Rat der
Europäischen Union

Brüssel, den 4. November 2026
(OR. en)

8543/1/26
REV 1

Interinstitutionelles Dossier:
2023/0210(COD)

EF 129
ECOFIN 524
CODEC 759
ECB
PARLNAT

GESETZGEBUNGSAKTE UND ANDERE RECHTSINSTRUMENTE

Betr.:	Standpunkt des Rates in erster Lesung für den Erlass der VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 260/2012, (EU) 2017/2394 und (EU) 2021/1230 – Vom Rat am 29. Oktober 2026 angenommen

VERORDNUNG (EU) 2026/…
DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom …

über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 260/2012, (EU) 2017/2394 und (EU) 2021/1230

(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 der Europäischen Zentralbank[1],

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[2],

gemäß dem ordentlichen Gesetzgebungsverfahren[3],

---

1 ABl. C, C/2024/3869, 19.6.2024, ELI: http://data.europa.eu/eli/C/2024/3869/oj.
2 ABl. C, C/2024/1594, 5.3.2024, ELI: http://data.europa.eu/eli/C/2024/1594/oj.
3 Standpunkt des Europäischen Parlaments vom 23. April 2024 (ABl. C, C/2025/3725, 17.9.2025, ELI: http://data.europa.eu/eli/C/2025/3725/oj) und Standpunkt des Rates in erster Lesung vom 29. Oktober 2026 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom … (noch nicht im Amtsblatt veröffentlicht).

in Erwägung nachstehender Gründe:

(1) Seit der Annahme der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates[4] hat sich der Markt für Massenzahlungsdienste vor allem durch die zunehmende Nutzung von Karten und digitalen Zahlungsmitteln, die abnehmende Verwendung von Bargeld und die zunehmende Präsenz neuer Akteure und Dienste, einschließlich digitaler Brieftaschen (Digital Wallets) 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 vom 24. September 2020 über eine EU-Strategie für den Massenzahlungsverkehr 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.

---

[4] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(3) Mit der Richtlinie (EU) 2015/2366 wurde das Ziel verfolgt, Hindernisse für neue Arten von Zahlungsdiensten zu beseitigen und das Niveau des Verbraucherschutzes und der Sicherheit zu verbessern. Die Bewertung der Auswirkungen und der Anwendung der Richtlinie (EU) 2015/2366 durch die Kommission hat ergeben, 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 der genannten Richtlinie nicht 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 durch Open-Banking-Dienste, d.h. 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 dieser 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 der Auswirkungen und der Anwendung der Richtlinie (EU) 2015/2366 wurden auch Probleme im Zusammenhang mit der unterschiedlichen Umsetzung und Durchsetzung der genannten Richtlinie festgestellt, die sich unmittelbar auf den Wettbewerb zwischen Zahlungsdienstleistern ausgewirkt haben, indem sie in den Mitgliedstaaten zu faktisch unterschiedlichen Regulierungsbedingungen geführt haben, was die Aufsichtsarbitrage begünstigt. Es sollte keinen Raum für die Wahl des günstigsten Gerichtsstands (sog. „Forum-Shopping“) geben, bei dem sich ein Zahlungsdienstleister als Herkunftsland einen Mitgliedstaat aussuchen würde, in dem die Anwendung der Unionsvorschriften über Zahlungsdienste für ihn vorteilhafter ist, und gleichzeitig grenzüberschreitende Dienste in Mitgliedstaaten erbringen würde, die die Vorschriften strenger auslegen oder aktivere Durchsetzungsmaßnahmen in Bezug auf dort niedergelassene Zahlungsdienstleister anwenden. Diese Praxis verzerrt den Wettbewerb. Die Unionsvorschriften über Zahlungsdienste sollten daher weiter harmonisiert werden, indem Vorschriften über die Ausübung von Zahlungsdiensttätigkeiten, 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 klarer und detaillierter formuliert werden, um die Auslegungsspielräume so klein wie möglich zu halten.

(5) Während die Ausgabe von E-Geld durch die Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates[5] 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 externe 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 und die Eigenmittel, und einige grundlegende Schlüsselkonzepte für das E-Geld-Geschäft, wie z. B. die Ausgabe, der Vertrieb und der Rücktausch von E-Geld, von den von Zahlungsinstituten erbrachten Dienstleistungen. Diese Besonderheiten sollten daher bei der Zusammenführung der Bestimmungen der Richtlinie 2009/110/EG und der Richtlinie (EU) 2015/2366 beibehalten werden. Da die Richtlinie 2009/110/EG durch die Richtlinie (EU) 2026/… des Europäischen Parlaments und des Rates[6+] aufgehoben wird, sollten ihre Vorschriften, mit Ausnahme der Zulassungs- und Aufsichtsvorschriften, die in die Richtlinie (EU) 2026/…[++] aufgenommen wurden, mit geeigneten Anpassungen in einen einheitlichen Rahmen gemäß der vorliegenden Verordnung gebracht werden.

---

5 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, ELI: http://data.europa.eu/eli/dir/2009/110/oj).

6 Richtlinie (EU) 2026/… des Europäischen Parlaments und des Rates vom … über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinie 98/26/EG und der Verordnung (EU) 2023/1114 sowie zur Aufhebung der Richtlinien 2009/110/EG und (EU) 2015/2366 (ABl. L …, ELI: …).

\+ ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen und die entsprechenden Angaben in der Fußnote vervollständigen.

\++ ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(6) Um Rechtssicherheit und einen klaren Anwendungsbereich der für die Erbringung von Zahlungsdiensten und E-Geld-Diensten geltenden Regeln sicherzustellen, ist es erforderlich, die Kategorien von Zahlungsdienstleistern zu spezifizieren, die den Pflichten in Bezug auf die 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 werden gemäß der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates[7] zugelassen. Zahlungsinstitute dürfen keine Einlagen entgegennehmen. Sie können Geldbeträge der Nutzer halten und E-Geld ausgeben, das zur Ausführung von Zahlungsvorgängen verwendet werden kann. Sie werden gemäß der Richtlinie (EU) 2026/…[+] zugelassen. Postscheckämter, die nach nationalem 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.

---

[7] 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, 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, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(8) Die Ausnahme vom Anwendungsbereich der Richtlinie (EU) 2015/2366 für bestimmte Kategorien von Betreibern von Geldautomaten hat sich in der Praxis als schwer anwendbar erwiesen. Daher sollte die Kategorie der Geldautomatenbetreiber, die gemäß der Richtlinie (EU) 2015/2366 von der Anforderung einer Zulassung als Zahlungsdienstleister ausgenommen war, durch eine neue Kategorie von Geldautomatenbetreibern ersetzt werden, die keine Zahlungskonten führen. Diese Betreiber, die der Registrierung nach der Richtlinie (EU) 2026/…[+] unterliegen, sollten dann, wenn diese Geldautomatenbetreiber für Bargeldabhebungen Entgelte erheben, den Anforderungen an die Gebührentransparenz unterliegen.

(9) Um den Zugang zu Bargeld weiter zu verbessern, sollte es Einzelhändlern gestattet sein, im stationären Handel Bargeldabhebungsdienste anzubieten, auch wenn der Kunde keinen Kauf tätigt, ohne dass die Einzelhändler eine Zulassung oder Registrierung als Zahlungsdienstleister einholen oder als Agent eines Zahlungsinstituts auftreten müssen. Diese Bargeldabhebungsdienste sollten jedoch der Verpflichtung unterliegen, dem Kunden alle in Rechnung gestellten Gebühren offenzulegen. Diese Dienstleistungen sollten von Einzelhändlern auf freiwilliger Basis erbracht werden und von der Verfügbarkeit von Bargeld beim betreffenden Einzelhändler abhängen.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(10) Die Ausnahme vom Anwendungsbereich der Richtlinie (EU) 2015/2366 für Zahlungsvorgänge vom Zahler an den Zahlungsempfänger über einen im Auftrag des Zahlers oder des Zahlungsempfängers handelnden Handelsagenten wurde in den Mitgliedstaaten sehr unterschiedlich angewandt. Der Begriff des Handelsagenten wird in der Regel im nationalen Zivilrecht definiert, das von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein kann, was zu einer uneinheitlichen Behandlung derselben Dienstleistungen in verschiedenen Rechtsordnungen führt. Der Begriff des Handelsagenten, der unter diese Ausnahme fällt, sollte daher harmonisiert werden. Darüber hinaus sollte mehr Klarheit darüber geschaffen werden, unter welchen Bedingungen Zahlungsvorgänge vom Zahler an den Zahlungsempfänger über Handelsagenten vom Anwendungsbereich dieser Verordnung ausgenommen werden können. Zu diesem Zweck sollten die Handelsagenten durch eine Vereinbarung mit dem Zahler oder dem Zahlungsempfänger ermächtigt werden, den Verkauf oder den Kauf von Waren oder Dienstleistungen allein im Namen des Zahlers oder des Zahlungsempfängers, aber nicht im Namen beider, auszuhandeln oder abzuschließen, unabhängig davon, ob der Handelsagent im Besitz von Geldbeträgen des Kunden ist oder nicht. Plattformen für den elektronischen Geschäftsverkehr, die sowohl für einzelne Käufer als auch für Verkäufer als Handelsagent fungieren, ohne dass die Parteien über einen tatsächlichen Spielraum 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 durch die Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates[8] errichtete Europäische Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde) (EBA) sollte Leitlinien für die Ausnahme von Zahlungsvorgängen vom Zahler an den Zahlungsempfänger über einen Handelsagenten ausarbeiten, um für mehr Klarheit und Konvergenz zwischen den zuständigen Behörden zu sorgen. Diese Leitlinien könnten ein Verzeichnis der Anwendungsfälle umfassen, die in der Regel unter die Ausnahme für Handelsagenten fallen.

---

[8] 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

(11) Die Ausnahme vom Anwendungsbereich der Richtlinie (EU) 2015/2366 für Instrumente mit bestimmtem Verwendungszweck wurde in den Mitgliedstaaten unterschiedlich angewandt, obwohl Dienstleister, deren Instrumente unter diese Ausnahme fielen, verpflichtet waren, ihre Tätigkeit den zuständigen Behörden zu melden. Die EBA hat in ihren Leitlinien vom 24. Februar 2022 weitere Orientierungshilfen gegeben. Trotz dieser Versuche, die Anwendung der Ausnahme für Instrumente mit bestimmtem Verwendungszweck zu klären, gibt es nach wie vor Dienstleister, die beabsichtigen, von dieser Ausnahme Gebrauch zu machen, obwohl sie Dienste anbieten, die erhebliche Zahlungsvolumen und eine Vielzahl von Produkten, die einer großen Zahl von Kunden angeboten werden, mit sich bringen. In diesen Fällen profitieren die Verbraucher nicht von den erforderlichen Schutzvorkehrungen, und die betreffenden Dienste sollten nicht von der Ausnahme für Instrumente mit bestimmtem Verwendungszweck profitieren. Daher muss klargestellt werden, dass dasselbe Instrument mit bestimmtem Verwendungszweck nicht für die Durchführung von Zahlungsvorgängen zum Erwerb von Waren und Dienstleistungen innerhalb von mehr als einem begrenzten Netzwerk oder zum Erwerb eines unbegrenzten Waren- oder Dienstleistungsspektrums verwendet werden kann.

(12) Um zu beurteilen, ob ein begrenztes Netzwerk vom Anwendungsbereich dieser Verordnung ausgenommen ist, sollten die geografische Lage und die Zahl der Akzeptanzstellen dieses Netzwerks berücksichtigt werden. Instrumente mit bestimmtem Verwendungszweck sollten es dem Inhaber ermöglichen, Waren oder Dienstleistungen nur in den stationären Verkaufsstellen oder Online-Shops des Emittenten zu erwerben. Zu den Instrumenten mit bestimmtem Verwendungszweck sollten je nach den jeweiligen vertraglichen Regelungen Karten gehören, die nur in einer Ladenkette 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 könnten, um die in der Sozialgesetzgebung festgelegten Ziele zu erreichen, wie etwa Kinderbetreuungsgutscheine oder Gutscheine für ökologische Waren oder Dienstleistungen. Gleichzeitig sollte durch das Regelungsumfeld der Mitgliedstaaten für Gutscheine die Akzeptanz derartiger Gutscheine sichergestellt werden. Instrumente mit bestimmtem Verwendungszweck sollten auch E-Geld-basierte Instrumente umfassen, sobald sie die Anforderungen der 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 Netzwerk von Dienstleistern gedacht sind.

(13) Die Ausnahme für bestimmte 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 Verbraucher andernfalls in Form von Papiertickets erwerben würden, unter anderem in den Bereichen Beförderung, Unterhaltung, Parken und Eintritt zu Veranstaltungen, jedoch mit Ausnahme körperlicher Waren. Zahlungsvorgänge, die von einem bestimmten Anbieter elektronischer Kommunikationsnetze von oder über ein elektronisches Gerät ausgeführt und auf der entsprechenden Rechnung für die Entgegennahme gemeinnütziger Spenden verbucht werden, sollten ebenfalls ausgenommen werden. Diese Ausnahme sollte nur dann gelten, wenn der Wert von Zahlungsvorgängen unter einem bestimmten Schwellenwert liegt. Damit die Ausnahme gilt, sollte der Telekommunikationsbetreiber die Zahlungsdienste zusätzlich zu den elektronischen Kommunikationsdiensten erbringen, die er seinen Teilnehmern erbringt. Dies setzt voraus, dass zwischen dem Telekommunikationsbetreiber und dem Teilnehmer eine direkte vertragliche Vereinbarung über die Erbringung der elektronischen Kommunikationsdienste besteht und dass der Zahlungsdienst eine Zusatzleistung zu diesen Diensten darstellt. Es gibt Situationen, in denen ein Anbieter digitaler Inhalte oder ein Anbieter von Diensten, für die der Teilnehmer über seinen eigenen Telekommunikationsbetreiber bezahlt hat, weitere Diensteanbieter (im Folgenden „zwischengeschaltete Stellen“) für die Einziehung und den Transfer der Geldbeträge in Anspruch nimmt. Auch wenn diese zwischengeschalteten Stellen, darunter Empfängerbetreiber, Betreiber für den Forderungseinzug und Transitbetreiber, auch elektronische Kommunikationsdienste erbringen können, können sie nicht von der Ausnahme profitieren, da sie in Bezug auf die Erbringung von elektronischen Kommunikationsdiensten in keinem direkten Vertragsverhältnis zu dem Teilnehmer stehen.

(14) 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 und damit verbundene Dienstleistungen 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, einschließlich der Weiterverteilung von Geldbeträgen, die sie von externen Dritten im Namen von Gruppenunternehmen erhalten haben, durch gruppeninterne Zahlungsvorgänge, sowie des Einzugs von Zahlungsaufträgen und von Geldbeträgen im Namen der Gruppe durch ein Mutterunternehmen oder dessen Tochterunternehmen zur Weiterleitung und Abwicklung an einen Zahlungsdienstleister, der Zahlungsdienste für die Gruppe erbringt. Soweit Betreiber eines öffentlichen Dienstes im Sinne der Verordnung (EG) Nr. 1370/2007 des Europäischen Parlaments und des Rates[9] Ausgleichszahlungen und die Aufteilung der Einnahmen innerhalb eines geschlossenen Zahlungsabwicklungssystems von Verkehrsunternehmen oder über ihre Clearingstellen, Tariforganisationen oder Verbände abwickeln, sollten diese Zahlungsvorgänge ebenfalls vom Anwendungsbereich der vorliegenden Verordnung ausgenommen werden. Diese Ausnahmen sollten nicht dazu genutzt werden, das Unionsrecht oder das nationale Recht im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung oder die Vorschriften über die Zulassung und Beaufsichtigung von Zahlungsinstituten zu umgehen.

---

[9] Verordnung (EG) Nr. 1370/2007 des Europäischen Parlaments und des Rates vom 23. Oktober 2007 über öffentliche Personenverkehrsdienste auf Schiene und Straße und zur Aufhebung der Verordnungen (EWG) Nr. 1191/69 und (EWG) Nr. 1107/70 des Rates (ABl. L 315 vom 3.12.2007, S. 1, ELI: http://data.europa.eu/eli/reg/2007/1370/oj).

(15) 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 Informations- und Kommunikationstechnologie (IKT) und Kommunikationsnetzen sowie die Bereitstellung und Wartung von verbrauchergerichteten Schnittstellen zur Erfassung von Zahlungsinformationen, einschließlich der für Zahlungsdienste verwendeten Endgeräte und Einrichtungen. Zahlungsauslösedienste und Kontoinformationsdienste sind keine technischen Dienste.

(16) Technische Dienste stellen keine Zahlungsdienste dar, insofern als technische Dienstleister zu keinem Zeitpunkt die zu transferierenden Geldbeträge 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 – diese sollte sich auf den unmittelbaren finanziellen Schaden beschränken und den Betrag der betreffenden Vorgangs nicht übersteigen –, 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.

(17) 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 weiterhin zweckmäßig und technologieneutral bleiben.

(18) 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. Das Verfahren, das zur Ausführung eines Zahlungsvorgangs führt, wird entweder vom Zahler bzw. im Namen dieses Zahlers oder vom Zahlungsempfänger ausgelöst. Der Zahler löst den Zahlungsvorgang durch Erteilung eines Zahlungsauftrags aus. 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 Transfers des Geldbetrags.

(19) Angesichts der unterschiedlichen Auffassungen, die die Kommission in ihrer Überprüfung der Umsetzung der Richtlinie (EU) 2015/2366 festgestellt und die die 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 Vorgängen zu profitieren, die von einem Dritten getätigt wurden, ist ein charakteristisches Merkmal des Begriffs des Zahlungskontos. Ein Zahlungskonto sollte daher definiert werden als ein Konto, das verwendet werden kann, um Geldbeträge an Dritte zu senden und von Dritten zu empfangen. Jedes Konto, das diese Merkmale aufweist, sollte als Zahlungskonto gelten und für die Erbringung von Zahlungsauslösediensten und Kontoinformationsdiensten zugänglich sein. In bestimmten Fällen, z. B. bei einem Kreditkartenkonto oder wenn ein Konto nur für die Ausführung eines einzigen Vorgangs genutzt wird, sollte eine Einzelfallprüfung durchgeführt werden, um festzustellen, ob dieses Konto diese Merkmale aufweist. Fälle, in denen ein anderes zwischengeschaltetes Konto benötigt wird, um Zahlungsvorgänge von Dritten oder an Dritte auszuführen, sollten nicht unter die Definition eines Zahlungskontos fallen. Sparkonten, die nicht dazu verwendet werden können, Geldbeträge an Dritte zu senden oder von Dritten zu empfangen, fallen daher nicht unter die Definition eines Zahlungskontos.

(20) 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; dabei transferiert der Zahlungsdienstleister 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 die Bezahlung von Rechnungen von Versorgungsunternehmen und anderen regelmäßigen Haushaltsrechnungen als Dienstleistung an. Diese Dienstleistungen für die Bezahlung von Rechnungen sollten daher wie ein Finanztransfer behandelt werden.

(21) Angesichts des Aufkommens neuer Arten von Zahlungsinstrumenten, der sich weiterentwickelnden technologischen Lösungen für solche Instrumente und der Unsicherheiten, die auf dem Markt hinsichtlich der rechtlichen Einordnung solcher Instrumente bestehen, sollte die Definition des Begriffs „Zahlungsinstrument“ weiter präzisiert werden, indem 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“ gewisse Herausforderungen mit sich bringen, beispielsweise bezüglich der Anwendung einer starken Kundenauthentifizierung für kontaktlose Zahlungen an der Verkaufsstelle und der Haftungsregelung des Zahlungsdienstleisters. Die Nahfeldkommunikation sollte daher als Merkmal eines Zahlungsinstruments und nicht als Zahlungsinstrument als solches betrachtet werden.

(23) Die Definition des Begriffs „Zahlungsinstrument“ in der Richtlinie (EU) 2015/2366 bezog sich auf ein „personalisiertes Instrument“. Da es Karten auf Guthabenbasis gibt, bei denen der Name des Inhabers des Instruments nicht auf der Karte aufgedruckt ist, könnte die Anwendung dieser Definition dazu führen, dass Karten dieser Art nicht unter die Definition des Zahlungsinstruments fallen. Die Definition des Begriffs „Zahlungsinstrument“ sollte daher dahin gehend geändert werden, dass auf individualisierte Instrumente und nicht auf personalisierte Instrumente Bezug genommen wird, um klarzustellen, dass Karten auf Guthabenbasis, bei denen der Name des Inhabers des Instruments nicht auf der Karte aufgedruckt ist, in den Anwendungsbereich dieser Verordnung fallen.

(24) Digitale Pass-through-Brieftaschen, die entweder die Tokenisierung eines bestehenden Zahlungsinstruments, z. B. einer Zahlungskarte, oder eine Überweisung von einem Zahlungskonto beinhalten, sind als technische Dienste anzusehen und sollten daher von den in dieser Verordnung festgelegten Definitionen des Zahlungsinstruments und des Zahlungsauslösedienstes ausgenommen werden, sofern in der digitalen Brieftasche keine Geldbeträge gespeichert werden, der Anbieter der digitalen Brieftasche niemals in den Besitz dieser Geldbeträge gelangt und der Brieftaschenanbieter im Rahmen vertraglicher Vereinbarungen innerhalb eines geschlossenen Systems mit den Zahlungsdienstleistern tätig ist, die das Zahlungskonto des Zahlers führen oder das Zahlungsinstrument des Zahlers ausgeben. Ein Token an sich kann nicht als Zahlungsinstrument angesehen werden, sondern ist vielmehr eine Zahlungsanwendung im Sinne des Artikels 2 Nummer 21 der Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates[10]. Einige andere Kategorien digitaler Brieftaschen, nämlich vorausbezahlte elektronische Brieftaschen wie z. B. Staged-Wallets, die sich durch eine Aufladephase und eine Zahlungsphase auszeichnen, sollten jedoch als Zahlungsinstrumente und ihre Ausgabe als Zahlungsdienst betrachtet werden. Dies gilt sowohl für Brieftaschen, bei denen die Nutzer im Voraus Geldbeträge für künftige Vorgänge speichern, als auch für Brieftaschen, bei denen die Aufladephase und die Zahlungsphase gleichzeitig zum Zeitpunkt des Vorgangs erfolgen, einschließlich wenn die Brieftasche automatisch ganz oder teilweise über ein verbundenes Zahlungsinstrument oder Zahlungskonto aufgeladen wird.

---

[10] Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über grenzüberschreitende Zahlungen in der Union (ABl. L 123 vom 19.5.2015, S. 1, ELI: http://data.europa.eu/eli/reg/2015/751/oj).

(25) Die technologischen 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, stellen den Zahlungsdienstnutzern aggregierte Online-Informationen über eines oder mehrere ihrer bei einem oder mehreren Zahlungsdienstleistern geführten Zahlungskonten bereit, die über Online-Schnittstellen des kontoführenden Zahlungsdienstleisters zugänglich sind. Die Zahlungsdienstnutzer erhalten somit sofort 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 nicht für den Verbraucher, von dem sie die Einwilligung zum Zugriff auf die Daten und zur Aggregierung der Daten erhalten haben, sondern für eine andere Partei aggregieren und bereitstellen, um es dieser Partei zu ermöglichen, dem Verbraucher, der die Daten nutzt, andere Dienste zu erbringen. Es gibt jedoch unterschiedliche Ansichten darüber, ob diese Tätigkeit in den Anwendungsbereich regulierter Kontoinformationsdienste fällt. Diese Weiterentwicklung des Open-Banking-Geschäftsmodells hin zu einem der „Lizenz als Dienstleistung"-Modell kann eine Quelle innovativer, datengestützter Dienste sein, was letztlich den Endnutzern zugutekommt. Dieses Geschäftsmodell ermöglicht es den Endnutzern nämlich, Zugang zu ihren Zahlungskontodaten zu gewähren, um andere Dienstleistungen als Zahlungsdienste, wie Dienstleistungen der Kreditvergabe, der Buchhaltung und der 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 weiterentwickelte Open-Banking-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 Einwilligung 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 Zulassung erbracht werden, auch wenn die Daten letztlich an einen anderen Dienstleister übermittelt werden.

(27) Die Definition des Begriffs „Geldbetrag“ sollte für den Massenzahlungsverkehr ausgegebenes Zentralbankgeld umfassen, einschließlich Banknoten und Münzen, sowie jegliche künftige digitale Zentralbankwährung, E-Geld, einschließlich E-Geld-Token, und Geschäftsbankengeld. Zentralbankgeld, das für die Verwendung zwischen der Zentralbank und Geschäftsbanken, d. h. für die Verwendung bei Großbetragszahlungen in Zentralbankgeld im Inter-Banken-Verkehr, ausgegeben wird, sollte nicht erfasst werden.

(28) In der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates[11] ist festgelegt, dass E-Geld-Token im Sinne der genannten Verordnung als E-Geld gelten. Dies gilt unabhängig davon, ob die E-Geld-Token der Definition von E-Geld in der vorliegenden Verordnung entsprechen. Dementsprechend sollten Bezugnahmen auf E-Geld in der vorliegenden Verordnung so verstanden werden, dass sie auch E-Geld-Token umfassen, sofern in der vorliegenden Verordnung nichts anderes vorgesehen ist, und E-Geld-Token sollten als E-Geld in die Definition des Begriffs „Geldbetrag“ aufgenommen werden. Ebenso könnte die Erbringung von Transferdienstleistungen für Kryptowerte für Kunden im Sinne der Verordnung (EU) 2023/1114 in Bezug auf E-Geld-Token als Zahlungsdienst der Ausführung von Zahlungsvorgängen gelten, auch wenn diese Transfers im Rahmen anderer Kryptowerte-Dienstleistungen erbracht werden, es sei denn, diese Transfers fallen unter eine spezifische Ausnahme vom Anwendungsbereich der vorliegenden Verordnung und der Richtlinie (EU) 2026/…[+].

---

[11] Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (ABl. L 150 vom 9.6.2023, S. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(29) Angesichts der Marktentwicklung seit der Annahme der Richtlinie (EU) 2015/2366 und zur Vermeidung unverhältnismäßiger Anforderungen an Anbieter von Kryptowerte-Dienstleistungen, die Dienstleistungen mit E-Geld-Token gemäß der Verordnung (EU) 2023/1114 erbringen, sowie zur Gewährleistung von Rechtsklarheit hinsichtlich des Anwendungsbereichs der vorliegenden Verordnung und der Richtlinie (EU) 2026/…[+] im Hinblick auf Dienstleistungen mit E-Geld-Token ist es angezeigt, bestimmte Arten von Zahlungsvorgängen mit E-Geld-Token, bei denen E-Geld-Token für Investitions- oder Handelstätigkeiten verwendet werden, vom Anwendungsbereich der vorliegenden Verordnung und der Richtlinie (EU) 2026/… auszunehmen. Dies betrifft insbesondere den Tausch von E-Geld-Token gegen einen Geldbetrag oder gegen Kryptowerte durch Anbieter von Kryptowerte-Dienstleistungen, wenn die Anbieter von Kryptowerte-Dienstleistungen in eigenem Namen als Käufer oder Verkäufer dieser E-Geld-Token handeln, sowie den Tausch von E-Geld-Token gegen E-Geld-Token oder Kryptowerte durch einen Anbieter von Kryptowerte-Dienstleistungen, der zwischen Käufern und Verkäufern vermittelt. Diese Ausnahme sollte insbesondere für den Tausch von E-Geld-Token im Rahmen der Erbringung der Dienstleistung des Tauschs von Kryptowerten gegen einen Geldbetrag, des Tauschs von Kryptowerten gegen andere Kryptowerte, des Betriebs einer Handelsplattform für Kryptowerte, der Entgegennahme und Übermittlung von Aufträgen für Kryptowerte im Namen von Kunden oder der Ausführung von Aufträgen für Kryptowerte im Namen von Kunden im Sinne der Verordnung (EU) 2023/1114 gelten. Die Ausnahme sollte jedoch nicht Transferdienstleistungen umfassen, die von einem Anbieter von Kryptowerte-Dienstleistungen erbracht werden, wenn E-Geld-Token zur Bezahlung von Waren oder Dienstleistungen verwendet werden.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(30) Unter Berücksichtigung der in der Richtlinie (EU) 2015/2366 festgelegten spezifischen Ausnahme für Zahlungsvorgänge, die ohne zwischengeschaltete Stellen ausschließlich als unmittelbare Bargeldzahlungen vom Zahler an den Zahlungsempfänger erfolgen, ist es angezeigt, eine ähnliche Ausnahme in die vorliegende Verordnung für Vorgänge mit E-Geld-Token aufzunehmen, die ohne Beteiligung einer zwischengeschalteten Stelle durchgeführt werden. Diese Ausnahme sollte unter anderem für Transfers von E-Geld-Token zwischen zwei selbst gehosteten Adressen gelten, an denen weder auf der Seite des Zahlers noch auf der Seite des Zahlungsempfängers eine zwischengeschaltete Stelle beteiligt ist, und nicht für Zahlungsvorgänge zwischen einer elektronischen Geldbörse und einer selbst gehosteten Adresse.

(31) Um das Vertrauen von E-Geld-Inhabern zu erhalten, muss E-Geld rücktauschbar sein. Die Rücktauschbarkeit impliziert nicht, dass die im Tausch für E-Geld entgegengenommenen Geldbeträge als Einlagen oder andere rückzahlbare Geldbeträge im Sinne der Richtlinie 2013/36/EU 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 nationalen Steuer- bzw. Sozialgesetzgebung oder etwaiger Verpflichtungen des E-Geld-Emittenten aus anderen einschlägigen Rechtsvorschriften der Union oder der Mitgliedstaaten, einschließlich Rechtsvorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, jeglicher Maßnahmen betreffend das Einfrieren von Geldern oder etwaiger spezifischer Maßnahmen im Zusammenhang mit der Prävention und Aufklärung von Straftaten.

(32) Zahlungsdienstleister benötigen Zugang zu Zahlungssystemen und Zahlverfahren, um Nutzern Zahlungsdienste anbieten zu können. In der Regel werden zu diesen Zahlungssystemen die wichtigsten Systeme zur Abwicklung von Überweisungen und Lastschriften und zu den Zahlverfahren Vier-Parteien-Kartenzahlverfahren gezählt. Um zwischen den einzelnen Kategorien von zugelassenen Zahlungsdienstleistern eine unionsweite Gleichbehandlung sicherzustellen, sollten die Regeln für den Zugang zu Zahlungssystemen und Zahlverfahren präzisiert werden. Dieser Zugang kann direkt oder indirekt über einen anderen Teilnehmer dieses Zahlungssystems oder Zahlverfahrens erfolgen. Der Zugang sollte Anforderungen unterliegen, die die Integrität und Stabilität dieser Zahlungssysteme und Zahlverfahren sicherstellen. Zu diesem Zweck sollte der Zahlungssystembetreiber oder gegebenenfalls der Zahlverfahrenbetreiber eine Risikobewertung eines Zahlungsdienstleisters durchführen, der eine direkte Teilnahme beantragt. Bei dieser 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 oder Zahlverfahren beantragt, sollte die Entscheidung für ein System oder Verfahren auf eigenes Risiko treffen und gegenüber dem Zahlungssystem oder Zahlverfahren den Nachweis erbringen, dass seine internen Vorkehrungen hinreichend solide sind, um diese Arten von Risiken bewältigen zu können. Zahlungssystembetreiber und Zahlverfahrenbetreiber sollten einen Antrag auf direkte Teilnahme eines Zahlungsdienstleisters nur ablehnen, wenn der Zahlungsdienstleister die Regeln des Systems oder des Verfahrens nicht einhalten kann oder ein unannehmbar hohes Risiko darstellt.

(33) Zahlungsdienstleister und technische Dienstleister, die Dienste für Zahlungsdienstleister erbringen, sollten in der Lage sein, die Interoperabilität mit Hardware- und Softwarefunktionen, die für die wettbewerbsfähige Abwicklung und Ausführung von Zahlungsvorgängen online oder offline erforderlich sind und die von Originalgeräteherstellern mobiler Geräte (original equipment manufacturer – OEM) oder Anbietern elektronischer Kommunikationsdienste bereitgestellt oder kontrolliert werden, zu gewährleisten und für die Zwecke der Interoperabilität über Zugang zu diesen Funktionen zu verfügen. Zu diesen technischen Funktionen gehören Hard- und Software, die erforderlich sind, um den Transaktionsfluss zwischen der Zahlungsmethode und dem Akzeptanzgerät zu verwalten, wie z. B. NFC auf mobilen Geräten und der Kernel des Zahlungsterminals, oder um sicherzustellen, dass mobile Zahlungsanwendungen in einer sicheren Umgebung betrieben werden, in der kryptografische Schlüssel und Algorithmen, der PIN-Code des Kunden oder biometrische Daten wie die sogenannten sicheren Elemente (secure elements) mobiler Geräte, einschließlich der Universal Integrated Circuit Card (UICC), der eingebetteten SE (embedded SE, eSE) und microSD, geschützt sind. Originalgerätehersteller mobiler Geräte und Anbieter elektronischer Kommunikationsdienste sollten verpflichtet sein, die Interoperabilität mit und den Zugang zu allen Hardware- und Softwarefunktionen zu ermöglichen, die für die Abwicklung und Ausführung von Online- und Offline-Vorgängen zu fairen, angemessenen und diskriminierungsfreien Bedingungen erforderlich sind. Diese Verpflichtung sollte Artikel 6 Absatz 7 der Verordnung (EU) Nr. 2022/1925 des Europäischen Parlaments und des Rates[12] unberührt lassen, wonach Torwächter verpflichtet sind, kostenlos wirksame Interoperabilität mit – und Zugang für Zwecke der Interoperabilität zu – dem Betriebssystem, Hardware- oder Softwarefunktionen mobiler Gerätesicherzustellen, was für bestehende und neue digitale Zahlungsmittel gilt.

[12] Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (ABl. L 265 vom 12.10.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

(34) Die Zahlungssystembetreiber und Zahlverfahrenbetreiber sollten über Zugangsregeln und -verfahren verfügen, die verhältnismäßig, objektiv, nichtdiskriminierend und transparent sind. Die Zahlungssystembetreiber und Zahlverfahrenbetreiber sollten Zahlungsinstitute nicht in Bezug auf die Teilnahme diskriminieren, sofern die System- bzw. Verfahrensregeln eingehalten werden können und kein unannehmbares Risiko für das System bzw. das Verfahren besteht. Zu diesen Systemen gehören unter anderem die in der Richtlinie 98/26/EG des Europäischen Parlaments und des Rates[13] genannten Systeme. In Fällen, in denen das betreffende Zahlungssystem gemäß der Verordnung (EU) 2025/1355 der Europäischen Zentralbank[14] bereits der Überwachung des Europäischen Systems der Zentralbanken unterliegt, sollte(n) die Zentralbank(en) die Einhaltung dieser Vorschriften im Rahmen ihrer Überwachung beobachten. Bei anderen Zahlungssystemen oder Zahlverfahren sollten die Mitgliedstaaten zuständige nationale Behörden benennen, um sicherzustellen, dass die Zahlungssystembetreiber und Zahlverfahrenbetreiber diese Anforderungen einhalten, wenn diese Anforderungen nicht unter der Überwachung des Betriebs dieser anderen Zahlungssysteme oder Zahlverfahren durch das Eurosystem oder die Zentralbanken von Mitgliedstaaten, deren Währung nicht der Euro ist, durchgesetzt werden.

---

13 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, ELI: http://data.europa.eu/eli/dir/1998/26/oj).

14 Verordnung (EU) 2025/1355 der Europäischen Zentralbank vom 2. Juli 2025 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (EZB/2025/22) (ABl. L, 2025/1355, 14.7.2025, ELI: http://data.europa.eu/eli/reg/2025/1355/oj).

(35) Höhere Kosten für Zahlungsdienstleister, die Dienstleistungen zur Annahme und Abrechnung von kartengebundenen Zahlungsvorgängen erbringen, und für Händler ergeben sich aus der mangelnden Transparenz der von den Betreibern von Kartenzahlverfahren und den abwickelnden Stellen angewandten Preise. Dies könnte beispielsweise darauf zurückzuführen sein, dass Anbieter von Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen und Händler keine Kenntnis davon haben, welche Maßnahmen zur Vermeidung verhaltensbezogener Gebühren ergriffen werden müssen, welche Dienstleistung optional ist oder wie sie sich gegen eine optionale Dienstleistung entscheiden können. Dies schadet letztlich den Verbrauchern, da die Händler ihre gestiegenen Kosten für die Kartenakzeptanz weitergeben, was zu höheren Einzelhandelspreisen führt. Da die Verbraucher daher ihren Verbrauch wahrscheinlich verringern werden, wird der Umsatz der Händler negativ beeinflusst, es sei denn, die Händler absorbieren diese Kosten und senken damit ihre Gewinnspannen. Die Verfahrensgebühren und die Abwicklungsgebühren sollten daher transparent, aber auch vergleichbar sein, damit die Anbieter von Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen die Effizienz der von ihnen beschafften und erbrachten Verfahrens- und Abwicklungsdienste maximieren können, wodurch die Voraussetzungen für Effizienzgewinne geschaffen werden, die durch niedrigere Händlergebühren für die Akzeptanz kartengebundener Zahlungen zu den Händlern und durch niedrigere Einzelhandelspreise zu den Verbrauchern gelangen. Gleichzeitig können Anbieter von Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen und Händler nur dann wirklich fundierte Entscheidungen über den Verfahrens- und Abwicklungsdienst treffen, wenn sie unverzüglich über neue Verfahrens- und Abwicklungsgebühren oder Änderungen der Gebühren informiert werden. In der Verordnung (EU) 2015/751 über Interbankenentgelte für kartengebundene Zahlungsvorgänge sind Transparenzanforderungen festgelegt, denen Anbieter von Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen gegenüber Zahlungsempfängern unterliegen, mit denen sie Verträge schließen.

Anbieter von Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen sollten sicherstellen, dass die Informationen, die sie Händlern bei der Erfüllung ihrer Verpflichtungen gemäß der Verordnung (EU) 2015/751 zur Verfügung stellen, das gleiche Maß an Transparenz aufweisen wie die Informationen, die ihnen in Bezug auf Verfahrens- und Abwicklungsdienste und die entsprechenden Gebühren zur Verfügung gestellt wurden. Aufgrund der Komplexität der Abrechnungssysteme von Kartenzahlverfahren und abwickelnden Stellen, und damit die Transparenzanforderungen wirksam und verhältnismäßig sein können, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Rechtsakte zu erlassen, um die Informationen, die Zahlungsdienstleistern, die Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, in Bezug auf Verfahrens- und Abwicklungsdienste offenzulegen sind, sowie die entsprechenden Gebühren näher festzulegen.

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

(37) Die Bestimmungen über den Zugang zu den Zahlungssystemen und Zahlverfahren sollten nicht für Systeme und Verfahren gelten, die von einem einzigen Zahlungsdienstleister eingerichtet und betrieben werden. Solche Zahlungssysteme und Zahlverfahren können zwar auch in unmittelbarem Wettbewerb mit anderen Zahlungssystemen und Zahlverfahren stehen, in der Regel aber besetzen sie eine Marktnische, die von anderen Zahlungssystemen und Zahlverfahren nicht abgedeckt wird. Zu diesen Verfahren zählen Drei-Parteien-Systeme, 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 diesen Systemen zählen in der Regel auch Zahlungsdienste von Telekommunikationsanbietern, 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 Zahlverfahren und etablierten gängigen Zahlungssystemen und Zahlverfahren zu fördern, sollte Dritten der Zugang zu diesen geschlossenen proprietären Zahlungssystemen und Zahlverfahren nicht gewährt werden müssen. Allerdings sollten auch solche geschlossenen Systeme und Verfahren weiterhin allen Wettbewerbsvorschriften der Union und der Mitgliedstaaten unterliegen, nach denen der Zugang zu diesen Systemen oder Verfahren gewährt werden muss, um einen wirksamen Wettbewerb in den Zahlungsmärkten aufrechtzuerhalten.

(38) 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 Geldbeträge der Zahlungsdienstnutzer zu erfüllen. Zahlungsinstitute sollten sich auch bemühen, nicht alle Geldbeträge der Zahlungsdienstnutzer bei einem einzigen Kreditinstitut zu sichern, um gegebenenfalls ein Konzentrationsrisiko zu vermeiden. Wie jedoch insbesondere die EBA in ihrer Stellungnahme vom 5. Januar 2022 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 von Geldwäsche oder Terrorismusfinanzierung als höher eingeschätzt wird. Diese sogenannten „risikomindernden“ Praktiken stellen Zahlungsinstitute vor erhebliche Wettbewerbsherausforderungen.

(39) Kreditinstitute sollten daher Zahlungsinstituten und antragstellenden Zahlungsinstituten sowie ihren Agenten auf objektive, nichtdiskriminierende und verhältnismäßige Weise Zugang zu einem Zahlungskonto gewähren. Zahlungsinstitutsanwärter müssen in diese Bestimmung eingeschlossen werden, da ein Konto bei einem Kreditinstitut, auf dem Geldbeträge von Kunden gesichert werden können, eine Voraussetzung für den Erhalt einer Zulassung als Zahlungsinstitut ist. Kreditinstitute sollten den Zugang zu Zahlungskonten nur in Ausnahmefällen verweigern können, wenn schwerwiegende Gründe für eine Verweigerung vorliegen. Kreditinstitute sollten die Eröffnung eines Zahlungskontos für ein Zahlungsinstitut, seine Agenten oder einen Zahlungsinstitutsanwärter verweigern oder ein solches Zahlungskonto schließen können, wenn die Eröffnung oder Führung eines solchen Kontos zu einem Verstoß gegen die Verordnung (EU) 2024/1624 des Europäischen Parlaments und des Rates[15] führen würde. Kreditinstitute sollten diesen Zugang auch in Fällen verweigern können, in denen sie vom Antragsteller einschlägige Informationen oder Unterlagen für die Eröffnung eines Kontos nicht erhalten haben, da dies unter anderem ihre Fähigkeit zur Erfüllung der Sorgfaltspflichten in Bezug auf Kunden beeinträchtigen könnte. Ein Zahlungsinstitut oder seine Agenten oder ein Zahlungsinstitutsanwärter sollten 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.

---

15 Verordnung (EU) 2024/1624 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung (ABl. L, 2024/1624, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1624/oj).

Diese Begründung sollte sich auf spezifische Elemente in Bezug auf das betreffende Zahlungsinstitut beziehen, und nicht auf generelle oder allgemeine Erwägungen. Wird das Zahlungskonto mit der Begründung verweigert, dass die Eröffnung oder Führung eines solchen Kontos zu einem Verstoß gegen die Verordnung (EU) 2024/1624 führen würde, so sollte die dem Kunden oder dem Antragsteller vorgelegte Begründung nicht zur Offenlegung von gemäß Artikel 73 der genannten Verordnung geschützten Informationen führen. Um den zuständigen Behörden die Bearbeitung von Beschwerden gegen die Verweigerung oder den Entzug von Konten und deren Begründung zu erleichtern, sollte die EBA Entwürfe technischer Regulierungsstandards ausarbeiten, in denen die Darlegung der Begründung harmonisiert wird.

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

(41) Bei der Bereitstellung der erforderlichen Informationen für Zahlungsdienstnutzer sollten die Zahlungsdienstleister je nach dem spezifischen Zahlungsdienstvertrag den Bedürfnissen dieser Nutzer sowie praktischen Aspekten und der Kosteneffizienz Rechnung tragen. Zahlungsdienstleister sollten die Informationen entweder aktiv und rechtzeitig ohne Veranlassung durch den Zahlungsdienstnutzer kommunizieren oder sie den Zahlungsdienstnutzern auf deren Anfrage zur Verfügung stellen. Im zweiten Fall müssen Zahlungsdienstnutzer selbst aktiv werden, um sich die Informationen zu verschaffen, einschließlich durch ausdrückliche Anforderung von Informationen bei den Zahlungsdienstleistern, durch Einloggen in eine Mailbox des Bankkontos oder durch Einführen einer Bankkarte in den Kontoauszugdrucker. Zu diesen Zwecken sollten die Zahlungsdienstleister sicherstellen, dass die Informationen zugänglich sind und Zahlungsdienstnutzern zur Verfügung stehen.

(42) Da Verbraucher und Unternehmen nicht gleichermaßen schutzbedürftig sind, müssen sie nicht im selben Umfang geschützt werden. Obwohl die Verbraucherrechte durch Vorschriften geschützt werden müssen, die nicht vertraglich abbedungen werden können, ist es angemessen, es Unternehmen und Organisationen freizustellen, abweichende Vereinbarungen zu schließen, wenn es nicht um vertragliche Beziehungen zu Verbrauchern geht. Vorbehaltlich von durch die Kommission erlassenen Regulierungsstandards könnten solche Vereinbarungen mit Unternehmen und Organisationen, die keine Verbraucher sind, regeln, ob eine starke Kundenauthentifizierung durchzuführen ist. Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[16] könnten wie Verbraucher behandelt werden. Bestimmte Regeln sollten immer gelten, unabhängig vom Status des Nutzers.

---

16 Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

(43) Zahlungsdienstleister, einschließlich Geldautomatenbetreiber, sollten ihren Kunden sowohl vor Einleitung der Abhebung durch den Kunden als auch während der Abhebung auf klare, neutrale und verständliche Weise Informationen über sämtliche Entgelte anzeigen, etwa indem sie ihre Entgelte digital am Terminal anzeigen. Nach Abschluss des Vorgangs sollten die Informationen über die Entgelte auf einfaches Verlangen des Kunden in Papierform oder auf einem anderen dauerhaften Datenträger dokumentiert werden.

(44) 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 oder auf einem anderen dauerhaften Datenträger anfordern können.

(45) 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.

(46) Zahlungsinstrumente für Kleinbetragszahlungen sollten bei dem Erwerb von Waren und Dienstleistungen im Niedrigpreissegment 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 die technischen Möglichkeiten, die von Instrumenten für Kleinbetragszahlungen berechtigterweise erwartet werden können, berücksichtigt werden sollten. Trotz des niedrigeren regulatorischen Aufwands sollten die Zahlungsdienstnutzer unter Berücksichtigung der mit diesen Zahlungsinstrumenten verbundenen begrenzten Risiken, insbesondere mit Blick auf Zahlungsinstrumente auf Guthabenbasis, angemessen geschützt sein.

(47) Bei Einzelzahlungen sollten die Zahlungsdienstleister die wichtigsten Informationen stets von sich aus zur Verfügung stellen müssen. Da Zahler in der Regel anwesend sind, wenn sie den Zahlungsauftrag erteilen, sollte es nicht immer notwendig sein, die Informationen in Papierform oder auf einem anderen dauerhaften Datenträger mitzuteilen. Zahlungsdienstleister sollten die Informationen entweder mündlich mitteilen können oder sie anderweitig leicht zugänglich machen können, einschließlich des Aushangs der Vertragsbedingungen auf einer Tafel in den Geschäftsräumen. Ferner sollte – auch auf der Website – darauf hingewiesen werden, wo weitere, detailliertere Informationen erhältlich sind. Allerdings sollte der Verbraucher auf Verlangen die wichtigsten Informationen auch in Papierform oder auf einem anderen dauerhaften Datenträger von Zahlungsdienstleistern erhalten können.

(48) Die Informationen sollten in einem angemessenen Verhältnis zu den Bedürfnissen der Nutzer stehen. Die Informationspflichten für Einzelzahlungen sollten sich von den Informationspflichten für Rahmenverträge, die eine Serie von Zahlungsvorgängen betreffen, unterscheiden.

(49) 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 Zahlungsdienstnutzer zu erhöhen, sollten die Zahlungsdienstleister den Zahlungsdienstnutzern – in Papierform oder auf einem anderen dauerhaften Datenträger – Informationen über alle Entgelte für inländische Abhebungen an Geldautomaten in unterschiedlichen Situationen zur Verfügung stellen, je nachdem, von welchem Geldautomaten die Zahlungsdienstnutzer Bargeld abheben. Bei auf Euro lautenden Abhebungen an Geldautomaten sollten alle Entgelte, die von Zahlungsdienstnutzern an ihren Zahlungsdienstleister zu entrichten sind, auch wenn die Abhebungen an Geldautomaten erfolgen, die von unabhängigen Geldautomatenbetreibern betrieben werden, dem Grundsatz der Gleichheit der Entgelte gemäß Artikel 3 der Verordnung (EU) 2021/1230 des Europäischen Parlaments und des Rates[17] unterliegen. Die genannte Verordnung sollte entsprechend geändert werden.

(50) 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 in Papierform oder auf einem anderen dauerhaften Datenträger bereitgestellt werden. Zahlungsdienstleister und Zahlungsdienstnutzer sollten jedoch im Rahmenvertrag vereinbaren können, in welcher Weise die nachträgliche Information über ausgeführte Zahlungsvorgänge erfolgen soll.

---

[17] Verordnung (EU) 2021/1230 des Europäischen Parlaments und des Rates vom 14. Juli 2021 über grenzüberschreitende Zahlungen in der Union (ABl. L 274 vom 30.7.2021, S. 20, ELI: http://data.europa.eu/eli/reg/2021/1230/oj).

(51) 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, so sollte der Zahlungsdienstleister nicht die Möglichkeit haben, dieses Recht in Anspruch zu nehmen, nur weil der Zahlungsdienstnutzer seinen Wohnsitz innerhalb der Union geändert hat.

(52) Um die Mobilität der Zahlungsdienstnutzer zu erleichtern, sollten die Nutzer einen Rahmenvertrag gebührenfrei kündigen können. Wird ein Vertrag weniger als drei Monate nach Inkrafttreten vom Zahlungsdienstnutzer gekündigt, so 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 Vertragsbedingungen den Anforderungen des Rahmenvertrags in Bezug auf Kündigungsgebühren unterliegen. Die vereinbarte Kündigungsfrist sollte für den Verbraucher einen Monat nicht überschreiten und für den Zahlungsdienstleister mindestens drei 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 der Rechtsvorschriften zur Bekämpfung von Geldwäsche oder Terrorismusfinanzierung, jeglicher Maßnahmen betreffend das Einfrieren von Geldern oder jeglicher spezifischer Maßnahmen im Zusammenhang mit der Prävention und Aufklärung von Straftaten, zu kündigen.

(53) 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 monetärer Betrag in der Währung des Kontos des Zahlers und als prozentualer Aufschlag auf einen aggregierten durchschnittlichen Devisenmarktkurs, der den Markt genau widerspiegelt. Um sicherzustellen, dass der verwendete Wechselkurs zuverlässig ist und den Markt genau widerspiegelt, sollte er von einem vertrauenswürdigen Administrator bereitgestellt werden, der die geltenden Governance- und Kontrollanforderungen, wie die von der Internationalen Organisation der Wertpapieraufsichtsbehörden (IOSCO) herausgegebenen Grundsätze für finanzielle Referenzwerte, erfüllt. Ein Zahlungsdienstleister sollte durchgängig und für Umrechnungen in beide Richtungen denselben Referenzwert anwenden. Wird in dieser Verordnung auf „Entgelte“ Bezug genommen, so sollte dies gegebenenfalls auch Währungsumrechnungsentgelte einschließen.

(54) Der Zahlungsdienstleister des Zahlers sollte eine Schätzung des Zeitpunkts zur Verfügung stellen, zu dem die Geldbeträge aus Überweisungen und Finanztransfers bei dem außerhalb der Union ansässigen Zahlungsdienstleister des Zahlungsempfängers eingehen werden. Der Zahlungsdienstleister des Zahlers sollte den Zahler darauf hinweisen, dass dies kein genauer Zeitpunkt ist, da der Zeitpunkt des Eingangs von verschiedenen Faktoren abhängen kann, die sich manchmal der Kontrolle des Zahlungsdienstleisters des Zahlers entziehen.

