen:

a) die Maßnahme darf keine nachteiligen Auswirkungen auf die Effizienz des Zahlungsmarkts oder des E-Geld-Dienstemarkts oder auf Zahlungsdienste oder E-Geld-Dienstleister haben, die gemessen am Nutzen der Maßnahme unverhältnismäßig sind;

b) die Maßnahmen darf kein Risiko der Aufsichtsarbitrage schaffen und

c) vor der Maßnahme muss die jeweils zuständige nationale Behörde konsultiert worden sein.

(4) Bevor die EBA beschließt, Maßnahmen nach diesem Artikel zu ergreifen, unterrichtet sie die zuständigen Behörden über ihr geplantes Vorgehen.

(5) Die EBA gibt jeden Beschluss, im Sinne dieses Artikels Maßnahmen zu ergreifen, auf ihrer Website bekannt. In der Bekanntmachung sind die Einzelheiten des Verbots oder der Beschränkung sowie der Zeitpunkt anzugeben, ab dem die Maßnahmen im Anschluss an die Bekanntmachung wirksam werden, wobei zugleich sicherzustellen ist, dass Bekanntmachungen von Beschlüssen, die natürliche Personen betreffen, nur anonymisiert veröffentlicht werden. Ein Verbot oder eine Beschränkung gilt erst für Handlungen, die nach Wirksamwerden der Maßnahmen vorgenommen werden.

(6) Die EBA überprüft ein Verbot oder eine Beschränkung nach Absatz 1 in angemessenen Zeitabständen, mindestens jedoch alle drei Monate. Wird das Verbot oder die Beschränkung nach Ablauf dieser Dreimonatsfrist nicht verlängert, endet die Gültigkeit automatisch.

(7) Eine gemäß diesem Artikel beschlossene Maßnahme der EBA erhält Vorrang vor allen etwaigen früheren Maßnahmen einer zuständigen Behörde.

(8) Die Kommission erlässt delegierte Rechtsakte nach Artikel 106 zur Festlegung der Kriterien und Faktoren, die von der EBA zu berücksichtigen sind, wenn diese ermittelt, ob im Sinne von Absatz 2 Buchstabe a eine signifikante Zahl von Zahlungsdienstnutzern oder E-Geld-Dienstnutzern oder eine Bedrohung für die geordnete Funktionsweise der Zahlungs- oder E-Geld-Dienstemärkte und für die Integrität dieser Märkte oder die Stabilität der Gesamtheit oder eines Teils dieser Märkte in der Union vorliegt.

Zu diesen Kriterien und Faktoren gehören:

a) die Komplexität eines Zahlungsdienstes oder -instruments oder eines E-Geld-Dienstes oder -Instruments und die Beziehung zu der Art von Nutzern, insbesondere auch Verbrauchern, denen sie angeboten werden;

b) der Risikogehalt eines Zahlungsdienstes oder -instruments oder eines E-Geld-Dienstes oder -Instruments für die Verbraucher;

c) die mögliche Nutzung des Zahlungsdienstes oder -instruments oder des E-Geld-Dienstes oder -Instruments durch Betrüger;

d) die Größenordnung oder der Grad der Nutzung des Zahlungsdienstes oder -instruments oder des E-Geld-Dienstes oder -Instruments;

e) der Innovationsgehalt eines Zahlungsdienstes oder -instruments oder eines E-Geld-Dienstes oder -Instruments.

TITEL IV

DELEGIERTE RECHTSAKTE

Artikel 105

Delegierte Rechtsakte

Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte nach Artikel 106 zu erlassen, um diese Verordnung durch Aktualisierung der in Artikel 58 Absatz 1 genannten Beträge zu ändern.

Artikel 106

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 105 wird der Kommission auf unbestimmte Zeit ab dem Datum des Inkrafttretens dieser Verordnung übertragen.

(3) Die Befugnisübertragung gemäß Artikel 105 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 105 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

TITEL V

SCHLUSSBESTIMMUNGEN

Artikel 107

Günstigere Erstattungsansprüche und strengere Betrugsbekämpfungsmaßnahmen

(1) Die Mitgliedstaaten oder Zahlungsdienstleister können den Zahlungsdienstnutzern günstigere Erstattungsansprüche für autorisierte Überweisungen im Sinne der Artikel 57 und 59 einräumen und strengere Betrugsbekämpfungsmaßnahmen vorsehen, die über die in Artikel 83Absatz 1 und Artikel 84 festgelegten hinausgehen.

(2) Die Mitgliedstaaten teilen der Kommission bis zum [OP, bitte Datum einfügen = Datum des Inkrafttretens dieser Verordnung] die Vorschriften mit, die sie gemäß

Absatz 1 erlassen haben. Sie teilen der Kommission jede spätere Änderung unverzüglich mit.