(55) Da ein Zahlungsdienstleister dem Zahler den Namen des Zahlungsempfängers nur dann mitteilen oder zugänglich machen kann, wenn ihm diese Informationen zur Verfügung stehen, kann diese Anforderung in Fällen, in denen dies nicht möglich ist, nicht angewandt werden. Dies ist im Allgemeinen bei Finanztransfers der Fall, die als Einzelzahlung ausgeführt werden und bei denen der Zahlungsdienstleister des Zahlers keinen Zugang zum Namen des Zahlungsempfängers hat, es sei denn, er wird vom Zahler bereitgestellt. Daher sollte der Zahlungsdienstleister des Zahlers in solchen Fällen nicht verpflichtet sein, dem Zahler den Namen des Zahlungsempfängers mitzuteilen oder zugänglich zu machen.

(56) Eine Teilung der Entgelte zwischen Zahler und Zahlungsempfänger ist erfahrungsgemäß am effizientesten, da sie die durchgängig automatisierte 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 erhobene Entgelt kann auch null betragen, denn die Regeln sollten nicht die Praxis eines Zahlungsdienstleisters beeinträchtigen, der dem Zahler oder dem Zahlungsempfänger keine Entgelte in Rechnung stellt. Auch kann der Zahlungsdienstleister des Zahlungsempfängers – unbeschadet der Wettbewerbsvorschriften der Union und der Verordnung (EU) 2015/751 und je nach Vertragsbedingungen – lediglich beim Zahlungsempfänger Vergütung für die Nutzung des Zahlungsdienstes erheben, wenn ein solches Entgelt eine Entschädigung für den Zahlungsdienstleister des Zahlers umfasst und der Zahlungsdienstleister des Zahlers dem Zahler keine Entgelte in Rechnung stellt. Zahlungssysteme können Entgelte in Form einer Grundgebühr erheben. Die Bestimmungen über die transferierten Beträge oder etwaige erhobene Entgelte haben keine unmittelbaren Auswirkungen auf die Preisbildung oder die Vergütung zwischen Zahlungsdienstleistern oder sonstigen zwischengeschalteten Stellen.

(57) 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[18] Anwendung findet, d. h. Überweisungen und Lastschriften in Euro innerhalb der Union. Die Mitgliedstaaten durften gemäß der Richtlinie (EU) 2015/2366 dem Zahlungsempfänger die Erhebung von Entgelten ferner untersagen oder dieses Recht begrenzen, wobei die Notwendigkeit berücksichtigt wurde, den Wettbewerb und die Nutzung effizienter Zahlungsinstrumente zu fördern.

---

[18] 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, ELI: http://data.europa.eu/eli/reg/2012/260/oj).

(58) 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. Wird ein Aufschlag angewandt, wird er darüber hinaus 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.

(59) Open-Banking-Dienste sind Zahlungsdienste, die Zahlungsdienstleistern, die weder Geldbeträge des Kontoinhabers führen noch über ein Zahlungskonto verfügen, Zugang zu den Zahlungskontodaten eines Zahlungsdienstnutzers verschaffen. Kontoinformationsdienstleister erbringen eine Dienstleistung, mit der die Aggregation der Daten eines Nutzers auf Verlangen des Zahlungsdienstnutzers mit verschiedenen kontoführenden Zahlungsdienstleistern an einem einzigen Ort ermöglicht werden soll. Der Kontoinformationsdienstleister könnte die erhaltenen Zahlungskontodaten auch an einen Dritten übermitteln, der seinerseits eine Dienstleistung für den Zahlungsdienstnutzer erbringen würde, bei der diese Daten eingesetzt würden, möglicherweise mit zusätzlichen Mehrwertdiensten. Zahlungsauslösedienste ermöglichen die Auslösung einer Zahlung vom Konto des Nutzers, wie etwa eine Überweisung, auf eine für den Nutzer und den Zahlungsempfänger bequeme Weise, ohne dass ein Instrument wie eine Zahlungskarte verwendet wird. Für einen Zahlungsauslösedienst muss die Einwilligung des Zahlers für den Zugang zum Zahlungskonto vorliegen. Wie in der Verordnung (EU) 2024/1624 anerkannt, gehen einige Zahlungsauslösedienste eine Geschäftsbeziehung mit dem Zahlungsempfänger ein. Daher spiegelt die Definition des Zahlungsauslösedienstes die Tatsache wider, dass die Anbieter solcher Dienste dem Zahler und dem Zahlungsempfänger Zahlungsauslösedienste anbieten können. Die Bereitstellung einer digitalen Pass-through-Brieftasche, die es dem Nutzer ermöglicht, eine Zahlung vom Zahlungskonto des Nutzers auszulösen, sollte nicht als Zahlungsauslösedienst gelten, sofern in der digitalen Brieftasche keine Geldbeträge gespeichert sind, der Anbieter der digitalen Brieftasche nie in den Besitz solcher Geldbeträge gelangt und der Anbieter der Brieftasche im Rahmen vertraglicher Vereinbarungen mit den Zahlungsdienstleistern tätig ist, die das Konto des Zahlers führen.

(60) Kontoführende Zahlungsdienstleister sollten Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern Zugang zu Zahlungskontodaten gewähren, wenn der Zahlungsdienstnutzer online auf das Zahlungskonto zugreifen kann und der Zahlungsdienstnutzer die Einwilligung 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 Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern bedurfte, was zur Folge hatte, dass eine Entgelterhebung für den Datenzugang in der Praxis nicht möglich war. Seit dem Anwendungsbeginn der Richtlinie (EU) 2015/2366 erfolgt der Zugang zu Daten im Rahmen des Open Banking auf einer solchen außervertraglichen Grundlage und ist kostenlos. Würden regulierte Datenzugangsdienste entgeltpflichtig werden, was bisher nicht der Fall war, 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 der Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates[19], insbesondere mit Artikel 9 Absatz 3 der genannten Verordnung, der durch die vorliegende Verordnung nicht berührt wird.

[19] Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung) (ABl. L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(61) Kontoführende Zahlungsdienstleister sowie Kontoinformationsdienstleister 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 Gegenleistung vorsehen kann. Ein Beispiel für solche Mehrwertdienste, die über sogenannte „Premium“-Anwendungsprogrammierschnittstellen angeboten werden, ist die Möglichkeit, künftige variable wiederkehrende Zahlungen zu planen. Jede Gegenleistung für solche Dienste müsste mit den Kapiteln III und IV der Verordnung (EU) 2023/2854 in Einklang stehen, insbesondere in Bezug auf Artikel 9 Absätze 1 und 2 der genannten Verordnung über die Gegenleistung. Der Zugang von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern zu Zahlungskontodaten, die unter diese Verordnung fallen, ohne dass ein Vertragsverhältnis bestehen muss, 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.

(62) Um beim Datenzugang und -austausch ein hohes Maß an Sicherheit zu gewährleisten, sollte der Zugang zu Zahlungskonten und den darin enthaltenen Daten den Kontoinformationsdienstleistern 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 Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern einrichten. Damit keinerlei Unsicherheit darüber entsteht, wer auf die Daten des Zahlungsdienstnutzers zugreift, sollte die dedizierte Schnittstelle Kontoinformationsdienstleister 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. Kontoinformationsdienstleister und Zahlungsauslösedienstleister sollten wählen können, welche Authentifizierungsmethode sie dem Zahlungsdienstnutzer anbieten, um die am wenigsten aufwendige Option anzubieten. Kontoinformationsdienstleister und Zahlungsauslösedienstleister sollten die dedizierte Schnittstelle für Datenzugangszwecke nutzen. Bei einem Ausfall oder einer ungeplanten Nichtverfügbarkeit der dedizierten Schnittstelle wäre die Aufrechterhaltung der Geschäftskontinuität dieser Dienstleister dadurch gefährdet, dass sie nicht auf die Daten zugreifen können, für die ihnen die Einwilligung erteilt wurde. Es ist von wesentlicher Bedeutung, dass Kontoinformationsdienstleister und Zahlungsauslösedienstleister jederzeit auf die Daten zugreifen können, die für die Erbringung von Dienstleistungen für Kunden unerlässlich sind. Daher sollte die geplante Nichtverfügbarkeit der dedizierten Schnittstelle, die es den kontoführenden Zahlungsdienstleistern ermöglicht, die dedizierte Schnittstelle zu aktualisieren oder zu ändern, in der Regel auf den Zeitraum zwischen 0:00 Uhr und 6:00 Uhr gelegt werden. Während die Systemwartung in der Regel ein Upgrade des Systems in der Nacht zwischen 0:00 Uhr und 6:00 Uhr der Ortszeit des kontoführenden Zahlungsdienstleisters umfasst, kann ein umfangreiches Wartungsverfahren länger als mehrere Stunden dauern. Mit Ausnahme von Änderungen aufgrund von Notfällen sollte der kontoführende Zahlungsdienstleister auch die Zahlungsdienstleister, die die dedizierte Schnittstelle nutzen, in der Regel mindestens einen Monat im Voraus ordnungsgemäß über jede geplante Nichtverfügbarkeit und deren Dauer unterrichten.

(63) Um die Nutzung der dedizierten Schnittstelle zu erleichtern, sollten ihre technischen Spezifikationen unter Angabe der erforderlichen Routinen, Protokolle und Instrumente dokumentiert sein, und der kontoführende Zahlungsdienstleister sollte eine Zusammenfassung öffentlich zugänglich machen. Damit Open-Banking-Dienstleister ihren künftigen Zugang ordnungsgemäß vorbereiten und etwaige technische Probleme lösen können, sollte der kontoführende Zahlungsdienstleister Kontoinformationsdienstleister und Zahlungsauslösedienstleister in die Lage versetzen, eine Schnittstelle vor dem Datum, an dem sie aktiviert wird, zu testen. Nur zugelassene Kontoinformationsdienstleister und Zahlungsauslösedienstleister sollten über diese Schnittstelle Zugriff auf Zahlungskontodaten haben; dagegen sollten Antragsteller, die eine Zulassung als Kontoinformationsdienstleister und Zahlungsauslösedienstleister beantragen, die Möglichkeit haben, die technischen Spezifikationen einzusehen. Zur Sicherstellung der Interoperabilität der verschiedenen technischen Kommunikationslösungen sollte die Schnittstelle von internationalen oder europäischen Normungsorganisationen, einschließlich vom Europäischen Komitee für Normung (European Committee for Standardization, CEN) oder von der Internationalen Organisation für Normung (International Organization for Standardization, ISO), entwickelte Kommunikationsstandards oder andere weithin anerkannte Standards, die ein gleichwertiges Sicherheitsniveau bieten, verwenden, was es kontoführenden Zahlungsdienstleistern ermöglichen würde, von einem breiten Spektrum technologischer Lösungen zu profitieren, ohne die Sicherheit zu beeinträchtigen oder sich auf Nischenstandards zu stützen, deren Umsetzung für Drittanbieter schwierig wäre.

(64) Damit Kontoinformationsdienstleister und Zahlungsauslösedienstleister jederzeit ihre Geschäftskontinuität sicherstellen und für ihre Kunden hochwertige Dienstleistungen erbringen können, sollte die dedizierte Schnittstelle, die sie nutzen müssen, ein einfaches und nahtloses Nutzererlebnis ermöglichen, indem sie hohe Anforderungen in Bezug auf Leistung und Funktion erfüllt. 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 ermöglichen. Detailliertere Anforderungen an dedizierte Schnittstellen sollten in von der EBA entwickelten technischen Regulierungsstandards festgelegt werden.

(65) Für die Zwecke einer wirksamen Überprüfung vor der Auslösung einer Zahlung sollten kontoführende Zahlungsdienstleister sicherstellen, dass Zahlungsauslösedienstleister den vollständigen Namen des Kontoinhabers über die dedizierte Schnittstelle überprüfen können, und sollten daher keine Teilnamen oder verkürzten Namen angeben.

(66) Angesichts der dramatischen Auswirkungen, die eine längere ungeplante Nichtverfügbarkeit einer dedizierten Schnittstelle auf die Geschäftskontinuität von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern haben würde, sollten kontoführende Zahlungsdienstleister alles in ihrer Macht Stehende tun, um eine ungeplante Nichtverfügbarkeit oder unzureichende Leistung dieser Schnittstelle zu verhindern. Unter unzureichender Leistung sollte eine Leistung verstanden werden, die die Leistung der Schnittstelle, die der kontoführende Zahlungsdienstleister für die Authentifizierung und Kommunikation mit seinen Zahlungsdienstnutzern verwendet, unterschreitet. Kontoführende Zahlungsdienstleister sollten eine solche Nichtverfügbarkeit oder unzureichende Leistung unverzüglich beheben und eine optimale Wiederherstellungsdauer für die dedizierte Schnittstelle sicherstellen. Kontoführende Zahlungsdienstleister sollten Kontoinformationsdienstleister und Zahlungsauslösedienstleister über eine solche Nichtverfügbarkeit ihrer dedizierten Schnittstelle und die zu ihrer Behebung ergriffenen Maßnahmen unverzüglich unterrichten. Angesichts der wesentlichen Bedeutung der vollständigen Verfügbarkeit und Funktionalität der dedizierten Schnittstelle für die Geschäftsmodelle von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern sollte die dedizierte Schnittstelle die Verfügbarkeit und Leistungsfähigkeit gewährleisten, die mindestens derjenigen der Schnittstelle entspricht, die der kontoführende Zahlungsdienstleister für die Authentifizierung und Kommunikation mit seinen Nutzern verwendet. Die EBA sollte beauftragt werden, in Entwürfen technischer Regulierungsstandards die Anforderungen an vierteljährliche Statistiken über die Verfügbarkeit und Leistung dedizierter Schnittstellen und – zu Vergleichszwecken – der Schnittstellen, die der kontoführende Zahlungsdienstleister seinen Zahlungsdienstnutzern für den direkten Online-Zugriff auf ihr Zahlungskonto zur Verfügung stellt, sowie die Anforderungen an die Veröffentlichung dieser Statistiken auf der Website des kontoführenden Zahlungsdienstleisters und die Standards zur Festlegung einer optimalen Wiederherstellungsdauer im Falle einer ungeplanten Nichtverfügbarkeit der dedizierten Schnittstelle auf der Grundlage des Schweregrads des Vorfalls zu präzisieren. Bei diesem Schweregrad sollte unter anderem die Anzahl der betroffenen Kunden und die Art der bei Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern betroffenen Funktionen berücksichtigt werden.

(67) Kontoinformationsdienstleister und Zahlungsauslösedienstleister sollten sich stets ordnungsgemäß identifizieren und ihre Verpflichtungen einhalten, wie etwa die Grenzen der ihnen erteilten Einwilligung, und insbesondere nur auf die Daten zugreifen, die sie benötigen, um ihren vertraglichen Verpflichtungen nachzukommen und den regulierten Dienst zu erbringen. Ein Screenscraping von Daten, d. h. der Zugriff auf Daten von Zahlungskonten ohne ordnungsgemäße Identifizierung, sollte in keinem Fall erfolgen.

(68) Da die Einrichtung oder Pflege einer dedizierten Schnittstelle für bestimmte kontoführende Zahlungsdienstleister als unverhältnismäßig aufwendig angesehen werden könnte, sollte eine zuständige nationale Behörde einen kontoführenden Zahlungsdienstleister auf dessen Antrag von der Verpflichtung befreien können, über eine dedizierte Datenzugangsschnittstelle zu verfügen, und dem kontoführenden Zahlungsdienstleister erlauben, entweder den Zugang zu Zahlungsdaten nur über seine „Kundenschnittstelle“ anzubieten, sofern diese Schnittstelle bereits ein Endpunkt der Anwendungsprogrammierschnittstelle, d. h. ein bestimmter, sicherer digitaler Verbindungspunkt ist, der eine automatisierte Maschine-zu-Maschine-Kommunikation und einen automatisierten Datenaustausch ermöglicht, oder überhaupt keine Schnittstelle für den Zugang zu Open-Banking-Daten anzubieten. Je nach den Besonderheiten des Mitgliedstaats kann der Mitgliedstaat nationalen Zentralbanken, die nicht in ihrer Eigenschaft als Währungsbehörden oder andere Behörden handeln, gegebenenfalls eine Ausnahme von der Verpflichtung gewähren, über eine dedizierte Schnittstelle zu verfügen. Der Datenzugang über die Kundenschnittstelle kann, wenn es keine dedizierte Schnittstelle gibt, angemessen sein, wenn diese Schnittstelle bereits eine Anwendungsprogrammierschnittstelle ist, z. B. in Fällen zwischen Unternehmen, in denen keine mobilen Anwendungen oder Website-Schnittstellen zwischen dem kontoführenden Zahlungsdienstleister und seinem Kunden verwendet werden, oder wenn eine dedizierte Schnittstelle für den kontoführenden Zahlungsdienstleister eine erhebliche finanzielle und ressourcenbezogene Belastung darstellen würde, z. B. für sehr kleine Zahlungsdienstleister. 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 Befreiungen sollten in technischen Regulierungsstandards festgelegt werden, die von der EBA ausgearbeitet werden, wobei unter anderem die Größe, der Jahresumsatz und das Zahlungsvolumen des kontoführenden Zahlungsdienstleisters zu berücksichtigen sind. Solche Befreiungen sollten, sobald sie gewährt wurden, nicht aufrechterhalten werden, wenn sich die Umstände, die zu der Befreiung geführt haben, erheblich ändern.

(69) Um das Potenzial des Open Banking in der Union voll auszuschöpfen, ist es von entscheidender Bedeutung, jede diskriminierende Behandlung von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern durch kontoführende Zahlungsdienstleister zu verhindern. Hat ein Zahlungsdienstnutzer beschlossen, die Dienste eines Kontoinformationsdienstleisters oder eines Zahlungsauslösedienstleisters in Anspruch zu nehmen, so sollte der kontoführende Zahlungsdienstleister diesen Auftrag genauso behandeln wie eine Anfrage, die vom Zahlungsdienstnutzer direkt über die Kundenschnittstelle dieses Dienstleisters gestellt wird, es sei denn, der kontoführende Zahlungsdienstleister hat objektive Gründe, die Anfrage auf Zugang zum Konto anders zu behandeln, einschließlich eines schwerwiegenden Betrugsverdachts.

(70) Für die Erbringung von Zahlungsauslösediensten sollte der kontoführende Zahlungsdienstleister dem Zahlungsauslösedienstleister alle ihm verfügbaren Informationen über die Ausführung des Zahlungsvorgangs unmittelbar nach Eingang des Zahlungsauftrags sowie, auf Verlangen des Zahlungsauslösedienstleisters, auf kontinuierlicher Basis zur Verfügung stellen. Mitunter erhält der kontoführende Zahlungsdienstleister weitere Informationen, nachdem er den Zahlungsauftrag erhalten, aber den Zahlungsvorgang noch nicht ausgeführt hat. Sofern diese Informationen für den Zahlungsauftrag und die Ausführung des Zahlungsvorgangs relevant sind, sollte der kontoführende Zahlungsdienstleister diese Informationen dem Zahlungsauslösedienstleister zur Verfügung stellen. Dem Zahlungsauslösedienstleister sollten die Informationen zugänglich sein, die erforderlich sind, um das Risiko der Nichtausführung des ausgelösten Vorgangs einzuschätzen. Diese Informationen sind unerlässlich, damit der Zahlungsauslösedienstleister einem Zahlungsempfänger, in dessen Namen er den Vorgang auslöst, einen Dienst anbieten kann, dessen Qualität mit der Qualität anderer dem Zahlungsempfänger zur Verfügung stehender elektronischer Zahlungsmittel, einschließlich Zahlungskarten, vergleichbar ist.

(71) Um das Vertrauen in Open Banking zu stärken, ist es von wesentlicher Bedeutung, dass Zahlungsdienstnutzer, die Kontoinformationsdienste und Zahlungsauslösedienste nutzen, die volle Kontrolle über ihre Daten und Zugang zu klaren Informationen über die Datenzugangseinwilligungen haben, die diese Zahlungsdienstnutzer den Zahlungsdienstleistern erteilt haben, einschließlich des Zwecks der Einwilligung und der Kategorien der betreffenden Zahlungskontodaten wie die Identitätsdaten des Kontos, der Vorgang und der Kontosaldo. 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. Die Dashboards sollten keine abschreckenden oder abhaltenden Formulierungen enthalten, die einen Zahlungsdienstnutzer davon abbringen könnten, die Dienste eines Zahlungsauslösedienstleisters oder Kontoinformationsdienstleisters in Anspruch zu nehmen. Einwilligungen zur Auslösung einmaliger Zahlungen sollten nicht auf diesem Dashboard erscheinen. Ein Dashboard sollte es einem Zahlungsdienstnutzer nicht ermöglichen, neue Datenzugangseinwilligungen mit einem Kontoinformationsdienstleister oder Zahlungsauslösedienstleister zu erstellen, dem zuvor noch kein Datenzugang gewährt wurde. Kontoführende Zahlungsdienstleister sollten Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern unverzüglich Informationen über jeden Entzug des Datenzugangs verfügbar machen. Kontoinformationsdienstleister und Zahlungsauslösedienstleister sollten kontoführende Zahlungsdienstleister unverzüglich über neue und wiederhergestellte Datenzugangseinwilligungen unterrichten, die von Zahlungsdienstnutzern erteilt wurden, einschließlich der Geltungsdauer der Einwilligung 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 Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern erteilten Einwilligungen zu widerrufen. Das Dashboard sollte den Zahlungsdienstnutzer in standardisierter Form vor dem Risiko möglicher vertraglicher Folgen warnen, die aus dem Entzug des Datenzugangs eines Open-Banking-Dienstleisters entstehen, da das Dashboard nicht das Vertragsverhältnis zwischen dem Nutzer und einem Open-Banking-Dienstleister regelt, sondern es Sache des Zahlungsdienstnutzers ist, dieses Risiko zu überprüfen. Ein Dashboard für Einwilligungen sollte die Kunden in die Lage versetzen, ihre Einwilligungen 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 Dashboard für Einwilligungen sollten gegebenenfalls die Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates[20] berücksichtigt werden.

(72) Kontoinformationsdienstleister sollten zum Zweck der Erbringung des Kontoinformationsdienstes auf Informationen zu bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen zugreifen können, die von kontoführenden Zahlungsdienstleistern gespeichert werden, unabhängig davon, ob der Zahlungsdienstnutzer diese Informationen aktiv anfragt oder nicht. Beabsichtigt ein Kontoinformationsdienstleister, auf Informationen zuzugreifen, und fordert der Zahlungsdienstnutzer diese Informationen nicht aktiv an, so sollte der Kontoinformationsdienstleister den Zahlungsdienstnutzer von seiner Absicht in Kenntnis setzen. In diesem Fall muss der Informationspflicht nicht bei jedem einzelnen Zugriff nachgekommen werden, sondern kann dadurch erfüllt werden, dass diese Information in den Rahmenvertrag zwischen dem Kontoinformationsdienstleister und dem Zahlungsdienstnutzer aufgenommen wird.

---

[20] 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, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

(73) Die Überprüfung der Richtlinie (EU) 2015/2366 hat ergeben, dass Kontoinformationsdienstleister und Zahlungsauslösedienstleister trotz des erreichten Harmonisierungsgrads und des Verbots von Beeinträchtigungen nach Artikel 32 Absatz 3 der Delegierten Verordnung (EU) 2018/389 der Kommission[21] nach wie vor mit zahlreichen ungerechtfertigten Beeinträchtigungen konfrontiert sind. Diese Beeinträchtigungen schränken das volle Potenzial des Open Banking in der Union nach wie vor erheblich ein. Diese Beeinträchtigungen werden den Aufsichtsbehörden, den Regulierungsbehörden und der Kommission regelmäßig von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern gemeldet. Die EBA hat am 4. Juni 2020 ihre Stellungnahme veröffentlicht, in der sie diese Beeinträchtigungen analysiert hat. Trotz der Bemühungen um Klarstellung besteht auf dem Markt und bei den Aufsichtsbehörden nach wie vor große Unsicherheit darüber, was eine „unzulässige 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 von der EBA geleistete Arbeit zurückgegriffen werden sollte.

[21] 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. ELI: http://data.europa.eu/eli/reg_del/2018/389/oj).

(74) Gründe im Zusammenhang mit der Betrugsprävention oder der Einhaltung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[22] sollten nicht als allgemeine Grundlage dienen, Drittanbietern den Datenzugang zu verweigern, einzuschränken oder zu verzögern. Maßnahmen, die aus diesen Gründen ergriffen werden, könnten ausnahmsweise den Zugang zu Open-Banking-Dienstleistungen beschränken, sollten jedoch nur im Einzelfall zulässig sein, wenn dies auf der Grundlage objektiver und überprüfbarer Anhaltspunkte für einen Betrugsverdacht oder aufgrund einer spezifischen Pflicht gemäß der Verordnung (EU) 2016/679 hinreichend begründet ist, und sollten nach wie vor unbedingt erforderlich, verhältnismäßig und in Umfang und Dauer begrenzt sein. Sie sollten weder zu systematischen oder pauschalen Beschränkungen des Open Banking führen noch Beeinträchtigungen beim Datenzugang legitimieren, die nach der vorliegenden Verordnung verboten sind. Auch wenn kontoführende Zahlungsdienstleister berechtigterweise Maßnahmen zur Eindämmung von Betrug ergreifen könnten, sollten die Dienste der Anbieter von Zahlungsauslösediensten und Kontoinformationsdiensten durch diese Maßnahmen nicht diskriminiert werden. Daher sollten die Maßnahmen für solche Dienste ebenso gelten wie für Zahlungsdienste, die direkt oder indirekt vom kontoführenden Zahlungsdienstleister selbst erbracht werden, einschließlich kartengebundene Zahlungsdienste oder auf Überweisungen gestützte Zahlungsdienste, die für Zahlungsempfänger zur kommerziellen Nutzung erhältlich sind. Dieser Grundsatz sollte sowohl für das Authentifizierungserlebnis des Zahlers gelten als auch dafür, wie sicher es ist, dass eine ausgelöste Zahlung vom kontoführenden Zahlungsdienstleister ausgeführt wird.

---

[22] 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(75) Die Verpflichtung, personalisierte Sicherheitsmerkmale zu schützen, ist von größter Bedeutung, um die Geldbeträge des Zahlungsdienstnutzers zu schützen und die Risiken im Zusammenhang mit Betrug und unbefugtem Zugriff auf Zahlungskonten zu begrenzen. Die Geschäftsbedingungen oder andere dem Zahlungsdienstnutzer durch Zahlungsdienstleister auferlegte Pflichten zum Schutz personalisierter Sicherheitsmerkmale sollten jedoch nicht so formuliert 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 der Richtlinie (EU) 2026/…[+] 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 der Kundenidentifikator keine sensiblen Zahlungsdaten darstellen.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(76) 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 zentrale Behörde für die Durchsetzung der Rechte und Pflichten des Open Banking gibt, sind die zuständigen nationalen Behörden die ersten Stellen für die Durchsetzung der Vorschriften zum Open Banking. Daher ist es von wesentlicher Bedeutung, dass die zuständigen nationalen Behörden alles in ihrer Macht Stehende tun, um die Einhaltung des Rechtsrahmens der Union für Open Banking sicherzustellen. 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 erleichtern. Insbesondere muss sichergestellt werden, dass kontoführende Zahlungsdienstleister ihren Verpflichtungen in Bezug auf die dedizierte Schnittstelle zu jeder Zeit nachkommen. Kontoführende Zahlungsdienstleister sowie Kontoinformationsdienstleister 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 nationalen Behörden sollte die Durchsetzung erleichtern, und die Erhebung von Daten über den Markt für Open Banking sollte eine derzeit bestehende Datenlücke schließen, durch die eine wirksame Messung der tatsächlichen Inanspruchnahme von Open Banking in der Union behindert wird. Kontoführende Zahlungsdienstleister sowie Kontoinformationsdienstleister und Zahlungsauslösedienstleister sollten gemäß Artikel 10 der Verordnung (EU) 2023/2854 Zugang zu Streitbeilegungsstellen haben.

(77) Die dedizierte Schnittstelle sollte der primäre Zugangspunkt für Kontoinformationsdienste und Zahlungsauslösedienste sein. Einige kontoführende Zahlungsdienstleister könnten jedoch über zusätzliche Schnittstellen für andere Anwendungskontexte verfügen, die technisch so konzipiert sind, dass mit ihnen die gleichen Dienste für Kontoinformationsdienstleister und Zahlungsauslösedienstleister wie mit der dedizierten Schnittstelle erbracht werden können. Kontoinformationsdienstleister und Zahlungsauslösedienstleister sollten diese zusätzlichen Schnittstellen mit Einwilligung des kontoführenden Zahlungsdienstleisters nutzen können. Diese Möglichkeit darf jedoch weder als Verpflichtung des kontoführenden Zahlungsdienstleisters ausgelegt werden, den Zugang auf andere Weise als über die dedizierte Schnittstelle zu gewähren, noch wird durch sie das Recht für Kontoinformationsdienstleister und Zahlungsauslösedienstleister oder andere nicht regulierte Stellen geschaffen, einen solchen Zugang zu verlangen. Die zusätzlichen Schnittstellen können nur genutzt werden, wenn die Teilnehmer dies von sich aus wünschen, mit Einwilligung der kontoführenden Zahlungsdienstleister und unter denselben Sicherheitsbedingungen in Bezug auf Identifizierung und sichere Kommunikation, die auch für die dedizierte Schnittstelle gelten, und sofern die zusätzlichen Schnittstellen weithin anerkannte und interoperable Standards verwenden.

(78) Der Begriff der Einwilligung im Sinne dieser Verordnung lässt die in der Verordnung (EU) 2016/679 festgelegten Vorschriften über die rechtmäßige Verarbeitung personenbezogener Daten, einschließlich der Bestimmungen zu den Begriffen der Einwilligung und der ausdrücklichen Einwilligung, unberührt. Bei der Verarbeitung personenbezogener Daten obliegt es dem Verantwortlichen, die geeignete Rechtsgrundlage gemäß der Verordnung (EU) 2016/679 zu bewerten und sicherzustellen, dass alle in der genannten Verordnung festgelegten Bedingungen für diese Rechtsgrundlage erfüllt sind.

(79) Ein Zahlungsvorgang oder eine Serie von Zahlungsvorgängen sollte nur dann als autorisiert gelten, wenn der Zahler seine Einwilligung zur Ausführung des Zahlungsvorgangs in einer zwischen dem Zahler und dem kontoführenden Zahlungsdienstleister vereinbarten Weise erteilt hat. Sie sollte als nicht autorisiert gelten, wenn der Vorgang von einem Dritten ausgelöst oder geändert wurde, der ohne die Einwilligung des Zahlungsdienstnutzers handelt. Beispiele für Zahlungsvorgänge, die von einem Dritten ausgelöst oder geändert werden, der ohne die Einwilligung des Zahlungsdienstnutzers handelt, sind etwa Fälle, in denen dieser Dritte die auf betrügerische Weise erlangten personalisierten Sicherheitsmerkmale des Zahlungsdienstnutzers verwendet.

(80) Die Sicherheit von Überweisungen ist von grundlegender Bedeutung, um das Vertrauen der Zahlungsdienstnutzer in diese Dienste zu erhalten 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 zugeordnet ist. Um zur Verringerung von Betrug und Fehlern beizutragen, sollten Zahlungsdienstnutzer von einer Dienstleistung profitieren, mit der überprüft wird, ob der Kundenidentifikator des Zahlungsempfängers und der vom Zahler angegebene Name des Zahlungsempfängers übereinstimmen, und – falls eine Unstimmigkeit festgestellt wird – dem Zahler dies angezeigt wird. Handelt es sich bei dem Zahlungsempfänger um eine juristische Person, so könnte diese Dienstleistung darin bestehen, dass überprüft wird, ob Übereinstimmung zwischen dem Kundenidentifikator des Zahlungsempfängers und einem anderen Datenelement, beispielsweise einer Steuernummer, einer europäischen einheitlichen Kennung gemäß Artikel 16 Absatz 1 Unterabsatz 2 der Richtlinie (EU) 2017/1132 des Europäischen Parlaments und des Rates[23] oder einer Rechtsträgerkennung (Legal Entity Identifier, LEI), die eine eindeutige Identifizierung des Zahlungsempfängers ermöglicht, besteht, falls der Zahler dieses Datenelement über einen Zahlungsauslösekanal des Zahlungsdienstleisters des Zahlers übermitteln darf und dieses Datenelement in den internen Systemen des Zahlungsdienstleisters des Zahlungsempfängers verfügbar ist. Wird das Zahlungskonto des Zahlungsempfängers nicht durch eine internationale KontoNummer (IBAN) identifiziert, so sollte eine andere Art von Kundenidentifikator verwendet werden, um das Zahlungskonto des Zahlungsempfängers eindeutig zu identifizieren. Solche Dienstleistungen haben sich in den Ländern, in denen sie angeboten werden, sehr positiv bei der Verringerung von Betrug und Fehlern ausgewirkt. Angesichts der Bedeutung dieser Dienstleistung für die Betrugs- und Fehlerprävention sollte sie den Zahlungsdienstnutzern kostenlos zur Verfügung stehen.

---

[23] Richtlinie (EU) 2017/1132 des Europäischen Parlaments und des Rates vom 14. Juni 2017 über bestimmte Aspekte des Gesellschaftsrechts (ABl. L 169 vom 30.6.2017, S. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

Um unnötige Reibungsverluste oder Verzögerungen bei der Bearbeitung des Vorgangs zu vermeiden, sollte eine entsprechende Anzeige durch den Zahlungsdienstleister des Zahlers innerhalb höchstens weniger Sekunden ab dem Zeitpunkt erfolgen, zu dem der Zahler die Informationen zum Zahlungsempfänger eingegeben hat. Damit der Zahler entscheiden kann, ob er den beabsichtigten Vorgang fortsetzen will, sollte diese Anzeige des Zahlungsdienstleisters des Zahlers erfolgen, bevor der Zahler den Vorgang autorisiert. Den Zahlern könnten bestimmte Lösungen für die Auslösung von Überweisungen zur Verfügung stehen, die es ihnen ermöglichen, einen Zahlungsauftrag zu erteilen, ohne selbst den Kundenidentifikator und den Namen des Zahlungsempfängers einzugeben. In diesen Fällen sollte der Zahlungsdienstleister sicherstellen, dass der Zahlungsempfänger, an den der Zahler eine Überweisung tätigen möchte, korrekt identifiziert wird.

(81) In der Verordnung (EU) Nr. 260/2012 ist vorgesehen, dass den Nutzern von Überweisungen in Euro, einschließlich Echtzeitüberweisungen in Euro, eine Dienstleistung zur Überprüfung der Übereinstimmung zwischen dem Kundenidentifikator und dem Namen des Zahlungsempfängers oder einem anderen Datenelement angeboten wird. Um einen kohärenten Rahmen für alle Überweisungen zu schaffen und gleichzeitig unnötige Überschneidungen zu vermeiden, sollte die in der vorliegenden Verordnung genannte Überprüfungsdienstleistung nur für Überweisungen gelten, die nicht unter die Verordnung (EU) Nr. 260/2012 fallen, und an die Überprüfungsdienstleistung gemäß der Verordnung (EU) Nr. 260/2012 angepasst werden.

(82) Einige Merkmale des Namens des Zahlungsempfängers, auf dessen Konto der Zahler eine Überweisung tätigen möchte, könnten die Wahrscheinlichkeit erhöhen, dass der Zahlungsdienstleister eine Unstimmigkeit feststellt. Zu diesen Unstimmigkeiten gehören 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 in Fällen zu vermeiden, in denen der vom Zahler angegebene Name des Zahlungsempfängers und der mit der IBAN oder – wenn die IBAN nicht zur Identifizierung des Zahlungskontos verwendet wird – mit einer anderen vom Zahler angegebenen Art von Kundenidentifikator verknüpfte Name zwar nicht genau, aber dennoch nahezu übereinstimmen, und um dem Zahler die Entscheidung darüber zu erleichtern, ob er den beabsichtigten Vorgang fortsetzen will, sollten die Zahlungsdienstleister dem Zahler den Namen des Zahlungsempfängers, der mit der IBAN oder einer anderen vom Zahler angegebenen Art von Kundenidentifikator verknüpft ist, in einer Weise anzeigen, dass die Einhaltung der Verordnung (EU) 2016/679 gewährleistet ist.

(83) Wird ein Zahlungsvorgang autorisiert, obwohl mit der Abgleichdienstleistung eine Unstimmigkeit festgestellt und dem Zahlungsdienstnutzer angezeigt wurde, so kann dies dazu führen, dass der Geldbetrag an einen unbeabsichtigten Zahlungsempfänger überwiesen wird. Die Zahlungsdienstleister sollten die Zahlungsdienstnutzer über die möglichen Folgen ihrer Entscheidung, die angezeigte Unstimmigkeit zu ignorieren und mit der Ausführung des Vorgangs fortzufahren, informieren. Zahlungsdienstnutzer, bei denen es sich nicht um Verbraucher handelt, sollten sich gegen die Inanspruchnahme der Dienstleistung zur Überprüfung des Zahlungsempfängers entscheiden können, wenn sie Zahlungsaufträge über Zahlungsauslösekanäle einreichen, die auf automatisierten dedizierten Prozessen oder Protokollen beruhen und die nur Zahlungsdienstnutzern, bei denen es sich nicht um Verbrauchern handelt, zur Verfügung stehen. Auch nachdem sie sich dagegen entschieden haben, sollten die Zahlungsdienstnutzer weiterhin die Möglichkeit haben, diese Dienstleistung wieder in Anspruch zu nehmen. Damit die Empfängerüberprüfung reibungsloser in die Zahlungsmanagementprozesse dieser Zahlungsdienstnutzer integriert werden kann, sollten die Zahlungsdienstleister ihnen darüber hinaus die Möglichkeit einräumen, im Rahmenvertrag zu vereinbaren, dass die Empfängerüberprüfung in Bezug auf Zahlungsaufträge, die über solche Zahlungsauslösekanäle erteilt werden, nach der Autorisierung dieser Aufträge durchgeführt wird und dass der Zahlungsdienstleister des Zahlers – falls sich im Zuge der Empfängerüberprüfung bestimmte spezifische Ergebnisse ergeben – diese Aufträge ohne weitere Eingaben des Zahlungsdienstnutzers ausführt. Die Verordnung (EU) Nr. 260/2012 sollte entsprechend geändert werden.

(84) Zum eigenen Schutz des Zahlungsdienstnutzers sollte der Zahlungsdienstleister diesem die Möglichkeit einräumen, im Rahmenvertrag einen Betrag festzulegen, der höchstens mittels einer Zahlungsmethode oder eines Zahlungsinstruments transferiert werden kann. Darüber hinaus sollte es dem Zahlungsdienstnutzer möglich sein, für jedes Zahlungsmittel und jedes Zahlungsinstrument unterschiedliche Höchstbeträge festzulegen, die nach dem alleinigen Ermessen des Zahlungsdienstnutzers pro Vorgang oder für einen festen Zeitraum, etwa pro Tag oder pro Woche, gelten. Schlägt der Zahlungsdienstleister einen vom Zahlungsdienstnutzer festzulegenden Höchstbetrag für Überweisungen vor, so sollte der vorgeschlagene Höchstbetrag für verschiedene Arten von Überweisungen gleichermaßen gelten, damit der Zahlungsdienstnutzer nicht unwissentlich daran gehindert wird, dass er zu Echtzeitweisungen denselben Zugang wie zu anderen Arten von Überweisungen hat. Die Zahlungsdienstnutzer sollten auch in der Lage sein, die zuvor im Rahmenvertrag festgelegten Höchstbeträge zu ändern.

(85) Um die Wirksamkeit der Ausgabenobergrenzen zu gewährleisten, ist es wichtig, dass jede Anhebung des Höchstbetrags, die vom Zahlungsdienstnutzer über einen Fernzugang beantragt wird, erst nach einem Verzögerungszeitraum wirksam wird. Ohne einen solchen Verzögerungszeitraum könnte ein Betrüger ein Opfer dazu überreden, die Ausgabenobergrenzen des Opfers anzupassen, und wäre dann sofort in der Lage, das Opfer um einen viel höheren Wert zu betrügen. Ein Verzögerungszeitraum würde dem Zahlungsdienstnutzer hingegen Zeit lassen, zu erkennen, dass er von einem Betrüger kontaktiert und manipuliert wurde. Der Verzögerungszeitraum sollte vom Zahlungsdienstleister standardmäßig auf vier Stunden festgesetzt werden. Der Zahlungsdienstnutzer sollte die Möglichkeit haben, den Verzögerungszeitraum zu verlängern oder zu verkürzen oder sich gegen die Anwendung eines solchen Zeitraums zu entscheiden, wobei bei solchen Maßnahmen der geltende Verzögerungszeitraum zugrunde zu legen ist. Beantragt der Zahlungsdienstnutzer eine Anhebung der Ausgabenobergrenze über einen Fernzugang, so sollte die Anwendung einer starken Kundenauthentifizierung vorgeschrieben werden.

(86) Die Entscheidung des Zahlungsdienstleisters, ein Zahlungsinstrument zu sperren, sollte auf objektiv gerechtfertigten Gründen beruhen, die sich auf die im Rahmen des Transaktionsüberwachungsmechanismus erhobenen Daten stützen, und dem Risiko eines Betrugs, der die Sicherheit des Zahlungsinstruments und die Interessen des Zahlungsdienstnutzers gefährden könnte, Rechnung tragen. Beispiele für objektiv gerechtfertigte Gründe könnten unter anderem der Verdacht einer nicht autorisierten Nutzung, der Verdacht betrügerischer Vorgänge, die Sicherheit des Zahlungsinstruments oder die Gefahr einer Täuschung in Bezug auf Finanztätigkeiten und Vorgänge sein, die in einem ungerechtfertigt kurzen Zeitraum in großer Entfernung voneinander durchgeführt werden.

(87) Da Zahlungsdienste zunehmend digitalisiert werden, bieten viele Zahlungsdienstleister den Zahlungsdienstnutzern die Möglichkeit, mobile Anwendungen zur Auslösung von Zahlungsdiensten zu nutzen. Diese mobilen Anwendungen sind zwar nützlich und vorteilhaft für die Zahlungsdienstnutzer, bergen aber auch ein Betrugsrisiko. Um diesem Risiko vorzubeugen, sollte für den Vorgang der Aktivierung einer mobilen Anwendung auf einem Gerät die Nutzung verschiedener Kommunikationskanäle notwendig sein, sofern eine Kundenbeziehung zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister besteht, ebenso wie die Anwendung einer starken Kundenauthentifizierung. Bei der Begründung der Kundenbeziehung sollten der Zahlungsdienstleister und der Zahlungsdienstnutzer vereinbaren, dass die anschließende Aktivierung einer mobilen Anwendung erst nach einem bestimmten Zeitraum wirksam wird, damit der Zahlungsdienstnutzer eingreifen kann, falls er nicht derjenige ist, der die mobile Anwendung aktiviert. Um ein adäquates Verfahren für den Aufbau einer Kundenbeziehung, das sogenannte Onboarding, zu ermöglichen, sollte der Verzögerungszeitraum insbesondere dann nicht gelten, wenn die mobile Anwendung verwendet wird, um die Kundenbeziehung zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister herzustellen. Der Zahlungsdienstleister sollte einen Verzögerungszeitraum von vier Stunden festlegen. Anschließend sollte der Zahlungsdienstnutzer das Recht haben, die Anwendung eines solchen Zeitraums anzupassen oder diese abzulehnen; hierfür sollte eine starke Kundenauthentifizierung vorgeschrieben werden. Jede vom Zahlungsdienstnutzer beantragte Anpassung der Länge des Verzögerungszeitraums sollte wiederum dem vom Zahlungsdienstleister vorgeschlagenen Verzögerungszeitraum unterliegen und könnte länger oder kürzer sein als der Zeitraum von vier Stunden.

Falls eine Kundenbeziehung zwischen dem Zahlungsdienstleister und dem Zahlungsdienstnutzer besteht, sollte der Zahlungsdienstleister dem Zahlungsdienstnutzer zudem auf sichere Weise und über unterschiedliche Kommunikationskanäle die Aktivierung einer mit seinem Zahlungskonto verknüpften mobilen Anwendung auf einem Gerät anzeigen. Zweck der Anzeige ist es, die Wachsamkeit des Zahlungsdienstnutzers zu erhöhen, und sie sollte es dem Zahlungsdienstnutzer daher ermöglichen, den Zahlungsdienstleister zu warnen, wenn der betreffende Nutzer die mobile Anwendung nicht installiert hat. In diesem Fall sollte der Zahlungsdienstleister sicherstellen, dass die mobile Anwendung weder den Zugang zum Zahlungskonto des Zahlungsdienstnutzers noch die Auslösung von Zahlungsvorgängen ermöglicht. Diese Anzeigepflicht sollte weder für die Aktivierung einer mobilen Anwendung auf einem Gerät des Zahlungsdienstnutzers gelten, wenn diese vom Zahlungsdienstleister in seinen stationären Verkaufsstellen vorgenommen wird, noch sollte sie für die erstmalige Begründung der Kundenbeziehung zwischen dem Zahlungsdienstleister und dem Zahlungsdienstnutzer gelten, da zum Zeitpunkt der Begründung der Kundenbeziehung weder Geldbeträge noch ein Zahlungskonto des Zahlungsdienstnutzers über den Zahlungsdienstleister verfügbar sind und da der Zahlungsdienstleister keinen Kontakt mit dem betreffenden Zahlungsdienstnutzer aufnehmen könnte, da der Zahlungsdienstleister zum Zeitpunkt des Onboardings die Kontaktdaten des Zahlungsdienstnutzers noch nicht überprüft hat.

(88) Die Zahlungsdienstleister sollten in ihrer Kommunikation mit ihren Kunden gewährleisten, dass alle Informationen, die bei unbefugtem Abgreifen zu einer Beeinträchtigung der Sicherheit des Zahlungsinstruments oder der Zahlungsdaten führen könnten, dem Kunden über sichere und effiziente Kommunikationskanäle übermittelt werden.

(89) Für den Fall von Schäden durch nicht autorisierte Zahlungsvorgänge oder bestimmte autorisierte Überweisungen sollte die Verteilung von Verlusten geregelt werden. Für Zahlungsdienstnutzer, bei denen es sich nicht um Verbraucher handelt, 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.

(90) 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.

(91) Bestreitet ein Zahlungsdienstnutzer, einen ausgeführten Zahlungsvorgang autorisiert zu haben, oder behauptet er, dass der Zahlungsvorgang nicht korrekt ausgeführt worden sei, so sollte die Verwendung eines Zahlungsinstruments in der vom Zahlungsdienstleister und Zahlungsdienstnutzer vereinbarten Form für sich genommen nicht zwangsläufig als ausreichender Nachweis dafür angesehen werden, dass der Zahlungsvorgang vom Zahler autorisiert worden ist. Die Authentifizierung oder die Verwendung der vom Zahlungsdienstleister, gegebenenfalls einschließlich des Zahlungsauslösedienstleisters, aufgezeichneten starken Kundenauthentifizierung sollte für sich genommen nicht zwangsläufig ein ausreichender Nachweis dafür sein, dass der Zahlungsvorgang vom Zahler autorisiert wurde oder dass der Zahler betrügerisch gehandelt hat oder einer oder mehreren Pflichten des Zahlungsdienstnutzers in Bezug auf Zahlungsinstrumente und personalisierte Sicherheitsmerkmale vorsätzlich oder grob fahrlässig nicht nachgekommen ist.

(92) Damit der Zahlungsdienstnutzer einen leichteren Zugang zum Zahlungsdienstleister hat, sollte dieser einen Kommunikationskanal einrichten und bereitstellen, damit der Zahlungsdienstnutzer die Möglichkeit hat, Vorfälle anzuzeigen oder die Aufhebung der Sperrung des Zahlungsinstruments gemäß dieser Verordnung zu verlangen. Dieser Kommunikationskanal sollte es dem Zahlungsdienstnutzer auch ermöglichen, einen betrügerischen Vorgang anzuzeigen. Zahlungsdienstleister könnten diesen Kanal nutzen, um einen Kunden zu beraten, der den Verdacht hegt, Opfer eines Betrugsangriffs zu sein, und um Zahlungsdienstnutzern Probleme im Zusammenhang mit ausgeführten Zahlungsvorgängen anzuzeigen, etwa Fehler der einschlägigen Geräte bei der Ausführung von Zahlungsvorgängen.

(93) Angesichts der zunehmenden Komplexität und der sich rasch verändernden Betrugsmuster sollte sichergestellt werden, dass – bevor ein Zahlungsdienstleister den Schluss zieht, dass ein Zahlungsdienstnutzer betrügerisch, vorsätzlich oder grob fahrlässig gehandelt hat und letzterem daher eine Erstattung gemäß dieser Verordnung verweigert – dieser Zahlungsdienstnutzer die Möglichkeit erhält, seinem Zahlungsdienstleister zur Begründung seines Anspruchs alle einschlägigen Informationen oder Nachweise über die Umstände des strittigen Zahlungsvorgangs oder der strittigen Serie von Zahlungsvorgängen vorzulegen. Bestreitet ein Zahlungsdienstnutzer, einen Zahlungsvorgang oder eine Serie von Zahlungsvorgängen autorisiert zu haben, oder macht ein Zahlungsdienstnutzer, bei dem es sich um einen Verbraucher handelt, geltend, dass ein Zahlungsvorgang oder eine Serie von Zahlungsvorgängen Ergebnis eines Betrugs unter Vortäuschung der Identität des Zahlungsdienstleisters im Sinne dieser Verordnung waren, so sollte der Zahlungsdienstleister in diesem Zusammenhang nicht zu dem Schluss gelangen, dass dieser Zahlungsdienstnutzer bzw. Verbraucher betrügerisch, vorsätzlich oder grob fahrlässig gehandelt hat, ohne zuvor den Zahlungsdienstnutzer proaktiv und unmissverständlich aufgefordert zu haben, diesbezügliche Informationen oder Nachweise vorzulegen, und ohne dies bei seiner Bewertung gebührend berücksichtigt zu haben. Die Verpflichtung des Zahlungsdienstleisters, dem Zahlungsdienstnutzer zu ermöglichen, relevante Nachweise oder Informationen zur Stützung seiner Ansprüche beizubringen, sollte als Recht des Zahlungsdienstnutzers auf eine ordnungsgemäße Bewertung aller relevanten Informationen über die Umstände des strittigen Zahlungsvorgangs oder der strittigen Serie von Zahlungsvorgängen durch den Zahlungsdienstleister verstanden werden. Dieses Recht des Zahlungsdienstnutzers sollte nicht als Rechtfertigung für die Schlussfolgerung des Zahlungsdienstleisters verstanden werden, dass der Zahlungsdienstnutzer betrügerisch, vorsätzlich oder grob fahrlässig gehandelt hat, wenn der Zahlungsdienstnutzer Nachweise, die vernünftigerweise nicht von ihm erwartet werden können, beispielsweise die Aufzeichnung von Telefongesprächen, nicht beibringt oder wenn der Zahlungsdienstnutzer keinerlei Nachweise oder Informationen vorlegt.

(94) Im Falle eines nicht autorisierten Zahlungsvorgangs sollte der Zahlungsdienstleister dem Zahler unverzüglich den Betrag, der Gegenstand dieses Zahlungsvorgangs war, erstatten. Hegt der Zahlungsdienstleister jedoch den Verdacht, dass der nicht autorisierte Zahlungsvorgang darauf zurückzuführen ist, dass der Zahler einer oder mehrerer seiner Pflichten in Bezug auf die Sicherheit von Zahlungsinstrumenten und personalisierten Sicherheitsmerkmalen vorsätzlich oder grob fahrlässig nicht nachgekommen ist, oder auf ein betrügerisches Verhalten des Zahlers zurückgeht, und stützt sich dieser Verdacht auf objektiv gerechtfertigte Gründe, so sollte der Zahlungsdienstleister, bevor er eine Erstattung an den Zahler vornimmt, eine Untersuchung durchführen können. Der Zahlungsdienstleister sollte dem Zahler innerhalb von 15 Geschäftstagen, nachdem er Kenntnis von dem Zahlungsvorgang erhalten hat oder dieser ihm angezeigt wurde, entweder den Betrag des nicht autorisierten Zahlungsvorgangs erstatten oder dem Zahler die Gründe und unterstützende Beweise für die Ablehnung der Erstattung vorlegen und die Stellen angeben, an die sich der Zahler wenden kann, falls er die angegebenen Gründe nicht akzeptiert. Lehnt der Zahlungsdienstleister die Erstattung ab, nachdem er aufgrund seiner Untersuchung zu dem Schluss gekommen ist, dass der Zahler betrügerisch gehandelt hat, so sollte der Zahlungsdienstleister der zuständigen nationalen Behörde die Gründe für diese Schlussfolgerung mitteilen. Die Mitgliedstaaten sollten klar öffentlich bekanntmachen, an welche zuständige nationale Behörde eine solche Mitteilung des Zahlungsdienstleisters zu richten ist. 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 und Verlust sowie jede missbräuchliche Verwendung eines Zahlungsinstruments oder personalisierter Sicherheitsmerkmale 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 betrügerisch oder grob fahrlässig gehandelt.

In dieser Hinsicht ist zum Zeitpunkt der Annahme dieser Verordnung ein Betrag von 50 EUR zur Sicherstellung eines harmonisierten und hochgradigen Schutzes der Nutzer innerhalb der Union angemessen. Es sollte keine Haftung bestehen, wenn der Zahler außerstande ist, den Verlust, den Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments oder der personalisierten Sicherheitsmerkmale zu bemerken. Auch sollte ein Zahlungsdienstnutzer, sobald er seinem Zahlungsdienstleister angezeigt hat, dass sein Zahlungsinstrument oder seine personalisierten Sicherheitsmerkmale kompromittiert worden sein könnten, keine weiteren durch die nicht autorisierte Nutzung dieses Zahlungsinstruments oder dieser personalisierten Sicherheitsmerkmale verursachten Schäden tragen müssen. Zahlungsdienstleister sollten für die technische Sicherheit ihrer eigenen Produkte verantwortlich sein.

(95) Haftungsbestimmungen für autorisierte Überweisungen bei fehlerhafter Erbringung oder Fehlfunktion der Dienstleistung zur Feststellung der Übereinstimmung von Name und Kundenidentifikator eines Zahlungsempfängers würden die richtigen Anreize für Zahlungsdienstleister setzen, eine voll funktionsfähige Dienstleistung zu erbringen, um die Gefahr von Zahlungsautorisierungen auf der Grundlage von Falschinformationen zu verringern. Der Zahlungsdienstleister des Zahlers sollte für den vollen Betrag einer fehlerhaften Überweisung, die darauf zurückzuführen ist, dass dieser Zahlungsdienstleister die Dienstleistung zur Überprüfung des Zahlungsempfängers für den Zahler nicht oder nicht ordnungsgemäß erbracht hat, haften und dem Zahler diesen Betrag unverzüglich erstatten. Ist die Haftung des Zahlungsdienstleisters des Zahlers dem Zahlungsdienstleister des Zahlungsempfängers oder dem Zahlungsauslösedienstleister zuzurechnen, so sollte der Zahlungsdienstleister des Zahlungsempfängers oder gegebenenfalls der Zahlungsauslösedienstleister den Zahlungsdienstleister des Zahlers für den entstandenen finanziellen Schaden entschädigen.

(96) Die Zahlungsdienstleister sollten mit den Zahlungsdienstnutzern und den zuständigen Behörden zusammenarbeiten, wenn Zweifel bestehen, dass die Dienstleistung der Überprüfung des Zahlungsempfängers korrekt erbracht wurde.

(97) Zahlungsdienstnutzer sollten angemessen vor Betrug durch sogenanntes Social Engineering geschützt werden, bei dem ein Betrüger einen Zahlungsdienstnutzer so manipuliert, dass dieser eine bestimmte Handlung durchführt, etwa einen Zahlungsvorgang auslöst oder den Betrügern seine eigenen Sicherheitsmerkmale übergibt. Die Zahl der Fälle dieser Art von Social Engineering hat in den letzten Jahren erheblich zugenommen. Durch diese neuen Arten des Betrugs wird die in der Richtlinie (EU) 2015/2366 getroffene Unterscheidung zwischen autorisierten und nicht autorisierten Zahlungsvorgängen verwischt. Auch die Mittel, bei denen davon ausgegangen werden kann, dass die Einwilligung erteilt wurde, werden immer schwieriger zu identifizieren, da Betrüger die Kontrolle über den gesamten Einwilligungs- und Authentifizierungsprozess, einschließlich des Abschlusses einer starken Kundenauthentifizierung, übernehmen können. Die Bedingungen, unter denen der Kunde einen Zahlungsvorgang autorisiert hat, indem er seine Einwilligung erteilt hat, sollten – auch von Gerichten – gebührend berücksichtigt werden, wenn es darum geht, den betreffenden Vorgang als autorisiert oder nicht autorisiert einzustufen. Der betreffende Vorgang könnte tatsächlich in einer Situation autorisiert worden sein, in der die Autorisierung unter manipulierten Prämissen erteilt wurde, die die Integrität der Einwilligung beeinträchtigten. Es ist daher nicht mehr möglich, wie in der Richtlinie (EU) 2015/2366 der Fall, Erstattungen auf nicht autorisierte Zahlungsvorgänge zu beschränken. Es wäre jedoch für die Zahlungsdienstleister unverhältnismäßig und finanziell sehr aufwendig, bei allen betrügerischen Vorgängen, unabhängig davon, ob sie autorisiert wurden oder nicht, einen systematischen Erstattungsanspruch einzuräumen. Dies könnte auch zu Fehlanreizen und einer geringeren Wachsamkeit des Kunden führen. Daher müssen die Bedingungen festgelegt werden, unter denen ein Zahlungsdienstnutzer Anspruch auf Erstattung hat.

(98) Betrüger stützen sich häufig auf Instrumente und Techniken wie Spoofing von Anrufer-IDs, E-Mail-Adressen oder IP-Adressen. Solche Betrugsfälle sind komplex und betreffen häufig verschiedene Akteure entlang der Betrugskette. Die Zahlungsdienstleister haben mehr Handhabe als die Zahlungsdienstnutzer, um diesen Betrugsfällen ein Ende zu bereiten. Sowohl Zahlungsdienstleister als auch Anbieter elektronischer Kommunikationsdienste können durch angemessene Prävention und solide technische Maßnahmen eine entscheidende Rolle bei der Betrugsprävention spielen. Zahlungsdienstleister unterliegen besonderen Verpflichtungen gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates[24], die darauf abzielt, IKT-Risiken zu mindern. Gemäß der Verordnung (EU) 2022/2554 unterliegen Zahlungsdienstleister einem umfassenden Regelwerk über einen IKT-Risikomanagementrahmen, einschließlich Instrumenten, Strategien und Verfahren zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten, unabhängig davon, ob diese Daten gespeichert sind oder gerade verwendet oder übermittelt werden. Um diesen Verpflichtungen nachzukommen, sollten Zahlungsdienstleister über angemessene technische Maßnahmen und Instrumente verfügen, um die betrügerische Nachahmung und den Missbrauch des Domänennamens des Zahlungsdienstleisters und der Kommunikationskanäle, die für die Kommunikation zwischen dem Zahlungsdienstleister und dem Zahlungsdienstnutzer genutzt werden, einschließlich der E-Mail-Adresse und der RufNummer des Zahlungsdienstleisters, zu verhindern.

---

[24] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz 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, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

(99) An Betrug unter Vortäuschung der Identität des Zahlungsdienstleisters, auch Spoofing genannt, sind Betrüger beteiligt, die sich als Zahlungsdienstleister des Verbrauchers ausgeben und den Domänennamen oder die Kommunikationskanäle, die dem Zahlungsdienstleister des Verbrauchers zugewiesen sind, z. B. die E-Mail-Adresse, die Telefonnummer, die Website oder die mobile Anwendung des Zahlungsdienstleisters, missbräuchlich verwenden. Spoofing-Betrug schädigt den Ruf des Zahlungsdienstleisters und des Finanzsektors insgesamt und kann den Verbrauchern in der Union erheblichen finanziellen Schaden zufügen, wodurch ihr Vertrauen in den elektronischen Zahlungsverkehr und das Finanzsystem beeinträchtigt wird. Ein Verbraucher, der Opfer eines solchen Spoofing-Betrugs geworden ist, sollte daher Anspruch auf die Erstattung des vollen Betrags des betrügerischen Zahlungsvorgangs durch den Zahlungsdienstleister haben, es sei denn, der Verbraucher hat betrügerisch oder grob fahrlässig gehandelt. Betrifft der Betrug die Website oder mobile Anwendung des Zahlungsdienstleisters, so sollte der Erstattungsanspruch Fälle einschließen, in denen sich der Betrüger diese Kanäle zu eigen gemacht hat, sowie Fälle, in denen es um betrügerisch erstellte Versionen der Website oder mobilen Anwendung geht, die den Inhalt der echten Versionen spiegeln. Sobald der Verbraucher Kenntnis davon erhält, dass er Opfer dieser Art von Spoofing-Betrug oder Manipulation geworden ist, sollte er den Vorfall unverzüglich seinem Zahlungsdienstleister und der Polizei melden, vorzugsweise über Online-Beschwerdeverfahren, sofern diese von der Polizei zur Verfügung gestellt werden. Da es für besonders schutzbedürftige Verbraucher schwierig sein könnte, den Betrug rechtzeitig polizeilich zu melden, werden Zahlungsdienstleister ermutigt, den Verbraucher erforderlichenfalls bei einer solchen Meldung zu unterstützen.

(100) Zahlungsbetrug, einschließlich der Auslösung oder Änderung von Zahlungsaufträgen ohne Einwilligung des Zahlers, der Diebstahl sensibler Zahlungsdaten, einschließlich personalisierter Sicherheitsmerkmale, oder die Manipulation des Zahlers, auch durch Identitätsbetrug, umfassen häufig betrügerische Aktivitäten von Nutzern von Diensten wie interpersonellen Kommunikationsdiensten oder Hostingdiensten, die die Speicherung und gegebenenfalls die öffentliche Verbreitung von Online-Inhalten ermöglichen. Je nach den technischen Merkmalen der erbrachten Dienstleistung haben die Anbieter solcher Dienstleistungen Zugang zu verschiedenen Daten und somit zu verschiedenen Arten von Hinweisen auf potenziell betrügerische Aktivitäten. Daher sind diese Anbieter in der Lage, durch den Austausch einschlägiger Informationen mit Zahlungsdienstleistern zur gemeinsamen Bekämpfung von Betrug, auch in Form von Spoofing, beizutragen, um so die betrügerische Nutzung von interpersonellen Kommunikationsdiensten oder Hostingdiensten zu verhindern und aufzudecken. Einschlägige Informationen können beispielsweise die Zahlungskontodaten von Unternehmern umfassen, die Anbieter von Online-Plattformen zum Abschluss von Fernabsatzverträgen zwischen Verbrauchern und Unternehmen gemäß Artikel 30 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates[25] in Bezug auf von diesen Anbietern als rechtswidrig identifizierte Inhalte erhalten haben, oder Informationen über Zahlungsinstrumente, die Zahlungsdienstnutzer Zahlungsdienstleistern als gestohlen gemeldet haben.

[25] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 27.10.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

Die Verarbeitung personenbezogener Daten, die für die Zwecke der Betrugsprävention unbedingt erforderlich ist, stellt ein berechtigtes Interesse der Anbieter interpersoneller Kommunikationsdienste, der Hostingdiensteanbieter sowie der Zahlungsdienstleister und ihrer Kunden dar. Die Anbieter interpersoneller Kommunikationsdienste und Hostingdiensteanbieter sollten in der Lage sein, personenbezogene Daten mit Zahlungsdienstleistern auszutauschen, um Betrüger und betrügerische Verhaltensweisen zu ermitteln, sofern sämtliche Bedingungen des Artikels 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 erfüllt sind. Darüber hinaus sollten Anbieter interpersoneller Kommunikationsdienste und Hostingdiensteanbieter auch die Betrugsbekämpfung unterstützen, indem sie mit Zahlungsdienstleistern Informationen über Betrugsszenarien, Trends und Bedrohungen austauschen, die im Zusammenhang mit der Nutzung ihrer Dienste ermittelt wurden. So können sie dazu beitragen, die Wirksamkeit der Transaktionsüberwachungsmechanismen und der Aufklärungskampagnen und Schulungen zur Betrugsprävention, die im Einklang mit dieser Verordnung durchgeführt werden, zu verbessern.

(101) Wenn die einschlägigen Bedingungen, einschließlich der Anforderungen der Verordnung (EU) 2016/679, für den freiwilligen Austausch der Informationen, die zur Prävention und Aufdeckung von Betrug erforderlich sind, erfüllt sind, sollten Anbieter interpersoneller Kommunikationsdienste und Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen über spezielle Kommunikationskanäle verfügen oder Vereinbarungen über den Informationsaustausch oder über Systeme für eine wirksame Kommunikation mit Zahlungsdienstleistern schließen, wie die Vereinbarungen über den Informationsaustausch gemäß Artikel 29 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[26]. Diese Mechanismen sollten solide Schutzvorkehrungen in Bezug auf die Vertraulichkeit, den Datenschutz und die Nutzung von Informationen im Einklang mit der Verordnung (EU) 2016/679 enthalten.

[26] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(102) Gemäß der Richtlinie (EU) 2022/2555 müssen Anbieter öffentlich zugänglicher interpersoneller Kommunikationsdienste geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit ihrer Dienste zu gewährleisten. Soweit davon ausgegangen werden kann, dass die betrügerische Manipulation der Rufnummernanzeige oder der E-Mail-Adresse die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit dieser Dienste beeinträchtigt, sollten diese Anbieter bereits gemäß der Richtlinie (EU) 2022/2555 verpflichtet sein, Maßnahmen zur Bewältigung dieses Risikos zu ergreifen. Unbeschadet dieser Verpflichtungen sollten Anbieter öffentlich zugänglicher interpersoneller Kommunikationsdienste geeignete organisatorische und technische Maßnahmen treffen, um die Nutzung ihrer Dienste zum Zwecke des Identitätsbetrugs, auch durch Manipulation der Rufnummernanzeige oder der E-Mail-Adresse, aufzudecken und zu verhindern, wenn diese Nutzung darauf abzielt, Zahlungsdienstnutzer zu einer Zahlung oder zu einer Handlung zu veranlassen, die die Sicherheit des Zahlungskontos beeinträchtigen würde. Alle Maßnahmen, die ergriffen werden, um die Nutzung dieser Dienste zum Zwecke des Identitätsbetrugs zu verhindern oder aufzudecken, müssen den Vorschriften der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[27] entsprechen. Insbesondere sollten diese Maßnahmen keine allgemeine und unterschiedslose Überwachung des Inhalts der Kommunikation oder aller Verkehrsdaten umfassen.

---

[27] 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 (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(103) Die Verordnung (EU) 2022/2065 enthält vollständig harmonisierte Vorschriften für die Erbringung von Vermittlungsdiensten im Binnenmarkt und für besondere Sorgfaltspflichten, die auf bestimmte Kategorien von Anbietern von Vermittlungsdiensten zugeschnitten sind, nämlich „reine Durchleitung“, „Caching“ und „Hosting“. Insbesondere werden Online-Plattformen und Online-Suchmaschinen, einschließlich solcher, die als sehr große Online-Plattformen oder sehr große Online-Suchmaschinen eingestuft wurden, besondere Sorgfaltspflichten auferlegt. Solche Sorgfaltspflichten spielen eine wichtige Rolle bei der Verhinderung der Verbreitung rechtswidriger Online-Inhalte wie Finanzbetrug. Beispielsweise sind Hostingdiensteanbieter verpflichtet, benutzerfreundliche Melde- und Abhilfeverfahren einzurichten, um die Meldung rechtswidriger Inhalte, wie rechtswidrige Angebote von Finanzdienstleistungen oder versuchter Betrug, an den Hostingdienst zu ermöglichen. Anbieter von Online-Plattformen sind auch verpflichtet, Meldungen vertrauenswürdiger Hinweisgeber vorrangig zu bearbeiten. Kann auf der Grundlage der dem Zahlungsdienstleister vom Zahler bereitgestellten Informationen oder anderer dem Zahlungsdienstleister zur Verfügung stehender Informationen davon ausgegangen werden, dass ein betrügerischer Zahlungsvorgang seinen Ursprung in einer Einzelinformation im Internet hat, sollten Zahlungsdienstleister die in Artikel 16 der Verordnung (EU) 2022/2065 genannten Meldeverfahren nutzen, um Hostingdiensteanbietern zu melden, dass diese Einzelinformation in ihren Diensten vorhanden ist. Wenn Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen Artikel 16 der Verordnung (EU) 2022/2065 nachkommen, insbesondere durch die Einrichtung leicht zugänglicher und benutzerfreundlicher Melde- und Abhilfeverfahren, sollte davon ausgegangen werden, dass sie der in der vorliegenden Verordnung festgelegten Verpflichtung nachkommen, die Nutzer ihrer Dienste über das Verfahren zur Meldung betrügerischer Aktivitäten in ihren Diensten zu informieren. Zahlungsdienstleister sollten auch den Status des „vertrauenswürdigen Hinweisgebers“ gemäß Artikel 22 der Verordnung (EU) 2022/2065 beantragen können.

(104) Mit der Verordnung (EU) 2022/2065 wird die Ausarbeitung freiwilliger Verhaltenskodizes auf Unionsebene gefördert und erleichtert, um zur ordnungsgemäßen Anwendung der genannten Verordnung beizutragen, wobei insbesondere den besonderen Herausforderungen bei der Bekämpfung verschiedener Arten rechtswidriger Inhalte und systemischer Risiken Rechnung getragen wird und gleichzeitig die Prävention gefördert, die Sicherheit verbessert und Zahlungs- und Finanzbetrug bekämpft wird. Die Ausarbeitung eines freiwilligen Verhaltenskodex auf Unionsebene in den unter die vorliegende Verordnung fallenden Bereichen sollte ebenfalls erleichtert werden.

(105) Die betrügerische Werbung für und das betrügerische Anbieten von Finanzdienstleistungen, wie die Werbung für Kredit-, Versicherungs- und Anlageprodukte und -dienstleistungen, einschließlich Kryptowerte, die von oder im Namen von Stellen angeboten werden, die nach dem Unionsrecht oder nationalem Recht zur Umsetzung des Unionsrechts für die Bereitstellung solcher Produkte und Dienstleistungen weder zugelassen noch registriert sind, kann mit Betrug bei Zahlungen aufgrund der Täuschung und Manipulation der Einwilligung der Zahlungsdienstnutzer in die Auslösung eines Zahlungsvorgangs oder einer Serie von Zahlungsvorgängen oder des Diebstahls sensibler Zahlungsdaten, einschließlich personalisierter Sicherheitsmerkmale, in Verbindung gebracht werden. Um diese betrügerische Werbung für und dieses betrügerische Anbieten von Finanzdienstleistungen zu verringern, sollten Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen von Werbetreibenden für regulierte Finanzdienstleistungen Informationen wie Zulassungs- oder Registrierungsnummern verlangen, aus denen hervorgeht, dass der Anbieter der beworbenen regulierten Finanzdienstleistung in einem Mitgliedstaat oder auf Unionsebene für die Erbringung solcher Dienstleistungen zugelassen oder registriert wurde. Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen sollten sicherstellen, dass ihre Dienste nicht zu Werbezwecken angeboten werden, bis der Werbetreibende die Informationen über die Registrierung oder Zulassung der Stelle, in deren Namen die Werbung getätigt wird, als regulierter Finanzdienstleister bereitstellt.

Diese Anforderung sollte weder auf eine Verpflichtung der betreffenden Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen hinauslaufen, die von Unternehmern über ihre Dienste angebotenen Produkte oder Dienstleistungen generell zu überwachen, noch auf eine allgemeine Verpflichtung zur Sachverhaltsaufklärung, insbesondere zur Bewertung der Richtigkeit der von Werbetreibenden bereitgestellten Informationen. Die betreffenden Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen sollten sich jedoch – nach Erhalt der Informationen über die Zulassung oder Registrierung des Anbieters der beworbenen regulierten Finanzdienstleistungen von den Werbetreibenden und bevor sie dem Werbetreibenden die Nutzung ihres Dienstes zum Zwecke der Werbung für diese regulierten Finanzdienstleistungen gestatten – nach besten Kräften bemühen, zu bewerten, ob die Informationen, für deren Richtigkeit für die Zwecke dieser Verordnung die Werbetreibenden verantwortlich sind, zuverlässig und vollständig sind, sofern die Bewertung in verhältnismäßiger Weise mithilfe automatisierter Instrumente durchgeführt werden kann. Die Europäischen Aufsichtsbehörden, d. h. die EBA, die durch die Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates[28] errichtete Europäische Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde) (ESMA) und die durch die Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates[29] errichtete Europäische Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung) (EIOPA), führen bereits öffentliche Register der Finanzdienstleister nach den geltenden Rechtsvorschriften. Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen könnten diese Register bei ihren Bemühungen nutzen, sicherzustellen, dass die vom potenziellen Werbetreibenden bereitgestellten Informationen zuverlässig und vollständig sind.

---

[28] Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

[29] Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

(106) Während Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen Transparenz- und Sorgfaltspflichten in Bezug auf Online-Werbung gemäß der Verordnung (EU) 2022/2065 haben, wird in der vorliegenden Verordnung weiter festgelegt, wie diese Pflichten im besonderen Fall der Werbung für regulierte Finanzdienstleistungen gelten sollten. Um ihrer Pflicht nachzukommen, angemessene Anstrengungen zu unternehmen, um sicherzustellen, dass die Informationen in ihren gemäß Artikel 39 der Verordnung (EU) 2022/2065 eingerichteten Archiven richtig und vollständig sind, könnten Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen insbesondere die Register zugelassener oder registrierter Anbieter regulierter Finanzdienstleistungen nutzen, die im Einklang mit dem einschlägigen Unionsrecht, einschließlich der Richtlinie (EU) 2026/…[+], zur Verfügung gestellt werden, einschließlich der von den Europäischen Aufsichtsbehörden geführten öffentlichen Register.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(107) Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen sind gemäß der Verordnung (EU) 2022/2065 verpflichtet, alle systemischen Risiken, die sich aus der Konzeption oder dem Betrieb ihrer Dienste ergeben, einschließlich der Verbreitung rechtswidriger Inhalte über ihre Dienste, wie schädliche oder betrügerische Inhalte im Internet im Sinne der vorliegenden Verordnung, sorgfältig zu ermitteln, zu analysieren und zu bewerten. Gegebenenfalls sollten Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen im Anschluss an diese Bewertung angemessene, verhältnismäßige und wirksame Risikominderungsmaßnahmen gemäß Artikel 35 der Verordnung (EU) 2022/2065 ergreifen, um diesen Risiken unter der direkten Aufsicht der Kommission entgegenzuwirken. Wenn Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen gemäß Artikel 35 der Verordnung (EU) 2022/2065 Risikominderungsmaßnahmen in Bezug auf das von ihnen gemäß Artikel 34 der genannten Verordnung ermittelte Risiko betrügerischer Werbung für regulierte Finanzdienstleistungen ergreifen müssen, könnten Maßnahmen, die im Einklang mit den in der vorliegenden Verordnung festgelegten Pflichten ergriffen werden, als eine Möglichkeit betrachtet werden, um sicherzustellen, dass diese Anbieter Artikel 35 Absatz 1 Buchstabe e der Verordnung (EU) 2022/2065 einhalten. Die Einhaltung der in der vorliegenden Verordnung festgelegten Pflichten sollte jedoch nicht unbedingt als ausreichend angesehen werden, um die Einhaltung von Artikel 35 Absatz 1 Buchstabe e der Verordnung (EU) 2022/2065 durch diese Anbieter sicherzustellen, und sollte daher weitere Risikominderungsmaßnahmen, die diese Anbieter möglicherweise ergreifen müssen, unberührt lassen.

(108) Zur Feststellung einer möglichen Fahrlässigkeit oder groben Fahrlässigkeit des Zahlungsdienstnutzers sollten alle individuellen Umstände des Falls berücksichtigt werden. Ob und in welchem Maße fahrlässig gehandelt wurde, sollte nach nationalem Recht beurteilt werden. Während der Begriff der Fahrlässigkeit einen Verstoß gegen eine Sorgfaltspflicht impliziert, sollte der Begriff „grobe Fahrlässigkeit“ mehr als reine Fahrlässigkeit bedeuten, sondern ein Verhalten bezeichnen, das ein erhebliches Maß an mangelnder Sorgfalt aufweist; beispielsweise die Aufbewahrung der zur Autorisierung eines Zahlungsvorgangs verwendeten Sicherheitsmerkmale neben dem Zahlungsinstrument in einem Format, das für Dritte offen und leicht auffindbar ist. Bei der Untersuchung der Möglichkeit einer groben Fahrlässigkeit des Zahlungsdienstnutzers sollten alle tatsächlichen Umstände berücksichtigt werden, beispielsweise die innovative Natur und Komplexität des Betrugs; die Mittel oder Strategien, die von Dritten eingesetzt werden, um die personalisierten Sicherheitsmerkmale des Zahlungsdienstnutzers rechtswidrig zu übernehmen; ob der Zahlungsdienstnutzer zuvor Opfer derselben Art von Betrug geworden ist; im Falle einer neuen Art von Betrug, ob die Zahlungsdienstleister ihren Pflichten aus dieser Verordnung nachgekommen sind, auch in Bezug auf ihre schutzbedürftigsten Kundengruppen; ob der Zahlungsdienstnutzer angemessene Schritte unternommen hat, um die Vertraulichkeit seiner personalisierten Sicherheitsmerkmale ordnungsgemäß zu gewährleisten; alle bekannten Merkmale des Zahlungsdienstnutzers, die die Wahrscheinlichkeit, Opfer von Betrug zu werden, erhöhen könnten; ob die Zahlungsdienstleister dem Zahler klare, spezifische und maßgeschneiderte Warnungen an die Hand gegeben haben und ob der Zahlungsdienstnutzer bestimmte, gezielte Eingriffe seines Zahlungsdienstleisters nicht berücksichtigt hat. Diese Liste ist nicht erschöpfend, kumulativ oder verbindlich und berührt nicht das Ermessen der Gerichte der Union oder der nationalen Gerichte oder der Streitbeilegungsstellen.

(109) Da der Begriff „grobe Fahrlässigkeit“ in der Union sehr unterschiedlich ausgelegt wird, wird die EBA aufgefordert, Leitlinien herauszugeben, um die tatsächlichen Umstände näher zu bestimmen, die bei der Untersuchung der Möglichkeit einer groben Fahrlässigkeit des Zahlungsdienstnutzers zu berücksichtigen sind.

(110) Vertragsbedingungen 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.

(111) Verbraucher sind besonders schutzbedürftig in Fällen von Zahlungsvorgängen, bei denen der genaue Betrag zum Zeitpunkt, an dem der Zahler seine Einwilligung 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 Zahlungsvorgangs im Verhältnis steht, der vom Zahler vernünftigerweise erwartet werden kann, und nur dann, wenn der Zahler dem Blockieren genau dieses Betrags zugestimmt hat. Diese Geldbeträge sollten unmittelbar nach Erhalt der Informationen über den exakten 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 exakten Betrag des Zahlungsvorgangs sicherzustellen, sollte der Zahlungsempfänger den Zahlungsdienstleister unverzüglich nach der Erbringung der Dienstleistung oder der Lieferung der Waren an den Zahler informieren.

(112) Die Mitgliedstaaten sollten 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 anderweitig geschützt ist, keinen Erstattungsanspruch hat. Ein Grund dafür könnte entweder sein, dass der Zahler die Einwilligung 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 Weise 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 die Abgleichdienstleistung fehlerhaft angewandt wurde oder ein Betrug unter Vortäuschung der Identität des Zahlungsdienstleisters verübt wurde, durch die allgemeine Erstattungsregel geschützt sein.

(113) 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, ab wann Rechte und Pflichten gelten, nämlich wenn der Zahlungsdienstleister den Zahlungsauftrag erhält – auch wenn der Zahlungsauftrag ihm über die im Zahlungsdienstvertrag vereinbarten Kommunikationsmittel zugegangen ist. Dies gilt ungeachtet einer vorherigen Beteiligung an dem Prozess, der zur Erstellung und Übermittlung des Zahlungsauftrags führt, einschließlich Sicherheits- oder Deckungsprüfungen, 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 zu dem er von seinem Zahlungsdienstleister eine Vorfinanzierung der entsprechenden Beträge (Gutschrift unter Vorbehalt) erhält, sollte hingegen unerheblich sein.

(114) Die Zahlungsdienstnutzer 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 oder anderweitig auf diese Ausführung zu verzichten, wie die Verpflichtungen gemäß der vorliegenden Verordnung oder der Verordnung (EU) 2024/1624.

(115) Da Betrug eine kriminelle Tätigkeit im Sinne des Artikels 2 Nummer 1 der Richtlinie (EU) 2018/1673 des Europäischen Parlaments und des Rates[30] ist, gilt er für die Zwecke der Verordnung (EU) 2024/1624 als Vortat. Aus diesem Grund gelten die in der genannten Verordnung festgelegten Pflichten zur Meldung verdächtiger Transaktionen gemäß Artikel 69 der genannten Verordnung und zum Verzicht auf die Durchführung dieser verdächtigen Transaktionen gemäß Artikel 71 der genannten Verordnung auch in Fällen, in denen ein Zahlungsdienstleister weiß oder vermutet, dass ein Zahlungsvorgang betrügerisch ist. Diese Pflichten gelten auch, wenn der Zahlungsdienstleister hinreichenden Grund zu der Annahme hat, dass ein Zahlungsvorgang im Zusammenhang mit einer kriminellen Tätigkeit steht, z. B. wenn der Zahlungsdienstleister des Zahlers hinreichenden Grund zu der Annahme hat, dass ein vom Zahler ausgelöster Zahlungsvorgang auf Betrug zurückzuführen sein könnte, oder wenn der Zahlungsdienstleister des Zahlungsempfängers, bevor er dem Zahlungsempfänger die Geldbeträge zur Verfügung stellt, hinreichenden Grund zu der Annahme hat, dass ein Zahlungsvorgang, der seinem Konto gutgeschrieben wurde oder gutgeschrieben werden wird, auf Betrug zurückzuführen sein könnte.

---

[30] Richtlinie (EU) 2018/1673 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 über die strafrechtliche Bekämpfung der Geldwäsche (ABl. L 284 vom 12.11.2018, S. 22, ELI: http://data.europa.eu/eli/dir/2018/1673/oj).

(116) Es ist notwendig, zwischen dem Ziel, zu verhindern, dass Zahlungsdienstnutzer Opfer von Betrug werden, dem Ziel, die Einhaltung der Verordnung (EU) 2024/1624 in Bezug auf verdächtige Transaktionen zu gewährleisten, und dem Ziel, die Auswirkungen auf Zahlungsdienstnutzer zu mindern, die sich aus Verzögerungen bei der Ausführung rechtmäßiger Zahlungsvorgänge oder der Ablehnung dieser Vorgänge ergeben, für Kohärenz zu sorgen. Aus diesem Grund sollte die Ablehnung eines Zahlungsdienstleisters, einen Zahlungsvorgang gemäß der vorliegenden Verordnung auszuführen, andere Verpflichtungen unberührt lassen, die sich für diesen Zahlungsdienstleister in Bezug auf diesen Zahlungsvorgang gemäß der Verordnung (EU) 2024/1624 ergeben, wie etwa die Verpflichtung, einen Verdacht gemäß Artikel 69 der genannten Verordnung der zentralen Meldestelle zu berichten. Im Falle von Überweisungen könnte das Ergebnis der gemäß der Verordnung (EU) Nr. 260/2012 und der vorliegenden Verordnung angewandten Dienstleistung zur Überprüfung des Zahlungsempfängers zwar ein relevantes Element bei der Transaktionsüberwachung durch den Zahlungsdienstleister im Hinblick auf die Aufdeckung von Betrug darstellen, doch sollte dieses Ergebnis nicht der einzige Grund für die Entscheidung des Zahlungsdienstleisters sein, die Ausführung des Zahlungsvorgangs abzulehnen, um das Recht des Zahlers sicherzustellen, den betreffenden Zahlungsvorgang gemäß Artikel 5c der Verordnung (EU) Nr. 260/2012 und der vorliegenden Verordnung zu autorisieren.

(117) Damit der Zahlungsdienstleister bewerten kann, ob es objektiv gerechtfertigte Gründe für den Verdacht gibt, dass ein Zahlungsvorgang betrügerisch ist, und damit er die Ausführung dieses Zahlungsvorgangs ablehnen kann, und um die Auswirkungen auf Zahlungsdienstnutzer in Bezug auf rechtmäßige Zahlungsvorgänge zu begrenzen, sollte sich der Zahlungsdienstleister des Zahlers an den Zahler wenden, um die für die Zwecke dieser Bewertung erforderlichen Informationen einzuholen, wobei die Vorschriften über das Verbot der Informationsweitergabe von Verdachtsfällen gemäß der Verordnung (EU) 2024/1624 uneingeschränkt einzuhalten sind. Der Zahlungsdienstleister des Zahlers sollte dem Zahler alle Informationen oder Maßnahmen mitteilen, die er vom Zahler für seine Bewertung benötigt, und ausreichende Informationen bereitstellen, damit der Zahler die vom Zahlungsdienstleister ermittelten Risiken verstehen kann. Der Zahlungsdienstleister des Zahlers sollte sicherstellen, dass der Zahler jederzeit über geeignete Mittel verfügt, um mit dem Zahlungsdienstleister Kontakt aufzunehmen, damit der Zahler die in dieser Mitteilung angeforderten Informationen bereitstellen oder die darin verlangten Maßnahmen ausführen kann, und der Zahlungsdienstleister sollte alle zumutbaren Anstrengungen unternehmen, um den Zahler zu kontaktieren, bevor er dem Konto des Zahlungsdienstleisters des Zahlungsempfängers die Geldbeträge gutschreibt. Gemäß Artikel 73 der Verordnung (EU) 2024/1624 sollte der Zahler oder gegebenenfalls der Zahlungsauslösedienstleister in dieser Kommunikation zwischen dem Zahlungsdienstleister des Zahlers und dem Zahler zu keinem Zeitpunkt davon in Kenntnis gesetzt werden, dass Zahlungsvorgänge oder -tätigkeiten gemäß Artikel 69 der Verordnung (EU) 2024/1624 bewertet werden oder wurden, dass gemäß den Artikeln 69 oder 70 der Verordnung (EU) 2024/1624 eine Informationsweitergabe stattfindet, stattfinden wird oder stattgefunden hat oder dass eine entsprechende Analyse stattfindet oder stattfinden könnte.

(118) Da der Betrag einer Echtzeitüberweisung in Euro gemäß der Verordnung (EU) Nr. 260/2012 innerhalb von zehn Sekunden nach Eingang des Zahlungsauftrags beim Zahlungsdienstleister des Zahlers auf dem Zahlungskonto des Zahlungsempfängers verfügbar sein sollte, sollten die Vorschriften, nach denen der Zahlungsdienstleister des Zahlers verpflichtet ist, den Zahler zu benachrichtigen und zu kontaktieren, wenn er die Ausführung eines Zahlungsvorgangs aufgrund eines Betrugsverdachts aussetzt, im Falle von Echtzeitüberweisungen nicht gelten. In diesen Fällen und in Fällen, in denen der Zahlungsdienstleister des Zahlers nach Benachrichtigung des Zahlers und Kontaktaufnahme mit diesem die erforderlichen Informationen dennoch nicht vor Ablauf der gesetzlichen Frist für die Gutschrift des Geldbetrags auf das Konto des Zahlungsdienstleisters des Zahlungsempfängers erhalten konnte, sollte der Zahlungsdienstleister des Zahlers seine Bewertung, ob objektiv gerechtfertigte Gründe für einen Betrugsverdacht vorliegen oder nicht, sowie seine Entscheidung, die Ausführung des Zahlungsvorgangs abzulehnen oder nicht, auf der Grundlage des Transaktionsüberwachungsmechanismus und aller anderen einschlägigen Informationen, die dem Zahlungsdienstleister zur Verfügung stehen, vornehmen, jedoch nicht allein aufgrund des Ergebnisses der Dienstleistung zur Überprüfung des Zahlungsempfängers.

(119) Für die Zwecke dieser Verordnung sollte die Tatsache, dass ein Zahlungsauftrag oder ein Zahlungsvorgang ungewöhnlich ist, weder automatisch einen Grund für den Verdacht darstellen, dass es sich um einen betrügerischen Zahlungsvorgang handelt, noch sollte sie für sich genommen einen objektiv gerechtfertigten Grund für einen Betrugsverdacht darstellen. Jeder ungewöhnliche Zahlungsauftrag oder Zahlungsvorgang könnte jedoch ein frühzeitiger Hinweis auf Betrug sein, der den Zahlungsdienstleister warnen sollte und möglicherweise weiter untersucht werden muss. Bei der Beurteilung, ob objektiv gerechtfertigte Gründe für einen Betrugsverdacht im Zusammenhang mit einem Zahlungsauftrag oder einem Zahlungsvorgang vorliegen, sollte der Zahlungsdienstleister die besonderen Umstände des einzelnen Auftrags oder Vorgangs sowie die umfassendere Bewertung des sich entwickelnden Betrugsrisikos durch den Zahlungsdienstleister auf der Grundlage der Transaktionsüberwachung des Zahlungsdienstleisters oder aller einschlägigen Informationen, die dem Zahlungsdienstleister zur Verfügung stehen, berücksichtigen. Beruht eine Entscheidung über die Ablehnung oder Aussetzung der Ausführung eines Zahlungsvorgangs ausschließlich auf einer automatisierten Abwicklung, wäre diese Entscheidung nur dann zulässig, wenn geeignete Maßnahmen ergriffen wurden, um die Rechte, Freiheiten und berechtigten Interessen des Zahlungsdienstnutzers zu schützen.

(120) Lehnt der Zahlungsdienstleister die Ausführung eines Zahlungsvorgangs ab, so sollte die Ablehnung und der Grund für die Ablehnung dem Zahler, dem Zahlungsdienstleister des Zahlungsempfängers und gegebenenfalls dem Zahlungsauslösedienstleister vorbehaltlich der Anforderungen des Unionsrechts und des nationalen Rechts unverzüglich oder im Falle von Echtzeitüberweisungen innerhalb von zehn Sekunden nach Eingang des Zahlungsauftrags beim Zahlungsdienstleister des Zahlers mitgeteilt werden. Darüber hinaus sollte der Zahlungsdienstleister des Zahlers den Zahler über das Verfahren informieren, das es dem Zahler ermöglicht, die Bewertung, die zur Ablehnung geführt hat, zu berichtigen oder diese Entscheidung rückgängig zu machen. 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. Der Zahlungsdienstleister des Zahlers sollte keine Gebühren erheben, wenn er die Ausführung eines Zahlungsvorgangs aufgrund eines Betrugsverdachts ablehnt.

(121) Angesichts der Geschwindigkeit, mit der vollautomatisierte Zahlungssysteme Zahlungen abwickeln, die dazu führt, dass Zahlungsaufträge ab einem bestimmten Zeitpunkt nicht ohne kostspieligen manuellen Eingriff widerrufen werden können, muss eine Widerrufsfrist für Zahlungen festgelegt werden. Allerdings sollten die Parteien je nach Art des Zahlungsdienstes und des Zahlungsauftrags unterschiedliche Widerrufsfristen 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.

(122) Die Unwiderrufbarkeit eines Zahlungsauftrags sollte nicht die Rechte oder Pflichten eines Zahlungsdienstleisters nach dem Recht der Mitgliedstaaten – basierend auf dem Rahmenvertrag des Zahlers, nationalen Rechts- und Verwaltungsvorschriften oder Leitlinien – in Bezug auf die Erstattung des Betrags, der Gegenstand des ausgeführten Zahlungsvorgangs war, an den Zahler im Falle einer Streitigkeit zwischen dem Zahler und dem Zahlungsempfänger berühren. Eine solche Erstattung sollte als neuer Zahlungsauftrag gelten. Mit Ausnahme dieser Fälle sollten Rechtsstreitigkeiten, die sich aus der dem Zahlungsauftrag zugrunde liegenden Beziehung ergeben, ausschließlich zwischen Zahler und Zahlungsempfänger geregelt werden.

(123) 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 den Zahlungsdienstleister zum Abzug seiner 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 Geldbeträge in voller Höhe, sondern auch die abgezogenen Entgelte aufgeführt werden.

(124) Die Verpflichtungen dieser Verordnung in Bezug auf Open-Banking-Schnittstellen und die Überprüfung des Zahlungsempfängers sollten nicht für Zahlungsvorgänge mit E-Geld-Token gelten. Die Ausweitung der Anwendung solcher Anforderungen auf Zahlungsvorgänge mit E-Geld-Token kann angesichts der hohen Kosten, die mit der Operationalisierung dieser Anforderungen verbunden sind, erheblichen Investitionsbedarf und eine unangemessene Belastung für die Unternehmen, die diese Dienste erbringen, mit sich bringen. Darüber hinaus ist es angesichts der Tatsache, dass Zahlungsvorgänge mit E-Geld-Token noch nicht so weit verbreitet sind wie typische Zahlungsvorgänge, weniger dringlich und schafft es weniger Mehrwert, solche Anforderungen für Zahlungsvorgänge mit E-Geld-Token vorzuschreiben.

(125) Um die Effizienz von Zahlungen in der gesamten Union zu verbessern, sollte für alle vom Zahler ausgelösten Zahlungsaufträge in Euro oder in der Währung eines Mitgliedstaats, dessen Währung nicht der Euro ist, einschließlich für andere Überweisungen als Echtzeitüberweisungen und für Finanztransfers, eine Ausführungsfrist von maximal einem Tag gelten, es sei denn, in den einschlägigen Rechtsvorschriften der Union oder der Mitgliedstaaten im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung ist etwas anderes vorgesehen. Für alle anderen Zahlungen, z. B. solche, die vom oder über den Zahlungsempfänger ausgelöst werden, einschließlich Lastschriften oder Kartenzahlungen, und sofern Zahlungsdienstleister und Zahler nicht ausdrücklich eine längere Ausführungsfrist vereinbart haben, sollte ebenfalls eine Eintagesfrist gelten. Diese Fristen sollten um einen zusätzlichen Geschäftstag verlängert werden können, wenn ein Zahlungsauftrag in Papierform erteilt wird, damit auch weiterhin Zahlungsdienste für Verbraucher erbracht werden können, die nur Papierform gewohnt 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 Abwicklung 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.

(126) Damit Zahler ihre Geldbeträge rasch wiedererlangen können, wenn ein hohes Risiko besteht, dass bei einem Zahlungsvorgang oder einer Serie von Zahlungsvorgängen Betrug vorliegen könnte, sollte in dieser Verordnung klargestellt werden, dass in Fällen, in denen der Zahlungsdienstleister des Zahlungsempfängers objektiv gerechtfertigte Gründe für den Verdacht hat, dass bei einem Zahlungsvorgang, der seinem Konto gutgeschrieben wurde oder gutgeschrieben werden soll, bzw. bei einer Serie von Zahlungsvorgängen, die seinem Konto gutgeschrieben wurden oder gutgeschrieben werden sollen, Betrug vorliegen könnte, und in denen dieser Zahlungsdienstleister es unterlässt, diese Geldbeträge auf dem Zahlungskonto des Zahlungsempfängers zur Verfügung zu stellen, um seiner Verpflichtung gemäß Artikel 71 der Verordnung (EU) 2024/1624 nachzukommen, auf die Durchführung verdächtiger Transaktion zu verzichten, dieser Zahlungsdienstleister entweder den seinem Konto gutgeschriebenen Geldbetrag an den Zahlungsdienstleister des Zahlers zurückzahlen oder den Zahlungsvorgang oder die Serie von Zahlungsvorgängen, die seinem Konto vom Zahlungsdienstleister des Zahlers gutgeschrieben werden sollen, ablehnen kann. Um den Schutz der Zahler zu verbessern, sollte vorgeschrieben werden, dass in bestimmten Fällen, in denen stärkere Hinweise auf Betrug vorliegen, der Zahlungsdienstleister des Zahlungsempfängers den Geldbetrag entweder an den Zahlungsdienstleister des Zahlers zurückzuzahlen oder den Zahlungsvorgang oder die Serie von Zahlungsvorgängen, der bzw. die vom Zahlungsdienstleister des Zahlers seinem Konto gutzuschreiben ist bzw. sind, abzulehnen hat. Um übermäßige risikomindernde Praktiken zu vermeiden, sollte eine höhere Beweisschwelle festgelegt werden, ab der diese Verpflichtung und die entsprechende Haftung gelten sollten, wenn der Zahlungsdienstleister des Zahlungsempfängers stichhaltige, kohärente und unstreitige Beweise oder Anhaltspunkte hat, die ohne plausible alternative Erklärung zu dem Schluss führen, dass der Zahlungsvorgang oder die Serie von Zahlungsvorgängen das Ergebnis von Betrug ist.

(127) Um das Vertrauen der Zahlungsdienstnutzer in die Zuverlässigkeit von Zahlungsdiensten zu erhalten, muss sichergestellt werden, dass Maßnahmen zur Betrugsprävention, die Auswirkungen auf die Ausführung von Zahlungsvorgängen haben, dem Zahler, seinem Zahlungsdienstleister und gegebenenfalls dem Zahlungsauslösedienstleister innerhalb der in der vorliegenden Verordnung und in der Verordnung (EU) Nr. 260/2012 festgelegten Fristen für die Ausführung dieser Zahlungsvorgänge, in ausreichendem Maße mitgeteilt werden, wobei die in der Verordnung (EU) 2024/1624 festgelegten Vorschriften über das Verbot der Informationsweitergabe in vollem Umfang einzuhalten sind. Um eine uneinheitliche Anwendung dieser Schutz- und Transparenzmaßnahmen bei Echtzeitüberweisungen in Euro und bei Echtzeitüberweisungen in anderen Währungen zu verhindern, sollte in der vorliegenden Verordnung festgelegt werden, dass bei jeder Echtzeitüberweisung, bei der sich der Zahlungsdienstleister des Zahlungsempfängers im Einklang mit der vorliegenden Verordnung weigert, dem Zahlungsempfänger den Geldbetrag zur Verfügung zu stellen, und den Geldbetrag gegebenenfalls an den Zahlungsdienstleister des Zahlers zurückzahlt oder der Zahlungsdienstleister des Zahlungsempfängers den Zahlungsvorgang oder die Serie von Zahlungsvorgängen, der bzw. die vom Zahlungsdienstleister des Zahlers seinem Konto gutzuschreiben ist bzw. sind, ablehnt, der Zahlungsdienstleister des Zahlungsempfängers den Zahlungsdienstleister des Zahlers innerhalb von zehn Sekunden nach Eingang des Zahlungsauftrags für diese Echtzeitüberweisung oder Serie von Echtzeitüberweisungen über diese Weigerung unterrichtet. Nach Erhalt einer solchen Mitteilung sollte der Zahlungsdienstleister des Zahlers das Zahlungskonto des Zahlers unverzüglich wieder auf den Stand bringen, auf dem es sich ohne den Zahlungsvorgang befunden hätte, und den Zahler und gegebenenfalls den Zahlungsauslösedienstleister kostenlos über die Rückzahlung des Geldbetrags und darüber informieren, dass der Geldbetrag aufgrund von Betrugsbekämpfungsmaßnahmen nicht auf dem Zahlungskonto des Zahlungsempfängers bereitgestellt wurde. Gemäß Artikel 73 der Verordnung (EU) 2024/1624 sollte der Zahler oder gegebenenfalls der Zahlungsauslösedienstleister in diesen Mitteilungen zu keinem Zeitpunkt davon in Kenntnis gesetzt werden, dass Zahlungsvorgänge oder -tätigkeiten gemäß Artikel 69 der Verordnung (EU) 2024/1624 bewertet werden oder wurden, dass gemäß den Artikeln 69 oder 70 der Verordnung (EU) 2024/1624 eine Informationsweitergabe stattfindet, stattfinden wird oder stattgefunden hat oder dass eine entsprechende Analyse stattfindet oder stattfinden könnte.

(128) Ist einer der Zahlungsdienstleister nicht in der Union ansässig, sollten die Regeln über die Gutschrift des vollen Betrags und die Ausführungsfrist als bewährte Praxis gelten. Bei der Ausführung von Überweisungen oder Finanztransfers an einen außerhalb der Union ansässigen Zahlungsempfänger sollte der Zahlungsdienstleister des Zahlers dem Zahler eine Schätzung des Zeitraums zur Verfügung stellen, der für die Gutschrift der Überweisung oder des Finanztransfers an den Zahlungsdienstleister des Zahlungsempfängers außerhalb der Union benötigt wird. Von einem Zahlungsdienstleister in der Union kann nicht erwartet werden, dass er den Zeitraum schätzt, den ein Zahlungsdienstleister außerhalb der Union benötigt, um den Geldbetrag nach Erhalt dem Konto des Zahlungsempfängers gutzuschreiben.

(129) 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 dementsprechend 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.

(130) Der Zahlungsdienstleister sollte unmissverständlich angeben können, welche Informationen für die ordnungsgemäße Ausführung eines Zahlungsvorgangs erforderlich sind. Unbeschadet seiner Verpflichtung, die Dienstleistung zur Überprüfung des Zahlungsempfängers zu erbringen, sollte der Zahlungsdienstleister des Zahlers mit der gebotenen Sorgfalt handeln und überprüfen, ob der Kundenidentifikator kohärent ist, und wenn das nicht der Fall ist und der betreffende Zahlungsvorgang daher nicht ausgeführt werden kann, diesen Zahlungsauftrag zurückweisen und den Zahler davon unterrichten.

(131) 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. Es ist der Zahlungsdienstleister, der den Zahlungsvorgang ausführt, Vorkehrungen trifft, um fehlgeleitete oder falsch zugewiesene Geldbeträge zurückzurufen, und in den meisten Fällen darüber entscheidet, welche zwischengeschalteten Stellen an dieser Ausführung beteiligt werden. Daher ist es, außer im Falle außergewöhnlicher und unvorhersehbarer Umstände und sofern in dieser Verordnung oder anderen einschlägigen Rechtsvorschriften der Union nichts anderes vorgesehen ist, angemessen, 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 die zwischengeschaltete Stelle (üblicherweise eine unparteiische Stelle wie eine Zentralbank oder eine Clearingstelle), die 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 diesen Zahlungsdienstleister auf Gutschrift des Betrags auf seinem Konto haben.

(132) Der Zahlungsdienstleister des Zahlers, also der kontoführende Zahlungsdienstleister oder gegebenenfalls der Zahlungsauslösedienstleister, sollte die Haftung für die ordnungsgemäße Ausführung des Zahlungsvorgangs, einschließlich des vollen Betrags und der Ausführungsfrist, sowie die volle Verantwortung für Fehler anderer Parteien in der Zahlungskette bis zum Zahlungskonto des Zahlungsempfängers übernehmen. Infolge dieser Haftung sollte der Zahlungsdienstleister des Zahlers, 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. Aufgrund der Haftung des Zahlungsdienstleisters sollten Zahler oder Zahlungsempfänger im Zusammenhang mit einer fehlerhaften Zahlung keine Kosten tragen. Im Fall einer nicht erfolgten, fehlerhaften oder verspäteten Ausführung von Zahlungsvorgängen sollte das Wertstellungsdatum korrigierender Zahlungen durch Zahlungsdienstleister stets dem Datum der Wertstellung bei korrekter Ausführung entsprechen.

(133) 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 fehlerhaften Zahlungsvorgangs sollten Gegenstand einer Vereinbarung sein.

(134) Für die Zwecke der Verordnung (EU) 2022/2065 sollte der Begriff rechtswidrige Inhalte so ausgelegt werden, dass er sich unabhängig von der Form dieser Inhalte auf Informationen bezieht, die nach geltenden Rechtsvorschriften der Union oder der Mitgliedstaaten entweder an sich rechtswidrig sind, oder nach dem geltenden Recht rechtswidrig sind, weil sie mit rechtswidrigen Handlungen zusammenhängen. Beispiele hierfür sind Angebote von Finanzdienstleistungen, einschließlich Zahlungsdiensten, die nicht den Anforderungen entsprechen, die nach der vorliegenden Verordnung, der Richtlinie (EU) 2026/…[+] oder anderen Rechtsvorschriften der Union oder der Mitgliedstaaten für das Angebot solcher Dienste gelten, oder Inhalte, die angesichts der nationalen Rechtsvorschriften über Betrug, einschließlich Verstöße, die in den gemäß der Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates[31] erlassenen nationalen Rechtsvorschriften festgelegt sind, rechtswidrig sind.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

[31] Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates (ABl. L 123 vom 10.5.2019, S. 18, ELI: http://data.europa.eu/eli/dir/2019/713/oj).