Artikel 108

Überprüfungsklausel

(1) Die Kommission legt spätestens fünf Jahre nach dem Geltungsbeginn dieser Verordnung dem Europäischen Parlament, dem Rat, der EZB und dem Europäischen Wirtschafts- und Sozialausschuss einen Bericht über die Anwendung und die Auswirkungen dieser Verordnung und insbesondere über folgende Aspekte vor:

a) die Angemessenheit und die Auswirkungen der Vorschriften für den Zugang zu Zahlungskontodaten sowie die Geschäftstätigkeit von Kontoinformationsdiensten und Zahlungsauslösediensten und insbesondere der Vorschriften über dedizierte Schnittstellen und der zugehörigen Ausnahmeregelungen gemäß den Artikeln 38 und 39 auf den Wettbewerb und die Nutzung von Open Banking;

b) die Auswirkungen der Vorschriften nach Artikel 34, wonach keine vertraglichen Vereinbarungen bestehen müssen und der Zugang von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern zu Schnittstellen kostenfrei möglich sein muss;

c) die Angemessenheit und die Auswirkungen der Vorschriften über Entgelte, insbesondere auch über Entgeltaufschläge, nach Artikel 28;

d) die Angemessenheit und die Auswirkungen der Vorschriften über die Betrugsprävention und die Regressmöglichkeiten bei Betrug sowohl im Falle autorisierter als auch nicht autorisierter Zahlungsvorgänge.

Gegebenenfalls fügt die Kommission diesem Bericht einen Gesetzgebungsvorschlag bei.

(2) Die Kommission legt dem Europäischen Parlament, Rat, der EZB und dem Europäischen Wirtschafts- und Sozialausschuss bis zum [OP, bitte Datum einfügen: drei Jahre nach dem Datum des Inkrafttretens dieser Verordnung] einen Bericht über den Anwendungsbereich dieser Verordnung, insbesondere mit Blick auf Zahlungssysteme, Zahlverfahren und technische Dienstleister vor. Gegebenenfalls fügt die Kommission diesem Bericht einen Gesetzgebungsvorschlag bei.

Artikel 109

Änderung der Verordnung (EU) Nr. 1093/2010

Die Verordnung (EU) Nr. 1093/2010 wird wie folgt geändert:

1. Artikel 1 Absatz 2 Satz 1 erhält folgende Fassung:

„Die Behörde handelt im Rahmen der ihr durch diese Verordnung übertragenen Befugnisse und innerhalb des Anwendungsbereichs der Richtlinie 2002/87/EG, der Richtlinie 2008/48/EG[1], der Richtlinie 2009/110/EG, der Verordnung (EU) Nr. 575/2013[2], der Richtlinie 2013/36/EU[3], der Richtlinie 2014/49/EU[4], der Richtlinie 2014/92/EU[5], der

Richtlinie (EU) [...] (PSD3), der Verordnung (EU) [...] (PSR) des Europäischen Parlaments und des Rates und, soweit diese Gesetzgebungsakte sich auf Kredit- und Finanzinstitute sowie die zuständigen Behörden, die diese beaufsichtigen, beziehen, der einschlägigen Teile der Richtlinie 2002/65/EG, einschließlich sämtlicher Richtlinien, Verordnungen und Beschlüsse, die auf der Grundlage dieser Gesetzgebungsakte angenommen wurden, sowie aller weiteren verbindlichen Rechtsakte der Union, die der Behörde Aufgaben übertragen."

2. Artikel 4 Absatz 2 wird wie folgt geändert:

a) Ziffer i erhält folgende Fassung:

„zuständige Behörden oder Aufsichtsbehörden innerhalb des Anwendungsbereichs der in Artikel 1 Absatz 2 genannten sektoralen Rechtsakte, einschließlich der Europäischen Zentralbank in Bezug auf Angelegenheiten, die die ihr durch die Verordnung (EU) Nr. 1024/2013 übertragenen Aufgaben betreffen;"

b) Die Ziffern iii, vi, vii und viii werden gestrichen.

Artikel 110

Änderung der Verordnung (EU) Nr. 2017/2394

Im Anhang der Verordnung (EU) 2017/2394 wird folgende Nummer angefügt:

„29. Verordnung (EU) xxxx des Europäischen Parlaments und des Rates vom xxxx über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/2010."

Artikel 111

Entsprechungstabelle

Bezugnahmen auf die Richtlinie (EU) 2015/2366 und die Richtlinie 2009/110/EG gelten als Bezugnahmen auf die Richtlinie (EU) (PSD3) oder die vorliegende Verordnung und sind nach Maßgabe der Entsprechungstabelle in Anhang III der vorliegenden Verordnung zu lesen.

Artikel 112

Inkrafttreten und Geltungsbeginn

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem … [Amt für Veröffentlichungen, bitte Datum einfügen: 18 Monate nach dem Datum des Inkrafttretens dieser Verordnung].

Die Artikel 50 und 57 gelten jedoch ab dem [Amt für Veröffentlichungen, bitte Datum einfügen: 24 Monate nach dem Datum des Inkrafttretens dieser Verordnung].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident // Die Präsidentin*