(135) Ansprüche eines Zahlungsdienstleisters gegen andere Anbieter, z. B. Anbieter elektronischer Kommunikationsdienste oder Anbieter von Vermittlungsdiensten, wegen eines im Zusammenhang mit Betrug entstandenen finanziellen Schadens sollten im Einklang mit dem nationalen Recht geltend gemacht werden.

(136) In Bezug auf Anbieter von Vermittlungsdiensten wird mit der Verordnung (EU) 2022/2065 ein vollständig harmonisierter Rahmen für den bedingten Haftungsausschluss dieser Anbieter unter bestimmten Bedingungen und nach der Auslegung des Gerichtshofs der Europäischen Union geschaffen. Um den Haftungsausschluss für Hostingdienste gemäß der Verordnung (EU) 2022/2065 in Anspruch nehmen zu können, sollten Hostingdiensteanbieter, einschließlich Online-Plattformen, rechtswidrige Inhalte unverzüglich entfernen oder den Zugang dazu sperren, sobald sie tatsächliche Kenntnis davon erhalten oder – im Falle von Schadensersatzansprüchen – ein entsprechendes Bewusstsein erlangen, insbesondere in Fällen, in denen Hostingdiensteanbieter auf Tatsachen oder Umstände aufmerksam gemacht wurde, auf deren Grundlage ein sorgfältiger Wirtschaftsakteur die betreffende Rechtswidrigkeit hätte erkennen müssen. Insbesondere in Bezug auf Hostingdiensteanbieter im Sinne des Artikels 3 Buchstabe g Ziffer iii der Verordnung (EU) 2022/2065 sollten Zahlungsdienstleister, wenn diese Voraussetzungen für einen Haftungsausschluss nach Artikel 6 Absatz 1 der genannten Verordnung nicht erfüllt sind und Hostingdiensteanbieter für in ihren Diensten gespeicherte Inhalte haften, und wenn diese Inhalte zu einem oder einer Serie von nicht autorisierten oder betrügerischen, autorisierten Zahlungsvorgängen im Sinne der vorliegenden Verordnung geführt haben, von den Hostingdiensteanbietern eine Entschädigung für den Betrag verlangen können, der ihren Kunden für diese Zahlungsvorgänge im Rahmen der vorliegenden Verordnung erstattet wurde.

(137) Keine Bestimmung dieser Verordnung sollte als allgemeine Verpflichtung der Hostingdiensteanbieter ausgelegt werden, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen, oder als Verpflichtung dieser Anbieter, aktiv nach Fakten oder Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hindeuten, wie etwa die Vortäuschung der Identität eines Zahlungsdienstleisters.

(138) Das Erbringen von Zahlungsdiensten durch 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[32], einschließlich der Grundsätze der Zweckbindung, der Datenminimierung und der Speicherbegrenzung, erfolgen. In allen im Rahmen der vorliegenden 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 Anwendung der vorliegenden Verordnung zuständig sein.

---

32 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(139) Wie in der Mitteilung der Kommission über eine EU-Strategie für den Massenzahlungsverkehr anerkannt wird, ist das reibungslose Funktionieren der Zahlungsmärkte in der Union, einschließlich der Sicherheit von Zahlungen und des Schutzes der Zahlungsdienstnutzer vor Betrug, von erheblichem öffentlichen Interesse. Wenn dies im Zusammenhang mit der vorliegenden Verordnung für die Erbringung von Zahlungsdiensten und die Einhaltung der vorliegenden Verordnung erforderlich ist, sollten Zahlungsdienstleister und Zahlungssystembetreiber 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 im Einklang mit Artikel 9 Absatz 2 Buchstabe g bzw. Artikel 10 Absatz 2 Buchstabe g der genannten Verordnungen zu verarbeiten. Werden besondere Kategorien personenbezogener Daten verarbeitet, sollten Zahlungsdienstleister und Zahlungssystembetreiber 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.

(140) 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.

(141) Betrüger richten sich häufig gegen die schutzbedürftigsten Personen unserer Gesellschaft. Die rechtzeitige Aufdeckung betrügerischer Zahlungsvorgänge ist von wesentlicher Bedeutung, und die Transaktionsüberwachung spielt bei dieser Aufdeckung eine wichtige Rolle. Es ist daher angezeigt, sowohl dem Zahlungsdienstleister des Zahlers als auch dem Zahlungsdienstleister des Zahlungsempfängers vorzuschreiben, dass sie über Transaktionsüberwachungsmechanismen verfügen müssen – was den entscheidenden Beitrag dieser Mechanismen zur Betrugsprävention widerspiegelt – die über den Schutz hinausgehen, den eine starke Kundenauthentifizierung in Bezug auf Zahlungsvorgänge, einschließlich Zahlungsauslösediensten, bietet. Der Zahlungsdienstleister des Zahlers sollte eine solche Transaktionsüberwachung vor der Ausführung eines Zahlungsvorgangs durchführen, was bei Echtzeitüberweisungen in Echtzeit bedeutet. Der Zahlungsdienstleister des Zahlungsempfängers sollte eine solche Transaktionsüberwachung durchführen, bevor er dem Zahlungsempfänger den Geldbetrag zur Verfügung stellt. Kommt ein Zahlungsdienstleister seinen Verpflichtungen bei der Anwendung der Transaktionsüberwachung in Bezug auf einen Zahlungsvorgang oder eine Serie von Zahlungsvorgängen nicht nach und wurde dieser Zahlungsvorgang oder diese Serie von Zahlungsvorgängen auf betrügerische Weise oder auf andere Weise infolge von Betrug ausgelöst, so sollte dem Zahler von seinem Zahlungsdienstleister der volle Betrag dieses Zahlungsvorgangs oder dieser Serie von Zahlungsvorgängen erstattet werden. Ist der Zahlungsdienstleister des Zahlungsempfängers derjenige Zahlungsdienstleister, der keine Transaktionsüberwachung durchgeführt hat, so sollte er dem Zahlungsdienstleister des Zahlers den Betrag erstatten, den dieser dem Zahler erstattet hat.

(142) Die EBA sollte Entwürfe technischer Regulierungsstandards zu den spezifischen technischen Anforderungen in Bezug auf Transaktionsüberwachungsmechanismen ausarbeiten. Diese Anforderungen sollten auf dem Mehrwert aufbauen, der sich aus umgebungs- und verhaltensbezogenen Merkmalen im Zusammenhang mit den Zahlungsgewohnheiten des Zahlungsdienstnutzers ergibt.

(143) Zahlungsdienstleister sollten in der Lage sein, Informationen über die Transaktionen ihrer Kunden und ihre Zahlungskonten in dem Umfang zu verarbeiten, der erforderlich ist, um sicherzustellen, dass die Transaktionsüberwachungsmechanismen es ihnen wirksam ermöglichen, Betrug aufzudecken und zu verhindern, insbesondere durch die Aufdeckung atypischer Verhaltensweisen des Zahlungsdienstnutzers, die auf einen potenziell betrügerischen Vorgang oder eine potenziell betrügerische Nutzung des Zahlungskontos hindeuten könnten. Die von Zahlungsdienstleistern durchgeführte Transaktionsüberwachung könnte, soweit dies zur Aufdeckung von Betrug erforderlich ist, die Verarbeitung von Informationen umfassen, die über die Dienstleistung zur Überprüfung des Zahlungsempfängers oder im Rahmen von Vereinbarungen über den Informationsaustausch gemäß dieser Verordnung oder anderen einschlägigen Rechtsvorschriften der Union ausgetauscht werden.

(144) Zahlungsdienstleister sollten Daten, die zum Zwecke der Erfüllung ihrer Pflichten in Bezug auf die Transaktionsüberwachung und den Informationsaustausch über Betrug verarbeitet werden, nur so lange speichern, wie dies für diese Zwecke erforderlich ist, und in jedem Fall nur höchstens fünf Jahre nach Beendigung der Kundenbeziehung. Wie aus den überarbeiteten Empfehlungen der Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung“ hervorgeht, sollten die Verpflichteten die erforderlichen Informationen, die sie durch Kundensorgfaltsmaßnahmen erlangt haben, sowie die Aufzeichnungen über Transaktionen mindestens fünf Jahre lang aufbewahren, um eine umfassende Kooperation leisten und den Informationsersuchen der zuständigen Behörden zwecks Verhinderung, Aufdeckung und Untersuchung von Geldwäsche oder Terrorismusfinanzierung zeitnah nachkommen zu können. Dementsprechend ist in der Verordnung (EU) 2024/1624 festgelegt, dass die Aufbewahrungsfrist für personenbezogene Daten, die im Einklang mit der genannten Verordnung verarbeitet werden, einschließlich in Bezug auf Informationen, die im Rahmen von Partnerschaften für den Informationsaustausch gemäß Artikel 75 der genannten Verordnung verarbeitet werden, auf fünf Jahre nach Beendigung einer Geschäftsbeziehung oder einer gelegentlichen Transaktion festgesetzt werden sollte. Da Betrug für die Zwecke der Verordnung (EU) 2024/1624 als Vortat gilt, ist es angemessen, eine maximale Aufbewahrungsfrist für gemäß der vorliegenden Verordnung verarbeitete personenbezogene Daten festzulegen, die ebenfalls auf fünf Jahre nach Beendigung einer Geschäftsbeziehung oder einer gelegentlichen Transaktion festgesetzt werden sollte, um Rechtssicherheit und Kohärenz zwischen den Präventions- und Aufdeckungsmaßnahmen im Bereich der Finanzstraftaten zu gewährleisten.

(145) Betrug ist naturgemäß wandelbar und umfasst eine unerschöpfliche Vielfalt an Verfahren und Techniken, einschließlich des Diebstahls von Authentifizierungsdaten, der Manipulation von Rechnungen und sozialer Manipulation. Um immer neue Arten von Betrug verhindern zu können, sollte die Transaktionsüberwachung daher kontinuierlich verbessert werden, wobei Technologien wie künstliche Intelligenz sowie Informationen zu Betrugsfällen, die so vollständig und aktuell wie möglich sein sollten, zu nutzen sind. Häufig hat ein Zahlungsdienstleister keinen vollständigen Überblick über alle Elemente und Indikatoren, die zur zeitnahen Aufdeckung potenziell betrügerischer Aktivitäten bei einem bestimmten Zahlungsvorgang führen könnten. Der Informationsaustausch zwischen Zahlungsdienstleistern kann die Möglichkeiten verbessern, potenziellen Betrug besser aufzudecken und die Zahlungsdienstnutzer besser zu schützen. Aus diesem Grund sollten Zahlungsdienstleister für die Zwecke der Transaktionsüberwachung die von anderen Zahlungsdienstleistern weitergegeben Daten über Zahlungsbetrug nutzen, und diese Daten im Rahmen von Vereinbarungen über den Informationsaustausch auf multilateraler Basis an andere Zahlungsdienstleistern weitergeben. Umfasst die Weitergabe von Informationen die Verarbeitung personenbezogener Daten, so sollte diese Weitergabe auf die Arten personenbezogener Daten beschränkt sein, die Zahlungsdienstleister zum Zwecke der Transaktionsüberwachung gemäß dieser Verordnung verarbeiten können. Umgebungs- und verhaltensbezogene Merkmale, die für den Zahlungsdienstnutzer bei normaler Verwendung der personalisierten Sicherheitsmerkmale typisch sind, sollten jedoch nicht weitergegeben werden. Die weitergegebenen Daten sollten sich auf die spezifischen Zahlungsvorgänge beziehen, bei denen der Zahlungsdienstleister einen Betrugsverdacht hat, und nicht auf damit verbundene frühere oder nachfolgende Zahlungsvorgänge. Die Zahlungsdienstleister sollten auch die objektiv gerechtfertigten Gründe mitteilen, die zu dem Verdacht auf betrügerische Aktivitäten im Zusammenhang mit dem betreffenden Zahlungsvorgang geführt haben, und, wenn dieser Zahlungsvorgang mit einer potenziell betrügerischen Einzelinformation in Verbindung steht, die von einem Hostingdiensteanbieter gespeichert wird, auch die Informationen über die Meldung an diesen Hostingdiensteanbieter mitteilen.

(146) Der Informationsaustausch sollte soliden, aktuellen Garantien in Bezug auf Vertraulichkeit, Datenschutz und Nutzung von Informationen, wie Pseudonymisierung und Verschlüsselung, Zugangs- und Nutzerkontrolle, unterliegen und im Einklang mit der Verordnung (EU) 2016/679 stehen. Bevor Zahlungsdienstleister eine Vereinbarung über den Informationsaustausch schließen, sollten sie eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der genannten Verordnung 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 genannten Verordnung 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. Ferner sollten darin die Rollen und Zuständigkeiten aller beteiligten Zahlungsdienstleister im Einklang mit den Datenschutzvorschriften festgelegt werden, auch im Falle gemeinsam Verantwortlicher.

(147) Zahlungsdienstleister können Daten im Zusammenhang mit Zahlungsvorgängen bei Verdacht auf Betrug mit anderen Teilnehmern von gemäß Artikel 75 der Verordnung (EU) 2024/1624 eingerichteten Partnerschaften für den Informationsaustausch austauschen, einschließlich zuständiger Behörden wie zentraler Meldestellen, Aufsichtsbehörden und Behörden, deren Aufgabe es ist, Geldwäsche, deren Vortaten oder Terrorismusfinanzierung zu untersuchen oder strafrechtlich zu verfolgen, oder deren Aufgabe es ist, Vermögenswerte aus Straftaten zu ermitteln, sicherzustellen oder einzufrieren und einzuziehen, im Einklang mit den Grundrechten und den gerichtlichen Verfahrensgarantien. Zahlungsdienstleister können im Rahmen von Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen gemäß Artikel 45 der Verordnung (EU) 2022/2554 zudem Daten im Zusammenhang mit Bedrohungen für die Sicherheit ihrer IKT-Systeme, auch wenn Spoofing, Phishing und Schadsoftware zum Betrug gegen Zahlungsdienstnutzer verwendet werden, an andere Zahlungsdienstleister und andere Teilnehmer, einschließlich Behörden, weitergeben. Da solche Partnerschaften oder Vereinbarungen bereits einen angemessenen Rahmen für die Beteiligung von Behörden, einschließlich Strafverfolgungsbehörden, an der freiwilligen Weitergabe von Daten im Zusammenhang mit Betrug vorbehaltlich angemessener Garantien bieten, wird es nicht als notwendig erachtet, im Rahmen dieser Verordnung eine zusätzliche Regelung für einen solchen Austausch zu schaffen.

(148) Beteiligt sich ein Zahlungsdienstleister an Partnerschaften oder Vereinbarungen über den Informationsaustausch, die gemäß Artikel 75 der Verordnung (EU) 2024/1624 und Artikel 45 der Verordnung (EU) 2022/2554 eingerichtet wurden, und ermöglichen diese Partnerschaften oder Vereinbarungen über den Informationsaustausch es dem Zahlungsdienstleister, Daten auszutauschen, die für die Aufdeckung und Verhinderung von Betrug gemäß der vorliegenden Verordnung erforderlich sind, so sollte der Datenaustausch im Rahmen dieser Partnerschaften über den Informationsaustausch als ausreichend angesehen werden, um sicherzustellen, dass der Zahlungsdienstleister seinen Verpflichtungen aus der vorliegenden Verordnung zur Weitergabe von Daten über Zahlungsbetrug im Rahmen von Vereinbarungen über den Informationsaustausch nachkommt. Beteiligen sich Zahlungsdienstleister an diesen Partnerschaften oder Vereinbarungen über den Informationsaustausch, um den Verpflichtungen aus der vorliegenden Verordnung nachzukommen, so sollten sie personenbezogene Daten, die im Rahmen solcher Partnerschaften oder Vereinbarungen ausgetauscht werden, verarbeiten dürfen, um den in der vorliegenden Verordnung festgelegten Pflichten zur Transaktionsüberwachung nachzukommen.

(149) Um zu verhindern, dass ein rechtmäßiger Informationsaustausch über potenziell betrügerische Aktivitäten zu ungerechtfertigten risikomindernden Maßnahmen oder einem ungerechtfertigten Entzug von Zahlungskontodiensten für Zahlungsdienstnutzer führt, ohne dass eine Erklärung gegeben wird oder ein Rückgriffsrecht besteht, sollten Schutzmaßnahmen vorgesehen werden. Im Rahmen einer multilateralen Vereinbarung über den Informationsaustausch weitergegebene Daten über Zahlungsbetrug, die die Offenlegung personenbezogener Daten, einschließlich Kundenidentifikatoren von Zahlungsempfängern, welche möglicherweise an betrügerischen Überweisungen beteiligt sind, nach sich ziehen könnten, sollten von Zahlungsdienstleistern nur zur Verbesserung der Transaktionsüberwachung verwendet werden. Zahlungsdienstleister sollten zusätzliche Schutzvorkehrungen treffen, wie z. B. die Kontaktaufnahme mit dem Kunden, wenn dieser der Zahler einer Überweisung ist, die als betrügerisch angesehen werden kann, sowie die weitere Überwachung eines Kontos, wenn der als potenziell betrügerisch gekennzeichnete Kundenidentifikator einen Kunden dieses Zahlungsdienstleisters benennt. Daten über Zahlungsbetrug, die im Rahmen solcher Vereinbarungen zwischen Zahlungsdienstleistern weitergegeben werden, sollten ohne eingehende Untersuchung keinen Grund für den Entzug von Zahlungskontodiensten darstellen.

(150) Bei der Entwicklung von Maßnahmen zur Betrugsbekämpfung im Bereich der Zahlungsdienste ist es besonders wichtig, angemessene Konsultationen mit den einschlägigen Interessenträgern durchzuführen, um bewährte Verfahren und Erfahrungen auszutauschen. Diese Konsultationen sollten sich auf Beiträge von Sachverständigen aus dem öffentlichen und privaten Sektor stützen, die nachweislich über Kenntnisse und Erfahrungen in den betreffenden Bereichen verfügen. Zu diesem Zweck sollte die Kommission eine Plattform zur Betrugsbekämpfung einrichten. Die Plattform zur Betrugsbekämpfung sollte sich aus Sachverständigen zusammensetzen und kann beispielsweise Vertreter der einschlägigen Einrichtungen der Union, der zuständigen nationalen Behörden, Zahlungsdienstleister, technische Dienstleister, Anbieter von Online-Plattformen, Telekommunikationsanbieter, Internetdiensteanbieter, Sachverständige, die verschiedene Zahlungssysteme oder Zahlverfahren vertreten, Händler, Verbraucherorganisationen und Streitbeilegungsstellen umfassen.

(151) Die Plattform zur Betrugsbekämpfung sollte gemäß den geltenden horizontalen Vorschriften für die Einsetzung und Arbeitsweise von Sachverständigengruppen der Kommission eingerichtet werden, auch im Hinblick auf das Auswahlverfahren. Ziel des Auswahlverfahrens sollte es sein, ein hohes Maß an Fachwissen, eine ausgewogene geografische Verteilung und ein ausgewogenes Geschlechterverhältnis sowie ein ausgewogenes Vorhandensein einschlägiger Kenntnisse und Erfahrungen zu gewährleisten, wobei die spezifischen Aufgaben der Plattform zur Betrugsbekämpfung zu berücksichtigen sind. Während des Auswahlverfahrens sollte die Kommission im Einklang mit diesen horizontalen Vorschriften eine Bewertung durchführen, um festzustellen, ob potenzielle Interessenkonflikte zwischen den Bewerbern, die zur Auswahl stehen, bestehen, und geeignete Maßnahmen ergreifen, um solche Konflikte zu verhindern oder zu bewältigen.

(152) Die Plattform zur Betrugsbekämpfung sollte die Kommission bei der Ausarbeitung und Überwachung der Umsetzung von Rechtsakten zur Betrugsbekämpfung im Bereich der Zahlungsdienste beraten. Für die Zwecke der Ausarbeitung eines freiwilligen Verhaltenskodex zur Förderung der Prävention, zur Erhöhung der Sicherheit und zur Bekämpfung von Zahlungs- und Finanzbetrug sollte die Plattform zur Betrugsbekämpfung Empfehlungen an die Kommission und das Europäische Gremium für digitale Dienste richten. Die Plattform zur Betrugsbekämpfung sollte ferner Informationen über und Analysen von Betrugstrends im Bereich der Zahlungsdienste, Informationen über Maßnahmen zur Betrugsbekämpfung im Bereich der Zahlungsdienste, einschließlich Risikominderungsmaßnahmen, und Informationen darüber, wie die grenzüberschreitende und sektorübergreifende Zusammenarbeit bei der Betrugsbekämpfung im Bereich der Zahlungsdienste verbessert werden kann, teilen. Die Plattform für Betrugsbekämpfung sollte ihre Aufgaben im Einklang mit dem Grundsatz der Transparenz wahrnehmen. Sie sollte auch die Arbeit bestehender Initiativen zur Bekämpfung von Zahlungsbetrug berücksichtigen, um Doppelarbeit zu vermeiden, und eng mit ihnen zusammenarbeiten.

(153) 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 zu helfen, zu erkennen, dass sie Opfer eines Betrugsversuchs sind. Zahlungsdienstleister sollten ihren Kunden über verschiedene Medien angemessene Informationen über Betrug zur Verfügung stellen, indem sie ihnen klare Botschaften und Warnungen geben und ihnen dabei helfen, angemessen zu reagieren, wenn sie potenziell betrügerischen Situationen ausgesetzt sind. Die EBA sollte dazu angehalten werden, Leitlinien zu den verschiedenen Programmen auszuarbeiten, die von Zahlungsdienstleistern zu Zahlungsbetrugsrisiken zu entwickeln sind, wobei dem sich ständig wandelnden Charakter von Betrugsrisiken Rechnung zu tragen ist, wenn sie dies für erforderlich hält, um die Kohärenz solcher Programme in der gesamten Union zu erreichen.

(154) Das Bewusstsein für Betrugsbedrohungen ist von entscheidender Bedeutung, um den Schutz der Zahlungsdienstnutzer vor solchen Bedrohungen und damit ihr Vertrauen in die Nutzung von Zahlungsdiensten in der gesamten Union zu verbessern, insbesondere angesichts der sich rasch wandelnden Techniken und Strategien, die von Betrügern eingesetzt werden. Die Mitgliedstaaten können eine entscheidende Rolle dabei spielen, das Bewusstsein und die Vorsorge der Bürger in dieser Hinsicht gemeinsam zu verbessern, und zwar über die individuellen Informationen hinaus, die die Diensteanbieter ihren Kunden zur Verfügung stellen. Gemäß der Richtlinie (EU) 2022/2555 sind die Mitgliedstaaten bereits verpflichtet, nationale Cybersicherheitsstrategien zu entwickeln, in deren Rahmen spezifische Konzepte zur Förderung und Entwicklung der allgemeinen und beruflichen Bildung im Bereich der Cybersicherheit, von Kompetenzen, Sensibilisierungsmaßnahmen und Forschungs- und Entwicklungsinitiativen im Bereich der Cybersicherheit sowie der Anleitung zu guten Vorgehensweisen und Kontrollen im Bereich der Cyberhygiene eingeführt werden sollten, die darauf abzielen, das Bewusstsein und die Vorsorge der Bürger, Interessenträger und Einrichtungen für Cybersicherheitsrisiken zu verbessern, einschließlich Techniken, die für Betrugszwecke eingesetzt werden, wie Phishing, Spoofing, Schadsoftware und andere Formen des Social Engineering. Darüber hinaus sind die Mitgliedstaaten gemäß der Richtlinie (EU) 2019/713 verpflichtet, Strategien zur Verhütung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und Maßnahmen zur Verminderung der Gefahr, dass derartige Straftaten, einschließlich des Versuchs von Betrugsdelikten wie Phishing und Skimming, stattfinden, in der Form von Informations- und Sensibilisierungskampagnen und Bildungsprogrammen einzuführen oder zu fördern. Im Einklang mit ihren Verpflichtungen nach diesen Richtlinien sollten die Mitgliedstaaten ständige und angemessene Maßnahmen entwickeln und auf dem neuesten Stand halten, um die Öffentlichkeit für bestehende und sich abzeichnende Muster des Zahlungsbetrugs, die gemäß der vorliegenden Verordnung einzuhaltenden Verfahren zur Ermittlung und Meldung von Betrugsversuchen und die Rechte und Pflichten der Zahlungsdienstnutzer in Bezug auf Betrug im Rahmen der vorliegenden Verordnung zu sensibilisieren. Die Mitgliedstaaten sollten die Kommission über die getroffenen Maßnahmen unterrichten.

(155) Die Mitgliedstaaten sollten sicherstellen, dass ausreichende Mittel für solche Sensibilisierungs- und Bildungsmaßnahmen zur Verfügung stehen und dass sie angemessen ausgerichtet sind, insbesondere auf die Bedürfnisse und Interessen schutzbedürftiger Verbrauchergruppen, einschließlich junger und älterer Menschen und Menschen mit beschränkten digitalen Kompetenzen. Zahlungsdienstleister, Anbieter interpersoneller Kommunikationsdienste im Sinne der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates[33] und Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen sollten bei der Entwicklung und Aktualisierung solcher Sensibilisierungskampagnen gegen Betrug mit Mitgliedstaaten zusammenarbeiten, unter anderem durch die Bereitstellung von Informationen über Betrugsbedrohungen und -muster, die in ihren Diensten ermittelt wurden, sowie von bewährten Verfahren zur Sensibilisierung der Nutzer. Diese Zusammenarbeit sollte unter angemessenen und verhältnismäßigen Bedingungen kostenlos sein.

(156) 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.

---

[33] 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, ELI: http://data.europa.eu/eli/dir/2018/1972/oj).

(157) Die Anforderungen an eine starke Kundenauthentifizierung sollten gegenüber den bestehenden Anforderungen der Richtlinie (EU) 2015/2366 nicht wesentlich geändert werden. Die starke Kundenauthentifizierung wird weiterhin auf mindestens zwei Elementen aus den Kategorien Wissen, Besitz und Inhärenz beruhen, die voneinander unabhängig sind. Die Kategorie Inhärenz bezieht sich auf die physikalischen Eigenschaften von Körperteilen, die physiologischen Merkmale und die vom Körper hervorgerufenen Verhaltensprozesse sowie jede Kombination davon. Mindestens zwei der verwendeten Elemente müssen aus verschiedenen Kategorien stammen. Um Innovationen bei Authentifizierungstechnologien zu ermöglichen, wird mit einer Ausnahme von diesem Grundsatz die Verwendung von zwei Elementen aus der Kategorie Inhärenz erlaubt, sofern dadurch das Sicherheitsniveau nicht gesenkt wird. Um ein hohes Maß an Sicherheit und die einheitliche Anwendung dieser Ausnahme durch die zuständigen nationalen Behörden zu gewährleisten, sollte die EBA Leitlinien dazu ausarbeiten, wie die Unabhängigkeit der beiden Elemente in solchen Fällen zu bewerten ist.

(158) Die starke Kundenauthentifizierung sollte insbesondere nicht durch eine ungerechtfertigte Berufung auf Ausnahmen von der starken Kundenauthentifizierung umgangen werden. Es sollten klare Definitionen der Begriffe „vom Händler ausgelöster Vorgang“ und „schriftlich oder telefonisch ausgelöster Vorgang“ 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 Vorgänge sollte bei der Festlegung des anfänglichen Mandats eine starke Kundenauthentifizierung angewandt werden, ohne dass für nachfolgende von Händlern ausgelöste Vorgänge eine starke Kundenauthentifizierung erforderlich ist. In Bezug auf schriftlich oder telefonisch ausgelöste Vorgänge sollte nur die Erteilung des Zahlungsauftrags – und nicht auch seine Authentifizierung oder Ausführung – nicht digital sein müssen, damit ein Vorgang als schriftlich oder telefonisch ausgelöster Vorgang betrachtet werden kann und daher nicht unter die Verpflichtung zur Anwendung der starken Kundenauthentifizierung fällt. In diesem Sinne könnte ein kartengebundener Zahlungsvorgang als schriftlich oder telefonisch ausgelöster Vorgang angesehen werden, wenn die Erteilung des Zahlungsauftrags nicht elektronisch erfolgt, z. B. wenn Zahlungsdaten vom Karteninhaber über nicht elektronische Kanäle an einen Händler übermittelt werden. Zahlungsvorgänge auf der Grundlage von papiergestützten Zahlungsaufträgen oder schriftlich oder telefonisch ausgelöste Vorgänge, 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, die einen Rückgriff auf einen außerhalb der Union niedergelassenen Anbieter von Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen beinhalten, um sich den Anforderungen an die starke Kundenauthentifizierung zu entziehen.

(159) 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 Vorgänge ohne jegliche Interaktion oder Beteiligung des Zahlers ausgelöst werden. Der Regulierungsansatz für von Händlern ausgelöste Vorgänge und Lastschriften, die beide vom Zahlungsempfänger ausgelöst werden, sollte angeglichen werden und dieselben Verbraucherschutzmaßnahmen beinhalten, mit Ausnahme des bedingungslosen Anspruchs auf Erstattung, der nur für Lastschriften gelten sollte.

(160) Um gleiche Wettbewerbsbedingungen für die verschiedenen Zahlungsinstrumente zu schaffen, sollte es möglich sein, eine oder mehrere wiederkehrende Überweisungen, auch in unterschiedlicher Höhe, ohne Verpflichtung zur Anwendung einer starken Kundenauthentifizierung auszulösen, wenn diese Überweisungen vom Zahlungsdienstleister des Zahlers auf Antrag des Zahlungsempfängers ausgelöst werden, sofern bestimmte kumulative Bedingungen erfüllt sind. Dies sollte insbesondere möglich sein, wenn der Antrag des Zahlungsempfängers auf einer Vereinbarung des Zahlungsempfängers mit dem Zahler beruht, in der die Bedingungen für die Häufigkeit der Zahlungen und die zu zahlenden Beträge festgelegt sind, wenn der Zahler mit seinem Zahlungsdienstleister eine Vereinbarung schließt, die einer starken Kundenauthentifizierung unterliegt und den Zahlungsdienstleister anweist, die jeweiligen Überweisungen im Einklang mit der Vereinbarung des Zahlers mit dem Zahlungsempfänger auszuführen, und wenn die Auslösung der jeweiligen Überweisungen durch den Zahlungsdienstleister des Zahlers keine zusätzlichen Maßnahmen des Zahlers erfordert. Um gleichwertige Garantien zu gewährleisten, sollten die Bestimmungen über Erstattungen und Erstattungsanträge, die für von einem oder über einen Zahlungsempfänger ausgelöste Zahlungsvorgänge gelten, für Überweisungen, die unter diesen Rahmen fallen, unter denselben Bedingungen gelten wie für von Händlern ausgelöste Vorgänge. Um ungehinderte Innovationen zu fördern und die breitere Verfügbarkeit effizienter Zahlungsmethoden für Zahler und Zahlungsempfänger am Interaktionspunkt zu beschleunigen, ist es darüber hinaus erforderlich, die Auslösung einer oder mehrerer wiederkehrender Überweisungen innerhalb dieses Rahmens ab dem Tag des Inkrafttretens dieser Verordnung zu ermöglichen.

(161) Um die finanzielle Inklusion zu verbessern und im Einklang mit der Richtlinie (EU) 2019/882 sollten alle Zahlungsdienstnutzer, einschließlich Menschen mit Behinderungen, ältere Menschen, Menschen mit beschränkten 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-Vorgänge durchzuführen, weil sie 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 kostenlos sein und nicht von einer einzigen Technologie, einem Gerät oder Mechanismus oder vom Besitz eines Smartphones oder eines sonstigen intelligenten Geräts abhängen.

(162) Europäische Brieftaschen für die Digitale Identität, die gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates[34] umgesetzt werden, sind elektronische Identifizierungsmittel, die Identifizierungs- und Authentifizierungsinstrumente für den grenzüberschreitenden Zugang zu Finanzdienstleistungen, einschließlich Zahlungsdiensten, bieten. Die Einführung der europäischen Brieftasche für die Digitale Identität soll die grenzüberschreitende digitale Identifizierung und Authentifizierung für sichere digitale Zahlungen weiter erleichtern und die Entwicklung einer gesamteuropäischen digitalen Zahlungslandschaft fördern. Gemäß Artikel 5f Absatz 2 der Verordnung (EU) Nr. 910/2014 sind Zahlungsdienstleister verpflichtet, die Verwendung von europäischen Brieftaschen für die Digitale Identität zu akzeptieren, um die Erfüllung der Erfordernisse einer starken Kundenauthentifizierung für die Online-Identifizierung für die Zwecke der Kontoanmeldung und der Auslösung von Vorgängen im Bereich Zahlungsdienste zu unterstützen. Die EBA sollte mit der Ausarbeitung technischer Regulierungsstandards beauftragt werden, in denen insbesondere die Verwendung von europäischen Brieftaschen für die Digitale Identität zur Unterstützung der Erfüllung der Erfordernisse einer starken Kundenauthentifizierung für die oben genannten Zwecke berücksichtigt werden sollte.

(163) Die Zunahme des elektronischen Geschäftsverkehrs 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 Vorgängen auf dynamische Codes stützen, um den Zahlungsdienstnutzer jederzeit über den Betrag der Zahlung und den Zahlungsempfänger des Vorgangs zu informieren, den der Zahlungsdienstnutzer autorisiert.

---

[34] 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, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

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

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

(166) 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 dieser Analyse zu erlassen, die klare Prüfungsanforderungen einführen und detailliertere und bessere Definitionen der Anforderungen an die Risikoüberwachung und die weiterzugebenden Daten bereitstellen, und die potenziellen Vorteile zu bewerten, die sich daraus ergäben, dass Zahlungsdienstleister betrügerische Vorgänge, für die sie allein haften, melden könnten. Die EBA sollte daher Entwürfe technischer Regulierungsstandards mit Vorschriften für die Transaktionsrisikoanalyse ausarbeiten.

(167) Die Sicherheitsmaßnahmen sollten dem Risikoniveau der Zahlungsdienste angemessen sein. Um die Entwicklung benutzerfreundlicher und zugänglicher Zahlungsmittel für Zahlungen mit einem niedrigen Risiko wie kontaktlose Kleinbetragszahlungen an der Verkaufsstelle oder von juristischen Personen ausgelöste Zahlungsvorgänge, unabhängig davon, ob diese Zahlungen über ein Mobiltelefon erfolgen, zu ermöglichen, sollten in 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 betrügerischen Handlungen einzuschränken. Der Nutzer sollte sich darauf verlassen können, dass Vorkehrungen getroffen werden, die die Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale schützen.

(168) 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.

(169) Es gibt kein einheitliches Verständnis der Marktteilnehmer in allen Mitgliedstaaten über die Anforderungen an die starke Kundenauthentifizierung, die für die Registrierung von Zahlungsinstrumenten, insbesondere Zahlungskarten, in digitalen Brieftaschen gelten. Die Erstellung eines Tokens oder der Vorgang für den Austausch eines Tokens kann die Gefahr von Zahlungsbetrug oder anderen Formen des Missbrauchs bergen. Die Erstellung oder der Austausch eines Tokens eines Zahlungsinstruments, die bzw. der 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 Austauschs des Tokens erfordern. Durch die Anwendung der starken Kundenauthentifizierung in der Phase der Erstellung oder des Austauschs 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.

(170) 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 der Zahler zu schließen, damit sie weiterhin diese Überprüfungen durchführen können, aber auch dazu verpflichtet werden, die wesentlichen Sicherheitsanforderungen zu erfüllen. Die Zahlungsdienstleister der Zahler sollten im Rahmen solcher Vereinbarungen die volle Haftung für den Fall behalten, dass Betreiber digitaler Pass-through-Brieftaschen die starke Kundenauthentifizierung nicht anwenden, und sollten das Recht haben, die Sicherheitsbestimmungen des Betreibers der Brieftasche zu prüfen und zu kontrollieren.

(171) Wenn technische Dienstleister oder Betreiber von Zahlverfahren für Zahlungsempfänger oder Zahlungsdienstleister von Zahlungsempfängern oder von 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 zentrale Sicherheitsanforderungen für Massenzahlungen ordnungsgemäß umgesetzt werden, unter anderem durch die Bereitstellung geeigneter IT-Lösungen, sollten technische Dienstleister und Betreiber von Zahlverfahren für unmittelbaren finanziellen Schaden haftbar gemacht werden, der Zahlungsempfängern, Zahlungsdienstleistern von Zahlungsempfängern oder von Zahlern dadurch entsteht, dass sie im Rahmen ihrer Vertragsbeziehung nicht die Leistungen erbringen, die erforderlich sind, um die Durchführung einer starken Kundenauthentifizierung zu ermöglichen, auf verhältnismäßige Weise und nicht über den Betrag des betreffenden Vorgangs hinaus.

(172) Die Mitgliedstaaten sollten sicherstellen, dass die von den Mitgliedstaaten gemäß Artikel 18 der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates[35] benannten zuständigen Behörden die in den Artikeln 19 und 20 der genannten Richtlinie festgelegten Aufgaben in Bezug auf in ihrem Hoheitsgebiet eingerichtete Streitbeilegungsstellen wahrnehmen, die für die Beilegung von Streitigkeiten, die die Rechte und Pflichten aus dieser Verordnung betreffen, als alternative Streitbeilegungsstellen (im Folgenden „AS-Stellen“) angesehen werden möchten.

(173) Die zuständigen Behörden sollten befugt sein, von Anbietern von Vermittlungsdiensten im Sinne der Verordnung (EU) 2022/2065, die zum Betrieb nicht zugelassener Zahlungsdienste beitragen, Informationen anzufordern und sie anzuweisen, den Zugang zu Websites von Betreibern nicht zugelassener Zahlungsdienste zu sperren oder zu beschränken. Im Interesse der vorübergehenden Sicherung von Geldbeträge von Kunden und anderen Vermögenswerten sollte diese Befugnis bereits im Untersuchungszeitraum zur Verfügung stehen, wenn ein hinreichender Verdacht auf der Grundlage von Tatsachen besteht, die die Annahme rechtfertigen, dass nicht zugelassene Geschäftstätigkeiten stattfinden.

---

[35] 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, ELI: http://data.europa.eu/eli/dir/2013/11/oj).

(174) Unbeschadet des Rechts der Kunden, die Gerichte anzurufen, sollten die Mitgliedstaaten sicherstellen, dass leicht zugängliche, angemessene, unabhängige, unparteiische, transparente und wirksame alternative Verfahren zur Beilegung von Streitigkeiten zwischen Zahlungsdienstleistern und Zahlungsdienstnutzern bestehen. Die Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates[36] 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 Vertragsbedingungen 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 alternativen Streitbeilegungsverfahren im Einklang mit den Qualitätsanforderungen der Richtlinie 2013/11/EU anschließen, um Streitigkeiten beizulegen, bevor ein Gericht angerufen wird. Bei vertraglichen Streitigkeiten zwischen Verbrauchern und Unternehmen bezüglich des Erwerbs von Waren oder Dienstleistungen stellt die Richtlinie 2013/11/EU sicher, dass die Verbraucher und Unternehmen in der Union Zugang zu zertifizierten Stellen für außergerichtliche Streitbeilegungsverfahren haben, die die in der Richtlinie 2013/11/EU festgelegten Qualitätsanforderungen erfüllen. Die Teilnahme an alternativen Verfahren zur Beilegung von Streitigkeiten zwischen Zahlungsdienstleistern und Verbrauchern über die Rechte und Pflichten gemäß der vorliegenden Verordnung sollte für Zahlungsdienstleister verpflichtend sein. Dies würde es Verbrauchern, die nicht über dieselben Mittel und Ressourcen wie juristische Personen verfügen, ermöglichen, ihre Rechte gemäß der vorliegenden Verordnung durchzusetzen, und ihnen Zugang zu zweckmäßigeren und kostengünstigeren Durchsetzungsmitteln gewähren. Die Verbraucher sollten jedoch nicht gezwungen werden, an diesen alternativen Streitbeilegungsverfahren teilzunehmen.

---

[36] Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I) (ABl. L 177 vom 4.7.2008, S. 6, ELI: http://data.europa.eu/eli/reg/2008/593/oj).

(175) Das Recht auf einen wirksamen Rechtsbehelf und das Recht auf ein unparteiisches Gericht gehören zu den in Artikel 47 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) niedergelegten Grundrechten. Daher sollten alternative Streitbeilegungsverfahren nicht so gestaltet sein, dass sie gerichtliche Verfahren ersetzen, und sollten Verbrauchern oder Unternehmern nicht das Recht nehmen, den Schutz ihrer Rechte vor Gericht einzufordern. Diese Verordnung sollte die Parteien in keiner Weise daran hindern, ihr Recht auf Zugang zum Gerichtssystem wahrzunehmen. Konnte eine Streitigkeit nicht mit Hilfe eines bestimmten alternativen Streitbeilegungsverfahrens, dessen Ergebnis nicht verbindlich ist, beigelegt werden, so sollten die Parteien in der Folge nicht daran gehindert werden, ein Gerichtsverfahren hinsichtlich dieser Streitigkeit einzuleiten. Es sollte den Mitgliedstaaten freistehen, die geeigneten Mittel zur Erreichung dieses Ziels zu wählen. Sie sollten unter anderem die Möglichkeit haben vorzusehen, dass Verjährungsfristen nicht während eines alternativen Streitbeilegungsverfahrens ablaufen.

(176) Die Verbraucher sollten berechtigt sein, ihre Rechte in Bezug auf die Pflichten, die Zahlungsdienstleistern gemäß dieser Verordnung auferlegt werden, durch Verbandsklagen gemäß der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates[37] durchzusetzen.

[37] Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25. November 2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG (ABl. L 409 vom 4.12.2020, S. 1, ELI: http://data.europa.eu/eli/dir/2020/1828/oj).

(177) Es sollten geeignete Verfahren eingeführt werden, um gegen Zahlungsdienstleister, die ihren Pflichten nicht nachkommen, Beschwerde zu erheben, und sicherzustellen, dass gegebenenfalls wirksame, verhältnismäßige und abschreckende Sanktionen verhängt werden. Um die wirksame Einhaltung der vorliegenden Verordnung zu gewährleisten, sollten die Mitgliedstaaten zuständige Behörden benennen, die die Bedingungen der Verordnung (EU) Nr. 1093/2010 erfüllen und unabhängig von den Zahlungsdienstleistern handeln. Die Mitgliedstaaten sollten der Kommission mitteilen, welche Behörden benannt wurden, einschließlich einer genauen Beschreibung ihrer Aufgaben.

(178) Angesichts der Tatsache, dass einige Bestimmungen der Richtlinie (EU) 2015/2366, wie die Bestimmungen über die *Ex-Ante*-Transparenz der Kosten und der Ausführungsfrist, für traditionelle elektronische Zahlungen konzipiert wurden und den Besonderheiten des Einsatzes der Distributed-Ledger-Technologie oder ähnlicher Technologien bei Zahlungsvorgängen mit E-Geld-Token nicht Rechnung tragen, ist es wichtig, festzulegen, ob diese Anforderungen für Zahlungsvorgänge mit E-Geld-Token gelten, und diesbezüglich Übergangsbestimmungen einzuführen.

(179) Die Befugnisse der zuständigen Behörden müssen stärker aneinander angeglichen werden, um so die Voraussetzungen für ein vergleichbares Maß der Durchsetzung auf dem gesamten integrierten Zahlungsmarkt zu schaffen. Den zuständigen Behörden sollten alle Aufsichts-, Untersuchungs- und Sanktionsbefugnisse eingeräumt werden, die erforderlich sind, um die Einhaltung dieser Verordnung zu gewährleisten. In dieser Verordnung sollte daher ein gemeinsamer Mindestkatalog der Befugnisse, mit denen die zuständigen Behörden ausgestattet werden sollten, in Verbindung mit angemessenen Ressourcen festgelegt werden, um die Wirksamkeit der Aufsicht sicherzustellen. Um die Verbraucher zu schützen und jederzeit für angemessene Informationen für den Markt zu sorgen, sollten die zuständigen Behörden befugt sein, frühzeitige Aufsichtsmaßnahmen zu ergreifen, wie etwa die Aussetzung oder das Verbot der Erbringung, Vermarktung und Werbung in Bezug auf Dienste oder die Veröffentlichung von Bekanntmachungen, um die Öffentlichkeit vor einem tatsächlichen oder mutmaßlichen Verstoß gegen diese Verordnung zu warnen. Die zuständigen Behörden sollten von diesen Befugnissen insbesondere bei folgenden Verstößen Gebrauch machen: bei nicht zugelassenen Zahlungsdiensten, bei der Verbreitung falscher oder irreführender Informationen über den Zahlungsmarkt sowie, im allgemeineren Sinne, bei der Nichterfüllung der Verpflichtungen gemäß dieser Verordnung durch einen Zahlungsdienstleister oder einen Dritten, der an der Erbringung von Zahlungsdiensten beteiligt ist. Erweisen sich die von den zuständigen Behörden in Bekanntmachungen veröffentlichten Informationen als falsch oder unvollständig oder die ihnen zugrunde liegenden Umstände als unrichtig, so sollten die zuständigen Behörden sie unverzüglich über dieselben Kommunikationskanäle berichtigen, die zur Unterrichtung der Öffentlichkeit genutzt wurden.

(180) In einem digitalen Umfeld sollten die zuständigen Behörden in der Lage sein, Verstöße gegen diese Verordnung rasch und wirksam zu unterbinden, insbesondere wenn die Person, die den Verstoß begeht, ihre Identität verschleiert oder innerhalb der Union oder in einen Drittstaat umzieht, um sich der Durchsetzung zu entziehen. In Fällen, in denen die Gefahr einer schwerwiegenden Schädigung von Verbraucherinteressen besteht, sollten die zuständigen Behörden vorläufige Maßnahmen ergreifen können, darunter die Löschung von Inhalten einer Online-Schnittstelle oder die Anordnung, dass den Verbrauchern beim Zugriff auf eine Online-Schnittstelle ein ausdrücklicher Warnhinweis angezeigt wird. Diese Maßnahmen sollten nicht über das Maß hinausgehen, das für die Verwirklichung des Ziels, den Verstoß gegen diese Verordnung zu beenden oder zu untersagen, erforderlich ist.

(181) Unbeschadet des Rechts, die Gerichte anzurufen, 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 verwaltungsrechtliche Maßnahmenaufzuerlegen, 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 Verbraucherinteressen bestehen. Die zuständigen Behörden sollten wirksame Mechanismen einrichten, um die Meldung potenzieller oder tatsächlicher Verstöße zu fördern. Die Verteidigungsrechte von Personen, gegen die ein Vorwurf erhoben wird, sollten von diesen Mechanismen unberührt bleiben.

(182) Die Mitgliedstaaten sollten verpflichtet werden, wirksame, verhältnismäßige und abschreckende verwaltungsrechtliche Sanktionen und verwaltungsrechtliche Maßnahmen im Zusammenhang mit Verstößen gegen die Bestimmungen dieser Verordnung vorzusehen. Diese verwaltungsrechtlichen Sanktionen, Zwangsgelder und verwaltungsrechtlichen Maßnahmen sollten bestimmten Mindestanforderungen genügen, einschließlich der Mindestbefugnisse, die den zuständigen Behörden übertragen werden sollten, um sie verhängen zu können, sowie 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.

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

(184) Bei der Verhängung von verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen sollten die zuständigen Behörden bei der Festlegung der Art der verwaltungsrechtlichen Sanktionen oder anderen verwaltungsrechtlichen Maßnahmen und der Höhe der Verwaltungsstrafen 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 der Sanktionen und anderen verwaltungsrechtlichen Maßnahmen, die zu Sanktionszwecken verhängt werden, in Fällen einer Kumulierung von Verwaltungs- und Strafverfahren auf das Maß beschränkt ist, das angesichts der Schwere des betreffenden Verstoßes erforderlich ist.

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

(186) Die Wirksamkeit des Unionsrahmens für Zahlungsdienste hängt von der Zusammenarbeit zwischen einem breiten Spektrum zuständiger Behörden, einschließlich nationaler Steuerbehörden, und anderen Durchsetzungsbehörden ab. Die Mitgliedstaaten sollten sicherstellen, dass ihre Rechtsrahmen diese Zusammenarbeit ermöglichen und erleichtern, um die Ziele des Unionsrahmens für Zahlungsdienste zu erreichen, unter anderem durch die ordnungsgemäße Durchsetzung seiner Vorschriften. Diese Zusammenarbeit sollte den Informationsaustausch sowie die Amtshilfe bei der wirksamen Durchsetzung von verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen, insbesondere bei der grenzüberschreitenden Beitreibung von Geldbußen, umfassen.

(187) 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 betreffenden mutmaßlichen Verstoßes und seiner Folgen zu erreichen, bevor ein förmliches Sanktionsverfahren eingeleitet wird. Aufgrund der unterschiedlichen rechtlichen Ansätze auf nationaler Ebene erscheint es nicht angebracht, eine Harmonisierung der von den Mitgliedstaaten eingeführten Durchsetzungsmethoden auf Unionsebene anzustreben. Es sollte jedoch anerkannt werden, dass solche Methoden es den zuständigen Behörden, die sie umsetzen können, ermöglichen, Verfahren wegen Regelverstößen unter bestimmten Umständen schneller, kostengünstiger und insgesamt effizienter zu bearbeiten, und diese Methoden sollten daher gefördert werden. Die Mitgliedstaaten sollten jedoch weder verpflichtet sein, solche Durchsetzungsmethoden in ihre Rechtsrahmen aufzunehmen, noch sollten sie verpflichtet sein, die zuständigen Behörden zur Anwendung dieser Methoden zu zwingen, wenn sie dies nicht für angemessen halten.

(188) Die Mitgliedstaaten haben eine Vielzahl von verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen für Verstöße gegen die wichtigsten Bestimmungen des Unionsrechts zur Regelung der Erbringung von Zahlungsdiensten eingeführt und sehen diese derzeit vor, und es bestehen uneinheitliche Ansätze für die Untersuchung und Sanktionierung von Verstößen gegen diese Bestimmungen. Wenn nicht genauer festgelegt würde, welche Kernbestimmungen eine hinreichend abschreckende Durchsetzung in jedem Mitgliedstaat auslösen müssen, würde dies die Verwirklichung des Binnenmarkts für Zahlungsdienste behindern und die Gefahr bergen, Anreize für die Wahl des günstigsten Gerichtsstands (sog. Forum-Shopping) zu schaffen, da die zuständigen Behörden nicht in gleichem Maße in der Lage sind, Verstöße gegen diese Bestimmungen rasch und mit derselben Abschreckungswirkung zu ahnden.

(189) Da der Zweck der Zwangsgelder, die im Einklang mit dem nationalen Recht verhängt werden, darin besteht, natürliche oder juristische Personen, die als für einen andauernden Verstoß gegen das Unionsrecht verantwortlich identifiziert wurden oder einer Anordnung einer 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 oder andere verwaltungsrechtliche Maßnahmen für denselben Verstoß zu verhängen.

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

(191) Die zuständigen Behörden sollten von den Mitgliedstaaten ermächtigt werden, verwaltungsrechtliche Sanktionen und verwaltungsrechtliche Maßnahmen gegen Zahlungsdienstleister oder gegebenenfalls andere natürliche oder juristische Personen zu verhängen, um den Verstoß gegen diese Verordnung zu beheben. Das Spektrum der Sanktionen und Maßnahmen, die den zuständigen Behörden zur Verfügung stehen, sollten ausreichend breit gefächert sein, damit die Mitgliedstaaten und die zuständigen Behörden den Unterschieden zwischen Zahlungsdienstleistern, insbesondere zwischen Kreditinstituten und anderen Zahlungsinstituten, in Bezug auf ihre Größe, ihre Merkmale und die Art ihrer Geschäftstätigkeit Rechnung tragen können.

(192) Die Veröffentlichung einer verwaltungsrechtlichen Sanktion oder einer Verwaltungsmaßnahme aufgrund von Verstößen gegen die Bestimmungen dieser Verordnung kann eine starke abschreckende Wirkung gegen die Wiederholung solcher Verstöße haben. Zudem werden durch die Veröffentlichung andere Stellen über die Risiken informiert, die mit dem sanktionierten Zahlungsdienstleister verbunden sind, bevor sie eine Geschäftsbeziehung eingehen, und die zuständigen Behörden in anderen Mitgliedstaaten werden in Bezug auf die Risiken unterstützt, die mit einem Zahlungsdienstleister verbunden sind, wenn dieser in ihrem Hoheitsgebiet grenzüberschreitend tätig ist. Aus diesen Gründen sollte die Veröffentlichung von Entscheidungen über verwaltungsrechtliche Sanktionen und verwaltungsrechtliche Maßnahmen sowie von Informationen über das Recht auf Einlegung eines Rechtsbehelfs und das Ergebnis eines solchen Rechtsbehelfs 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 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.

(193) 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 Umfang der Daten, die die zuständigen Behörden der EBA melden, auszuweiten und deren Qualität 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 Mitgliedstaaten Bericht erstatten.

(194) Der Kommission sollte die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen, um diese Verordnung zu ergänzen, indem die Gebühreninformationen näher festgelegt werden, die Kartenzahlverfahren und abwickelnde Stellen den Anbietern von Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen offenlegen müssen; indem der Betrag aktualisiert wird, bis zu dem ein Zahler dazu verpflichtet werden kann, mit nicht autorisierten Zahlungsvorgängen zusammenhängende Verluste, die infolge des Verlusts, des Diebstahls oder der missbräuchlichen Verwendung eines Zahlungsinstruments oder personalisierter Sicherheitsmerkmale entstehen, zu tragen; indem die Vorschriften für Zahlungsvorgänge mit E-Geld-Token in Anbetracht der Technologie- und Marktentwicklungen angepasst werden und indem die Kriterien und Faktoren festgelegt werden, die von der EBA bei der Festlegung bestimmter Bedingungen im Zusammenhang mit den Befugnissen zur vorübergehenden Intervention zu berücksichtigen sind. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[38] niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

---

[38] ABl. L 123 vom 12.5.2016, S. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

(195) Um eine einheitliche Anwendung der vorliegenden Verordnung sicherzustellen, sollte sich die Kommission auf das Fachwissen und die Unterstützung der EBA verlassen können, die die Aufgabe haben sollte, Leitlinien und Entwürfe technischer Regulierungs- und Durchführungsstandards auszuarbeiten. Der Kommission sollte die Befugnis übertragen werden, diese Entwürfe technischer Regulierungsstandards zu erlassen. Bei der Ausarbeitung von Leitlinien, Entwürfen technischer Regulierungsstandards und Entwürfen technischer Durchführungsstandards gemäß der vorliegenden Verordnung und im Einklang mit der Verordnung (EU) Nr. 1093/2010 sollte die EBA alle einschlägigen Interessenträger, einschließlich derer des Zahlungsdienstmarktes, anhören und den Interessen aller Beteiligten Rechnung tragen.

(196) Die EBA sollte im Einklang mit Artikel 9 Absatz 5 der Verordnung (EU) Nr. 1093/2010 mit Produktinterventionsbefugnissen ausgestattet werden, um in der Union eine bestimmte Art von Zahlungsdienst oder ein bestimmtes Merkmal eines solchen Dienstes vorübergehend verbieten oder beschränken zu können, wenn festgestellt wurde, dass dies den Verbrauchern schaden könnte und dadurch das ordnungsgemäße Funktionieren und die Integrität der Finanzmärkte gefährdet würde. Die Verordnung (EU) Nr. 1093/2010 sollte daher entsprechend geändert werden.

(197) Um die grenzüberschreitende Zusammenarbeit bei der Durchsetzung der vorliegenden Verordnung zu erleichtern, sollte der Anhang der Verordnung (EU) 2017/2394 des Europäischen Parlaments und des Rates[39] dahin gehend geändert werden, dass ein Verweis auf die vorliegende Verordnung aufgenommen wird.

---

[39] 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. 2006/2004 (ABl. L 345 vom 27.12.2017, S. 1, ELI: http://data.europa.eu/eli/reg/2017/2394/oj).

(198) Da das Ziel dieser Verordnung, nämlich die weitere Integration eines Binnenmarktes für Zahlungsdienste, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, da dies 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.

(199) Da mit dieser Verordnung und der Richtlinie (EU) 2026/…[+] der Rechtsrahmen für die Erbringung von Zahlungsdiensten in der Union festgelegt wird, um Rechtssicherheit und die Kohärenz des Rechtsrahmens der Union sicherzustellen, sollte diese Verordnung ab demselben Zeitpunkt gelten wie die Rechts- und Verwaltungsvorschriften, die die Mitgliedstaaten erlassen müssen, um der Richtlinie (EU) 2026/… nachzukommen. Die Bestimmungen, nach denen Zahlungsdienstleister bei Überweisungen Abweichungen zwischen dem Namen und dem Kundenidentifikator eines Zahlungsempfängers überprüfen müssen, und die entsprechende Haftungsregelung sollten jedoch ab dem … [27 Monate nach dem Tag des Inkrafttretens dieser Verordnung] gelten, sodass die Zahlungsdienstleister genügend Zeit haben, um die erforderlichen Schritte zur Anpassung ihrer internen Systeme zu unternehmen, um diesen Anforderungen nachzukommen.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(200) 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. Sieben Jahre werden als angemessener Zeitraum angesehen. Während bei der Überprüfung diese Verordnung als Ganzes berücksichtigt werden sollte, sollte bestimmten Themen besondere Aufmerksamkeit gewidmet werden, nämlich dem Funktionieren des Open Banking, weiteren Lösungen zur Betrugsbekämpfung sowie der Angemessenheit und den Auswirkungen der Vorschriften über die Reichweite der Situationen, in denen ein Verbraucher ein Recht auf Erstattung autorisierter Vorgänge hat. In Bezug auf andere Themen, nämlich die Entgeltpraktiken für Zahlungsdienste, die den Anbietern elektronischer Kommunikationsdienste und den Hostingdiensteanbietern auferlegten Verpflichtungen zur Verhinderung von Zahlungsbetrug, den Anwendungsbereich dieser Verordnung sowie die Angemessenheit und die Auswirkungen der in dieser Verordnung festgelegten Vorschriften in Bezug auf Zahlungsvorgänge mit E-Geld-Token, ist es jedoch angesichts der grundlegenden Bedeutung dieser Themen für das Funktionieren eines wettbewerbsfähigen, innovativen und sicheren Zahlungsmarkts in der Union angezeigt, vor dem … [sieben Jahre nach dem Tag des Inkrafttretens dieser Verordnung] eine Überprüfung durchzuführen. 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.

(201) Angesichts der zunehmenden Bedeutung virtueller IBANs, die für rechtmäßige Geschäftszwecke in der Union verwendet werden, ist es von wesentlicher Bedeutung, die Rechtssicherheit zu erhöhen und die Einhaltung der Verordnung (EU) Nr. 260/2012 sicherzustellen. Daher muss präzisiert werden, dass virtuelle IBANs denselben Vorschriften wie IBANs unterliegen und die durch die ISO spezifizierten Elemente enthalten. Die Verordnung (EU) Nr. 260/2012 sollte daher entsprechend geändert werden. Darüber hinaus sind virtuelle IBANs als gültige Identifikatoren für Zahlungskonten zulässig, wenn die Verwendung einer IBAN erforderlich ist. Angesichts der mit virtuellen IBANs verbundenen Risiken und Herausforderungen, einschließlich aus der Perspektive der Bekämpfung von Geldwäsche und Terrorismusfinanzierung, einerseits und ihrer Vorteile andererseits sollte die Kommission dem Europäischen Parlament, dem Rat, der EZB und dem Europäischen Wirtschafts- und Sozialausschuss einen Bericht vorlegen, in dem bewertet wird, ob die Einführung weiterer Maßnahmen zur Regulierung virtueller IBANs auf Unionsebene erforderlich ist, und gegebenenfalls zusammen mit dem Bericht einen Gesetzgebungsvorschlag vorlegen.

(202) Im Einklang mit den Grundsätzen der besseren Rechtsetzung sollte diese Verordnung auf die Angemessenheit und die Auswirkungen der in den Titeln II und III dieser Verordnung festgelegten Vorschriften in Bezug auf Zahlungsvorgänge mit E-Geld-Token überprüft werden. Bei ihrer Überprüfung sollte die Kommission bewerten, ob es angesichts der Entwicklungen wünschenswert wäre, die Anforderungen an die Überprüfung des Zahlungsempfängers und Open Banking gemäß dieser Verordnung auf Zahlungsvorgänge mit E-Geld-Token auszuweiten.

(203) Diese Verordnung steht im Einklang mit den Grundrechten und den mit der Charta 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 muss unter Wahrung dieser Rechte und Grundsätze angewandt werden.

(204) Verweise auf Beträge in Euro sind als Verweise auf den von jedem Mitgliedstaat, dessen Währung nicht der Euro ist, festgelegten entsprechenden Gegenwert in seiner nationalen Währung zu verstehen. Verweise auf Zahlungsvorgänge in Euro oder anderen Währungen sind als Verweise auf Zahlungsvorgänge mit auf Euro oder andere Währungen lautenden Geldbeträgen zu verstehen, einschließlich auf Euro oder andere Währungen lautender E-Geld-Token.

(205) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und hat am 22. August 2023[40] eine Stellungnahme abgegeben —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

[40] ABl. C, C/2023/1019, 16.11.2023, ELI: http://data.europa.eu/eli/C/2023/1019/oj.

TITEL I
GEGENSTAND, ANWENDUNGSBEREICH UND BEGRIFFSBESTIMMUNGEN

Artikel 1

Gegenstand

(1) Mit dieser Verordnung werden für die Erbringung von Zahlungsdiensten einheitliche Vorschriften in Bezug auf Folgendes festgelegt:

a) die Transparenz der Vertragsbedingungen und die Informationspflichten,

b) die jeweiligen Rechte und Pflichten von Zahlungsdienstnutzern und Zahlungsdienstleistern.

(2) Sofern nicht anders angegeben, ist eine Bezugnahme auf Zahlungsdienste in dieser Verordnung als Bezugnahme auf alle in Anhang I der Richtlinie (EU) 2026/…[+] genannten Zahlungsdienste zu verstehen.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

Artikel 2

Anwendungsbereich

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

a) Kreditinstituten im Sinne des Artikels 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates[41], einschließlich deren Zweigniederlassungen, sofern sich diese Zweigniederlassungen in der Union befinden, unabhängig davon, ob sich die Hauptverwaltungen dieser Zweigniederlassungen innerhalb oder außerhalb der Union befinden,

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

c) Zahlungsinstituten,

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

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

---

41 Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1, ELI: http://data.europa.eu/eli/reg/2013/575/oj).

(2) Diese Verordnung gilt auch für Dienstleistungen, die innerhalb der Union von folgenden Einrichtungen erbracht werden:

a) technischen Dienstleistern für die Zwecke des Artikels 23 Absatz 2 und der Artikel 59, 94, 96, 97, 101 und 103,

b) Zahlungssystembetreibern und Betreibern von Zahlverfahren für die Zwecke der Artikel 31, 84, 101 und 103, Betreibern von Zahlverfahren, einschließlich Kartenzahlverfahren, für die Zwecke des Artikels 59 und Betreibern von Kartenzahlverfahren und abwickelnden Stellen für die Zwecke des Artikels 32,

c) Anbietern interpersoneller Kommunikationsdienste für die Zwecke der Artikel 61, 90, 96, 101 und 103,

d) Anbietern elektronischer Kommunikationsdienste für die Zwecke des Artikels 96,

e) Hostingdiensteanbietern für die Zwecke der Artikel 61, 82 und 101,

f) Anbietern sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen für die Zwecke der Artikel 61, 62, 90 und 98,

g) Originalgeräteherstellern mobiler Geräte für die Zwecke des Artikels 96.

(3) Diese Verordnung gilt nicht für:

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

b) Zahlungsvorgänge, die ohne zwischengeschaltete Stellen ausschließlich als E-Geld-Token unmittelbar vom Zahler an den Zahlungsempfänger erfolgen,

c) Zahlungsvorgänge vom Zahler an den Zahlungsempfänger über einen Handelsagenten, sofern die folgenden Bedingungen erfüllt sind:

   i) der Handelsagent 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 im Namen beider, auszuhandeln oder abzuschließen, und

   ii) eine solche Vereinbarung verschafft dem Handelsagenten einen tatsächlichen Spielraum, mit dem Zahler oder dem Zahlungsempfänger zu verhandeln oder den Verkauf oder Erwerb von Waren oder Dienstleistungen abzuschließen,

d) Zahlungsvorgänge, die in der nicht gewerbsmäßigen Entgegennahme und Übergabe von Bargeld im Rahmen einer Tätigkeit ohne Erwerbszweck oder einer gemeinnützigen Tätigkeit bestehen,

e) 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 dieses Zahlungsvorgangs ausdrücklich darum gebeten hat,

f) Dienste, bei denen sich Einzelhandelsgeschäfte bereit erklären, auf ausdrücklichen Wunsch des Zahlungsdienstnutzers, jedoch unabhängig von der Ausführung eines Zahlungsvorgangs und ohne jede Verpflichtung zum Erwerb von Waren oder Dienstleistungen, Bargeld bereitzustellen,

g) Zahlungsvorgänge, denen eines der folgenden Dokumente zugrunde liegt, das auf den Zahlungsdienstleister gezogen ist und die Bereitstellung von Geldbeträgen 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 Abkommen 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 oder ein physischer Gutschein ähnlicher Art,

vi) ein Reisescheck in Papierform,

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

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

i) 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 h genannten Personen oder von Wertpapierdienstleistungen erbringenden Wertpapierfirmen, Kreditinstituten, Organismen für gemeinsame Anlagen oder Vermögensverwaltungsgesellschaften und jeder anderen Stelle, die für die Verwahrung von Finanzinstrumenten zugelassen ist, durchgeführt werden,

j) Zahlungsvorgänge, die von einem Anbieter von Kryptowerte-Dienstleistungen durchgeführt werden, der zwischen einem Käufer und einem Verkäufer vermittelt, wenn E-Geld-Token gegen andere E-Geld-Token oder andere Kryptowerte getauscht werden, oder der Tausch von E-Geld-Token gegen Geldbeträge, einschließlich E-Geld-Token, oder gegen Kryptowerte, der von einem Anbieter von Kryptowerte-Dienstleistungen durchgeführt wird, der im eigenen Namen als Käufer oder Verkäufer dieser E-Geld-Token handelt;

k) Dienste, die auf bestimmten Zahlungsinstrumenten, einschließlich auf E-Geld-basierten Instrumenten, beruhen, die eine der folgenden Bedingungen erfüllen:

   i) die Instrumente gestatten ihrem Inhaber, Waren oder Dienstleistungen lediglich in den Geschäftsräumen, einschließlich stationärer Verkaufsstellen oder Online-Shops, 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, einschließlich Instrumente, die auf die Verwendung für Vorgänge zwischen Zahlungsdienstnutzern, die keine Verbraucher sind, beschränkt sind,

iii) die Instrumente sind nur in einem Mitgliedstaat gültig, werden auf Antrag 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, und können nicht in Bargeld umgewandelt werden,

l) Zahlungsvorgänge eines Anbieters elektronischer Kommunikationsnetze im Sinne des Artikels 2 Nummer 1 der Richtlinie (EU) 2018/1972 oder eines Anbieters von Diensten, die zusätzlich zu elektronischen Kommunikationsdiensten im Sinne des Artikels 2 Nummer 4 der genannten Richtlinie für einen Teilnehmer des Netzes oder des Dienstes bereitgestellt werden

i) im Zusammenhang mit dem Erwerb von digitalen Inhalten und Sprachdiensten, ungeachtet des für den Erwerb oder Konsum des digitalen Inhalts verwendeten Geräts, und die auf der entsprechenden Rechnung abgerechnet werden, oder

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

sofern der Wert jeder Einzelzahlung 60 EUR nicht überschreitet und

– der kumulative Wert der Zahlungsvorgänge eines einzelnen Teilnehmers 360 EUR monatlich nicht überschreitet oder

– der kumulative Wert der Zahlungsvorgänge 360 EUR monatlich nicht überschreitet, wenn ein Teilnehmer auf sein Konto bei einem Anbieter elektronischer Kommunikationsnetze oder -dienste Vorauszahlungen tätigt,

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

n) Zahlungsvorgänge, die zwischen Anbietern von Kryptowerte-Dienstleistungen oder ihren Zweigniederlassungen auf eigene Rechnung ausgeführt werden,

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

p) den physischen gewerbsmäßigen Transport von Banknoten und Münzen einschließlich ihrer Entgegennahme, Bearbeitung und Übergabe,

q) Bargeldwechselgeschäfte, sofern die betreffenden Geldbeträge nicht auf einem Zahlungskonto gehalten werden.

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

(5) Titel II, mit Ausnahme von Artikel 13 Absatz 1 Buchstabe b, Artikel 20 Absatz 2 Buchstabe e und Artikel 24 Buchstabe a, und Titel III, mit Ausnahme der Artikel 70 bis 76, 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 sind 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.

(6) Titel II, mit Ausnahme von Artikel 13 Absatz 1 Buchstabe b, Artikel 20 Absatz 2 Buchstabe e, Artikel 20 Absatz 5 Buchstabe h und Artikel 24 Buchstabe a, und Titel III, mit Ausnahme von Artikel 28 Absätze 2 und 3, Artikel 51, 58, 65, 66 und 70, Artikel 73 Absatz 1 und Artikel 79 und 82, 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.

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

(8) Zum Ausschluss der in Absatz 3 Buchstabe c des vorliegenden Artikels genannten, über einen Handelsagenten abgewickelten Zahlungsvorgänge vom Zahler an den Zahlungsempfänger vom Anwendungsbereich der vorliegenden Verordnung gibt die EBA gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 bis zum … [zwölf Monate nach dem Tag des Inkrafttretens dieser Verordnung] Leitlinien an die zuständigen Behörden aus.

(9) Die EBA arbeitet Entwürfe technischer Regulierungsstandards aus, in denen die Bedingungen für den Ausschluss von Dienstleistungen, die auf bestimmten in Absatz 3 Buchstabe k des vorliegenden Artikels genannten Zahlungsinstrumenten beruhen, vom Anwendungsbereich der vorliegenden Verordnung festgelegt werden. Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigt die EBA die Erfahrungen, die bei der Anwendung ihrer Leitlinien vom 24. Februar 2022 in Bezug auf den Ausschluss begrenzter Netze vom Anwendungsbereich der Richtlinie (EU) 2015/2366 gewonnen wurden.

Die EBA übermittelt der Kommission die in Unterabsatz 1 genannten Entwürfe technischer Regulierungsstandards bis zum … [zwölf Monate nach dem Tag des Inkrafttretens dieser Verordnung].

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

(10) Die Mitgliedstaaten teilen der Kommission bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach Absatz 7 erlassen. Die Mitgliedstaaten teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach Absatz 7 erlassen, umgehend mit.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Zahlungsdienst“ jede der in Anhang I der Richtlinie (EU) 2026/…[+] aufgeführten gewerblichen Tätigkeiten;

2. „Zahlungsdienstleister“ eine Stelle im Sinne des Artikels 2 Absatz 1 oder eine natürliche oder juristische Person, für die eine Ausnahme gemäß Artikel 33, Artikel 35 Absatz 1 oder Artikel 36 Absatz 1 der Richtlinie (EU) 2026/… gilt;

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

4. „Verbraucher“ eine natürliche Person, die bei den unter diese Verordnung fallenden Zahlungsdienstverträgen nicht für die Zwecke der gewerblichen, geschäftlichen oder beruflichen Tätigkeit dieser Person handelt;

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

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

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

7. „Geldbetrag“ für den Massenzahlungsverkehr ausgegebenes Zentralbankgeld, Giralgeld und E-Geld, einschließlich E-Geld-Token;

8. „Zahlungsvorgang“ die Bereitstellung, den Transfer oder die Abhebung eines Geldbetrags auf der Grundlage eines Zahlungsauftrags, der unabhängig von etwaigen zugrunde liegenden Verpflichtungen zwischen Zahler und Zahlungsempfänger vom Zahler oder im Namen des Zahlers oder vom Zahlungsempfänger oder im Namen des Zahlungsempfängers erteilt wurde;

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

10. „Ausführung eines Zahlungsvorgangs“ den Vorgang, der beginnt, sobald die Auslösung eines Zahlungsvorgangs abgeschlossen ist, und endet, sobald der bereitgestellte, abgehobene oder transferierte Geldbetrag dem Zahlungsempfänger zur Verfügung steht;

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

12. „Erteilung eines Zahlungsauftrags aus der Ferne“ einen Zahlungsvorgang, für den ein Zahlungsauftrag über das Internet erteilt wird;

13. „Zahlungsinstitut“ eine juristische Person, der nach Artikel 13 der Richtlinie (EU) 2026/…[+] eine Zulassung für die unionsweite Erbringung von Zahlungsdiensten erteilt wurde;

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

14. „Zahlungsinstitutsanwärter“ ein Unternehmen, das eine Zulassung gemäß Artikel 3 der Richtlinie (EU) 2026/…[+] beantragt hat und für das die Entscheidung noch aussteht;

15. „Herkunftsmitgliedstaat“

a) den Mitgliedstaat, in dem der Zahlungsdienstleister seinen eingetragenen Sitz hat, oder,

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

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

17. „Agent“ eine natürliche oder juristische Person, die bei der Erbringung von Zahlungsdiensten im Namen und im Auftrag eines Zahlungsinstituts handelt und entweder im Auftrag des Zahlungsinstituts in den Besitz des Geldbetrags gelangt oder direkt an der Erbringung von Zahlungsdiensten durch das Zahlungsinstitut beteiligt ist;

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

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

19. „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[42] genannte Beziehung miteinander verbunden sind, oder in den Artikeln 4, 5, 6 und 7 der delegierten Verordnung (EU) Nr. 241/2014 der Kommission[43] 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;

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

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

22. „technischer Dienstleister“ einen Anbieter von Diensten, die zwar keine Zahlungsdienste sind, aber die Erbringung von Zahlungsdiensten unterstützen, wobei der Anbieter zu keinem Zeitpunkt in den Besitz der zu transferierenden Geldbeträge gelangt;

---

[42] 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, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

[43] 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 für Institute geltenden Anforderungen an Eigenmittel und berücksichtigungsfähige Verbindlichkeiten (ABl. L 74 vom 14.3.2014, S. 8, ELI: http://data.europa.eu/eli/reg_del/2014/241/oj).

23. „Anbieter elektronischer Kommunikationsdienste“ einen Anbieter von elektronischen Kommunikationsdiensten im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972;

24. „Anbieter interpersoneller Kommunikationsdienste“ einen Anbieter von interpersonellen Kommunikationsdiensten im Sinne des Artikels 2 Nummer 5 der Richtlinie (EU) 2018/1972;

25. „Hostingdiensteanbieter“ einen Hostingdiensteanbieter im Sinne des Artikels 3 Buchstabe g Ziffer iii der Verordnung (EU) 2022/2065;

26. „Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen“ einen Anbieter von sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen im Sinne des Artikels 33 der Verordnung (EU) 2022/2065;

27. „Anbieter von Kryptowerte-Dienstleistungen“ einen Anbieter von Kryptowerte-Dienstleistungen im Sinne des Artikels 3 Absatz 1 Nummer 15 der Verordnung (EU) 2023/1114;

28. „Kryptowerte-Dienstleistung“ eine Kryptowerte-Dienstleistung im Sinne des Artikels 3 Absatz 1 Nummer 16 der Verordnung (EU) 2023/1114;

29. „E-Geld-Token“ ein E-Geld-Token im Sinne des Artikels 3 Absatz 1 Nummer 7 der Verordnung (EU) 2023/1114;

30. „E-Geld“ einen elektronisch, einschließlich magnetisch, gespeicherten monetären Wert, der gegen Zahlung eines Geldbetrags ausgestellt wird, um damit Zahlungsvorgänge durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem Emittenten angenommen wird;

31. „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;

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

33. „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;

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

35. „Zahlungskonto“ ein von einem Zahlungsdienstleister auf den Namen eines oder mehrerer Zahlungsdienstnutzer geführtes Konto, das für die Ausführung eines oder mehrerer Zahlungsvorgänge genutzt werden kann und es ermöglicht, Geldbeträge an Dritte zu senden und von Dritten zu empfangen;

36. „Mandat“ die Erteilung der Autorisierung des Zahlers gegenüber dem Zahlungsempfänger und – direkt oder indirekt über den Zahlungsempfänger – gegenüber dem Zahlungsdienstleister des Zahlers, aufgrund deren der Zahlungsempfänger einen Zahlungsvorgang zur Belastung des angegebenen Zahlungskontos des Zahlers auslösen und der Zahlungsdienstleister des Zahlers solchen Anweisungen Folge leisten darf;

37. „kontoführender Zahlungsdienstleister“ einen Zahlungsdienstleister, der für einen Zahlungsdienstnutzer ein Zahlungskonto bereitstellt und führt;

38. „Geldautomatenbetreiber“ eine natürliche oder juristische Person, die Bargeldabhebungsdienste gemäß Anhang I Nummer 1 der Richtlinie (EU) 2026/…[+] erbringt, bei der es sich nicht um einen kontoführenden Zahlungsdienstleister handelt und die auch keine der anderen in Anhang I der genannten Richtlinie aufgeführten Zahlungsdienste erbringt;

39. „dauerhafter Datenträger“ jedes Medium, das es dem Zahlungsdienstnutzer gestattet, an ihn persönlich gerichtete Informationen derart zu speichern, dass sie in der Folge für eine dem Zweck der Informationen angemessene Dauer eingesehen werden kann, und das die unveränderte Wiedergabe der gespeicherten Informationen ermöglicht;

40. „Geschäftsbezeichnung“ den Namen, der vom Zahlungsempfänger gewöhnlich bei der Ausübung und im Marketing seiner geschäftlichen Tätigkeit verwendet wird, um sich gegenüber dem Zahler zu identifizieren;

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

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

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

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

44. „Kontoinformationsdienst“ einen Online-Dienst, bei dem ein Anbieter auf ein oder mehrere online zugängliche Zahlungskonten eines Zahlungsdienstnutzers bei einem oder mehreren kontoführenden Zahlungsdienstleistern zugreift, um einen Aggregierungs- oder Konsolidierungsdienst in Bezug auf die Zahlungskontodaten für den Zahlungsdienstnutzer zu erbringen oder die Daten an eine andere Stelle zu übermitteln, die diesen Dienst für den Zahlungsdienstnutzer erbringen wird;

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

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

47. „Kartenzahlverfahren“ ein Kartenzahlverfahren im Sinne des Artikels 2 Nummer 16 der Verordnung (EU) 2015/751;

48. „Abwicklung“ im Zusammenhang mit Zahlungsvorgängen die Abwicklung im Sinne des Artikels 2 Nummer 27 der Verordnung (EU) 2015/751;

49. „abwickelnde Stelle“ eine abwickelnde Stelle im Sinne des Artikels 2 Nummer 28 der Verordnung (EU) 2015/751;

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

51. „Ausgabe von Zahlungsinstrumenten“ einen Zahlungsdienst, bei dem sich ein Zahlungsdienstleister vertraglich dazu verpflichtet, einem Zahler ein Zahlungsinstrument zur Auslösung und Abwicklung der Zahlungsvorgänge des Zahlers zur Verfügung zu stellen;

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

53. „Überweisung“ einen Zahlungsdienst, bei dem dem Zahlungskonto des Zahlungsempfängers auf Anweisung des Zahlers zulasten von dessen Zahlungskonto in einem Zahlungsvorgang oder in einer Serie von Zahlungsvorgängen durch den Zahlungsdienstleister, der das Zahlungskonto des Zahlers führt, ein Betrag gutgeschrieben wird;

54. „Echtzeitüberweisung“ eine Überweisung, die an jedem Kalendertag rund um die Uhr sofort ausgeführt wird;

55. „Wertstellungsdatum“ den Zeitpunkt, den ein Zahlungsdienstleister für die Berechnung der Zinsen auf die von einem Zahlungskonto abgebuchten oder diesem gutgeschriebenen Geldbeträge zugrunde legt;

56. „Referenzwechselkurs“ den Wechselkurs, der für die Berechnung etwaiger Währungsumrechnungskosten zugrunde gelegt und vom Zahlungsdienstleister offengelegt wird oder aus einer öffentlich zugänglichen Quelle stammt;

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

58. „aggregierter durchschnittlicher Devisenmarktkurs“ einen Kurs, der das arithmetische Mittel zwischen dem Ankaufs- und Verkaufspreis eines Währungspaars auf dem Devisenmarkt bildet und für dessen Berechnung Daten aus mehreren Quellen kombiniert werden, um die Marktbedingungen genau und in Echtzeit widerzuspiegeln;

59. „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;

60. „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) und Inhärenz (etwas, das der Nutzer ist), die insofern voneinander unabhängig sind, als die Überwindung eines Elements die Zuverlässigkeit der anderen nicht beeinträchtigt, und so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten sichergestellt ist;

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

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

63. „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;

64. „Geschäftstag“ einen Tag, an dem der an der Ausführung eines Zahlungsvorgangs beteiligte Zahlungsdienstleister des Zahlers bzw. des Zahlungsempfängers geöffnet hat, um einen Zahlungsvorgang, der keine Echtzeitüberweisung ist, auszuführen;

65. „selbst gehostete Adresse“ eine selbst gehostete Adresse im Sinne des Artikels 3 Nummer 20 der Verordnung (EU) 2023/1113;

66. „elektronische Geldbörse“ die Adresse einer Geldbörse für Kryptowerte, bei der ein Anbieter von Kryptowerte-Dienstleistungen die Verwahrung oder Kontrolle von Kryptowerten im Namen seines Kunden oder die Verwahrung oder Kontrolle der Mittel für den Zugang zu solchen Kryptowerten, gegebenenfalls in Form privater kryptografischer Schlüssel, sicherstellt;

67. „vom Händler ausgelöster Vorgang“ (Merchant-Initiated Transaction – MIT) einen Zahlungsvorgang, bei dem der Zahler dem Zahlungsempfänger ein Mandat erteilt hat, das diesen Zahlungsempfänger zur Erteilung eines Zahlungsauftrags für einen Zahlungsvorgang oder eine Serie von Zahlungsvorgängen mittels eines bestimmten Zahlungsinstruments ermächtigt, das ausgegeben wird, damit der Zahler es für die Erteilung von Zahlungsaufträgen für die Zahlungsvorgänge verwendet, sofern dieses Mandat auf einer Vereinbarung zwischen dem Zahler und dem Zahlungsempfänger über die Bereitstellung von Waren oder Dienstleistungen beruht und diesen Vorgängen keine bestimmte Handlung des Zahlers vorausgehen muss, damit ihre Auslösung durch den Zahlungsempfänger erfolgt;

68. „schriftlich oder telefonisch ausgelöster Vorgang“ (mail order or telephone order transaction – MOTO) einen Zahlungsvorgang, bei dem der Zahler Zahlungsaufträge auf anderem Wege als durch die Nutzung elektronischer Plattformen oder Geräte erteilt, etwa mittels papiergestützter Zahlungsaufträge oder schriftlich oder telefonisch ausgelöster Vorgänge, unabhängig davon, ob der Vorgang elektronisch ausgeführt wird oder nicht;

69. „Zwangsgelder“ periodische finanzielle Zwangsmaßnahmen, die darauf abzielen, anhaltende Verstöße gegen diese Verordnung oder gegen eine von einer zuständigen Behörde gemäß dieser Verordnung erlassene Entscheidung zu beenden und eine natürliche oder juristische Person zur Einhaltung der Bestimmungen oder Entscheidungen, gegen die verstoßen wurde, zu zwingen.

TITEL II

TRANSPARENZ DER VERTRAGSBEDINGUNGEN UND INFORMATIONSPFLICHTEN FÜR ZAHLUNGSDIENSTE

Kapitel 1

Allgemeine Vorschriften

Artikel 4

Anwendungsbereich

(1) Dieser Titel gilt für Einzelzahlungen und Rahmenverträge und für die unter solche Verträge fallenden Zahlungsvorgänge. Die an solchen Einzelzahlungen und Rahmenverträgen und unter solche Verträge fallenden Zahlungsvorgängen beteiligten Parteien können vereinbaren, dass dieser Titel insgesamt oder teilweise keine Anwendung findet, wenn es sich bei dem Zahlungsdienstnutzer nicht um einen Verbraucher handelt.

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

(3) Die Mitgliedstaaten teilen der Kommission bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach Absatz 2 erlassen. Sie teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach Absatz 2 erlassen, umgehend mit.

Artikel 5

Währung und Währungsumrechnung

(1) Die Zahlungsvorgänge erfolgen in der zwischen den Parteien vereinbarten Währung.

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

(3) Für die Zwecke von Absatz 2 des vorliegenden Artikels und Artikel 7, Artikel 13 Absatz 1 Buchstabe f und Artikel 20 Absatz 3 Buchstabe e spiegelt der verwendete aggregierte durchschnittliche Devisenmarktkurs den Markt mit einer Verzögerung von höchstens 10 Minuten genau wider; bei Währungen, bei denen dies nicht möglich ist, spiegelt er den letzten gehandelten Kurs eines angesehenen Handelsplatzes wider. Er wird von einem vertrauenswürdigen Administrator bereitgestellt, der die IOSCO-Grundsätze für finanzielle Referenzwerte einhält.

(4) Der Zahler erhält Gelegenheit, der Währungsumrechnung auf der Grundlage der gemäß Absatz 2 bereitgestellten Informationen 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 auf klare, neutrale und verständliche Weise mit.

(2) Verlangt der Zahlungsdienstleister oder eine andere, an dem Vorgang 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 auf klare, neutrale und verständliche Weise 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 Bargeldabhebungsdienste, einschließlich der in Artikel 36 der Richtlinie (EU) 2026/…[+] genannten, erbringen, zeigen ihren Kunden am Geldautomaten Informationen über sämtliche vom Kunden zu zahlenden Entgelte für die Abhebung an, gegebenenfalls einschließlich Umrechnungsentgelten gemäß Artikel 5 Absatz 2 der vorliegenden Verordnung. Die Informationen werden vor der Auslösung des Zahlungsvorgangs auf klare, neutrale und verständliche Weise angezeigt. Auf Verlangen des Kunden werden die Informationen über sämtliche Entgelte auch auf einem dauerhaften Datenträger zur Verfügung gestellt, 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.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

Artikel 9

Beweislast bei den Informationspflichten

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

Artikel 10

Ausnahmen von den Informationspflichten für Kleinbetragszahlungsinstrumente und E-Geld

(1) Bei Zahlungsinstrumenten, die dem betreffenden Rahmenvertrag zufolge nur einzelne Zahlungsvorgänge von höchstens 50 EUR betreffen oder die entweder eine Ausgabenobergrenze von höchstens 300 EUR haben oder Geldbeträge speichern, die zu keiner Zeit 300 EUR übersteigen,

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 anfallende Entgelte und andere wesentliche Informationen, die der Zahler für eine fundierte Entscheidung benötigt; ferner gibt er an, wo die weiteren in Artikel 20 vorgeschriebenen Informationen und Bedingungen 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 abweichend von den Artikeln 25 und 26 nach Ausführung eines Zahlungsvorgangs

i) der Zahlungsdienstleister dem Zahlungsdienstnutzer nur eine Referenz, 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 mitteilt oder zugänglich macht;

ii) der Zahlungsdienstleister die unter Ziffer i genannten Informationen nicht mitteilen bzw. zugänglich machen muss, wenn das Zahlungsinstrument anonym genutzt wird oder der Zahlungsdienstleister ansonsten technisch nicht zur Mitteilung dieser Informationen in der Lage ist; in diesen Fällen bietet der Zahlungsdienstleister dem Zahler die Gelegenheit zur Überprüfung der gespeicherten Geldbeträge.

(2) Bei Zahlungsinstrumenten auf Guthabenbasis dürfen die in Absatz 1 genannten Ausgaben- und Speicherobergrenzen 500 EUR nicht überschreiten.

Kapitel 2
Einzelzahlungen

Artikel 11
Anwendungsbereich

(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 mitzuteilen 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 Bedingungen für seine eigenen Dienste in leicht zugänglicher Form zur Verfügung. Auf Verlangen des Zahlungsdienstnutzers teilt ihm der Zahlungsdienstleister die Informationen und Bedingungen in Papierform oder auf einem anderen dauerhaften Datenträger mit. Die Informationen und Bedingungen sind in einer Amtssprache des Mitgliedstaats, in dem der Zahlungsdienst angeboten wird, oder in einer anderen zwischen den Parteien vereinbarten Sprache in leicht verständlichen Worten und auf klare, neutrale und verständliche Weise 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, so kommt er diesen Pflichten unverzüglich nach Ausführung des Zahlungsvorgangs nach.

(3) Zahlungsdienstleister können ihren in Absatz 1 genannten Pflichten 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 Bedingungen zur Verfügung stellen.

Artikel 13

Informationen und Bedingungen

(1) Folgende Informationen und Bedingungen werden den Zahlungsdienstnutzern von den Zahlungsdienstleistern mitgeteilt oder zugänglich gemacht:

a) die vom Zahlungsdienstnutzer mitzuteilenden Informationen oder Kundenidentifikatoren, die für die ordnungsgemäße Erteilung oder Ausführung eines Zahlungsauftrags erforderlich sind,

b) die maximale Ausführungsfrist für den zu erbringenden Zahlungsdienst,

c) wenn der Zahlungsdienstleister des Zahlungsempfängers außerhalb der Union ansässig ist, die geschätzte Dauer bis zum Eingang der Geldbeträge von Überweisungen und Finanztransfers bei diesem Zahlungsdienstleister,

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 monetärer Betrag in der Währung des Kontos des Zahlers und als prozentualer Aufschlag auf den aggregierten durchschnittlichen Devisenmarktkurs nach Artikel 5 Absatz 3,

g) ein Hinweis auf die alternativen Streitbeilegungsverfahren, die dem Zahlungsdienstnutzer gemäß den Artikeln 100, 104 und 105 zur Verfügung stehen.

Die in Unterabsatz 1 Buchstabe f genannten Informationen werden dem Zahler vor Auslösung des Zahlungsvorgangs offengelegt.

(2) Zahlungsauslösedienstleister teilen dem Zahler vor der Auslösung des Zahlungsvorgangs die folgenden klaren und umfassenden Informationen mit 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 Bedingungen sind dem Zahlungsdienstnutzer – falls zutreffend – in leicht zugänglicher Form zur Verfügung stellen.

Artikel 14

Informationen für Zahler und Zahlungsempfänger nach Erteilung eines Zahlungsauftrags

Wird ein Zahlungsauftrag über einen Zahlungsauslösedienstleister erteilt, so teilt dieser dem Zahler sowie gegebenenfalls dem Zahlungsempfänger unmittelbar nach der Auslösung alle nachstehenden Daten mit 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 Vorgang 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 teilt der Zahlungsdienstleister des Zahlers dem Zahler in der in Artikel 12 Absatz 1 vorgesehenen Weise alle nachstehenden Daten in Bezug auf seine eigenen Dienste mit oder macht sie für den Zahler zugänglich:

a) eine Referenz, die dem Zahler die Identifizierung des Zahlungsvorgangs ermöglicht, und die Informationen, die der Zahler zur zweifelsfreien Identifizierung des Zahlungsempfängers benötigt, einschließlich der Geschäftsbezeichnung des Zahlungsempfängers und – soweit dem Zahlungsdienstleister bekannt und falls abweichend von der Geschäftsbezeichnung – der Firma 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 teilt der Zahlungsdienstleister des Zahlungsempfängers dem Zahlungsempfänger in der in Artikel 12 Absatz 1 vorgesehenen Weise alle nachstehenden Daten in Bezug auf seine eigenen Dienste mit 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 den Geldbetrag 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 der Gutschrift.

Kapitel 3
Rahmenverträge

Artikel 18
Anwendungsbereich

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

Artikel 19
Allgemeine vorvertragliche Informationen

(1) Der Zahlungsdienstleister teilt dem Zahlungsdienstnutzer die in Artikel 20 genannten Informationen und Bedingungen in Papierform oder auf einem anderen dauerhaften Datenträger rechtzeitig mit, bevor der Zahlungsdienstnutzer durch einen Rahmenvertrag oder ein Vertragsangebot gebunden ist. Die Informationen und Bedingungen sind in einer Amtssprache des Mitgliedstaats, in dem der Zahlungsdienst angeboten wird, oder in einer anderen zwischen den Parteien vereinbarten Sprache in leicht verständlichen Worten und auf klare, neutrale und verständliche Weise 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 unmittelbar nach Abschluss des Rahmenvertrags nach.

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

Artikel 20

Informationen und Bedingungen

(1) Der Zahlungsdienstleister teilt dem Zahlungsdienstnutzer folgende Informationen und Bedingungen in Bezug auf den Zahlungsdienstleister mit:

a) den Namen des Zahlungsdienstleisters, 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 Anschriften einschließlich der E-Mail-Adresse, die für die Kommunikation mit dem Zahlungsdienstleister von Belang sind;

b) Informationen über die im Rahmen der Richtlinie (EU) 2026/…[+] benannten zuständigen Aufsichtsbehörden und die in den Artikeln 17 und 18 der genannten Richtlinie vorgesehenen 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.

(2) Der Zahlungsdienstleister teilt dem Zahlungsdienstnutzer folgende Informationen und Bedingungen in Bezug auf die Nutzung des Zahlungsdienstes mit:

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

b) die vom Zahlungsdienstnutzer mitzuteilenden Informationen oder Kundenidentifikatoren, die für die ordnungsgemäße Erteilung oder Ausführung eines Zahlungsauftrags erforderlich sind;

c) die Form und das Verfahren für die Erteilung eines Zahlungsauftrags oder die Erteilung der Einwilligung zur Ausführung eines Zahlungsvorgangs und für den Widerruf der Einwilligung gemäß den Artikeln 50 und 69;

d) den Zeitpunkt des Eingangs eines Zahlungsauftrags gemäß Artikel 67 und gegebenenfalls den vom Zahlungsdienstleister festgelegten Annahmeschluss;

e) die maximale Ausführungsfrist für die zu erbringenden Zahlungsdienste;

f) die geschätzte Dauer bis zum Eingang der Geldbeträge von Überweisungen bei einem außerhalb der Union ansässigen Zahlungsdienstleister des Zahlungsempfängers;

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

g) die Festlegung von Ausgabenobergrenzen für die Nutzung von Zahlungsinstrumenten und Zahlungsmitteln durch den Zahlungsdienstnutzer gemäß Artikel 52 Absatz 1 mit Informationen über die Dauer einer Verzögerung für das Wirksamwerden einer daraus folgenden Erhöhung der Ausgabenobergrenzen und darüber, wie der Zahlungsdienstnutzer diese Ausgabenobergrenzen ändern und diesen Verzögerungszeitraum anpassen oder ablehnen kann;

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

(3) Der Zahlungsdienstleister teilt dem Zahlungsdienstnutzer folgende Informationen und Bedingungen in Bezug auf Entgelte, Zinsen und Wechselkurse mit:

a) alle Entgelte, die der Zahlungsdienstnutzer an den Zahlungsdienstleister zu entrichten hat, einschließlich derjenigen, die damit zusammenhängen, wie und wie oft die Informationen gemäß dieser Verordnung mitgeteilt oder zugänglich gemacht werden, sowie gegebenenfalls eine betragsmäßige Aufschlüsselung dieser Entgelte;

b) alle etwaigen Entgelte für Abhebungen an Geldautomaten im Inland, die Zahlungsdienstnutzer an ihren Zahlungsdienstleister entrichten müssen, wenn es sich um einen Geldautomaten der folgenden Arten handelt:

i) ihres Zahlungsdienstleisters,

ii) eines Zahlungsdienstleisters, der demselben Geldautomatennetz angehört wie der Zahlungsdienstleister des Nutzers,

iii) eines Zahlungsdienstleisters, der einem Geldautomatennetz angehört, mit dem der Zahlungsdienstleister des Nutzers eine vertragliche Beziehung unterhält,

iv) eines Geldautomatenbetreibers;

c) falls zutreffend, die zugrunde zu legenden Zinssätze und Wechselkurse oder – wenn Referenzzinssätze und Referenzwechselkurse anzuwenden sind – 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 Referenzwechselkurses;

d) sofern vereinbart, die unmittelbare Anwendung von Änderungen des Referenzzinssatzes oder Referenzwechselkurses und die Informationspflichten in Bezug auf diese Änderungen gemäß Artikel 22 Absatz 3;

e) falls zutreffend, die geschätzten Entgelte für die Währungsumrechnung bei einer Überweisung, ausgedrückt als monetärer Betrag in der Währung des Kontos des Zahlers und als prozentualer Aufschlag auf einen aggregierten durchschnittlichen Devisenmarktkurs nach Artikel 5 Absatz 3.

Die in Unterabsatz 1 Buchstabe e genannten Informationen werden dem Zahler vor Auslösung jedes Zahlungsvorgangs offengelegt.

(4) Der Zahlungsdienstleister teilt dem Zahlungsdienstnutzer folgende Informationen und Bedingungen in Bezug auf die Kommunikation mit:

a) 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;

b) Angaben dazu, wie und wie oft die Informationen gemäß dieser Verordnung mitzuteilen oder zugänglich zu machen sind;

c) 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;

d) ein Hinweis auf das Recht des Zahlungsdienstnutzers, die Vertragsbedingungen des Rahmenvertrags und die Informationen und Bedingungen gemäß Artikel 21 zu erhalten.

(5) Der Zahlungsdienstleister teilt dem Zahlungsdienstnutzer folgende Informationen und Bedingungen in Bezug auf Schutz- und Abhilfemaßnahmen mit:

a) falls zutreffend, eine Beschreibung der Vorkehrungen, die der Zahlungsdienstnutzer für die sichere Aufbewahrung eines Zahlungsinstruments zu treffen hat, und wie der Anzeigepflicht gegenüber dem Zahlungsdienstleister nach Artikel 53 Absatz 1 Buchstabe b nachzukommen ist;

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

c) die Bedingungen, unter denen sich der Zahlungsdienstleister das Recht vorbehält, ein Zahlungsinstrument gemäß Artikel 52 zu sperren;

d) Informationen zur Haftung des Zahlers gemäß Artikel 60 Absatz 4 und Artikel 63, einschließlich Informationen zum relevanten Betrag;

e) Angaben dazu, wie und innerhalb welcher Frist der Zahlungsdienstnutzer den Zahlungsdienstleister über etwaige nicht autorisierte oder fehlerhaft ausgelöste oder ausgeführte Zahlungsvorgänge gemäß Artikel 55, sowie die Polizei im Falle des in Artikel 60 genannten Identitätsbetrugs, unterrichten muss;

f) Informationen über die Haftung des Zahlungsdienstleisters bei nicht autorisierten Zahlungsvorgängen gemäß Artikel 57, bei fehlerhafter Anwendung der Abgleichdienstleistung für Namen und Kundenidentifikator gemäß Artikel 58 und bei Identitätsbetrug gemäß Artikel 60;

g) Informationen über die Haftung des Zahlungsdienstleisters bei der Auslösung oder Ausführung von Zahlungsvorgängen gemäß den Artikeln 79 und 80;

h) die Bedingungen für Erstattungen gemäß den Artikeln 65 und 66.

(6) Der Zahlungsdienstleister teilt dem Zahlungsdienstnutzer folgende Informationen und Bedingungen in Bezug auf Änderungen des Rahmenvertrags und dessen Kündigung mit:

a) sofern vereinbart, die Angabe, dass die Zustimmung des Zahlungsdienstnutzers zu einer Änderung der Bedingungen 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;

b) die Laufzeit des Rahmenvertrags;

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

(7) Der Zahlungsdienstleister teilt dem Zahlungsdienstnutzer folgende Informationen und Bedingungen in Bezug auf Abhilfe mit:

a) die Vertragsklauseln über das für den Rahmenvertrag geltende Recht oder die zuständigen Gerichte;

b) Informationen über die alternativen Streitbeilegungsverfahren, die dem Zahlungsdienstnutzer gemäß den Artikeln 100, 104 und 105 zur Verfügung stehen.

Artikel 21

Zugänglichkeit der Informationen und der Bedingungen des Rahmenvertrags

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

Artikel 22

Änderungen des Rahmenvertrags

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

(2) Falls zutreffend unterrichtet der Zahlungsdienstleister den Zahlungsdienstnutzer gemäß Artikel 20 Absatz 6 Buchstabe a darüber, dass dessen Zustimmung zu diesen Änderungen als erteilt gilt, wenn er dem Zahlungsdienstleister seine Ablehnung nicht vor dem vorgeschlagenen Tag des Inkrafttretens dieser Änderungen angezeigt hat. Der Zahlungsdienstleister unterrichtet den Zahlungsdienstnutzer ferner über sein Recht, den Rahmenvertrag jederzeit vor dem Tag des Geltungsbeginns 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 Änderungen der Zinssätze oder Wechselkurse auf dem gemäß Artikel 20 Absatz 3 Buchstaben c und d vereinbarten Referenzzinssatz oder Referenzwechselkurs 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 mitzuteilen oder zugänglich zu machen sind. Für den Zahlungsdienstnutzer vorteilhafte Änderungen der Zinssätze oder Wechselkurse können vom Zahlungsdienstleister jedoch ohne Benachrichtigung angewandt werden.

(4) Änderungen der bei Zahlungsvorgängen zugrunde gelegten Zinssätze oder Wechselkurse 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. Die 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 drei Monate in Kraft. Sofern für die Kündigung des Rahmenvertrags Entgelte anfallen, müssen diese angemessen und an den Kosten ausgerichtet sein. Werden unter dem Rahmenvertrag Zahlungsdienste gemeinsam mit technischen Diensten angeboten, die die Erbringung von Zahlungsdiensten unterstützen und vom Zahlungsdienstleister oder einem Dritten erbracht werden, mit dem der Zahlungsdienstleister eine Partnerschaft eingegangen ist, so unterliegen diese technischen Dienste den gleichen Anforderungen des Rahmenvertrags über Kündigungsentgelte.

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

(4) Regelmäßig erhobene Zahlungsdienstentgelte sind vom Zahlungsdienstnutzer nur anteilig bis zur Kündigung des Vertrags zu entrichten. Werden solche Entgelte im Voraus entrichtet, sind sie vom Zahlungsdienstleister anteilig 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 … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach Absatz 6 erlassen. Sie teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach Absatz 6 erlassen, umgehend mit.

Artikel 24

Information 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 vor der Auslösung des Zahlungsvorgangs ausdrückliche Information über Folgendes mit:

a) die maximale Ausführungsfrist,

b) die vom Zahler zu entrichtenden Entgelte und

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 folgende Informationen mit:

a) eine Referenz, die dem Zahler die Identifizierung jedes Zahlungsvorgangs ermöglicht, und die Informationen, die zur zweifelsfreien Identifizierung des Zahlungsempfängers benötigt werden, einschließlich der Geschäftsbezeichnung des Zahlungsempfängers und – sofern dem Zahlungsdienstleister bekannt und falls abweichend von der Geschäftsbezeichnung – der Firma 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 hat eine Klausel zu enthalten, wonach der Zahler verlangen kann, dass die in Absatz 1 genannten Informationen regelmäßig, in einer vom Zahler festgelegten Häufigkeit, kostenlos und nach einem vereinbarten Verfahren so mitgeteilt oder zugänglich gemacht werden, dass der Zahler sie unverändert aufbewahren und reproduzieren kann. Der Zahler ist berechtigt, mindestens die monatliche Mitteilung oder Zugänglichmachung dieser Informationen zu verlangen.

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

(4) Die Mitgliedstaaten teilen der Kommission bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach Absatz 3 erlassen. Sie teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach Absatz 3 erlassen, 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 folgende Informationen 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 der Gutschrift.

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

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

(4) Die Mitgliedstaaten teilen der Kommission bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach Absatz 3 erlassen. Sie teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach Absatz 3 erlassen, umgehend mit.

TITEL III
RECHTE UND PFLICHTEN BEI DER ERBRINGUNG UND NUTZUNG VON ZAHLUNGSDIENSTEN

Kapitel 1
Allgemeine Bestimmungen

Artikel 27

Anwendungsbereich

(1) Handelt es sich bei dem Zahlungsdienstnutzer nicht um einen Verbraucher, können der Zahlungsdienstnutzer und der Zahlungsdienstleister vereinbaren, dass Artikel 28 Absatz 1, Artikel 50 Absatz 7 sowie die Artikel 56, 63, 65, 66, 69, 79 und 80 ganz oder teilweise keine Anwendung finden. Zahlungsdienstnutzer und Zahlungsdienstleister können auch andere als die in Artikel 55 festgelegten Fristen vereinbaren.

(2) Die Mitgliedstaaten können vorsehen, dass Artikel 105 keine Anwendung findet, wenn es sich bei dem Zahlungsdienstnutzer nicht um einen Verbraucher handelt.

(3) Die Mitgliedstaaten können diesen Titel in gleicher Weise auf Kleinstunternehmen anwenden wie er auf Verbraucher Anwendung findet.

(4) Die Mitgliedstaaten teilen der Kommission bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach den Absätzen 2 und 3 erlassen. Sie teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach den Absätzen 2 und 3 erlassen, 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 68 Absatz 3, Artikel 69 Absatz 5 und Artikel 78 Absatz 3 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, trägt der Zahlungsempfänger die vom Zahlungsdienstleister des Zahlungsempfängers erhobenen Entgelte und der Zahler die vom Zahlungsdienstleister des Zahlers erhobenen Entgelte.

(3) Für die Nutzung von Zahlungsinstrumenten, für die die Interbankenentgelte in Kapitel II der Verordnung (EU) 2015/751 festgelegt sind, oder für Überweisungen, einschließlich Echtzeitüberweisungen, 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 es die Mitgliedstaaten Zahlungsempfängern untersagen, für die Nutzung anderer Zahlungsinstrumente als der in Absatz 3 genannten Instrumente Entgelte zu verlangen, oder ein entsprechendes Recht des Zahlungsempfängers begrenzen.

(5) Der Zahlungsdienstleister darf den Zahlungsempfänger nicht daran hindern, dem Zahler eine Ermäßigung anzubieten oder dem Zahler anderweitig einen Anreiz zur Nutzung eines bestimmten Zahlungsinstruments zu geben. 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. 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 … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach Absatz 4 erlassen. Sie teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach Absatz 4 erlassen, umgehend mit.

Artikel 29

Ausnahmeregelung für Kleinbetragszahlungsinstrumente und E-Geld

(1) Bei Zahlungsinstrumenten, die dem Rahmenvertrag zufolge nur einzelne Zahlungsvorgänge von höchstens 50 EUR betreffen oder die entweder eine Ausgabenobergrenze von höchstens 300 EUR haben oder Geldbeträge speichern, die zu keiner Zeit 300 EUR übersteigen, können die Zahlungsdienstleister mit ihren Zahlungsdienstnutzern vereinbaren, dass

a) Artikel 53 Absatz 1 Buchstabe b, Artikel 54 Absatz 1 Unterabsatz 1 Buchstaben c und d und Artikel 63 Absatz 5 keine Anwendung finden, wenn das Zahlungsinstrument nicht gesperrt werden oder seine weitere Nutzung nicht verhindert werden kann,

b) die Artikel 56 und 57 sowie Artikel 63 Absätze 1 und 5 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 68 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 69 der Zahler den Zahlungsauftrag nach dessen Übermittlung oder nach Autorisierung des Zahlungsvorgangs gegenüber dem Zahlungsempfänger nicht widerrufen kann,

e) abweichend von den Artikeln 73 und 74 andere Ausführungsfristen gelten.

(2) Bei Zahlungsinstrumenten auf Guthabenbasis dürfen die in Absatz 1 genannten Ausgabenobergrenzen und Speichergrenzen 500 EUR nicht überschreiten.

(3) Die Artikel 57 und 63 gelten 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.

(4) Die Mitgliedstaaten teilen der Kommission bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach Absatz 3 erlassen. Sie teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach Absatz 3 erlassen, umgehend mit.

Artikel 30

Ausgabe und Rücktauschbarkeit von E-Geld

(1) E-Geld-Emittenten geben E-Geld zum Nennwert des entgegengenommenen Geldbetrags 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 deutlich erkennbar 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 Vertragsablauf,

b) der Vertrag sieht ein Ablaufdatum vor und der E-Geld-Inhaber beendet 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 des E-Geldes vor Vertragsablauf, so kann dieses Verlangen entweder einen Teil oder den gesamten Betrag betreffen.

(6) Verlangt der E-Geld-Inhaber den Rücktausch des E-Geldes zum Vertragsablauf oder bis zu einem Jahr nach Vertragsablauf, so ergreift der E-Geld-Emittent eine der folgenden beiden Maßnahmen:

a) er tauscht den vollen monetären Wert des E-Gelds zurück;

b) er tauscht den gesamten vom E-Geld-Inhaber verlangten Geldbetrag zurück, falls das Zahlungsinstitut andere gewerbliche Tätigkeiten nach Artikel 10 Absatz 1 Buchstabe c der Richtlinie (EU) 2026/…[+] ausübt und im Voraus nicht bekannt ist, welcher Anteil des Geldbetrags von den E-Geld-Inhabern als E-Geld verwendet werden soll.

(7) Ungeachtet 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 ausgibt, darf einem E-Geld-Inhaber keine Zinsen oder sonstigen Vorteile gewähren, die im Zusammenhang mit dem Zeitraum stehen, in dem dieser E-Geld-Inhaber das E-Geld hält.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

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 unternehmerische Risiko oder für den Schutz der finanziellen und operativen Stabilität des Zahlungssystems erforderlich ist.

(2) Ein Zahlungssystembetreiber stellt die Regeln und Verfahren, nach denen er die Zulassung für die Teilnahme an seinem Zahlungssystem erteilt, sowie die Kriterien und Methodik, nach denen er das Risiko für eine solche Teilnahme bewertet, 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 mit Risiken für das System gemäß Absatz 1 verbunden ist. Der Zahlungssystembetreiber teilt dem antragstellenden Zahlungsdienstleister schriftlich mit, ob seinem Teilnahmeantrag stattgegeben wird oder nicht und begründet jede Ablehnung ordnungsgemäß.

(4) Zahlungssystembetreiber dürfen Folgendes nicht auferlegen:

a) restriktive Regeln hinsichtlich der effektiven Teilnahme an anderen Zahlungssystemen;

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

c) Beschränkungen aufgrund des institutionellen Status.

(5) Die Absätze 1 bis 4 gelten für Betreiber von Zahlverfahren. Diese Absätze gelten nicht für Zahlungssystembetreiber oder für Betreiber von Zahlverfahren, die ausschließlich aus Zahlungsdienstleistern derselben Gruppe bestehen.

(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 zu begründen.

(7) Die Mitgliedstaaten benennen eine zuständige Behörde, die die Einhaltung der Absätze 1 bis 4 und gegebenenfalls des Absatzes 6 durch Zahlungssysteme und Zahlverfahren, die ihrem nationalen Recht unterliegen, sicherstellt, außer in Fällen, in denen diese Anforderungen vom Eurosystem oder den Zentralbanken der Mitgliedstaaten, deren Währung nicht der Euro ist, im Rahmen der Aufsicht über den Betrieb dieser Zahlungssysteme oder Zahlverfahren – wie der Zahlungssysteme, die der Verordnung (EU) 2025/1355 unterliegen –, durch- oder umgesetzt wird.

Artikel 32

Transparente Praktiken bei Kartenzahlverfahren, abwickelnden Stellen und Anbietern von Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen

(1) Betreiber von Kartenzahlverfahren und abwickelnde Stellen stellen sicher, dass die Gebühren, die Zahlungsdienstleistern, die Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, auferlegt werden, klar und einheitlich kategorisiert und offengelegt werden, sodass die Abrechnungskategorien von Zahlverfahren und abwickelnden Stellen mindestens auf der Grundlage der folgenden Gebührenkategorien vergleichbar sind:

a) Interbankenentgelte;

b) Abwicklungsgebühren und

c) Gebühren für Zahlverfahren, darunter:

i) Pflichtgebühren;

ii) Gebühren in Verbindung mit einem bestimmten Verhalten oder der Nutzung oder Nichtnutzung einer Technologie und

iii) Gebühren im Zusammenhang mit optionalen Dienstleistungen.

Die Gebührenkategorien müssen klar definiert sein.

Die in Unterabsatz 1 genannten Informationen werden Zahlungsdienstleistern, die Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, in einer Weise offengelegt, die vollständige Klarheit darüber gewährleistet, welche Gebühren welchen Dienstleistungen entsprechen.

Die in Unterabsatz 1 genannten Informationen müssen so präzise wie möglich sein und, wenn möglich, zwischen den erhobenen Gebühren nach Kartenkategorie, Vertriebsweg, Volumen und Wert der Zahlungsvorgänge des Händlers und geografischem Standort unterscheiden.

(2) Zahlungsdienstleister, die Dienstleistungen im zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, verwenden die gemäß Absatz 1 des vorliegenden Artikels offengelegten Informationen, wenn sie ihren Verpflichtungen gemäß den Artikeln 9 und 12 der Verordnung (EU) 2015/751 nachkommen.

(3) Für die Zwecke des Absatzes 1 verfahren die Betreiber von Kartenzahlverfahren und die abwickelnden Stellen wie folgt:

a) sie informieren die Zahlungsdienstleister, die Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, über neue Gebühren sowie Änderungen der Gebühren für Zahlverfahren und der Abwicklungsgebühren spätestens sechs Monate vor deren Einführung unmissverständlich und auf transparente und kohärente Weise;

b) sie unterhalten ein gemeinsames öffentliches Unionsregister für ihre Verfahren sowie die Regeln für Zahlverfahren und die Abwicklung sowie die Gebühren für Zahlverfahren und Abwicklungsgebühren entsprechend den in Absatz 1 genannten Gebührenkategorien.

(4) Die Kommission erlässt bis zum … [15 Monate nach dem Tag des Inkrafttretens dieser Verordnung] einen delegierten Rechtsakt gemäß Artikel 115, um diese Verordnung durch die weitere Präzisierung der den Zahlungsdienstleistern, die Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, gemäß Absatz 1 offenzulegenden Informationen zu ergänzen.

Artikel 33

Bereitstellung von Zahlungskonten an Zahlungsinstitute durch Kreditinstitute

(1) Kreditinstitute gewähren Zahlungsinstituten, ihren Agenten und Zahlungsinstitutsanwärtern auf objektiver, nicht-diskriminierender und verhältnismäßiger Grundlage Zugang zu Zahlungskonten. Ein solcher Zugang muss so umfassend sein, dass Zahlungsinstitute Zahlungsdienste ungehindert und effizient erbringen können.

(2) Ein Kreditinstitut darf nur in nachstehend genannten Fällen die Eröffnung eines Zahlungskontos für ein Zahlungsinstitut oder dessen Agenten oder für einen Zahlungsinstitutsanwärter verweigern oder ein solches Konto schließen:

a) die Eröffnung oder Führung eines solchen Zahlungskontos würde zu einem Verstoß gegen die Verordnung (EU) 2024/1624 führen;

b) das Zahlungsinstitut oder seine Agenten oder ein Zahlungsinstitutsanwärter begehen eine erhebliche Vertragsverletzung oder haben eine solche begangen;

c) der Antragsteller für ein Konto hat einschlägige Informationen und Unterlagen nicht vorgelegt;

d) die zuständige Behörde hat eine Zulassung als Zahlungsinstitut verweigert oder entzogen.

(3) Ein Zugang, der einem Agenten gemäß Absatz 1 gewährt wird, gilt ausschließlich für die Erbringung von Zahlungsdiensten im Namen eines Zahlungsinstituts.

(4) Ein Kreditinstitut setzt das Zahlungsinstitut oder dessen Agenten oder den Zahlungsinstitutsanwärter sowie die zuständige Behörde unverzüglich, spätestens jedoch einen Monat nach Eingang eines vollständigen Antrags, über jede Entscheidung in Kenntnis, die Eröffnung eines Zahlungskontos für ein Zahlungsinstitut oder dessen Agenten oder für einen Zahlungsinstitutsanwärter zu verweigern. Eine solche Entscheidung ist ordnungsgemäß zu begründen und muss die Risiken angeben, mit denen die Tätigkeit oder geplante Tätigkeit dieses Zahlungsinstituts oder seiner Agenten oder dieses Zahlungsinstitutsanwärters nach Einschätzung des Kreditinstituts und basierend auf den in Absatz 2 genannten Gründen verbunden ist, und darf nicht allgemeiner Natur sein.

Das Kreditinstitut teilt dem Zahlungsinstitut oder dessen Agenten oder dem Zahlungsinstitutsanwärter sowie der zuständigen Behörde die Entscheidung, das Zahlungskonto zu schließen, mindestens vier Monate vor der Schließung mit. Jede Entscheidung über die Schließung eines Zahlungskontos ist ordnungsgemäß begründet, ist spezifisch und basiert auf den in Absatz 2 des vorliegenden Artikels genannten Gründen, wobei die Fähigkeit des Zahlungsinstituts, die Sicherungsanforderung gemäß Artikel 9 der Richtlinie (EU) 2026/…[+] zu erfüllen, berücksichtigt wird.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

Abweichend von den Unterabsätzen 1 und 2 des vorliegenden Absatzes gilt für die Kreditinstitute in den in Absatz 2 Buchstabe a genannten Fällen Folgendes:

a) sie teilen dem Zahlungsinstitut, dessen Agenten oder dem Zahlungsinstitutsanwärter lediglich mit, dass die Eröffnung oder Führung eines Zahlungskontos einen Verstoß gegen die Verordnung (EU) 2024/1624 darstellen würde, und legen keine Einzelheiten zur Art dieses Verstoßes offen;

b) sie haben das Recht, das Zahlungskonto nach einer kürzeren Kündigungsfrist zu schließen.

(5) Die zuständige Behörde kann aggregierte Daten zu verweigerten Eröffnungen und Schließungen von Zahlungskonten veröffentlichen.

(6) Ein Zahlungsinstitut oder seine Agenten oder ein Zahlungsinstitutsanwärter, die von einer Entscheidung eines Kreditinstituts, die Eröffnung eines Zahlungskontos zu verweigern oder ein Zahlungskonto zu schließen, betroffen sind, können bei der zuständigen Behörde Beschwerde einlegen.

(7) Die EBA arbeitet Entwürfe technischer Regulierungsstandards aus, in denen das harmonisierte Format und die Informationen, die in der in Absatz 4 genannten Mitteilung und der dort genannten Entscheidung enthalten sein müssen, festgelegt werden.

Die EBA übermittelt der Kommission die in Unterabsatz 1 genannten Entwürfe technischer Regulierungsstandards bis zum … [zwölf Monate nach dem Tag des Inkrafttretens dieser Verordnung].

Der Kommission wird die Befugnis übertragen, diese 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 34

Rechte der Zahlungsdienstnutzer

(1) Zahlungsdienstleister hindern Zahlungsdienstnutzer nicht daran, Zahlungsauslösedienstleister in Anspruch zu nehmen, um Zahlungsauslösedienste zu erhalten. Diese Verpflichtung gilt für alle online zugänglichen Zahlungskonten des Zahlungsdienstnutzers.

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

Artikel 35

Vertragliche Beziehungen

(1) Die Bereitstellung von Kontoinformationsdiensten 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 multilaterale vertragliche Vereinbarung und stehen die unter diese Verordnung fallenden Zahlungskontodaten auch im Rahmen dieser multilateralen vertraglichen Vereinbarung zur Verfügung, so müssen Kontoinformationsdienstleister und Zahlungsauslösedienstleister stets auf die unter diese Verordnung fallenden Zahlungskontodaten zugreifen können, ohne dass diese Dienstleister Partei der multilateralen vertraglichen Vereinbarung sein müssen.

ABSCHNITT 2

DATENZUGANGSSCHNITTSTELLEN FÜR KONTOINFORMATIONSDIENSTE UND ZAHLUNGSAUSLÖSEDIENSTE

Artikel 36

Bereitstellung dedizierter Zugangsschnittstellen

(1) Kontoführende Zahlungsdienstleister, die einem Zahler ein online zugängliches Zahlungskonto bereitstellen, verfügen für den Datenaustausch mit Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern über mindestens eine dedizierte Schnittstelle.

(2) Ein kontoführender Zahlungsdienstleister richtet die in Absatz 1 genannte dedizierte Schnittstelle innerhalb von drei Monaten nach Erhalt seiner Zulassung ein. Um sicherzustellen, dass die dedizierte Schnittstelle so bald wie möglich genutzt werden kann, stellt der kontoführende Zahlungsdienstleister die einschlägige technische Dokumentation für die dedizierte Schnittstelle auf Verlangen der zugelassenen Zahlungsauslösedienstleister, der zugelassenen Kontoinformationsdienstleister oder von Unternehmen, die bei ihren zuständigen Behörden die entsprechende Zulassung beantragt haben, unverzüglich zur Verfügung.

Kontoführende Zahlungsdienstleister gewähren stets den Zugang zu der in Absatz 1 genannten dedizierten Schnittstelle, um Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern die Geschäftskontinuität zu ermöglichen.

(3) Ein kontoführender Zahlungsdienstleister gewährleistet, dass die in Absatz 1 genannte dedizierte Schnittstelle den von europäischen oder internationalen Normungsorganisationen – einschließlich des Europäischen Komitees für Normung (CEN) oder der Internationalen Organisation für Normung (ISO) – herausgegebenen Standards für die Kommunikation oder anderen einschlägigen, weithin anerkannten Standards, die eine gleichwertige Sicherheit bieten, entspricht. Ein kontoführender Zahlungsdienstleister gewährleistet zudem, dass die technischen Spezifikationen einer in Absatz 1 genannten dedizierten Schnittstelle unter Angabe der Routinen, Protokolle und Tools, die von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern benötigt werden, um die Interoperabilität ihrer Software und ihrer Anwendungen mit den Systemen des kontoführenden Zahlungsdienstleisters zu ermöglichen, dokumentiert sind. Kontoführende Zahlungsdienstleister machen die Dokumentation der technischen Spezifikationen für ihre in Absatz 1 genannten dedizierten Schnittstellen auf Verlangen der zugelassenen Zahlungsauslösedienstleister, der zugelassenen Kontoinformationsdienstleister oder der Zahlungsdienstleister, die bei ihren zuständigen Behörden die entsprechende Zulassung beantragt haben, kostenfrei und unverzüglich zugänglich und veröffentlichen eine Zusammenfassung dieser Dokumentation auf ihrer Website.

(4) Ein kontoführender Zahlungsdienstleister gewährleistet, dass jegliche Änderung der technischen Spezifikationen der in Absatz 1 genannten dedizierten Schnittstelle den zugelassenen Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern oder einschlägigen Zahlungsinstitutsanwärtern so bald wie möglich im Voraus und mindestens zwei Monate vor der Umsetzung dieser Änderung zumindest durch Veröffentlichung auf seiner Website zur Verfügung gestellt wird, es sei denn, er wird durch eine Notfallsituation daran gehindert. Kontoführende Zahlungsdienstleister dokumentieren Notfallsituationen, in denen Änderungen ohne vorherige Ankündigung der entsprechenden Informationen umgesetzt wurden, und machen die Dokumentation den zuständigen Behörden auf Verlangen zugänglich.

(5) Kontoführende Zahlungsdienstleister veröffentlichen auf ihren Websites vierteljährliche Statistiken über die Verfügbarkeit, die ungeplante Nichtverfügbarkeit und die Leistung ihrer dedizierten Schnittstellen sowie – zu Vergleichszwecken – der Schnittstellen, die sie ihren Zahlungsdienstnutzern für den direkten Online-Zugriff auf Zahlungskonten zur Verfügung stellen. 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) Ein kontoführender Zahlungsdienstleister stellt eine Testumgebung, einschließlich Unterstützung, für Konnektivitäts- und Funktionstests dedizierter Schnittstellen zur Verfügung, damit die zugelassenen Zahlungsauslösedienstleister und Kontoinformationsdienstleister oder einschlägige Zahlungsinstitutsanwärter ihre Software und die Anwendungen testen können, die sie verwenden, um Nutzern 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 des Identifizierungs- oder Authentifizierungsverfahrens oder während des Austauschs von Datenelementen über seine 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 37

Anforderungen an dedizierte Datenzugangsschnittstellen

(1) Ein kontoführender Zahlungsdienstleister gewährleistet, dass die dedizierte Schnittstelle, die er nach Artikel 36 Absatz 1 einrichtet, folgende Sicherheits- und Leistungsanforderungen erfüllt:

a) während der Authentifizierung des Zahlungsdienstnutzers baut die dedizierte Schnittstelle Kommunikationssitzungen zwischen dem kontoführenden Zahlungsdienstleister, dem Kontoinformationsdienstleister, dem Zahlungsauslösedienstleister und dem betreffenden Zahlungsdienstnutzer auf und erhält diese aufrecht;

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 auf Zugangsanfragen von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern überschreitet nicht die Antwortzeit der Schnittstelle, die der kontoführende Zahlungsdienstleister seinen Zahlungsdienstnutzern für den direkten Online-Zugriff auf ihr Zahlungskonto zur Verfügung stellt.

(2) Ein kontoführender Zahlungsdienstleister gewährleistet, dass die in Absatz 1 genannte dedizierte Schnittstelle es Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern ermöglicht,

a) sich gegenüber dem kontoführenden Zahlungsdienstleister zu identifizieren;

b) den kontoführenden Zahlungsdienstleister anzuweisen, ausgehend von der Einwilligung, die der Zahlungsdienstnutzer dem Kontoinformationsdienstleister oder dem Zahlungsauslösedienstleister gemäß Artikel 50 Absatz 3 erteilt hat, mit der Authentifizierung zu beginnen;

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

(3) Kontoführende Zahlungsdienstleister ermöglichen es Kontoinformationsdienstleistern, über die in Absatz 1 genannte 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. Diese Informationen umfassen den Kundenidentifikator für das Konto, die zugehörigen Namen der Kontoinhaber, die Währungen, den Kontosaldo und über ein Zahlungsinstrument ausgelöste Zahlungsvorgänge, mit denen das Zahlungskonto noch nicht belastet wurde, sofern diese Vorgänge bereits in der Kundenschnittstelle sichtbar sind.

(4) Kontoführende Zahlungsdienstleister gewährleisten, dass die in Absatz 1 genannte dedizierte Schnittstelle es Zahlungsauslösedienstleistern zumindest ermöglicht,

a) einen Dauerauftrag zu erteilen und zu widerrufen;

b) eine Einzelzahlung auszulösen;

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

d) Zahlungsvorgänge an mehrere Begünstigte auszulösen;

e) Zahlungsvorgänge auszulösen, unabhängig davon, ob der Zahlungsempfänger auf der Liste der Begünstigten des Zahlers steht, es sei denn, der Zahlungsdienstnutzer ist nicht in der Lage, diese Zahlungsvorgänge über die Kundenschnittstelle auszuführen;

f) auf sichere Weise zu kommunizieren, um einen Zahlungsauftrag vom Zahlungskonto des Zahlers 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 des Zahlungsvorgangs den Namen des Kontoinhabers zu überprüfen, unabhängig davon, ob der Name des Kontoinhabers über die direkte Schnittstelle verfügbar ist;

h) in Fällen, in denen der kontoführende Zahlungsdienstleister mehrere Authentifizierungsverfahren anbietet, zu entscheiden, welches Authentifizierungsverfahren dem Zahler angeboten wird;

i) vor Auslösung des Zahlungsvorgangs den Kundenidentifikator für das Konto, die zugehörigen Namen des Kontoinhabers und, sofern sie dem Zahlungsdienstnutzer zur Verfügung stehen, die Währungen einzusehen.

(5) Kontoführende Zahlungsdienstleister gewährleisten, dass die in Absatz 1 genannte 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) so bald wie möglich die Bestätigung des kontoführenden Zahlungsdienstleisters übermittelt, dass der Zahlungsvorgang ausgehend von den ihm vorliegenden Informationen ausgeführt wurde oder ausgeführt werden wird, wobei etwaige bereits erteilte Zahlungsaufträge, die die vollständige Ausführung des erteilten Zahlungsauftrags beeinflussen könnten, berücksichtigt werden.

Die unter Unterabsatz 1 Buchstabe b genannten Informationen dürfen nicht an den Zahlungsauslösedienstleister weitergegeben werden, können vom kontoführenden Zahlungsdienstleister aber dafür verwendet werden, die Ausführung des Vorgangs zu bestätigen.

(6) Für die Zwecke der Tätigkeiten von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern stellen der Name des Kontoinhabers und der Kundenidentifikator für das Konto keine sensiblen Zahlungsdaten dar.

Artikel 38

Gleicher Datenzugang bei dedizierter Zugangsschnittstelle und Kundenschnittstelle

(1) Unbeschadet des Artikels 37 gewährleistet ein kontoführender Zahlungsdienstleister, dass die in Artikel 36 Absatz 1 genannte dedizierte Schnittstelle jederzeit zumindest denselben Grad an Verfügbarkeit und Leistung, einschließlich technischer und IT-bezogener Unterstützung, aufweist wie die Schnittstellen, die der kontoführende Zahlungsdienstleister dem Zahlungsdienstnutzer für den direkten Online-Zugriff auf sein Zahlungskonto zur Verfügung stellt.

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

(3) Ein kontoführender Zahlungsdienstleister teilt Zahlungsauslösedienstleistern zumindest dieselben Informationen über die Auslösung und Ausführung des Zahlungsvorgangs mit, die auch dem Zahlungsdienstnutzer mitgeteilt oder zugänglich gemacht werden, wenn dieser den Vorgang direkt auslöst. Diese Informationen werden unmittelbar nach Eingang des Zahlungsauftrags übermittelt. Jede Aktualisierung dieser Informationen, einschließlich des Zahlungsstatus, wird dem Zahlungsauslösedienstleister über die dedizierte Schnittstelle kontinuierlich zugänglich gemacht, bis der Zahlungsvorgang ausgeführt oder abgelehnt wird.

Artikel 39

Verfügbarkeits- und Leistungsanforderungen an die dedizierte Schnittstelle

(1) Ein kontoführender Zahlungsdienstleister trifft alle in seiner Macht stehenden Maßnahmen, um jede geplante Nichtverfügbarkeit der dedizierten Schnittstelle auf das unbedingt erforderliche Maß zu begrenzen und eine ungeplante Nichtverfügbarkeit und unzureichende Leistung der dedizierten Schnittstelle zu verhindern. Nichtverfügbarkeit gilt als gegeben, wenn fünf aufeinanderfolgende Informationsanfragen für die Erbringung von Zahlungsauslösediensten oder Kontoinformationsdiensten innerhalb von 30 Sekunden mit „Serverfehler“ beantwortet werden oder innerhalb von 30 Sekunden keine Antwort von der dedizierten Schnittstelle des kontoführenden Zahlungsdienstleisters erfolgt.

(2) Im Falle einer geplanten Nichtverfügbarkeit der dedizierten Schnittstelle unterrichten die kontoführenden Zahlungsdienstleister – mit Ausnahme von Änderungen aufgrund von Notfällen – die Zahlungsdienstleister, die die dedizierte Schnittstelle nutzen, mindestens einen Monat im Voraus über die geplante Nichtverfügbarkeit und deren Dauer. Eine geplante Nichtverfügbarkeit wird in der Regel auf den Zeitraum zwischen 0:00 Uhr und 6:00 Uhr gelegt.

(3) Im Falle einer ungeplanten Nichtverfügbarkeit der dedizierten Schnittstelle teilen die kontoführenden Zahlungsdienstleister den Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern, die die dedizierte Schnittstelle nutzen, rechtzeitig mit, welche Maßnahmen zur Wiederherstellung der Verfügbarkeit der Schnittstelle getroffen werden, und wie lange die Lösung des Problems schätzungsweise in Anspruch nehmen wird. Kontoführende Zahlungsdienstleister stellen eine optimale Wiederherstellungsdauer für die dedizierte Schnittstelle sicher.

(4) Ein kontoführender Zahlungsdienstleister stellt sicher, dass die dedizierte Schnittstelle mindestens die gleiche Verfügbarkeit und Leistung bietet wie die Schnittstelle, die der kontoführende Zahlungsdienstleister für die Authentifizierung und Kommunikation mit seinen Zahlungsdienstnutzern verwendet.

(5) Die EBA arbeitet Entwürfe technischer Regulierungsstandards aus, in denen Folgendes festgelegt wird:

a) die Anforderungen an vierteljährliche Statistiken über die Verfügbarkeit und Leistung der Schnittstellen gemäß Artikel 36 Absatz 5 und an deren Veröffentlichung;

b) die Standards zur Festlegung einer optimalen Wiederherstellungsdauer im Falle einer ungeplanten Nichtverfügbarkeit einer dedizierten Schnittstelle gemäß Absatz 3 auf der Grundlage des Schweregrads des Vorfalls.

Für die Zwecke von Unterabsatz 1 Buchstabe b werden bei einer Bewertung des Schweregrads unter anderem die Anzahl der betroffenen Kunden von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern und die Arten der bei diesen Dienstleistern betroffenen Funktionen berücksichtigt.

Die EBA übermittelt der Kommission die in Unterabsatz 1 genannten Entwürfe technischer Regulierungsstandards bis zum … [neun Monate nach dem Tag des Inkrafttretens dieser Verordnung].

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

Artikel 40

Ausnahme von der Pflicht zur Bereitstellung einer dedizierten Datenzugangsschnittstelle

(1) Abweichend von Artikel 36 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

a) als Schnittstelle für den sicheren Datenaustausch eine der Schnittstellen anzubieten, die der kontoführende Zahlungsdienstleister für die Authentifizierung und Kommunikation mit seinen Zahlungsdienstnutzern verwendet, sofern diese Schnittstelle gleichwertige Funktionen zur Unterstützung des Zugangs von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern bietet und weithin anerkannte und interoperable Standards verwendet, oder,

b) wenn dies gerechtfertigt ist, keine Schnittstelle für den sicheren Datenaustausch anzubieten.

Soweit angemessen können die Mitgliedstaaten nationale Zentralbanken, die gemäß Artikel 2 Absatz 1 Buchstabe d nicht in ihrer Eigenschaft als Währungsbehörden oder andere Behörden handeln, von der Pflicht, über eine dedizierte Schnittstelle zu verfügen, befreien.

(2) Die EBA arbeitet Entwürfe technischer Regulierungsstandards aus, in denen die Kriterien festgelegt werden, auf deren Grundlage es gemäß Absatz 1 gerechtfertigt ist, dass ein kontoführender Zahlungsdienstleister keine Schnittstelle für einen sicheren Datenaustausch anbietet. Bei der Festlegung dieser Kriterien berücksichtigt die EBA unter anderem die Größe, den Jahresumsatz und das Zahlungsvolumen des kontoführenden Zahlungsdienstleisters.

Die EBA übermittelt der Kommission die in Unterabsatz 1 genannten Entwürfe technischer Regulierungsstandards bis zum … [zwölf Monate nach dem Tag des Inkrafttretens dieser Verordnung].

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

ABSCHNITT 3

RECHTE UND PFLICHTEN KONTOFÜHRENDER ZAHLUNGSDIENSTLEISTER

Artikel 41
Pflichten kontoführender Zahlungsdienstleister in Bezug auf Zahlungsauslösedienste

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

a) er kommuniziert auf sichere Weise mit Zahlungsauslösedienstleistern;

b) unmittelbar nach Eingang des Zahlungsauftrags sowie, auf Verlangen eines Zahlungsauslösedienstleisters, auf kontinuierlicher Basis, stellt er diesem alle Informationen über die Auslösung des Zahlungsvorgangs sowie alle Informationen, über die er selbst hinsichtlich der Ausführung des Zahlungsvorgangs verfügt, zur Verfügung;

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 von Unterabsatz 1 Buchstabe b gewährleistet der kontoführende Zahlungsdienstleister für den Fall, dass ein Teil oder alle der dort genannten Informationen unmittelbar nach Eingang des Zahlungsauftrags nicht verfügbar sind, dass dem Zahlungsauslösedienstleister sämtliche Informationen über die Ausführung des Zahlungsvorgangs, einschließlich der aktualisierten Informationen zum Zahlungsstatus, unmittelbar zur Verfügung gestellt werden, nachdem sie dem kontoführenden Zahlungsdienstleister zur Verfügung stehen.

Artikel 42

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 Datenanfragen, die über die Dienste eines Kontoinformationsdienstleisters übermittelt werden, als wären die Daten durch den Zahlungsdienstnutzer über die Schnittstelle angefragt worden, die der kontoführende Zahlungsdienstleister seinen Zahlungsdienstnutzern zur Verfügung stellt, um ihnen direkten Zugriff auf ihr Zahlungskonto zu ermöglichen.

(2) Der kontoführende Zahlungsdienstleister gestattet Kontoinformationsdienstleistern den Zugriff auf Informationen von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen, die von diesem kontoführenden Zahlungsdienstleister zwecks Bereitstellung von Kontoinformationsdiensten gespeichert werden, unabhängig davon, ob der Zahlungsdienstnutzer diese Informationen aktiv anfragt oder nicht.

(3) Beabsichtigt der Kontoinformationsdienstleister, zu einem Zeitpunkt auf Informationen gemäß Absatz 2 zuzugreifen, zu dem der Zahlungsdienstnutzer diese Informationen nicht aktiv anfragt, so stellt er sicher, dass der Zahlungsdienstnutzer von dieser Absicht ordnungsgemäß Kenntnis hat, bevor er diese Funktion nutzt.

Artikel 43

Beschränkung des Zugangs zu Zahlungskonten für Kontoinformationsdienstleister 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 Zugriff auf das Zahlungskonto durch diesen Kontoinformationsdienstleister oder diesen Zahlungsauslösedienstleister in Zusammenhang stehen, der als nicht autorisiert – gemäß Artikel 50 Absatz 4 – oder als betrügerisch gilt, was auch die nicht autorisierte oder betrügerische Auslösung eines Zahlungsvorgangs einschließt. In solchen Fällen informiert der kontoführende Zahlungsdienstleister den Zahlungsdienstnutzer darüber, dass der Zugang zum Zahlungskonto verweigert wird, sowie über die Gründe für diese Verweigerung. Diese Information ist dem Zahlungsdienstnutzer möglichst vor Verweigerung des Zugangs, spätestens jedoch unmittelbar danach mitzuteilen, es sei denn, die Bereitstellung dieser Information würde die Sicherheit aus objektiv gerechtfertigten Gründen beeinträchtigen oder ist nach sonstigem einschlägigen Recht der Union oder der Mitgliedstaaten verboten.

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

Artikel 44

Datenzugangsmanagement durch die Zahlungsdienstnutzer

(1) Der kontoführende Zahlungsdienstleister stellt dem Zahlungsdienstnutzer ein in seine Benutzeroberfläche integriertes Dashboard für die Überwachung und das Management der Einwilligungen 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 jederzeit und in einem leicht verständlichen Format einen Überblick über jede aktive Einwilligung geben, die für die Zwecke von Kontoinformationsdiensten 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 Einwilligung,

iv) die Geltungsdauer der Einwilligung, einschließlich des Datums, zu dem der Zahlungsdienstnutzer diese Einwilligung erteilt hat,

v) die Kategorien der weitergegebenen Daten,

vi) das jeweilige Datum, an dem ein Zugriff auf die Daten erfolgte,

b) es dem Zahlungsdienstnutzer ermöglichen, allen Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern oder einem bestimmten Kontoinformationsdienstleister oder Zahlungsauslösedienstleister jederzeit kostenlos das Recht auf Datenzugriff zu entziehen,

c) es dem Zahlungsdienstnutzer für 48 Stunden nach dem Widerruf einer Einwilligung ermöglichen, den entzogenen Datenzugriff wiederherzustellen,

d) eine sich über zwei Jahre erstreckende Aufstellung der widerrufenen oder abgelaufenen Einwilligungen in Bezug auf den Datenzugriff umfassen.

(3) Beschließt ein Zahlungsdienstnutzer, das Recht auf Datenzugriff gemäß Absatz 2 Buchstabe b zu entziehen, so muss der betreffende Zahlungsauslösedienstleister oder Kontoinformationsdienstleister

a) den Zugriff auf die Daten und deren Nutzung einstellen; und

b) die Daten, die er infolge der vom Zahlungsdienstnutzer erteilten Einwilligung zum Datenzugriff erhalten hat, unverzüglich, jedoch nicht vor Ablauf von 48 Stunden nach Widerruf einer Einwilligung, zu löschen.

Abweichend von Unterabsatz 1 Buchstabe b kann der betreffende Zahlungsdienstleister die Daten aufbewahren, falls der Zahlungsdienstnutzer dies ausdrücklich wünscht.

(4) Der kontoführende Zahlungsdienstleister gewährleistet, dass das Dashboard in seiner Benutzeroberfläche leicht auffindbar ist und dass die im Dashboard enthaltenen Informationen klar, neutral, richtig und für den Zahlungsdienstnutzer leicht verständlich sind und keine abschreckenden oder entmutigenden Formulierungen enthalten, die den Zahlungsdienstnutzer davon abhalten könnten, die Dienste eines Zahlungsauslösedienstleisters oder Kontoinformationsdienstleisters in Anspruch zu nehmen.

Der kontoführende Zahlungsdienstleister darf,

a) den Zahlungsdienstnutzer nicht dazu veranlassen, eine Einwilligung, die für die Zwecke von Kontoinformationsdiensten oder Zahlungsauslösediensten erteilt wurde, zu widerrufen,

b) sein Dashboard nicht in einer Weise gestalten, organisieren oder betreiben, dass der Zahlungsdienstnutzer getäuscht, manipuliert oder dazu angehalten wird, Einwilligungen zu erteilen, die nicht im besten Interesse des Nutzers sind, oder dass die Fähigkeit des Nutzers, freie und fundierte Entscheidungen zu treffen, wesentlich verfälscht oder beeinträchtigt wird.

(5) Der Kontoinformationsdienstleister oder Zahlungsauslösedienstleister, dem die Einwilligung erteilt wurde, übermittelt dem kontoführenden Zahlungsdienstleister unverzüglich die in Absatz 2 Buchstabe a genannten Informationen. Der kontoführende Zahlungsdienstleister stellt diese Informationen nur insoweit zur Verfügung, als sie ihm von dem Kontoinformationsdienstleister oder Zahlungsauslösedienstleister, dem die entsprechende Einwilligung erteilt wurde, übermittelt wurden.

(6) Der kontoführende Zahlungsdienstleister und der Kontoinformationsdienstleister oder Zahlungsauslösedienstleister, dem die Einwilligung erteilt wurde, arbeiten zusammen, um dem Zahlungsdienstnutzer über das Dashboard unverzüglich Informationen zur Verfügung zu stellen.

Der kontoführende Zahlungsdienstleister stellt dem Kontoinformationsdienstleister oder dem Zahlungsauslösedienstleister unverzüglich Informationen über alle Änderungen, die der Zahlungsdienstnutzer über das Dashboard an einer Einwilligung vorgenommen hat, einschließlich des Widerrufs einer Einwilligung, zur Verfügung.

Ein Kontoinformationsdienstleister oder ein Zahlungsauslösedienstleister unterrichtet den kontoführenden Zahlungsdienstleister unverzüglich über eine von einem Zahlungsdienstnutzer erteilte neue Einwilligung in Bezug auf ein von diesem kontoführenden Zahlungsdienstleister bereitgestelltes Zahlungskonto; dies umfasst die in Absatz 2 Buchstabe a Ziffern i bis v aufgeführten Informationen.

(7) Der kontoführende Zahlungsdienstleister haftet in keiner Weise dafür, dass der Zahlungsdienstnutzer Handlungen gemäß Absatz 2 Buchstaben b und c vornimmt.

Artikel 45

Unzulässige Hindernisse für den Datenzugriff

(1) Kontoführende Zahlungsdienstleister gewährleisten, dass ihre dedizierten Schnittstellen die Bereitstellung von Zahlungsauslösediensten und Kontoinformationsdiensten nicht behindern.

Ein unzulässiges Hindernis liegt u. a. vor, wenn

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

b) verlangt wird, dass Zahlungsdienstnutzer zur Inanspruchnahme von Kontoinformationsdiensten oder Zahlungsauslösediensten ihren Kundenidentifikator manuell in der Domäne des kontoführenden Zahlungsdienstleisters eingeben,

c) die Überprüfung der Einwilligung, die der Zahlungsdienstnutzer einem Zahlungsauslösedienstleister oder Kontoinformationsdienstleister erteilt hat, verlangt wird,

d) von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern eine zusätzliche Registrierung verlangt wird, damit sie auf das Zahlungskonto des Zahlungsdienstnutzers oder auf die dedizierte Schnittstelle zugreifen können,

e) von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern verlangt wird, dass sie ihre Kontaktdaten vorab beim kontoführenden Zahlungsdienstleister registrieren, es sei denn, dies ist erforderlich, um den Informationsaustausch zwischen kontoführenden Zahlungsdienstleistern und Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern insbesondere bezüglich der Aktualisierung des in Artikel 44 genannten Dashboards zu erleichtern,

f) die Fähigkeit eines Zahlungsdienstnutzers, Zahlungen über einen Zahlungsauslösedienstleister auszulösen, auf solche Zahlungsempfänger beschränkt wird, die auf der Liste der Begünstigten des Zahlers stehen, es sei denn, der Zahlungsdienstnutzer ist nicht in der Lage, diese Zahlungen über die Kundenschnittstelle auszuführen;

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

h) häufiger eine starke Kundenauthentifizierung verlangt wird als der kontoführende Zahlungsdienstleister beim direkten Zugriff der Zahlungsdienstnutzer auf ihre Zahlungskonten oder bei der Auslösung von Zahlungen direkt beim kontoführenden Zahlungsdienstleister verlangt,

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

j) für Kontoinformationen oder Zahlungsauslösungen ein Verlauf im Rahmen eines Ansatzes der Weiterleitung (Redirection) oder der Entkopplung (Decoupled) vorgeschrieben wird, 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 von Zahlungen direkt beim kontoführenden Zahlungsdienstleister angeboten wird, zusätzliche Schritte oder Maßnahmen erfordert,

k) die automatische Weiterleitung eines Nutzers in der Phase der Authentifizierung auf die Website des kontoführenden Zahlungsdienstleisters vorgeschrieben wird, wenn die dedizierte Schnittstelle nicht alle Authentifizierungsverfahren unterstützt, die der kontoführende Zahlungsdienstleister seinem Zahlungsdienstnutzer zur Verfügung stellt;

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

(2) Maßnahmen kontoführender Zahlungsdienstleister, die zur Bekämpfung von Verdachtsfällen auf Betrug gemäß der vorliegenden Verordnung oder zur Einhaltung der Verordnung (EU) 2016/679 erforderlich sind, gelten nicht als Hindernisse für den Datenzugriff, es sei denn, es handelt sich bei diesen Maßnahmen um unzulässige Hindernisse gemäß Absatz 1 Buchstaben a bis l des vorliegenden Artikels.

ABSCHNITT 4

RECHTE UND PFLICHTEN VON KONTOINFORMATIONSDIENSTLEISTERN UND ZAHLUNGSAUSLÖSEDIENSTLEISTERN

Artikel 46

Nutzung der Kundenschnittstelle durch Kontoinformationsdienstleister und Zahlungsauslösedienstleister

(1) Kontoinformationsdienstleister und Zahlungsauslösedienstleister dürfen außer unter den in Artikel 40 Absatz 1 genannten Umständen oder in Ausnahmefällen, in denen der Zugriff über eine andere sichere und effiziente Schnittstelle erfolgt, ausschließlich über die in Artikel 36 genannte dedizierte Schnittstelle auf Zahlungskontodaten zugreifen.

(2) Hat ein Zahlungsauslösedienstleister oder ein Kontoinformationsdienstleister lediglich Zugriff über die in Artikel 40 Absatz 1 Buchstabe a genannte Schnittstelle, so ist der Kontoinformationsdienstleister oder der Zahlungsauslösedienstleister dazu verpflichtet,

a) sich stets gegenüber dem kontoführenden Zahlungsdienstleister zu identifizieren,

b) stets Informationen gemäß Artikel 44 Absatz 2 Buchstabe a Ziffern ii bis v bereitzustellen,

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

d) stets die notwendigen Maßnahmen zu 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,

e) stets die Daten zu 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 zu stellen, damit die zuständige Behörde ermitteln kann, ob dieser Abschnitt eingehalten wurde.

Für die Zwecke des Unterabsatzes 1 Buchstabe e werden Protokolle drei Jahre nach ihrer Erstellung gelöscht. Protokolle dürfen auch länger aufbewahrt werden, sofern sie für bereits laufende Überwachungsverfahren benötigt werden.

Artikel 47

Konkrete Pflichten von Zahlungsauslösedienstleistern

(1) Zahlungsauslösedienstleister

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

b) dürfen ihre Dienste nur auf der Grundlage der Einwilligung des Zahlungsdienstnutzers gemäß Artikel 50 erbringen,

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

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

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

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

g) müssen in der Lage sein, die Auslösung eines Zahlungsvorgangs aus sachlich gerechtfertigten Gründen abzulehnen.

(2) Zahlungsauslösedienstleister dürfen

a) unbeschadet des Artikels 46 Absatz 2 Buchstabe e keine sensiblen Zahlungsdaten des Zahlungsdienstnutzers 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 Zahlungsdienstnutzer 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 48

Konkrete Pflichten von Kontoinformationsdienstleistern und sonstige Bestimmungen für Kontoinformationsdienstleister

(1) Der Kontoinformationsdienstleister

a) darf seine Dienste nur mit der Einwilligung des Zahlungsdienstnutzers gemäß Artikel 50 erbringen,

b) muss gewährleisten, dass die personalisierten Sicherheitsmerkmale des Zahlungsdienstnutzers außer für den Nutzer und den Emittenten der personalisierten Sicherheitsmerkmale nicht für andere Parteien 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 über bezeichnete Zahlungskonten und zugehörige Zahlungsvorgänge zugreifen,

e) muss über geeignete und wirksame Mechanismen verfügen, damit der Zugriff auf andere Informationen als die über bezeichnete Zahlungskonten und zugehörige Zahlungsvorgänge gemäß der Einwilligung des Zahlungsdienstnutzers verhindert wird.

(2) Der Kontoinformationsdienstleister darf

a) nicht auf sensible Zahlungsdaten zugreifen, die mit den Zahlungskonten in Verbindung stehen,

b) Daten nicht für andere Zwecke als für die vom Zahlungsdienstnutzer erlaubte Erbringung des Kontoinformationsdienstes verarbeiten.

(3) Die Artikel 4 bis 8, die Artikel 10, 11 und 12, die Artikel 14 bis 19, die Artikel 21 bis 29, die Artikel 51 und 52, die Artikel 54 bis 83 sowie die Artikel 87 und 90 gelten nicht für Kontoinformationsdienstleister.

ABSCHNITT 5

DURCHFÜHRUNG

Artikel 49

Rolle der zuständigen Behörden

(1) Die zuständigen Behörden gewährleisten, dass kontoführende Zahlungsdienstleister ihren Pflichten bezüglich der in Artikel 36 Absatz 1 und Artikel 39 genannten dedizierten Schnittstelle jederzeit nachkommen und dass jedes in Artikel 45 aufgeführte festgestellte unzulässige Hindernis vom betreffenden kontoführenden Zahlungsdienstleister unmittelbar beseitigt wird. Wird – u. a. durch Informationen von Zahlungsauslösedienstleistern oder Kontoinformationsdienstleistern – festgestellt, dass dedizierte Schnittstellen nicht den Anforderungen dieser Verordnung genügen oder unzulässige Hindernisse bestehen, ergreifen die zuständigen Behörden unverzüglich die notwendigen und geeigneten Durchsetzungsmaßnahmen und verhängen angemessene Sanktionen.

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

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

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

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

(6) Die zuständigen Behörden halten auf eigene Initiative für die Zwecke von Absatz 7 gemeinsame Sitzungen mit kontoführenden Zahlungsdienstleistern, Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern ab.

(7) Die zuständigen Behörden bemühen sich nach besten Kräften sicherzustellen, dass mögliche Probleme zwischen kontoführenden Zahlungsdienstleistern, Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern, die sich aus der Nutzung von Schnittstellen für den Datenaustausch und dem Zugang zu solchen Schnittstellen ergeben, rasch und dauerhaft behoben werden.

(8) Kontoführende Zahlungsdienstleister stellen den zuständigen Behörden Daten über den Zugriff von Kontoinformationsdienstleistern 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 deren Tätigkeiten verlangen.

Die EBA koordiniert die in Unterabsatz 1 des vorliegenden Absatzes genannte Überwachungstätigkeit der zuständigen Behörden gemäß ihren Befugnissen nach Artikel 29 Absatz 1 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 Kontoinformationsdienste und Zahlungsauslösedienste in der Union. Diese Berichte können gegebenenfalls Empfehlungen enthalten.

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

Die EBA legt der Kommission die in Unterabsatz 1 genannten Entwürfe technischer Regulierungsstandards bis zum … [18 Monate nach dem Tag des Inkrafttretens dieser Verordnung] vor.

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

Kapitel 4
Autorisierung von Zahlungsvorgängen

Artikel 50

Autorisierung

(1) Ein Zahlungsvorgang oder eine Serie von Zahlungsvorgängen ist nur dann autorisiert, wenn der Zahler seine Einwilligung zur Ausführung des Zahlungsvorgangs erteilt hat. Der Zahler kann einen Zahlungsvorgang entweder vor oder – sofern zwischen dem Zahler und dem Zahlungsdienstleister so vereinbart – nach der Ausführung autorisieren.

(2) Ein Zahlungsvorgang gilt als nicht autorisiert, wenn er von einem Dritten ausgelöst oder geändert wurde, der ohne Einwilligung des Zahlers handelt, auch dann, wenn die auf betrügerische Weise erlangten personalisierten Sicherheitsmerkmale des Zahlers genutzt wurden.

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

(4) Liegt keine Einwilligung vor, gilt der Zahlungsvorgang oder der Zugriff eines Kontoinformationsdienstleisters oder eines Zahlungsauslösedienstleisters auf ein Zahlungskonto als nicht autorisiert.

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

(6) Die in den Absätzen 1 und 3 genannte Einwilligung wird in der zwischen dem Zahlungsdienstnutzer und dem betreffenden Zahlungsdienstleister vereinbarten Form erteilt. Die Einwilligung zur Ausführung eines Zahlungsvorgangs kann auch über den Zahlungsempfänger oder den Zahlungsauslösedienstleister erteilt werden.

Das Verfahren für die Erteilung der Einwilligung wird zwischen dem Zahlungsdienstnutzer und dem betreffenden Zahlungsdienstleister vereinbart.

(7) Der Zahler kann die Einwilligung, einen Zahlungsvorgang auszuführen oder für die Zwecke von Zahlungsauslösediensten auf ein Zahlungskonto zuzugreifen, jederzeit widerrufen, jedoch nur bis zu dem Zeitpunkt, an dem nach Artikel 69 die Unwiderruflichkeit eintritt. Der Zahlungsdienstnutzer kann die Einwilligung, für die Zwecke von Kontoinformationsdiensten auf ein Zahlungskonto zuzugreifen, jederzeit widerrufen. Der Zahler kann auch die Einwilligung, eine Serie von Zahlungsvorgängen auszuführen, widerrufen; in diesem Fall gilt jeder nachfolgende Zahlungsvorgang in dieser Serie als nicht autorisiert.

Artikel 51

Unstimmigkeiten zwischen Namen
und Kundenidentifikator des Zahlungsempfängers bei Überweisungen

Bei Überweisungen kommen die Zahlungsdienstleister Artikel 5c Absätze 1 bis 7 und Artikel 5b Absatz 2 der Verordnung (EU) Nr. 260/2012 nach, und diese Artikel sind auf alle Überweisungen, einschließlich derer, die nicht in den Anwendungsbereich der Verordnung (EU) Nr. 260/2012 fallen, entsprechend anwendbar.

Wird das Zahlungskonto des Zahlungsempfängers nicht durch den Identifikator für Zahlungskonten nach Nummer 1 Buchstabe a des Anhangs der Verordnung (EU) Nr. 260/2012 identifiziert, so gelten für die Zwecke des Unterabsatzes 1 des vorliegenden Absatzes die Bezugnahmen auf den Identifikator des Zahlungskontos in Artikel 5c jener Verordnung als Bezugnahmen auf den Kundenidentifikator, der zur eindeutigen Identifizierung des Zahlungskontos des Zahlungsempfängers verwendet wird.

Artikel 52

Begrenzung und Sperrung der Nutzung des Zahlungsinstruments

(1) Der Zahlungsdienstleister bietet dem Zahlungsdienstnutzer im Rahmenvertrag die Möglichkeit an, in diesem Vertrag eine Obergrenze für einen Höchstbetrag, der transferiert werden kann, festzulegen, die je nach Zahlungsmittel, einschließlich Überweisungen, und je nach Zahlungsinstrument unterschiedlich sein kann. Eine Obergrenze kann nach dem alleinigen Ermessen des Zahlungsdienstnutzers pro Vorgang oder für einen festgelegten Zeitraum festgelegt werden.

Die Zahlungsdienstleister dürfen die Ausgabenobergrenzen, die im Rahmenvertrag mit ihren Zahlungsdienstnutzern festgelegt wurden, nicht einseitig ändern.

Der Zahlungsdienstnutzer hat die Möglichkeit, die im Rahmenvertrag festgelegten Ausgabenobergrenzen zu ändern. Die Zahlungsdienstleister stellen sicher, dass der Zahler die festgelegten Ausgabenobergrenzen vor der Erteilung eines Zahlungsauftrags ändern kann.

(2) Erhöht der Zahlungsdienstnutzer die Ausgabenobergrenzen aus der Ferne, so setzen die Zahlungsdienstleister eine Wartefrist von vier Stunden bis zum Wirksamwerden dieser Erhöhung fest. Die Zahlungsdienstnutzer haben das Recht, diese Wartefrist anzupassen oder nicht anzuwenden. Ist eine Wartefrist festgesetzt, so gilt sie, bis eine spätere Anpassung oder Nichtanwendung wirksam wird.

Die Zahlungsdienstleister benachrichtigen die Zahlungsdienstnutzer unmittelbar in einer vereinbarten Weise, wenn eine Änderung einer Ausgabenobergrenze beantragt wird, dass die in Unterabsatz 1 genannte Wartefrist abgelaufen ist oder dass die in Unterabsatz 1 genannte Anpassung oder Nichtanwendung wirksam geworden ist.

(3) Übersteigt der Zahlungsauftrag eines Zahlungsdienstnutzers den Höchstbetrag oder führt der Zahlungsauftrag zu einer Überschreitung des Höchstbetrags, so führt der Zahlungsdienstleister des Zahlers den Zahlungsauftrag nicht aus und unterrichtet den Zahlungsdienstnutzer über die Gründe dafür sowie darüber, wie der Höchstbetrag geändert werden kann.

(4) Der Zahlungsdienstleister kann das Zahlungsinstrument sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit des Zahlungsinstruments dies rechtfertigen, der Verdacht einer nicht autorisierten oder betrügerischen Nutzung des Zahlungsinstruments besteht oder im Fall eines Zahlungsinstruments mit einer Kreditlinie ein beträchtlich erhöhtes Risiko besteht, dass der Zahler seiner Zahlungsverpflichtung nicht nachkommen könnte.

(5) Wird ein Zahlungsinstrument gemäß Absatz 4 gesperrt, so unterrichtet der Zahlungsdienstleister den Zahler möglichst vor, spätestens jedoch unmittelbar nach der Sperrung des Zahlungsinstruments in einer vereinbarten Weise von der Sperrung und den spezifischen Gründen hierfür, es sei denn, dies würde gegen sonstiges einschlägiges Recht der Union oder der Mitgliedstaaten verstoßen. Der Zahlungsdienstleister des Zahlers prüft unverzüglich, spätestens jedoch innerhalb von zwei Geschäftstagen, ob die Gründe für die Sperrung des Zahlungsinstruments noch gerechtfertigt sind.

(6) 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.

(7) Bietet der Zahlungsdienstleister dem Zahlungsdienstnutzer die Möglichkeit, Zahlungsvorgänge über eine mobile Anwendung auszulösen oder seine Einwilligung zu Zahlungsvorgängen über die mobile Anwendung zu erteilen, so verlangt der Zahlungsdienstleister eine starke Kundenauthentifizierung und die Nutzung verschiedener Kommunikationskanäle zur Aktivierung dieser mobilen Anwendung.

(8) Aktiviert der Zahlungsdienstnutzer die mobile Anwendung aus der Ferne, so setzt der Zahlungsdienstleister eine Wartefrist von vier Stunden bis zum Wirksamwerden dieser Aktivierung fest. Der Zahlungsdienstnutzer hat das Recht, diese Wartefrist anzupassen oder nicht anzuwenden. Ist eine Wartefrist festgesetzt, so gilt sie, bis eine spätere Anpassung oder Nichtanwendung wirksam wird.

(9) Der Zahlungsdienstleister benachrichtigt den Zahlungsdienstnutzer unmittelbar in einer vereinbarten Weise und über verschiedene Kommunikationskanäle über die Aktivierung einer mobilen Anwendung. Die Benachrichtigung enthält Anweisungen für den Fall, dass der Zahlungsdienstnutzer die mobile Anwendung nicht selbst installiert hat.

Das Verfahren für die Benachrichtigung gemäß diesem Absatz wird zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister vereinbart.

(10) Benachrichtigt der Zahlungsdienstnutzer den Zahlungsdienstleister gemäß dem in Absatz 9 genannten Verfahren, dass er die mit seinem Zahlungskonto verknüpfte mobile Anwendung nicht aktiviert hat, so stellt der Zahlungsdienstleister unverzüglich sicher, dass es nicht möglich ist, über die mobile Anwendung auf das Zahlungskonto des Zahlungsdienstnutzers zuzugreifen oder Zahlungsvorgänge auszulösen oder die Einwilligung zu Zahlungsvorgängen zu erteilen.

(11) Die Absätze 7, 8 und 9 gelten weder für die anfängliche Begründung der Kundenbeziehung zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister durch die Nutzung einer mobilen Anwendung noch für die Aktivierung einer mobilen Anwendung auf einem Gerät des Zahlungsdienstnutzers durch den Zahlungsdienstleister in dessen stationären Verkaufsstellen.

(12) Dieser Artikel gilt für alle Überweisungen, einschließlich Überweisungen in Euro, ungeachtet der Verordnung (EU) Nr. 260/2012.

Artikel 53

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 oder der einschlägigen personalisierten Sicherheitsmerkmale unverzüglich an, nachdem er davon Kenntnis erhalten hat.

Für die Zwecke von Unterabsatz 1 Buchstabe a trifft der Zahlungsdienstnutzer unmittelbar nach Erhalt eines Zahlungsinstruments alle zumutbaren Vorkehrungen, um seine personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen.

Artikel 54

Pflichten des Zahlungsdienstleisters in Bezug auf Zahlungsinstrumente

(1) Der Zahlungsdienstleister, der ein Zahlungsinstrument ausgibt,

a) muss unbeschadet der Pflichten des Zahlungsdienstnutzers nach Artikel 53 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 und kostenlos die Möglichkeit hat, eine Anzeige gemäß Artikel 53 Absatz 1 Buchstabe b vorzunehmen oder die Aufhebung der Sperrung des Zahlungsinstruments gemäß Artikel 52 Absatz 6 zu verlangen, und dass für diese Zwecke zumindest während der Geschäftszeiten eine menschliche Unterstützung in einer der Amtssprachen des Mitgliedstaats, in dem der Zahlungsdienst erbracht wird, kostenlos zur Verfügung steht;

d) muss dem Zahlungsdienstnutzer die Möglichkeit bieten, eine Anzeige gemäß Artikel 53 Absatz 1 Buchstabe b kostenlos vorzunehmen, und darf nur etwaige direkt mit dem Zahlungsinstrument verbundene Ersatzkosten in Rechnung stellen;

e) muss jede Nutzung des Zahlungsinstruments verhindern, sobald eine Anzeige nach Artikel 53 Absatz 1 Buchstabe b erfolgt ist;

f) muss sicherstellen, dass dem Zahlungsdienstnutzer sensible Zahlungsdaten über sichere Kanäle übermittelt werden.

Für die Zwecke von Unterabsatz 1 Buchstabe c stellt der Zahlungsdienstleister dem Zahlungsdienstnutzer auf Verlangen bis zu 18 Monate nach der Anzeige Mittel zur Verfügung, mit denen dieser 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 55

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, 60 und 87 den betreffenden Zahlungsvorgang, der einen Anspruch, einschließlich eines Anspruchs nach Artikel 79, begründet, unverzüglich, nachdem er Kenntnis von dem Vorgang erhalten hat, in jedem Fall jedoch spätestens 18 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 mitgeteilt oder nicht zugänglich gemacht hat.

(2) Ist ein Zahlungsauslösedienstleister beteiligt, erwirkt der Zahlungsdienstnutzer unbeschadet des Artikels 57 Absatz 4 und des Artikels 79 Absatz 1 eine Korrektur von dem kontoführenden Zahlungsdienstleister gemäß Absatz 1.

Artikel 56

Nachweis der Autorisierung und 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, korrekt aufgezeichnet, verbucht 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 Tatsache, dass der Zahlungsvorgang authentifiziert – auch gegebenenfalls über eine starke Kundenauthentifizierung –, korrekt aufgezeichnet, verbucht und nicht durch eine technische Störung oder einen anderen Mangel des erbrachten Dienstes beeinträchtigt wurde, für sich genommen nicht notwendigerweise als Beweis dafür aus, dass der Zahler entweder den Zahlungsvorgang autorisiert hat oder betrügerisch gehandelt oder eine oder mehrere seiner Pflichten nach Artikel 53 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.

(3) Bevor der Zahlungsdienstleister zu dem Schluss kommt, dass ein Zahlungsdienstnutzer den Vorgang autorisiert, betrügerisch gehandelt oder eine oder mehrere seiner Pflichten nach Artikel 53 vorsätzlich oder grob fahrlässig verletzt hat, fordert er für die Zwecke der Absätze 1 und 2 des vorliegenden Artikels den Zahlungsdienstnutzer auf, Informationen über die Ereignisse, die zu dem Zahlungsvorgang geführt haben, bereitzustellen, und bezieht diese Informationen in seine Bewertung ein. Stellt der Zahlungsdienstnutzer diese Informationen nicht bereit, so darf dies für sich genommen den Zahlungsdienstleister nicht zu dem Schluss veranlassen, dass der Zahlungsdienstnutzer den Vorgang autorisiert, betrügerisch gehandelt oder eine oder mehrere seiner Pflichten nach Artikel 53 vorsätzlich oder grob fahrlässig verletzt hat. Von dem Zahlungsdienstnutzer darf nicht erwartet werden, dass er Informationen bereitstellt, die über die Informationen hinausgehen, von denen vernünftigerweise erwartet werden kann, dass dieser Zahlungsdienstnutzer über sie verfügt.

Artikel 57

Haftung des Zahlungsdienstleisters für nicht autorisierte Zahlungsvorgänge

(1) Unbeschadet des Artikels 55 erstattet der Zahlungsdienstleister des Zahlers im Falle eines nicht autorisierten Zahlungsvorgangs dem Zahler den Betrag des nicht autorisierten Zahlungsvorgangs unmittelbar, in jedem Fall jedoch spätestens bis zum Ende des folgenden Geschäftstags, nachdem er Kenntnis von dem nicht autorisierten Vorgang erhalten hat oder dieser ihm angezeigt wurde, es sei denn, der Zahlungsdienstleister des Zahlers hat objektiv gerechtfertigte Gründe für den Verdacht, dass der Zahler eine oder mehrere seiner Pflichten nach Artikel 53 vorsätzlich oder grob fahrlässig verletzt hat, und teilt dem Zahler diese Gründe schriftlich mit, oder er hat objektiv gerechtfertigte Gründe für den Verdacht, das der Zahler betrügerisch gehandelt hat.

(2) Hatte der Zahlungsdienstleister des Zahlers objektiv gerechtfertigte Gründe für den Verdacht, dass der Zahler betrügerisch gehandelt oder eine oder mehrere seiner Pflichten nach Artikel 53 vorsätzlich oder grob fahrlässig verletzt hat, so trifft der Zahlungsdienstleister des Zahlers innerhalb von 15 Geschäftstagen, nachdem er Kenntnis von dem Vorgang erhalten hat oder dieser ihm angezeigt wurde, eine der folgenden beiden Maßnahmen:

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 nicht betrügerisch gehandelt oder eine oder mehrere seiner Pflichten nach Artikel 53 nicht vorsätzlich oder grob fahrlässig verletzt hat;

b) er teilt dem Zahler eine Begründung mit, warum er die Erstattung ablehnt, und nennt die Stellen, an die sich der Zahler gemäß den Artikeln 100, 101, 103, 104 und 105 wenden kann, falls der Zahler die angegebenen Gründe nicht akzeptiert, und teilt für den Fall, dass der Zahlungsdienstleister zu dem Schluss kommt, dass der Zahler betrügerisch gehandelt hat, der zuständigen nationalen Behörde die Gründe für diesen Schluss mit.

Für die Zwecke von Unterabsatz 1 Buchstabe b veröffentlichen die Mitgliedstaaten den Namen der zuständigen nationalen Behörde, der die Begründung mitzuteilen ist.

(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 das Wertstellungdatum der Gutschrift auf dem Zahlungskonto des Zahlers nicht später ist als das 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 unmittelbar, 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) Haftet der Zahlungsauslösedienstleister für den nicht autorisierten Zahlungsvorgang, so entschädigt der Zahlungsauslösedienstleister den kontoführenden Zahlungsdienstleister auf dessen Verlangen unmittelbar für die infolge der Erstattung an den Zahler erlittenen Verluste oder gezahlten Beträge, einschließlich des Betrags des nicht autorisierten Zahlungsvorgangs. Im Einklang mit Artikel 56 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) Der Zahler kann für alle weiteren ihm entstandenen finanziellen Verluste nach dem auf den Vertrag zwischen dem Zahler und dem einschlägigen Zahlungsdienstleister anwendbaren Recht entschädigt werden.

Artikel 58

Haftung des Zahlungsdienstleisters für fehlerhafte Anwendung der Abgleichdienstleistung

Kommt ein Zahlungsdienstleister Artikel 51 nicht nach und führt dieses Versäumnis zu einem fehlerhaft ausgeführten Zahlungsvorgang, so erstattet der Zahlungsdienstleister des Zahlers dem Zahler unverzüglich den überwiesenen Betrag und bringt das belastete Zahlungskonto gegebenenfalls wieder auf den Stand, auf dem es sich ohne den ausgeführten Vorgang befunden hätte.

Kommt es zu dem Versäumnis, weil der Zahlungsdienstleister des Zahlungsempfängers oder der Zahlungsauslösedienstleister Artikel 51 nicht nachgekommen ist, so entschädigt der Zahlungsdienstleister des Zahlungsempfängers oder gegebenenfalls der Zahlungsauslösedienstleister den Zahlungsdienstleister des Zahlers für den finanziellen Schaden, der dem Zahlungsdienstleister des Zahlers durch dieses Versäumnis entstanden ist.

Der Zahler kann für alle weiteren ihm entstandenen finanziellen Verluste nach dem auf den Vertrag zwischen dem Zahler und dem einschlägigen Zahlungsdienstleister anwendbaren Recht entschädigt werden.

Artikel 59

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

Technische Dienstleister und Betreiber von Zahlverfahren, die für den Zahlungsempfänger oder für den Zahlungsdienstleister des Zahlungsempfängers bzw. des Zahlers Dienstleistungen erbringen, haften für den direkten finanziellen Schaden, der dem Zahlungsempfänger oder dem Zahlungsdienstleister des Zahlungsempfängers bzw. des Zahlers dadurch entsteht, dass sie im Rahmen ihrer Vertragsbeziehung nicht die Leistungen erbringen, die erforderlich sind, um die Anwendung einer starken Kundenauthentifizierung zu ermöglichen, wobei die Haftung in angemessenem Verhältnis zu dem Versäumnis stehen muss und den Betrag des betreffenden Vorgangs nicht übersteigen darf.

Artikel 60

Haftung des Zahlungsdienstleisters für Identitätsbetrug

(1) Die Zahlungsdienstleister verfügen über angemessene Präventionsmaßnahmen und robuste technische Schutzvorkehrungen, um zu verhindern, dass Betrüger ihre Kommunikationskanäle nachbilden und missbrauchen, um Zahlungsdienstnutzer irrezuführen und dadurch zu betrügerischen Vorgängen zu veranlassen.

(2) Wurde ein Zahlungsdienstnutzer, bei dem es sich um einen Verbraucher handelt, von einem Dritten manipuliert, der sich unter Verwendung von Kommunikationskanälen, die dem Zahlungsdienstleister des Verbrauchers zugeordnet werden, als der Zahlungsdienstleister des Verbrauchers ausgegeben hat, und hatte diese Manipulation anschließend betrügerische autorisierte Zahlungsvorgänge zur Folge, so erstattet der Zahlungsdienstleister dem Verbraucher den vollen Betrag des betrügerischen autorisierten Zahlungsvorgangs, sofern der Verbraucher den Betrug unverzüglich, nachdem er davon Kenntnis erhalten hat, seinem Zahlungsdienstleister angezeigt und polizeilich gemeldet hat.

(3) Innerhalb von 15 Geschäftstagen, nachdem er die Anzeige gemäß Absatz 2 und den Polizeibericht von dem Verbraucher erhalten hat, unternimmt der Zahlungsdienstleister eine der folgenden beiden Maßnahmen:

a) er erstattet dem Verbraucher den Betrag des betrügerischen autorisierten Zahlungsvorgangs;

b) hat der Zahlungsdienstleister objektiv gerechtfertigte Gründe für den Verdacht, dass der Verbraucher betrügerisch oder grob fahrlässig gehandelt hat, teilt er dem Verbraucher die Gründe mit, aus denen er die Erstattung ablehnt, und nennt die Stellen, an die sich der Verbraucher gemäß den Artikeln 100, 101, 103, 104 und 105 wenden kann, falls der Verbraucher die angegebenen Gründe nicht akzeptiert, und wenn der Zahlungsdienstleister zu dem Schluss kommt, dass der Verbraucher betrügerisch gehandelt hat, teilt er der in Artikel 57 Absatz 2 Unterabsatz 1 Buchstabe b genannten zuständigen nationalen Behörde die Gründe für diesen Schluss mit.

(4) Absatz 2 findet keine Anwendung, wenn der Verbraucher betrügerisch oder grob fahrlässig gehandelt hat.

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

Bevor der Zahlungsdienstleister zu dem Schluss kommt, dass der Verbraucher betrügerisch oder grob fahrlässig gehandelt hat, fordert er den Verbraucher auf, Informationen über die Ereignisse, die zu dem Zahlungsvorgang geführt haben, bereitzustellen, und berücksichtigt diese Informationen in seiner Bewertung. Stellt der Verbraucher diese Informationen nicht bereit, so darf dies für sich genommen den Zahlungsdienstleister nicht zu dem Schluss veranlassen, dass der Verbraucher betrügerisch oder grob fahrlässig gehandelt hat. Von dem Verbraucher darf nicht erwartet werden, dass er Informationen bereitstellt, die über die Informationen hinausgehen, von denen vernünftigerweise erwartet werden kann, dass dieser Verbraucher über sie verfügt.

Artikel 61

Sektorübergreifende Zusammenarbeit zum Zwecke der Betrugsprävention und -aufdeckung

(1) Geht der Zahlungsbetrug auf die Veröffentlichung betrügerischer Inhalte im Internet zurück, unterrichten die Zahlungsdienstleister die Hostingdiensteanbieter unverzüglich nach dem in Artikel 16 oder gegebenenfalls in Artikel 22 der Verordnung (EU) 2022/2065 festgelegten Verfahren.

(2) Soweit dies zur Prävention und zur Aufdeckung potenziell betrügerischer Zahlungsvorgänge, einschließlich Vorgängen unter Beteiligung von Zahlungsauslösediensten, erforderlich ist, können – wenn es objektiv gerechtfertigte Gründe für den Verdacht auf betrügerisches Verhalten eines Nutzers ihrer Dienste gibt – Daten ausgetauscht werden

a) zwischen Zahlungsdienstleistern und Hostingdiensteanbietern,

b) zwischen Zahlungsdienstleistern und Anbietern interpersoneller Kommunikationsdienste.

(3) Für die Zwecke des Absatzes 2 und unbeschadet der Richtlinie (EU) 2022/2555, der Richtlinie 2002/58/EG oder des Artikels 101 der vorliegenden Verordnung richten die Anbieter interpersoneller Kommunikationsdienste und die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen spezielle Kommunikationskanäle mit den Zahlungsdienstleistern ein oder beteiligen sich an einem System für wirksame Kommunikation oder an einem Mechanismus für den Informationsaustausch, um einen schnelleren und wirksameren Austausch im Einklang mit der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG zu ermöglichen.

(4) Die Anbieter interpersoneller Kommunikationsdienste und die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen verfügen über alle erforderlichen Aufklärungsmaßnahmen, einschließlich der Warnung der Nutzer ihrer Dienste mithilfe aller geeigneten Mittel und Medien, wenn neue Formen von Online-Betrug aufkommen, wobei sie den Bedürfnissen der schutzbedürftigsten Gruppen von Empfängern ihrer Dienste Rechnung tragen.

Für die Zwecke von Unterabsatz 1 dieses Absatzes geben die Anbieter interpersoneller Kommunikationsdienste den Nutzern ihrer Dienste klare Hinweise darauf,

a) wie sie Betrugsversuche erkennen können,

b) welche Maßnahmen und Vorkehrungen zu ergreifen sind, um keinen betrügerischen Aktivitäten zum Opfer zu fallen, und

c) nach welchem Verfahren sie betrügerische Aktivitäten melden können.

Für die Zwecke von Unterabsatz 1 dieses Absatzes geben die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen den Nutzern ihrer Dienste klare Hinweise darauf,

a) wie sie Betrugsversuche erkennen können,

b) welche Maßnahmen und Vorkehrungen zu ergreifen sind, um keinen betrügerischen Aktivitäten zum Opfer zu fallen, und

c) nach welchem Verfahren sie betrügerische Aktivitäten für die Zwecke der Einhaltung von Artikel 16 der Verordnung (EU) 2022/2065 melden können.

(5) Die Kommission und das Europäische Gremium für digitale Dienste fördern und erleichtern die Ausarbeitung eines freiwilligen Verhaltenskodex auf Unionsebene, um unter den in Artikel 45 der Verordnung (EU) 2022/2065 festgelegten Bedingungen die Prävention zu fördern, die Sicherheit zu erhöhen und Zahlungs- und Finanzbetrug zu bekämpfen.

(6) Unbeschadet der Richtlinie (EU) 2022/2555 treffen Anbieter interpersoneller Kommunikationsdienste angemessene organisatorische und technische Maßnahmen, um die Nutzung ihrer Dienste zum Zwecke des Identitätsbetrugs, auch durch Manipulation der Rufnummernanzeige oder der E-Mail-Adressen, aufzudecken und zu verhindern, wenn diese Nutzung darauf abzielt, Zahlungsdienstnutzer zu einer Zahlung oder zu einer Handlung zu veranlassen, die die Sicherheit des Zahlungskontos beeinträchtigen würde. Diese Maßnahmen müssen im Einklang mit dem geltenden Unionsrecht im Bereich des Datenschutzes, insbesondere der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG, stehen.

Artikel 62

Werbung für regulierte Finanzdienstleistungen auf sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen

(1) Für die Zwecke dieses Artikels bezeichnet der Ausdruck „regulierte Finanzdienstleistung“ jede Dienstleistung mit Banken-, Kredit-, Versicherungs-, Altersvorsorge-, Zahlungs- oder Investitionscharakter, einschließlich Kryptowerten und Crowdfunding, für die nach dem Unionsrecht die Zulassung von oder Registrierung bei einer zuständigen Behörde erforderlich ist.

(2) Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen verlangen von jedem Werbetreibenden für eine regulierte Finanzdienstleistung eine Zulassungsnummer, eine RegistrierungsNummer oder andere Informationen, die bescheinigt bzw. bescheinigen, dass dieser Werbetreibende ein Anbieter regulierter Finanzdienstleistungen ist, der für die Erbringung der beworbenen regulierten Finanzdienstleistung in einem Mitgliedstaat oder auf Unionsebene zugelassen oder registriert ist oder im Namen eines solchen Anbieters handelt.

(3) Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen bemühen sich, nach Erhalt der in Absatz 2 des vorliegenden Artikels genannten Informationen und bevor sie dem betreffenden Werbetreibenden die Nutzung ihres Dienstes zum Zwecke der Werbung für diese regulierten Finanzdienstleistungen gestatten, nach besten Kräften darum, unter anderem mittels der gemäß der Richtlinie (EU) 2026/…[+] oder anderen einschlägigen Rechtsvorschriften der Union zur Verfügung gestellten Register zugelassener oder registrierter Anbieter regulierter Finanzdienstleistungen zu bewerten, ob diese Informationen, für deren Richtigkeit die Werbetreibenden für die Zwecke dieser Verordnung allein verantwortlich sind, zuverlässig und vollständig sind, sofern die Bewertung in verhältnismäßiger Weise mithilfe automatisierter Instrumente durchgeführt werden kann.

(4) Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen, die die in Absatz 2 genannten Informationen nicht erhalten haben, verweigern dem Werbetreibenden regulierter Finanzdienstleistungen die Nutzung ihrer Dienste zum Zwecke der Werbung für diese regulierten Finanzdienstleistungen.

(5) Handelt es sich bei dem Gegenstand einer Werbung um eine regulierte Finanzdienstleistung, so nehmen Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen für die Zwecke der Einhaltung von Artikel 39 Absatz 2 Buchstaben a, b und c der Verordnung (EU) 2022/2065 in ihre Werbearchive Informationen darüber auf, dass es sich bei dem Gegenstand der Werbung um eine regulierte Finanzdienstleistung handelt und ob der Werbetreibende im Namen eines Anbieters regulierter Finanzdienstleistungen handelt.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

Artikel 63

Haftung des Zahlers für nicht autorisierte Zahlungsvorgänge

(1) Abweichend von Artikel 57 kann der Zahler dazu verpflichtet werden, alle mit nicht autorisierten Zahlungsvorgängen zusammenhängenden Verluste, die infolge des Verlusts, des Diebstahls oder der missbräuchlichen Verwendung eines Zahlungsinstruments oder personalisierter Sicherheitsmerkmale entstehen, bis höchstens 50 EUR zu tragen.

Unterabsatz 1 gilt nicht, wenn einer der folgenden Fälle eingetreten ist:

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

b) wenn 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.

Hat der Zahler weder betrügerisch gehandelt noch seine Pflichten nach Artikel 53 vorsätzlich verletzt, können die zuständigen nationalen Behörden, die Streitbeilegungsstellen 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) Der Zahler trägt alle mit nicht autorisierten Zahlungsvorgängen zusammenhängenden Verluste, wenn diese Verluste dadurch entstehen, dass der Zahler betrügerisch gehandelt oder eine oder mehrere seiner Pflichten nach Artikel 53 vorsätzlich oder grob fahrlässig verletzt hat. In diesen Fällen findet der Höchstbetrag nach Absatz 1 des vorliegenden Artikels keine Anwendung.

(3) Verletzt der Zahlungsdienstleister seine in Artikel 91 niedergelegte Pflicht, eine starke Kundenauthentifizierung zu verlangen, trägt der Zahler finanzielle Verluste nur im Falle eigenen betrügerischen Handelns. Ferner trägt der Zahler keine finanziellen Verluste, wenn entweder 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 Anwendung der starken Kundenauthentifizierung notwendig sind, zu entwickeln oder anzupassen, so erstattet der Zahlungsempfänger oder der Zahlungsdienstleister des Zahlungsempfängers den finanziellen Verlust, der dem Zahlungsdienstleister des Zahlers entstanden ist.

(4) 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.

(5) Nach einer Anzeige gemäß Artikel 53 Absatz 1 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 54 Absatz 1 Unterabsatz 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.

(6) Der Kommission wird die Befugnis übertragen, gemäß Artikel 115 einen delegierten Rechtsakt zur Änderung dieser Verordnung zu erlassen, um den in Absatz 1 des vorliegenden Artikels genannten Betrag zu aktualisieren.

Artikel 64

Zahlungsvorgänge, bei denen der Betrag nicht im Voraus bekannt ist

(1) Wird ein Zahlungsvorgang, insbesondere im Zusammenhang mit einem kartengebundenen Zahlungsvorgang oder einer Überweisung, 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 Geldbeträge auf dem Zahlungskonto des Zahlers nur dann blockieren, wenn der Zahler seine Einwilligung für die genaue Höhe des zu blockierenden Geldbetrags erteilt hat.

(2) Die Höhe des vom Zahlungsdienstleister des Zahlers gemäß Absatz 1 blockierten Geldbetrags muss in einem angemessenen Verhältnis zu dem Betrag des Zahlungsvorgangs stehen, den der Zahler vernünftigerweise erwarten kann.

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

(4) Der Zahlungsdienstleister des Zahlers gibt die auf dem Zahlungskonto des Zahlers gemäß Absatz 1 blockierten Geldbeträge unmittelbar nach Erhalt der Information über den genauen Betrag des Zahlungsvorgangs frei.

Artikel 65

Erstattung von Zahlungsvorgängen, die von einem oder über einen Zahlungsempfänger ausgelöst wurden

(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 vernünftigerweise hätte erwarten können.

Auf Verlangen des Zahlungsdienstleisters trägt der Zahler die Beweislast, dass diese Bedingungen erfüllt sind.

Erstattet wird der volle Betrag des ausgeführten Zahlungsvorgangs. Das Wertstellungsdatum der Gutschrift auf dem Zahlungskonto des Zahlers liegt nicht später als das Datum, an dem der Betrag belastet wurde.

Unbeschadet des Absatzes 3 des vorliegenden Artikels hat der Zahler bei Lastschriften zusätzlich zu dem in Unterabsatz 1 des vorliegenden Absatzes genannten Anspruch einen bedingungslosen Anspruch auf Erstattung innerhalb der in Artikel 66 festgelegten Fristen.

(2) Für die Zwecke von Absatz 1 Unterabsatz 1 Buchstabe b des vorliegenden Artikels darf der Zahler sich nicht auf mit möglichen Währungsumtauschkosten zusammenhängende Gründe berufen, wenn der mit seinem Zahlungsdienstleister gemäß Artikel 13 Absatz 1 Unterabsatz 1 Buchstabe e und Artikel 20 Absatz 3 Unterabsatz 1 Buchstabe c vereinbarte Referenzwechselkurs angewandt wurde.

(3) Der Zahler und der Zahlungsdienstleister können in einem Rahmenvertrag vereinbaren, dass der Zahler keinen Anspruch auf Erstattung 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 Weise 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 66

Verlangen der Erstattung von Zahlungsvorgängen, die von einem oder über einen Zahlungsempfänger ausgelöst wurden

(1) Der Zahler kann die in Artikel 65 genannte Erstattung eines autorisierten Zahlungsvorgangs, der von einem oder über einen Zahlungsempfänger ausgelöst wurde, innerhalb von acht Wochen ab dem Tag, an dem der Geldbetrag abgebucht wurde, verlangen.

(2) Innerhalb von 15 Geschäftstagen nach Erhalt eines Erstattungsverlangens unternimmt der Zahlungsdienstleister eine der folgenden beiden Maßnahmen:

a) er erstattet den vollen Betrag des Zahlungsvorgangs;

b) er teilt eine Begründung mit, warum er die Erstattung ablehnt, und nennt die Stellen, an die sich der Zahler gemäß den Artikeln 100, 101, 103, 104 und 105 wenden kann, falls der Zahler die angegebenen Gründe nicht akzeptiert.

Das Recht des Zahlungsdienstleisters nach Unterabsatz 1 dieses Absatzes, eine Erstattung abzulehnen, gilt nicht im Falle von Lastschriften.

Kapitel 5
Ausführung von Zahlungsvorgängen

ABSCHNITT 1
ZAHLUNGSAUFTRÄGE UND TRANSFERIERTE BETRÄGE

Artikel 67

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 den Geldbetrag zur Verfügung gestellt hat, beginnen soll, so gilt der vereinbarte Termin für die Zwecke des Artikels 73 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 Echtzeitüberweisungen in Euro, die in den Anwendungsbereich der Verordnung (EU) Nr. 260/2012 fallen.

Artikel 68

Ablehnung der Ausführung eines Zahlungsvorgangs durch den Zahlungsdienstleister des Zahlers

(1) Vorbehaltlich des Absatzes 2 und sofern die einschlägigen Rechtsvorschriften der Union oder der Mitgliedstaaten nichts anderes vorsehen, darf der Zahlungsdienstleister des Zahlers, wenn alle im Rahmenvertrag des Zahlers festgelegten Bedingungen erfüllt sind, die Ausführung eines autorisierten Zahlungsvorgangs, unabhängig davon, ob der Zahlungsauftrag von einem Zahler, einschließlich über einen Zahlungsauslösedienstleister, oder von einem oder über einen Zahlungsempfänger erteilt wurde, nicht ablehnen.

(2) Unbeschadet der Verordnung (EU) 2024/1624 lehnt der Zahlungsdienstleister des Zahlers die Ausführung eines Zahlungsvorgangs unter den im vorliegenden Absatz genannten Umständen ab.

Ungeachtet des Artikels 5c Absatz 5 der Verordnung (EU) Nr. 260/2012 sowie des Artikels 51 und des Artikels 73 Absatz 1 der vorliegenden Verordnung setzt der Zahlungsdienstleister des Zahlers die Ausführung eines Zahlungsvorgangs aus, wenn er auf der Grundlage der in Artikel 87 der vorliegenden Verordnung genannten Transaktionsüberwachung oder anderer einschlägiger Informationen, die dem Zahlungsdienstleister zur Verfügung stehen, jedoch nicht allein aufgrund des Ergebnisses der Dienstleistung zur Überprüfung des Zahlungsempfängers objektiv gerechtfertigte Gründe für den Verdacht hat, dass es sich um einen betrügerischen Zahlungsvorgang handelt.

Hat der Zahlungsdienstleister des Zahlers objektiv gerechtfertigte Gründe für den Verdacht, dass es sich um einen betrügerischen Zahlungsvorgang handelt, und setzt er die Ausführung des Zahlungsvorgangs nicht gemäß dem vorliegenden Artikel aus, so trägt der Zahler keine finanziellen Verluste, es sei denn, der Zahler hat betrügerisch gehandelt.

Die Beweislast dafür, dass kein Verstoß gegen den vorliegenden Artikel vorliegt, trägt der Zahlungsdienstleister.

Sofern dies nicht nach anderen einschlägigen Rechtsvorschriften der Union oder der Mitgliedstaaten untersagt ist, teilt der Zahlungsdienstleister dem Zahler unverzüglich nach der Aussetzung der Ausführung des Zahlungsvorgangs in einer vereinbarten Weise alle Informationen oder Maßnahmen mit, die vom Zahler benötigt werden, damit der Zahlungsdienstleister bewerten kann, ob die Gründe für die Aussetzung nach wie vor gerechtfertigt sind. Die Mitteilung muss dem Zahler ausreichende Informationen liefern, damit er die vom Zahlungsdienstleister ermittelten Risiken nachvollziehen kann. Innerhalb der in Artikel 73 Absatz 1 genannten Fristen unternimmt der Zahlungsdienstleister alle angemessenen Anstrengungen zur Kontaktaufnahme mit dem Zahler und stellt sicher, dass jederzeit geeignete Mittel zur Verfügung stehen, damit der Zahler den Zahlungsdienstleister kontaktieren kann, wenn der Zahlungsdienstleister zusätzliche Informationen anfordert, um zu bewerten, ob objektiv gerechtfertigte Gründe für einen Betrugsverdacht vorliegen.

Liegen auf der Grundlage der Bewertung nach Unterabsatz 5 weiterhin objektiv gerechtfertigte Gründe für einen Betrugsverdacht vor, so lehnt der Zahlungsdienstleister des Zahlers die Ausführung des Zahlungsvorgangs ab und bringt das belastete Zahlungskonto gegebenenfalls wieder auf den Stand, auf dem es sich ohne die Übermittlung des Zahlungsauftrags befunden hätte.

Die Pflicht zur Mitteilung an den Zahler gemäß Unterabsatz 5 gilt nicht im Falle von Echtzeitüberweisungen. In solchen Fällen oder wenn es dem Zahlungsdienstleister des Zahlers nicht möglich war, innerhalb der in Artikel 73 Absatz 1 genannten Fristen Informationen vom Zahler zu erhalten, bewertet der Zahlungsdienstleister auf der Grundlage der in Artikel 87 genannten Transaktionsüberwachung und anderer einschlägiger Informationen, die dem Zahlungsdienstleister zur Verfügung stehen, jedoch nicht allein aufgrund des Ergebnisses der Dienstleistung zur Überprüfung des Zahlungsempfängers, ob objektiv gerechtfertigte Gründe für einen Betrugsverdacht vorliegen; ist dies der Fall, lehnt er die Ausführung des Zahlungsvorgangs ab.

(3) Lehnt der Zahlungsdienstleister des Zahlers auf der Grundlage der Bewertung nach Absatz 2 die Ausführung eines Zahlungsvorgangs ab, so teilt er dies dem Zahler und dem Zahlungsdienstleister des Zahlungsempfängers mit und stellt dem Zahlungsauslösedienstleister gegebenenfalls die Ablehnung, die spezifischen Gründe für diese Ablehnung und gegebenenfalls das Verfahren zur Berichtigung der Entscheidung über die Ablehnung der Ausführung des Vorgangs zur Verfügung, es sei denn, eine solche Mitteilung ist nach den einschlägigen Rechtsvorschriften der Union oder der Mitgliedstaaten untersagt.

Der Zahlungsdienstleister des Zahlers nimmt die Mitteilung in der vereinbarten Weise vor und stellt die Informationen, falls zutreffend, dem Zahlungsauslösedienstleister unverzüglich, in jedem Fall aber innerhalb der in Artikel 73 genannten Fristen, zur Verfügung. Bei Echtzeitüberweisungen übermittelt der Zahlungsdienstleister des Zahlers die Mitteilung und stellt die Informationen, falls zutreffend, dem Zahlungsauslösedienstleister innerhalb von zehn Sekunden nach Eingang des Zahlungsauftrags beim Zahlungsdienstleister des Zahlers zur Verfügung.

Im Rahmenvertrag kann die Möglichkeit vorgesehen werden, dass der Zahlungsdienstleister für eine Ablehnung der Ausführung eines Zahlungsvorgangs ein angemessenes Entgelt in Rechnung stellt, sofern diese Ablehnung objektiv gerechtfertigt ist, jedoch nicht im Falle einer Ablehnung aufgrund eines Verdachts eines betrügerischen Vorgangs.

(4) Für die Zwecke des vorliegenden Artikels stellt die Tatsache, dass ein Zahlungsauftrag ungewöhnlich ist, für sich genommen keinen objektiv gerechtfertigten Grund für den Betrugsverdacht dar.

(5) Für die Zwecke der Artikel 73 und 79 gilt ein Zahlungsauftrag für einen Zahlungsvorgang, dessen Ausführung abgelehnt wurde, als nicht eingegangen.

Artikel 69

Unwiderruflichkeit von Zahlungsaufträgen

(1) Ein Zahlungsdienstnutzer kann einen Zahlungsauftrag nach dessen Eingang beim Zahlungsdienstleister des Zahlers nicht mehr widerrufen, sofern dieser Artikel nichts anderes vorsieht.

(2) Wurde der Zahlungsvorgang von einem Zahlungsauslösedienstleister oder vom Zahlungsempfänger oder über diesen ausgelöst, so darf der Zahler den Zahlungsauftrag nicht mehr widerrufen, nachdem er dem Zahlungsauslösedienstleister die Einwilligung zur Auslösung des Zahlungsvorgangs erteilt oder dem Zahlungsempfänger die Einwilligung zur Ausführung des Zahlungsvorgangs erteilt hat.

(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) Unter den in Artikel 67 Absatz 2 genannten Umständen 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 70

Transferierte und eingegangene Beträge

(1) Der Zahlungsdienstleister des Zahlers, der Zahlungsdienstleister des Zahlungsempfängers und alle 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, so stellt der Zahlungsdienstleister des Zahlers sicher, dass der Zahlungsempfänger den vollen Betrag des vom Zahler ausgelösten Zahlungsvorgangs erhält. Wird der Zahlungsvorgang von dem Zahlungsempfänger oder über diesen ausgelöst, so stellt der Zahlungsdienstleister des Zahlungsempfängers sicher, dass der Zahlungsempfänger den vollen Betrag des Zahlungsvorgangs erhält.

Artikel 71

Zahlungsvorgänge mit E-Geld-Token

(1) Abweichend von Artikel 13 Absatz 1 Unterabsatz 1 Buchstaben b und d, Artikel 20 Absatz 2 Buchstabe e, Artikel 20 Absatz 3 Unterabsatz 1 Buchstabe a und Artikel 24 teilen die Zahlungsdienstleister in Fällen, in denen sie aufgrund von ihnen nicht zuzurechnenden Umständen nicht in der Lage sind, den in den genannten Artikeln festgelegten Pflichten in Bezug auf Zahlungsvorgänge mit E-Geld-Token, die über den Distributed Ledger abgewickelt werden, nachzukommen, die in denselben Artikeln genannten Informationen so bald wie möglich, in jedem Fall aber vor der Autorisierung des Zahlungsvorgangs durch den Zahler, in Form einer begründeten Schätzung mit.

(2) Die Anforderungen der Artikel 41 und 42 an kontoführende Zahlungsdienstleister in Bezug auf Zahlungsauslösedienste und Kontoinformationsdienste gelten nicht für Zahlungsvorgänge mit E-Geld-Token.

(3) Die Artikel 51 und 58 gelten nicht für Zahlungsdienstleister in Bezug auf Zahlungsvorgänge mit E-Geld-Token.

(4) Der Kommission wird die Befugnis übertragen, gemäß Artikel 115 delegierte Rechtsakte zur Änderung dieser Verordnung zu erlassen, um die in den Absätzen 1, 2 und 3 des vorliegenden Artikels festgelegten Ausnahmen und Anforderungen in Bezug auf Zahlungsvorgänge mit E-Geld-Token anzupassen, um den Entwicklungen nach der Annahme dieser Verordnung und den Besonderheiten des Einsatzes der Distributed-Ledger-Technologie oder einer ähnlichen Technologie für solche Vorgänge Rechnung zu tragen.

ABSCHNITT 2

AUSFÜHRUNGSFRIST UND WERTSTELLUNGSDATUM

Artikel 72

Anwendungsbereich

(1) Dieser Abschnitt gilt für

a) Zahlungsvorgänge in Euro,

b) inländische Zahlungsvorgänge in Währungen der Mitgliedstaaten, deren Währung nicht der Euro ist,

c) Zahlungsvorgänge, bei denen nur eine Währungsumrechnung zwischen dem Euro und der Währung eines Mitgliedstaats, dessen Währung nicht der Euro ist, stattfindet, sofern die erforderliche Währungsumrechnung in dem betreffenden Mitgliedstaat, dessen Währung nicht der Euro ist, durchgeführt wird und – im Falle von grenzüberschreitenden Zahlungsvorgängen – der grenzüberschreitende Transfer in Euro stattfindet.

(2) Dieser Abschnitt findet auf in Absatz 1 des vorliegenden Artikels nicht genannte Zahlungsvorgänge Anwendung, sofern zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister nichts anderes vereinbart wurde; hiervon ausgenommen ist Artikel 77, 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 73 festgelegte Frist, so darf diese längere Frist fünf Geschäftstage ab dem in Artikel 67 genannten Zeitpunkt des Eingangs nicht überschreiten.

Artikel 73

Zahlungsvorgänge mit Übertragung auf ein Zahlungskonto

(1) Unbeschadet der einschlägigen Rechtsvorschriften der Union oder der Mitgliedstaaten im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung stellt der Zahlungsdienstleister des Zahlers sicher, dass nach dem in Artikel 67 genannten Zeitpunkt des Eingangs der Betrag des Zahlungsvorgangs dem Konto des Zahlungsdienstleisters des Zahlungsempfängers bis zum Ende des darauf folgenden Geschäftstags gutgeschrieben wird. Diese Frist kann für in Papierform ausgelöste Zahlungsvorgänge um einen weiteren Geschäftstag verlängert werden.

(2) Unbeschadet der einschlägigen Rechtsvorschriften der Union oder der Mitgliedstaaten im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung weist der Zahlungsdienstleister des Zahlungsempfängers dem Betrag des Zahlungsvorgangs im Einklang mit Artikel 77 ein Wertstellungsdatum zu und macht ihn auf dem Zahlungskonto des Zahlungsempfängers verfügbar, nachdem der Zahlungsdienstleister den Geldbetrag erhalten hat.

(3) Hat der Zahlungsdienstleister des Zahlungsempfängers auf der Grundlage der gemäß Artikel 87 durchgeführten Transaktionsüberwachung oder anderer einschlägiger Informationen, die dem Zahlungsdienstleister des Zahlungsempfängers zur Verfügung stehen, jedoch nicht allein aufgrund des Ergebnisses der Dienstleistung zur Überprüfung des Zahlungsempfängers objektiv gerechtfertigte Gründe für den Verdacht, dass ein Zahlungsvorgang, der seinem Konto gutgeschrieben wurde oder gutgeschrieben werden soll, betrügerisch ist, so kann dieser Zahlungsdienstleister abweichend von Absatz 2 des vorliegenden Artikels im Einklang mit seiner Verpflichtung nach Artikel 71 der Verordnung (EU) 2024/1624, keine verdächtigen Transaktionen durchzuführen, entscheiden, den Geldbetrag nicht auf dem Zahlungskonto des Zahlungsempfängers verfügbar zu machen und ihn an den Zahlungsdienstleister des Zahlers zurückzugeben, sofern diese Entscheidung innerhalb der in Artikel 77 der vorliegenden Verordnung festgelegten Frist erfolgt.

Sind die Gründe für den Verdacht, dass ein Zahlungsvorgang, der dem Konto des Zahlungsempfängers gutgeschrieben wurde oder gutgeschrieben werden soll, betrügerisch ist, klar und unbestreitbar, so macht der Zahlungsdienstleister des Zahlungsempfängers den Geldbetrag nicht auf dem Zahlungskonto des Zahlungsempfängers verfügbar und zahlt ihn an den Zahlungsdienstleister des Zahlers zurück.

Kommt der Zahlungsdienstleister des Zahlungsempfängers der Verpflichtung nach Unterabsatz 2 nicht nach, so trägt der Zahler keine finanziellen Verluste, es sei denn, der Zahler hat betrügerisch gehandelt.

Die Unterabsätze 1 und 2 des vorliegenden Absatzes gelten unbeschadet der Verpflichtung des Zahlungsdienstleisters des Zahlungsempfängers, verdächtige Transaktionen gemäß Artikel 69 der Verordnung (EU) 2024/1624 zu melden.

Für die Zwecke dieses Artikels stellt die Tatsache, dass ein Zahlungsvorgang ungewöhnlich ist, für sich genommen keinen objektiv gerechtfertigten Grund für den Betrugsverdacht dar.

Die Beweislast dafür, dass kein Verstoß gegen Unterabsatz 2 vorliegt, trägt der Zahlungsdienstleister des Zahlungsempfängers.

(4) Zahlt der Zahlungsdienstleister des Zahlungsempfängers den Geldbetrag gemäß Absatz 3 Unterabsatz 1 oder 2 an den Zahlungsdienstleister des Zahlers zurück, so muss der Zahlungsdienstleister des Zahlungsempfängers

a) dem Zahlungsdienstleister des Zahlers im Einklang mit den Vorschriften über das Verbot der Informationsweitergabe nach Artikel 73 Absatz 5 der Verordnung (EU) 2024/1624 unmittelbar die Rückzahlung des Geldbetrags und die Gründe für die Verweigerung der Verfügbarmachung des Geldbetrags auf dem Zahlungskonto des Zahlungsempfängers mitteilen und

b) sicherstellen, dass der Betrag des Zahlungsvorgangs dem Zahlungsdienstleister des Zahlers innerhalb der in Absatz 1 des vorliegenden Artikels genannten Frist gutgeschrieben wird.

(5) Nach Erhalt der Mitteilung gemäß Absatz 4 Buchstabe a des vorliegenden Artikels unterrichtet der Zahlungsdienstleister des Zahlers unbeschadet des Artikels 73 der Verordnung (EU) 2024/1624 den Zahler unmittelbar und kostenlos darüber, dass der Geldbetrag aufgrund von Maßnahmen zur Betrugsprävention nicht auf dem Zahlungskonto des Zahlungsempfängers verfügbar gemacht wurde, und stellt dem Zahlungsauslösedienstleister gegebenenfalls die Informationen zur Verfügung. Der Zahlungsdienstleister des Zahlers unterrichtet den Zahler auch über die Rückzahlung des Geldbetrags und die Frist für die Verfügbarmachung des Betrags des Zahlungsvorgangs auf dem Zahlungskonto des Zahlers. Der Zahlungsdienstleister des Zahlers weist dem Betrag des Zahlungsvorgangs, der seinem Konto gemäß Absatz 4 Buchstabe b des vorliegenden Artikels gutgeschrieben wurde, im Einklang mit Artikel 77 der vorliegenden Verordnung ein Wertstellungsdatum zu und macht ihn auf dem Zahlungskonto des Zahlers verfügbar.

(6) Zahlt der Zahlungsdienstleister des Zahlungsempfängers im Falle einer Echtzeitüberweisung den Geldbetrag gemäß Absatz 3 Unterabsatz 1 oder 2 an den Zahlungsdienstleister des Zahlers zurück, so muss der Zahlungsdienstleister des Zahlungsempfängers

a) dem Zahlungsdienstleister des Zahlers im Einklang mit den Vorschriften über das Verbot der Informationsweitergabe nach Artikel 73 Absatz 5 der Verordnung (EU) 2024/1624 innerhalb von zehn Sekunden nach Eingang des Zahlungsauftrags für eine Echtzeitüberweisung beim Zahlungsdienstleister des Zahlers die Rückzahlung des Geldbetrags und die Gründe für die Verweigerung der Verfügbarmachung des Geldbetrags auf dem Zahlungskonto des Zahlungsempfängers mitteilen und

b) sicherstellen, dass dieser Geldbetrag unmittelbar dem Zahlungsdienstleister des Zahlers gutgeschrieben wird, wenn der Geldbetrag des Vorgangs seinem Konto gutgeschrieben wurde.

(7) Unmittelbar nach Erhalt der Mitteilung gemäß Absatz 6 Buchstabe a muss der Zahlungsdienstleister des Zahlers

a) das Zahlungskonto des Zahlers wieder auf den Stand bringen, auf dem es sich ohne die Ausführung des Vorgangs befunden hätte, und

b) den Zahler kostenlos über die Rückzahlung des Geldbetrags und – unbeschadet des Artikels 73 der Verordnung (EU) 2024/1624 – darüber unterrichten, dass der Geldbetrag aufgrund von Maßnahmen zur Betrugsprävention nicht auf dem Zahlungskonto des Zahlungsempfängers verfügbar gemacht wurde, und dem Zahlungsauslösedienstleister gegebenenfalls die Informationen zur Verfügung stellen.

(8) 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 die Abwicklung zum vereinbarten Fälligkeitstermin. Absatz 3 ist entsprechend anzuwenden.

Artikel 74

Fehlen eines Zahlungskontos des Zahlungsempfängers beim Zahlungsdienstleister

Unterhält der Zahlungsempfänger beim Zahlungsdienstleister kein Zahlungskonto, so macht der Zahlungsdienstleister, der den Geldbetrag für den Zahlungsempfänger erhält, den Geldbetrag für den Zahlungsempfänger innerhalb der in Artikel 73 Absatz 1 genannten Frist verfügbar.

Bei Zahlungsvorgängen mit E-Geld-Token von einer elektronischen Geldbörse an eine selbst gehostete Adresse transferiert der Zahlungsdienstleister des Zahlers den Geldbetrag innerhalb der in Artikel 73 Absatz 1 genannten Frist an die selbst gehostete Adresse des Zahlungsempfängers.

Artikel 75

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 unmittelbar nach Eingang des Geldbetrags verfügbar gemacht und wertgestellt wird. Ist der Zahlungsdienstnutzer kein Verbraucher, so muss der Betrag spätestens an dem auf den Eingang des Geldbetrags folgenden Geschäftstag auf dem Konto des Zahlungsempfängers verfügbar gemacht und wertgestellt werden.

Artikel 76

Inländische Zahlungsvorgänge

Bei inländischen Zahlungsvorgängen können die Mitgliedstaaten kürzere als die in diesem Abschnitt vorgesehenen Ausführungsfristen vorsehen.

Die Mitgliedstaaten teilen der Kommission bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach Unterabsatz 1 erlassen. Sie teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach Unterabsatz 1 erlassen, umgehend mit.

Artikel 77

Wertstellungsdatum und Verfügbarkeit der Geldbeträge

(1) Das Wertstellungsdatum einer Gutschrift auf dem Zahlungskonto des Zahlungsempfängers liegt nicht später als der 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 unmittelbar zur Verfügung steht, nachdem dieser 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) Das Wertstellungsdatum der Belastung auf dem Zahlungskonto des Zahlers liegt nicht früher als der Zeitpunkt, zu dem das betreffende Zahlungskonto mit dem Betrag des Zahlungsvorgangs belastet wird.

Artikel 78

Fehlerhafte Kundenidentifikatoren

(1) Wird ein Zahlungsvorgang gemäß dem Kundenidentifikator ausgeführt, so gilt der Zahlungsvorgang im Hinblick auf den durch den Kundenidentifikator bezeichneten Zahlungsempfänger als korrekt ausgeführt.

(2) Ist der vom Zahlungsdienstnutzer angegebene Kundenidentifikator fehlerhaft, so haftet der Zahlungsdienstleister nicht gemäß Artikel 79 für die nicht erfolgte oder fehlerhafte Ausführung des Zahlungsvorgangs.

Der Zahlungsdienstleister des Zahlers bemüht sich im Rahmen des Zumutbaren, den Geldbetrag, der 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 Wiedererlangung des Geldbetrags maßgeblichen Informationen übermittelt.

Ist die Wiedererlangung des Geldbetrags nach Unterabsatz 2 nicht möglich, so teilt der Zahlungsdienstleister des Zahlers dem Zahler auf schriftlichen Antrag hin alle Informationen mit, über die der Zahlungsdienstleister des Zahlers verfügt und die für den Zahler relevant sind, damit der Zahler seinen Anspruch auf Rückerstattung des Geldbetrags auf dem Rechtsweg geltend machen kann.

(3) Falls im Rahmenvertrag vereinbart, kann der Zahlungsdienstleister dem Zahlungsdienstnutzer für die Rückerstattung ein Entgelt in Rechnung stellen. Dieses Entgelt muss angemessen und verhältnismäßig zu den entstandenen Kosten sein.

(4) Teilt der Zahlungsdienstnutzer zusätzlich zu den in Artikel 13 Absatz 1 Buchstabe a oder Artikel 20 Absatz 2 Buchstabe b genannten Informationen weitere Informationen mit, so haftet der Zahlungsdienstleister nur für die Ausführung von Zahlungsvorgängen gemäß dem vom Zahlungsdienstnutzer angegebenen Kundenidentifikator.

(5) Ist der vom Zahlungsauslösedienstleister angegebene Kundenidentifikator fehlerhaft, so haften die Zahlungsdienstleister gemäß Artikel 80.

Artikel 79

Haftung der Zahlungsdienstleister für nicht erfolgte, fehlerhafte oder verspätete Ausführung von Zahlungsvorgängen

(1) Wird ein Zahlungsauftrag vom Zahler direkt erteilt, so haftet der Zahlungsdienstleister des Zahlers unbeschadet des Artikels 55, des Artikels 78 Absatz 2 und des Artikels 83 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 73 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 fehlerhaften Zahlungsvorgangs unmittelbar und bringt das belastete Zahlungskonto gegebenenfalls wieder auf den Stand, auf dem es sich ohne den fehlerhaften Zahlungsvorgang befunden hätte.

Das Wertstellungsdatum der Gutschrift auf dem Zahlungskonto des Zahlers liegt nicht später als das Datum, an dem der Betrag belastet wurde.

Haftet der Zahlungsdienstleister des Zahlungsempfängers nach Unterabsatz 1, so stellt er dem Zahlungsempfänger den Betrag des Zahlungsvorgangs unmittelbar zur Verfügung und schreibt den entsprechenden Betrag gegebenenfalls dem Zahlungskonto des Zahlungsempfängers gut.

Das Wertstellungsdatum der Gutschrift auf dem Zahlungskonto des Zahlungsempfängers liegt nicht später als der Zeitpunkt, zu dem der Betrag bei korrekter Ausführung des Vorgangs gemäß Artikel 77 wertgestellt worden wäre.

Wird ein Zahlungsvorgang verspätet ausgeführt, so stellt der Zahlungsdienstleister des Zahlungsempfängers auf Verlangen des für den Zahler auftretenden Zahlungsdienstleisters des Zahlers sicher, dass das Wertstellungsdatum der Gutschrift auf dem Zahlungskonto des Zahlungsempfängers nicht später liegt als der Zeitpunkt, zu dem der Betrag bei korrekter Ausführung des Vorgangs wertgestellt worden wäre.

Im Falle eines nicht ausgeführten oder fehlerhaft ausgeführten Zahlungsvorgangs, bei dem der Zahlungsauftrag durch den Zahler erteilt wurde, bemüht sich der Zahlungsdienstleister des Zahlers auf Verlangen – ungeachtet der Haftung nach diesem Absatz und ohne dem Zahler ein Entgelt dafür in Rechnung zu stellen – unmittelbar darum, den Zahlungsvorgang zurückzuverfolgen, und unterrichtet den Zahler über das Ergebnis.

(2) Wird ein Zahlungsauftrag vom oder über den Zahlungsempfänger erteilt, so haftet der Zahlungsdienstleister des Zahlungsempfängers unbeschadet des Artikels 55, des Artikels 78 Absatz 2 und des Artikels 83 gegenüber dem Zahlungsempfänger für die korrekte Übermittlung des Zahlungsauftrags an den Zahlungsdienstleister des Zahlers gemäß Artikel 73 Absatz 8. Haftet der Zahlungsdienstleister des Zahlungsempfängers nach dem vorliegenden Unterabsatz, so übermittelt er den fraglichen Zahlungsauftrag unmittelbar erneut an den Zahlungsdienstleister des Zahlers.

Bei verspäteter Übermittlung des Zahlungsauftrags wird der Betrag auf dem Zahlungskonto des Zahlungsempfängers nicht später wertgestellt als zu dem Zeitpunkt, zu dem der Betrag bei korrekter Ausführung des Vorgangs wertgestellt worden wäre.

Unbeschadet des Artikels 55, des Artikels 78 Absatz 2 und des Artikels 83 haftet der Zahlungsdienstleister des Zahlungsempfängers gegenüber dem Zahlungsempfänger für die Bearbeitung des Zahlungsvorgangs gemäß seinen Verpflichtungen nach Artikel 77. Haftet der Zahlungsdienstleister des Zahlungsempfängers nach dem vorliegenden Unterabsatz, so stellt er sicher, dass der Betrag des Zahlungsvorgangs dem Zahlungsempfänger unmittelbar, nachdem der Betrag dem Konto des Zahlungsdienstleisters des Zahlungsempfängers gutgeschrieben wurde, zur Verfügung steht. Der Betrag wird auf dem Zahlungskonto des Zahlungsempfängers nicht später wertgestellt als zu dem Zeitpunkt, zu dem Betrag bei korrekter Ausführung des Vorgangswertgestellt 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, so erstattet er dem Zahler gegebenenfalls unverzüglich den Betrag des nicht ausgeführten oder fehlerhaften Zahlungsvorgangs und bringt das belastete Zahlungskonto wieder auf den Stand, auf dem es sich ohne den fehlerhaften Zahlungsvorgang befunden hätte. Das Wertstellungsdatum der Gutschrift auf dem Zahlungskonto des Zahlers liegt nicht später als das Datum, an dem der Betrag belastet wurde.

Die Verpflichtung gemäß Unterabsatz 4 gilt nicht für den Zahlungsdienstleister des Zahlers, 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 wird der Betrag vom Zahlungsdienstleister des Zahlungsempfängers auf dem Zahlungskonto des Zahlungsempfängers nicht später wertgestellt als zu dem Zeitpunkt, zu dem der Betrag bei korrekter Ausführung des Zahlungsvorgangs wertgestellt worden wäre.

Im Falle eines nicht ausgeführten oder fehlerhaft ausgeführten Zahlungsvorgangs, bei dem der Zahlungsauftrag vom oder über den Zahlungsempfänger erteilt wurde, bemüht sich der Zahlungsdienstleister des Zahlungsempfängers auf Verlangen – ungeachtet der Haftung nach diesem Absatz und ohne dem Zahler ein Entgelt dafür in Rechnung zu stellen– unmittelbar darum, den Zahlungsvorgang zurückzuverfolgen, und unterrichtet den Zahlungsempfänger 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 80

Haftung im Fall 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 55 und des Artikels 78 Absatz 2 dem Zahler den Betrag des nicht ausgeführten oder fehlerhaften Zahlungsvorgangs und bringt das belastete Zahlungskonto gegebenenfalls wieder auf den Stand, auf dem es sich ohne den fehlerhaften Zahlungsvorgang befunden hätte.

Der Zahlungsauslösedienstleister trägt die Beweislast, dass der Zahlungsauftrag gemäß Artikel 67 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 Zahlungsvorgangs 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 unmittelbar für die infolge der Erstattung an den Zahler erlittenen Verluste oder gezahlten Beträge.

Artikel 81

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 82

Regressanspruch

(1) Wenn die Haftung eines Zahlungsdienstleisters nach den Artikeln 57, 58, 60, 68 Absatz 2, 73 Absatz 3, 79, 80 und 87 einem anderen Zahlungsdienstleister oder einer zwischengeschalteten Stelle zuzurechnen ist, entschädigt dieser andere Zahlungsdienstleister oder diese zwischengeschaltete Stelle den erstgenannten Zahlungsdienstleister für alle nach den Artikeln 57, 58, 60, 68 Absatz 2, 73 Absatz 3, 79, 80 und 87 erlittenen Verluste oder gezahlten Beträge. Dies beinhaltet auch eine Entschädigung in dem Fall, dass einer der Zahlungsdienstleister keine starke Kundenauthentifizierung anwendet.

(2) Erfüllt ein Hostingdiensteanbieter die in Artikel 6 Absatz 1 Buchstaben a und b der Verordnung (EU) 2022/2065 festgelegten Bedingungen in Bezug auf die Speicherung rechtswidriger Inhalte im Sinne des Artikels 3 Buchstabe h der genannten Verordnung nicht und führen diese Inhalte zu einem oder einer Serie von nicht autorisierten Zahlungsvorgängen gemäß Artikel 57 der vorliegenden Verordnung oder zu einem oder einer Serie von betrügerischen autorisierten Zahlungsvorgängen gemäß Artikel 60 der vorliegenden Verordnung, so entschädigt dieser Anbieter den Zahlungsdienstleister für alle gemäß den Artikeln 57 und 60 der vorliegenden Verordnung erlittenen Verluste oder gezahlten Beträge.

(3) 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 83

Ungewöhnliche und unvorhersehbare Umstände

Die Haftung nach Kapitel 4 oder dem vorliegenden Kapitel besteht nicht im Falle ungewöhnlicher und unvorhersehbarer Umstände, auf die die Partei, die sich darauf beruft, keinen Einfluss hat und deren Folgen trotz aller Bemühungen zur Verhinderung nicht abwendbar gewesen wären, oder wenn ein Zahlungsdienstleister durch andere rechtliche Verpflichtungen nach Unionsrecht oder nationalem Recht gebunden ist.

Kapitel 6
Datenschutz

Artikel 84
Datenschutz

Zahlungssysteme, Zahlverfahren, abwickelnde Stellen 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 Binnenmarkts für Zahlungsdienste verarbeiten, soweit dies für die Erbringung von Zahlungsdiensten und für die Erfüllung der Verpflichtungen im Rahmen der vorliegenden 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, einschließlich technischer Beschränkungen für die Weiterverwendung von Daten und die Anwendung modernster Sicherheits- und Datenschutzvorkehrungen, wie Pseudonymisierung, oder Verschlüsselung;

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 85

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 gilt unbeschadet der Anwendung von Kapitel II der Verordnung (EU) 2022/2554 auf

a) die in Artikel 2 Absatz 1 Buchstaben a, b und d der vorliegenden Verordnung genannten Zahlungsdienstleister,

b) die in Artikel 35 Absatz 1 der Richtlinie (EU) 2026/…[+] genannten Kontoinformationsdienstleister und

c) Zahlungsinstitute, die gemäß Artikel 33 Absatz 1 der Richtlinie (EU) 2026/… ausgenommen sind.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(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 Cybersicherheit (ENISA) im Bereich der operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit Zahlungsdiensten.

Artikel 86

Betrugsmeldung

(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.

Die statistischen Daten zu Betrug umfassen die Anzahl und den Wert der erstatteten betrügerischen Zahlungsvorgänge und der Zahlungsvorgänge, bei denen eine Erstattung gemäß dieser Verordnung abgelehnt wurde, zusammen mit den Gründen für diese Ablehnung, z. B. die Feststellung, dass der Verbraucher betrügerisch oder grob fahrlässig gehandelt hat.

(2) Die zuständigen Behörden können Zahlungsdienstleistern gestatten, der Pflicht nach Absatz 1 nachzukommen, indem sie Daten über Betrug im Rahmen einer anderen Meldepflicht für Daten melden, sofern diese Pflicht nicht weniger umfangreich ist als die Meldepflicht nach diesem Artikel und sofern Vereinbarungen getroffen wurden, nach denen die EBA und die EZB die nach diesem Artikel zu übermittelnden Daten erhalten.

(3) Die EBA und die EZB veröffentlichen in einem jährlichen gemeinsamen Bericht die statistischen Daten in aggregierter Form und eine Analyse der auf der Grundlage dieser Daten beobachteten Trends.

(4) Die EBA erarbeitet in enger Zusammenarbeit mit der EZB Entwürfe technischer Regulierungsstandards, in denen festgelegt wird, welche statistischen Daten zu Betrug nach Absatz 1 bereitzustellen sind.

Die EBA übermittelt der Kommission den Entwurf der in Unterabsatz 1 genannten technischen Regulierungsstandards bis zum … [zwölf Monate nach dem Tag des Inkrafttretens dieser Verordnung].

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

(5) Die EBA erarbeitet Entwürfe technischer Durchführungsstandards, in denen die Standardformulare und -meldebögen für die in Absatz 1 genannte Übermittlung von Zahlungsbetrugsdaten durch die zuständigen Behörden an die EBA festgelegt werden. Diese technischen Durchführungsstandards finden keine Anwendung, wenn die zuständige Behörde von der in Absatz 2 genannten Möglichkeit Gebrauch macht.

Die EBA übermittelt der Kommission die in Unterabsatz 1 genannten technischen Durchführungsstandards bis zum … [zwölf Monate nach dem Tag des Inkrafttretens dieser Verordnung].

Der Kommission wird die Befugnis übertragen, diese technischen Durchführungsstandards gemäß Artikel 15 der Verordnung (EU) Nr. 1093/2010 zu erlassen.

Artikel 87

Transaktionsüberwachungsmechanismen

(1) Die Zahlungsdienstleister müssen über Transaktionsüberwachungsmechanismen verfügen, um

a) die Anwendung der starken Kundenauthentifizierung gemäß Artikel 91 zu unterstützen,

b) Ausnahmen von der Anwendung der starken Kundenauthentifizierung auf Grundlage der in Artikel 91 Absatz 9 genannten Kriterien unter genau festgelegten und eingeschränkten Bedingungen vorzusehen, die auf dem jeweiligen Risiko sowie der Art und den Einzelheiten der vom Zahlungsdienstleister bewerteten Daten beruhen;

c) potenziell betrügerische Zahlungsvorgänge, einschließlich Vorgänge unter Beteiligung von Zahlungsauslösediensten, zu verhindern und aufzudecken.

Die Transaktionsüberwachungsmechanismen stützen sich auf die Analyse früherer Zahlungsvorgänge und den Online-Zugriff auf Zahlungskonten.

(2) Die Zahlungsdienstleister stellen sicher, dass ihre Transaktionsüberwachungsmechanismen zumindest alle nachstehend genannten risikobasierten Faktoren einbeziehen:

a) Listen der kompromittierten oder gestohlenen Authentifizierungselemente,

b) den Betrag eines jeden Zahlungsvorgangs,

c) bekannte Betrugsszenarien bei der Erbringung von Zahlungsdienstleistungen,

d) Anzeichen für eine Malware-Infektion in jeglicher Sitzung des Authentifizierungsverfahrens,

e) in Fällen, in denen das Zugangsgerät oder die Software vom Zahlungsdienstleister bereitgestellt wird, ein Protokoll über die Nutzung des Zugangsgeräts oder der Software, das bzw. die dem Zahlungsdienstnutzer zur Verfügung gestellt wird, sowie über die ungewöhnliche Nutzung des Zugangsgeräts oder der Software.

(3) Der Zahlungsdienstleister des Zahlers führt die in Absatz 1 vorgesehene Transaktionsüberwachung vor der Ausführung eines Zahlungsvorgangs durch.

Der Zahlungsdienstleister des Zahlungsempfängers führt die Transaktionsüberwachung gemäß Absatz 1 des vorliegenden Artikels durch, bevor der Geldbetrag dem Zahlungsempfänger gemäß Artikel 73 Absatz 2 zur Verfügung gestellt wird.

Führt ein Zahlungsdienstleister die Transaktionsüberwachung gemäß dem vorliegenden Artikel in Bezug auf einen Vorgang nicht durch und entsteht dem Zahler ein finanzieller Schaden, so haftet dieser Zahlungsdienstleister für diesen finanziellen Schaden.

Weist der Zahlungsdienstleister des Zahlers dem Zahler nicht nach, dass die Transaktionsüberwachung von beiden Dienstleistern durchgeführt wurde, so erstattet er dem Zahler den Betrag des Vorgangs.

Der Zahler trägt keine finanziellen Folgen aus diesem Vorgang, es sei denn, er hat betrügerisch gehandelt.

Die Beweislast dafür, dass kein Verstoß gegen den vorliegenden Absatz vorliegt, trägt der betreffende Zahlungsdienstleister.

(4) Die Verarbeitung durch den Zahlungsdienstleister des Zahlers ist, soweit dies zur Erreichung der in Absatz 1 genannten Zwecke erforderlich ist, auf folgende Daten beschränkt:

a) Informationen zum Zahler, einschließlich umgebungs- und verhaltensbezogener Merkmale, die für den Zahler 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, Zahlungsinstrument, Währung, Datum und Zeitpunkt der Ausführung sowie Kundenidentifikator des Zahlungsempfängers;

d) Sitzungsdaten, einschließlich Internetprotokoll-Adressbereich des Geräts, von dem aus auf das Zahlungskonto zugegriffen wurde, von dem der Vorgang ausgelöst wurde;

e) Gerätdaten, einschließlich der Kennungen des Geräts, von dem aus der Vorgang ausgelöst wurde;

f) Informationen zum Zahlungsempfänger, einschließlich des Kundenidentifikators des Zahlungsempfängers;

g) im Rahmen der Vereinbarungen über den Informationsaustausch erhaltene Informationen.

(5) Die Verarbeitung durch den Zahlungsdienstleister des Zahlungsempfängers ist, soweit dies zur Erreichung der in Absatz 1 genannten Zwecke erforderlich ist, auf folgende Daten beschränkt:

a) Informationen zum Zahlungsempfänger;

b) im Rahmen der Vereinbarungen über den Informationsaustausch erhaltene Informationen;

c) Informationen über das Zahlungskonto des Zahlungsempfängers, einschließlich Zahlungsvorgangshistorie;

d) Informationen über den Vorgang, einschließlich Betrag des Vorgangs, Zahlungsinstrument, Währung, Datum und Zeitpunkt der Ausführung sowie Name des Zahlers.

(6) Zahlungsdienstleister speichern die in den Absätzen 4 und 5 genannten Daten nicht länger, als es für die in Absatz 1 festgelegten Zwecke erforderlich ist, auf keinen Fall aber länger als fünf Jahre nach Beendigung der Kundenbeziehung.

Artikel 88

Informationsaustausch zu Betrug

(1) Zahlungsdienstleister beteiligen sich an Vereinbarungen über den Informationsaustausch mit anderen Zahlungsdienstleistern gemäß Absatz 4 und tauschen Daten aus, soweit dies erforderlich ist, um ihren Verpflichtungen gemäß Artikel 87 Absatz 1 Unterabsatz 1 Buchstabe c der vorliegenden Verordnung nachzukommen, wenn der Zahlungsdienstleister objektiv gerechtfertigte Gründe für den Verdacht hat, dass ein Zahlungsdienstnutzer sich betrügerisch verhält. Die Kategorien der weiterzugebenden Daten beschränken sich auf die in Artikel 87 Absatz 4 Buchstaben a bis f und Absatz 5 Buchstaben a, c und d der vorliegenden Verordnung aufgeführten Daten, auf die objektiv gerechtfertigten Gründe des Zahlungsdienstleisters, die zu dem Verdacht auf betrügerisches Verhalten auf der Grundlage dieser Daten geführt haben, und auf Meldungen des Zahlungsdienstleisters an einen Hostingdiensteanbieter gemäß Artikel 16 der Verordnung (EU) 2022/2065. Informationen zu den umgebungs- und verhaltensbezogenen Merkmalen, die für den Zahler im Rahmen einer normalen Verwendung der personalisierten Sicherheitsmerkmale typisch sind, sind von dem Informationsaustausch gemäß dem vorliegenden Artikel ausgeschlossen.

(2) Zahlungsdienstleister ergreifen geeignete technische und organisatorische Maßnahmen, einschließlich Maßnahmen zur Pseudonymisierung, um ein Maß an Sicherheit und Vertraulichkeit zu gewährleisten, das in einem angemessenen Verhältnis zu der Art und dem Umfang der ausgetauschten Informationen steht.

(3) Die Zahlungsdienstleister speichern Daten, die sie im Zuge des in Absatz 1 des vorliegenden Artikels genannten Informationsaustauschs erhalten, nicht länger als für die in Artikel 87 Absatz 1 Unterabsatz 1 Buchstabe c genannten Zwecke erforderlich und auf keinen Fall länger als fünf Jahre nach dem mutmaßlichen betrügerischen Vorgang.

(4) In den Vereinbarungen über den Informationsaustausch sind die Einzelheiten der Beteiligung sowie die Einzelheiten der operativen Elemente, einschließlich der Nutzung dedizierter IT-Plattformen, festgelegt. Vor Abschluss derartiger Vereinbarungen führen die Zahlungsdienstleister gemeinsam eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der Verordnung (EU) 2016/679 und gegebenenfalls eine vorherige Konsultation der Aufsichtsbehörde gemäß Artikel 36 jener Verordnung durch.

(5) Zahlungsdienstleister dürfen nicht ausschließlich auf der Grundlage von Informationen, die sie von anderen Zahlungsdienstleistern, die einer Vereinbarung über den Informationsaustausch unterliegen, erhalten haben, Schlussfolgerungen ziehen oder Entscheidungen treffen, die sich auf die Geschäftsbeziehung mit dem Zahlungsdienstnutzer auswirken, wie z. B. die Beendigung des Vertragsverhältnisses mit dem Nutzer oder die Beeinträchtigung von dessen künftigem Onboarding, ohne diese Informationen geprüft zu haben.

Artikel 89

Plattform zur Betrugsbekämpfung

(1) Die Kommission richtet eine Plattform zur Betrugsbekämpfung im Bereich der Zahlungsdienste in der Union ein. Die Plattform zur Betrugsbekämpfung setzt sich aus einer breiten und ausgewogenen Mischung von Vertretern und Sachverständigen des öffentlichen und des privaten Sektors zusammen, die nachweislich über Kenntnisse und Erfahrungen im Bereich des Betrugs bei Zahlungsdiensten verfügen.

(2) Die Plattform zur Betrugsbekämpfung

a) berät die Kommission bei der Ausarbeitung und Überwachung der Umsetzung von Rechtsakten zur Betrugsbekämpfung im Bereich der Zahlungsdienste;

b) richtet Empfehlungen an die Kommission und das Europäische Gremium für digitale Dienste für die Zwecke der Ausarbeitung des in Artikel 61 Absatz 5 genannten freiwilligen Verhaltenskodex;

c) teilt Informationen über und Analysen von Betrugstrends im Bereich der Zahlungsdienste;

d) teilt Informationen über Maßnahmen zur Betrugsbekämpfung im Bereich der Zahlungsdienste, einschließlich Risikominderungsmaßnahmen;

e) teilt Informationen darüber, wie die grenzüberschreitende und sektorübergreifende Zusammenarbeit bei der Betrugsbekämpfung im Bereich der Zahlungsdienste verbessert werden kann.

(3) Den Vorsitz der Plattform zur Betrugsbekämpfung führt ein Vertreter der Kommission, und die Plattform wird gemäß den horizontalen Vorschriften für die Einsetzung und Arbeitsweise von Sachverständigengruppen der Kommission eingerichtet.

(4) Die Plattform zur Betrugsbekämpfung erstattet dem Europäischen Parlament und dem Rat jährlich Bericht über ihre Tätigkeiten.

Artikel 90

Zahlungsbetrugsrisiken und -trends

(1) 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. Zahlungsdienstleister geben ihren Kunden klare Leitlinien, wie sie Betrugsversuche erkennen können, und beraten sie zu den Maßnahmen und Vorkehrungen, die sie treffen müssen, um keinen betrügerischen Aktivitäten zum Opfer zu fallen. Die Zahlungsdienstleister informieren ihre Kunden darüber, wo sie betrügerische Aktivitäten melden und in Sachen Betrug schnell Informationen erhalten können.

(2) Die Mitgliedstaaten verfügen über geeignete und mit angemessenen Mitteln ausgestattete Maßnahmen, um die Öffentlichkeit für die Trends und neuen Formen des Zahlungsbetrugs, die Verfahren zur Aufdeckung von Betrugsversuchen und die Rechte und Pflichten, die sich aus dieser Verordnung in Bezug auf Betrug ergeben, zu sensibilisieren. Die Kommunikationsmaßnahmen müssen ausreichend und zielgerichtet sein und insbesondere die schutzbedürftigsten Verbrauchergruppen, einschließlich jüngerer und älterer Menschen und Menschen mit beschränkten digitalen Kompetenzen, erreichen. Die Mitgliedstaaten unterrichten die Kommission über die getroffenen Maßnahmen.

(3) Zahlungsdienstleister, Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen und Anbieter interpersoneller Kommunikationsdienste arbeiten bei den in Absatz 2 genannten Maßnahmen kostenlos mit den Mitgliedstaaten zusammen.

(4) Die Zahlungsdienstleister organisieren für ihre Mitarbeiter, die im Bereich der Konzeption, der Aufrechterhaltung oder des Angebots von Zahlungsdiensten tätig sind, mindestens jährlich Schulungsprogramme zu den Risiken und Trends in Sachen Zahlungsbetrug und stellen sicher, dass ihre Mitarbeiter ordnungsgemäß ausgebildet sind, um ihre Aufgaben und Verantwortlichkeiten gemäß den einschlägigen Sicherheitsrichtlinien und -verfahren zur Minderung und Management von Zahlungsbetrugsrisiken wahrnehmen zu können.

Artikel 91

Starke Kundenauthentifizierung

(1) Ein Zahlungsdienstleister wendet eine starke Kundenauthentifizierung an, wenn der Zahler

a) online auf sein Zahlungskonto zugreift,

b) einen Zahlungsauftrag für einen elektronischen Zahlungsvorgang erteilt,

c) über einen Fernzugang eine andere Handlung vornimmt, die das Risiko von Zahlungsbetrug oder anderem Missbrauch birgt, einschließlich des Auftrags zur Erstellung oder zum Austausch eines tokenisierten Zahlungsinstruments über einen Fernzugang, der Erhöhung seiner Ausgabenobergrenzen gemäß Artikel 52, der Änderung seines Passworts über das Internet oder der Änderung seiner Kontaktinformationen über das Internet.

(2) Zahlungsvorgänge, die vom Zahlungsempfänger ausgelöst werden, unterliegen keiner starken Kundenauthentifizierung, sofern die betreffenden Vorgänge ohne jegliche Interaktion oder Beteiligung des Zahlers ausgelöst werden. Erstattungen, die vom ursprünglichen Zahlungsempfänger zugunsten des ursprünglichen Zahlers für solche Vorgänge veranlasst werden, unterliegen keiner starken Kundenauthentifizierung.

(3) Wird das Mandat des Zahlers an den Zahlungsempfänger zur Erteilung von Zahlungsaufträgen für vom Händler ausgelöste Vorgänge über einen Fernzugang unter Beteiligung des Zahlungsdienstleisters erteilt, so unterliegt die Einrichtung eines solchen Mandats einer starken Kundenauthentifizierung.

(4) Wird bei Lastschriften das Mandat, das der Zahler dem Zahlungsempfänger für die Auslösung einer oder mehrerer Lastschriften erteilt, über einen Fernzugang unter direkter Beteiligung des Zahlungsdienstleisters des Zahlers erteilt, so unterliegt die Einrichtung eines solchen Mandats einer starken Kundenauthentifizierung.

(5) Schriftlich oder telefonisch ausgelöste Vorgänge unterliegen keiner starken Kundenauthentifizierung, sofern der Zahlungsdienstleister des Zahlers Sicherheitsanforderungen und -kontrollen durchführt, die eine Form der Authentifizierung des Zahlungsvorgangs ermöglichen.

(6) Für die Erteilung eines Zahlungsauftrags nach Absatz 1 Buchstabe b aus der Ferne wenden die Zahlungsdienstleister eine starke Kundenauthentifizierung an, die Elemente umfasst, die den Vorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen.

(7) Für die Erteilung eines in Absatz 1 Buchstabe b genannten Zahlungsauftrags über ein Gerät des Zahlers, das Nahbereichstechnik für den Informationsaustausch mit der Infrastruktur des Zahlungsempfängers nutzt, wobei die Authentifizierung der Erteilung die Nutzung des Internets auf dem Gerät des Zahlers erfordert, wenden die Zahlungsdienstleister eine starke Kundenauthentifizierung an, die Elemente, die den Vorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen, oder harmonisierte Sicherheitsmaßnahmen mit gleicher Wirkung umfasst, die die Vertraulichkeit, die Authentizität und die Integrität des Betrags des Vorgangs und des Zahlungsempfängers in allen Phasen der Auslösung gewährleisten.

(8) Für die Zwecke des Absatzes 1 müssen die Zahlungsdienstleister über angemessene Sicherheitsmaßnahmen verfügen, um die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer zu schützen.

(9) Für jegliche Ausnahmen von der Anwendung der starken Kundenauthentifizierung, die nach Artikel 97 von der EBA ausgearbeitet werden, werden eines oder mehrere der folgenden Kriterien herangezogen:

a) das mit dem Dienst verbundene Niveau des Betrugsrisikos, insbesondere auf der Grundlage des Transaktionsüberwachungsmechanismus gemäß Artikel 87;

b) der Betrag des Vorgangs oder dessen Periodizität, oder beide;

c) der für die Ausführung des Vorgangs genutzte Zahlungsweg;

d) ob der Zahler ein Verbraucher ist oder nicht.

Ausnahmen von der Durchführung der starken Kundenauthentifizierung sind nicht obligatorisch. Ein Zahlungsdienstleister, der eine Ausnahme umsetzt, behält stets das Recht zu entscheiden, dass unter den gegebenen Umständen und auf der Grundlage einer Risikobewertung eine starke Kundenauthentifizierung erforderlich ist.

(10) Die in Artikel 3 Nummer 60 genannten mindestens zwei Elemente, die bei der starken Kundenauthentifizierung herangezogen werden, gehören verschiedenen Kategorien an.

Abweichend von Unterabsatz 1 des vorliegenden Absatzes kann ein Zahlungsdienstleister eine starke Kundenauthentifizierung mit zwei Elementen nur aus der Kategorie „Inhärenz“ durchführen, wenn er gegenüber der zuständigen nationalen Behörde nachweist, dass die Unabhängigkeit der beiden Elemente jederzeit vollständig gewahrt ist und das Authentifizierungsverfahren jederzeit ein hohes Maß an Sicherheit gewährleistet.

Die EBA arbeitet bis zum … [18 Monate nach dem Tag des Inkrafttretens dieser Verordnung] gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 Leitlinien dazu aus, wie zu bewerten ist, ob die Unabhängigkeit der beiden Elemente der Kategorie „Inhärenz“ vollständig gewahrt ist.

Artikel 92

Starke Kundenauthentifizierung bei bestimmten Überweisungen

(1) Abweichend von Artikel 91 Absatz 1 Buchstabe b gilt die Pflicht zur Anwendung einer starken Kundenauthentifizierung im Zusammenhang mit einer oder mehreren wiederkehrenden Überweisungen, die vom Zahlungsdienstleister des Zahlers gemäß dem vorliegenden Artikel ausgelöst werden, nicht, wenn alle folgenden Bedingungen erfüllt sind:

a) die Überweisungen werden vom Zahlungsdienstleister des Zahlers auf Antrag des Zahlungsempfängers ausgelöst;

b) der Antrag des Zahlungsempfängers beruht auf einer Vereinbarung zwischen dem Zahler und dem Zahlungsempfänger, in der die Zahlungsbedingungen in Bezug auf die Häufigkeit und die zu zahlenden Beträge festgelegt sind, einschließlich, ob die Beträge variieren können, und der Umstände, unter denen die Beträge variieren können;

c) der Zahler erklärt sich damit einverstanden, dass sein Zahlungsdienstleister die jeweiligen Überweisungen im Einklang mit der unter Buchstabe b des vorliegenden Absatzes genannten Vereinbarung ausführt, und der Abschluss einer solchen Vereinbarung unterliegt einer starken Kundenauthentifizierung;

d) der Zahler muss keine zusätzlichen Maßnahmen ergreifen, um die jeweiligen Überweisungen auszulösen.

(2) Findet Absatz 1 Anwendung, so gelten die Artikel 64, 65 und 66 entsprechend, mit Ausnahme von Artikel 65 Absatz 1 Unterabsatz 4 und von Artikel 66 Absatz 2 Unterabsatz 2.

Artikel 93

Starke Kundenauthentifizierung bei Zahlungsauslöse- und Kontoinformationsdiensten

(1) Artikel 91 Absätze 6, 7 und 10 gelten, wenn Zahlungsvorgänge über einen Zahlungsauslösedienstleister ausgelöst werden. Artikel 91 Absatz 8 gilt auch, wenn Zahlungen über einen Zahlungsauslösedienstleister ausgelöst werden und wenn die Informationen über einen Kontoinformationsdienstleister angefordert werden.

(2) Die kontoführenden Zahlungsdienstleister gestatten Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern, sich auf die Authentifizierungsverfahren zu stützen, die der kontoführende Zahlungsdienstleister dem Zahlungsdienstnutzer gemäß Artikel 91 Absätze 1 und 8 sowie in Fällen, in denen der Zahlungsauslösedienstleister beteiligt ist, gemäß Artikel 91 Absätze 1, 6, 7, 8 und 10 bereitstellt.

(3) Unbeschadet des Absatzes 2 darf der kontoführende Zahlungsdienstleister in dem Falle, dass ein Kontoinformationsdienstleister auf Zahlungskontodaten zugreift, eine starke Kundenauthentifizierung nur beim Erstzugriff des betreffenden Kontoinformationsdienstleisters auf Zahlungskontoinformationen anwenden, jedoch nicht bei weiteren Zugriffen dieses Kontoinformationsdienstleisters auf dieses Zahlungskonto, es sei denn, der kontoführende Zahlungsdienstleister hat berechtigte Gründe für einen Betrugsverdacht.

(4) Die Kontoinformationsdienstleister wenden eine starke Kundenauthentifizierung an, wenn der Zahlungsdienstnutzer über diesen Kontoinformationsdienstleister spätestens 180 Tage nach der letzten starken Kundenauthentifizierung auf die Zahlungskontodaten zugreift. Kontoinformationsdienstleister können ihre eigene oder die starke Kundenauthentifizierung des kontoführenden Zahlungsdienstleisters anwenden.

Artikel 94

Auslagerungsvereinbarungen für die Anwendung der starken Kundenauthentifizierung

Der Zahlungsdienstleister des Zahlers schließt mit dem technischen Dienstleister in Fällen, in denen dieser technische Dienstleister die Elemente der starken Kundenauthentifizierung bereitstellt und überprüft, eine Auslagerungsvereinbarung.

Artikel 95

Barrierefreiheitsanforderungen für die starke Kundenauthentifizierung

(1) Unbeschadet der Barrierefreiheitsanforderungen gemäß der Richtlinie (EU) 2019/882 stellen die Zahlungsdienstleister sicher, dass ihren Kunden, einschließlich Menschen mit Behinderungen, ältere Menschen, Menschen mit begrenzten digitalen Kompetenzen und Menschen ohne Zugang zu digitalen Kanälen oder Zahlungsinstrumenten, mindestens ein auf ihre besondere Situation abgestimmtes Mittel zur Verfügung steht, um eine starke Kundenauthentifizierung kostenlos durchführen zu können. In Fällen, in denen der Zahlungsdienstnutzer um Hilfe bittet oder Unterstützung benötigt, stellt der Zahlungsdienstleister sicher, dass Unterstützung geleistet wird. Diese Anforderung umfasst nicht die Bereitstellung von Geräten für den Zahlungsdienstnutzer. Die Zahlungsdienstleister stellen sicher, dass die Zahlungsdienstnutzer angemessen über die verschiedenen Mittel informiert werden, die ihnen zur Durchführung einer starken Kundenauthentifizierung zur Verfügung stehen.

(2) Die Zahlungsdienstleister dürfen die Durchführung der starken Kundenauthentifizierung nicht von der ausschließlichen Verwendung eines einzigen Authentifizierungsverfahrens abhängig machen und dürfen die Durchführung der starken Kundenauthentifizierung weder explizit noch implizit vom Besitz eines Smartphones oder eines sonstigen intelligenten Geräts abhängig machen, es sei denn, der Zahlungsdienstnutzer hat der Erbringung von Diensten ausschließlich über mobile Anwendungen auf einem solchen Gerät zugestimmt. Die Zahlungsdienstleister entwickeln mehr als ein Verfahren für die Durchführung der starken Kundenauthentifizierung, um der besonderen Situation ihrer Kunden, einschließlich der in Absatz 1 genannten, gerecht zu werden.

Artikel 96

Fairer, angemessener und diskriminierungsfreier Zugang zu mobilen Geräten

(1) Unbeschadet des Artikels 6 Absatz 7 der Verordnung (EU) 2022/1925 gewähren Originalgerätehersteller mobiler Geräte und Anbieter elektronischer Kommunikationsdienste Zahlungsdienstleistern und in ihrem Namen handelnden technischen Dienstleistern zu fairen, angemessenen und diskriminierungsfreien Bedingungen eine wirksame Interoperabilität mit den technischen Merkmalen, die für die Verarbeitung und sichere Ausführung von Zahlungsvorgängen erforderlich sind, wie Hardware- und Softwarefunktionen, und den Zugang zu diesen Merkmalen zum Zwecke der Interoperabilität.

(2) Originalgerätehersteller mobiler Geräte und Anbieter elektronischer Kommunikationsdienste werden nicht daran gehindert, unbedingt erforderliche und verhältnismäßige Maßnahmen zu ergreifen, um sicherzustellen, dass die Interoperabilität die Integrität der von der Interoperabilitätsverpflichtung betroffenen Hardware- und Softwarefunktionen nicht beeinträchtigt, sofern diese Maßnahmen ordnungsgemäß begründet sind.

(3) Zur Anwendung fairer, angemessener und diskriminierungsfreier Bedingungen für eine wirksame Interoperabilität und den Zugang gemäß Absatz 1 veröffentlichen die Originalgerätehersteller mobiler Geräte und die Anbieter elektronischer Kommunikationsdienste die für eine solche wirksame Interoperabilität und einen solchen Zugang geltenden allgemeinen Bedingungen.

Artikel 97

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 91 genannte starke Kundenauthentifizierung,

b) die Ausnahmen von der Anwendung des Artikels 91 Absätze 1, 6 und 7 nach den in Artikel 91 Absatz 9 niedergelegten Kriterien,

c) die Anforderungen, die Sicherheitsmaßnahmen gemäß Artikel 91 Absatz 8 erfüllen müssen, um die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer zu schützen,

d) die gemäß Artikel 94 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 87 genannten Transaktionsüberwachungsmechanismen.

Für die Zwecke von Unterabsatz 1 Buchstabe b wird mit Blick auf die Ausnahme von der Durchführung einer starken Kundenauthentifizierung bei Zahlungsvorgängen auf der Grundlage einer Transaktionsrisikoanalyse in den Entwürfen technischer Regulierungsstandards unter anderem Folgendes festgelegt:

a) die Bedingungen, die erfüllt sein müssen, damit ein elektronischer Fernzahlungsvorgang als risikoarm gilt;

b) die Methodiken und Modelle für die Durchführung der Transaktionsrisikoanalyse;

c) die Kriterien für die Berechnung der Betrugsraten, einschließlich der Verteilung der Betrugsraten zwischen den Zahlungsdienstleistern, die Dienstleistungen zur Ausgabe von Zahlungsinstrumenten sowie Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, oder innerhalb von Zahlungsdienstleistern, die über eine einzige juristische Einheit Dienstleistungen zur Ausgabe von Zahlungsinstrumenten sowie Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen;

d) 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 Geldbetrags 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;

f) der Notwendigkeit eines ausgewogenen Verhältnisses zwischen dem Betrugsrisiko bei einer betreffenden Dienstleistung oder Wirtschaftstätigkeit und dem Nutzererlebnis der Verbraucher, insbesondere im Hinblick auf Vorgänge von geringem Wert;

g) ob es sich bei den Zahlern der Vorgänge um Verbraucher handelt oder nicht.

Die EBA übermittelt der Kommission die in Absatz 1 genannten Entwürfe technischer Regulierungsstandards bis zum … [zwölf Monate nach dem Tag des Inkrafttretens dieser Verordnung].

Der Kommission wird die Befugnis übertragen, diese technischen Regulierungsstandards gemäß 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 aktualisierten Entwürfe technischer Regulierungsstandards regelmäßig und, falls erforderlich, entwickelt sie aktualisierte Entwürfe technischer Regulierungsstandards, 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 europäischen Brieftaschen für die Digitale Identität Rechnung zu tragen.

Kapitel 8

Durchsetzungsverfahren, zuständige Behörden und Sanktionen

ABSCHNITT 1

DURCHSETZUNG IN BEZUG AUF SEHR GROßE ONLINE-PLATTFORMEN UND SEHR GROßE ONLINE-SUCHMASCHINEN

Artikel 98

Durchsetzung der Bestimmungen für sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen

Die Kommission verfügt über ausschließliche Befugnisse zur Überwachung und Durchsetzung von Artikel 61 Absatz 4 Unterabsatz 3 Ziffer iii und Artikel 62, wenn die Pflichten gemäß diesen Bestimmungen für Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen gelten.

Für die Zwecke dieser Überwachung und Durchsetzung gilt Kapitel IV der Verordnung (EU) 2022/2065. Alle darin enthaltenen Bezugnahmen auf die Einhaltung der einschlägigen Bestimmungen der Verordnung (EU) 2022/2065 gelten auch als Bezugnahmen auf Artikel 61 Absatz 4 Unterabsatz 3 Ziffer iii und Artikel 62 der vorliegenden Verordnung, wenn die Pflichten gemäß diesen Bestimmungen für Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen gelten.

Soweit der Kommission gemäß Kapitel IV der Verordnung (EU) 2022/2065 Befugnisse übertragen werden, erstrecken sich diese Befugnisse auch auf die Anwendung von Artikel 61 Absatz 4 Unterabsatz 3 Ziffer iii und Artikel 62 der vorliegenden Verordnung, wenn diese Pflichten für Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen gelten.

ABSCHNITT 2

VERBOT DER ERBRINGUNG VON ZAHLUNGSDIENSTEN

Artikel 99

Verbot der Erbringung von Zahlungsdiensten durch Personen, die keine Zahlungsdienstleister sind

Natürliche oder juristische Personen, die weder zugelassene Zahlungsdienstleister sind noch aufgrund der Anwendung von Artikel 2 Absatz 3 vom Anwendungsbereich dieser Verordnung ausgenommen sind, dürfen keine Zahlungsdienste erbringen.

ABSCHNITT 3

BESCHWERDEVERFAHREN UND UNTERSUCHUNGSBEFUGNISSE

Artikel 100

Beschwerden

(1) Die Mitgliedstaaten richten Verfahren ein, nach denen Zahlungsdienstnutzer und andere interessierte Parteien, einschließlich Verbraucherverbänden, gegen mutmaßliche Verstöße der Zahlungsdienstleister gegen diese Verordnung bei den in Artikel 101 genannten zuständigen Behörden Beschwerden einlegen können.

(2) Sofern zweckmäßig und unbeschadet des Rechts, nach dem nationalen Prozessrecht die Gerichte anzurufen, informieren die zuständigen Behörden den Beschwerdeführer in ihrer Antwort auf die in Absatz 1 des vorliegenden Artikels genannten Beschwerden über die nach Artikel 105 eingerichteten alternativen Streitbeilegungsverfahren.

(3) Bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] gibt die EBA gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 Leitlinien zu den in Absatz 1 genannten Verfahren, insbesondere auch zu den Wegen für die Einreichung von Beschwerden, den von den Beschwerdeführern verlangten Informationen und der Offenlegung der Gesamtanalyse der Beschwerden heraus.

Artikel 101

Zuständige Behörden und Aufsichts- und Untersuchungsbefugnisse

(1) Die Mitgliedstaaten benennen die zuständigen Behörden, die für die Wahrnehmung der in dieser Verordnung vorgesehenen Aufgaben und Befugnisse verantwortlich sind. Die Mitgliedstaaten teilen der EBA und der Kommission diese zuständigen Behörden mit.

Zuständige Behörden sind entweder

a) Behörden oder

b) 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 der Wirtschaft unabhängig sein und Interessenkonflikte vermeiden. Unbeschadet des Unterabsatzes 2 Buchstabe b dürfen Zahlungsinstitute, Kreditinstitute und Postscheckämter nicht als zuständige Behörden benannt werden.

(2) Benennen die Mitgliedstaaten mehr als eine zuständige Behörde nach Absatz 1, so legen sie deren jeweilige Aufgaben fest und benennen eine zuständige Behörde als zentrale Kontaktstelle für die grenzüberschreitende Verwaltungszusammenarbeit zwischen den zuständigen Behörden sowie mit der EBA. Die Mitgliedstaaten können eine gesonderte zentrale Kontaktstelle für jede Art der Verwaltungszusammenarbeit benennen.

(3) Die zuständigen Behörden üben ihre Befugnisse zur Untersuchung potenzieller Verstöße gegen diese Verordnung aus und verhängen im Einklang mit dieser Verordnung Verwaltungsstrafen, Zwangsgelder und andere verwaltungsrechtliche Maßnahmen, die in ihrem nationalen Rechtsrahmen festgelegt sind, auf folgende Art und Weise:

a) unmittelbar,

b) in Zusammenarbeit mit anderen Behörden,

c) durch Übertragung von Befugnissen auf andere Behörden oder Stellen, wobei sie für die Aufsicht über die beauftragten Behörde oder Stelle verantwortlich bleiben,

d) durch Anrufung der zuständigen Justizbehörden.

Übertragen die zuständigen Behörden ihre Befugnisse gemäß Unterabsatz 1 Buchstabe c auf andere Behörden oder Stellen, so werden in dieser Befugnisübertragung die übertragenen Aufgaben und die Bedingungen, unter denen sie auszuführen sind und die Befugnisübertragung widerrufen werden kann, festgelegt. Die Behörden oder Stellen, auf die Befugnisse übertragen werden, sind so zu organisieren, dass Interessenkonflikte vermieden werden. Die zuständigen Behörden überwachen die Tätigkeit der Behörden oder Stellen, denen ihre Befugnisse übertragen werden.

(4) Die zuständigen Behörden treffen alle geeigneten Maßnahmen, um die wirksame Einhaltung dieser Verordnung sicherzustellen und zu überwachen.

(5) Die zuständigen Behörden verfügen über alle Aufsichts- und Untersuchungsbefugnisse sowie über angemessene Ressourcen, die zur Wahrnehmung ihrer Aufgaben erforderlich sind.

Diese Befugnisse umfassen mindestens:

a) im Rahmen der Verfahren zur Untersuchung potenzieller Verstöße gegen diese Verordnung die Befugnis, unter anderem von den folgenden natürlichen oder juristischen Personen sämtliche Informationen zu verlangen, die die zuständigen Behörden zur Wahrnehmung ihrer Aufgaben benötigen:

i) Zahlungsdienstleistern,

ii) technischen Dienstleistern, Betreibern von Zahlverfahren und Zahlungssystembetreibern, die nicht unter die Verordnung (EU) 2025/1355 fallen, unbeschadet der Beaufsichtigung der Tätigkeiten dieser Zahlungssysteme durch das Eurosystem oder die Zentralbanken von Mitgliedstaaten, deren Währung nicht der Euro ist,

iii) Geldautomatenbetreibern, die keine Zahlungskonten führen,

iv) Anbietern interpersoneller Kommunikationsdienste,

v) natürlichen Personen, die den unter den Ziffern i, ii und iii genannten Einrichtungen angehören,

vi) Dritten, an die die unter den Ziffern i, ii und iii genannten Einrichtungen operative Funktionen oder Tätigkeiten ausgelagert haben,

vii) Agenten und Zweigniederlassungen der unter den Ziffern i, ii und iii genannten Einrichtungen, die im Mitgliedstaat der zuständigen Behörde niedergelassen sind,

viii) soweit nach nationalem Recht zulässig, jede andere Person, insbesondere diejenigen, die an der Auslösung, Abwicklung oder Ausführung von Zahlungsdiensten beteiligt sind,

b) die Befugnis, alle erforderlichen Untersuchungen im Hinblick auf jede unter Buchstabe a genannte Person durchzuführen, die im Mitgliedstaat der zuständigen Behörde niedergelassen oder ansässig ist oder dort Dienstleistungen erbringt, 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 Ziffern i bis vii genannten Personen zu prüfen und Kopien oder Auszüge dieser Bücher und Aufzeichnungen anzufertigen,

iii) von jeder der unter Buchstabe a Ziffern i bis vii genannten Personen 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 betreffenden zuständigen Behörden alle erforderlichen Kontrollen in den Geschäftsräumen der juristischen Personen und an anderen Orten als der Privatwohnung der unter Buchstabe a genannten natürlichen Personen durchzuführen,

d) die Befugnis, die Räumlichkeiten natürlicher und juristischer Personen im Einklang mit dem nationalen Recht zu betreten, um Gegenstände, Unterlagen und Daten gleich welcher Form sicherzustellen, wenn ein hinreichender Grund zu der Annahme besteht, dass Gegenstände, Unterlagen oder Daten, die mit dem Gegenstand der Kontrolle oder Untersuchung in einem Zusammenhang stehen, für den Nachweis eines Verstoßes gegen diese Verordnung erforderlich und relevant sein könnten,

e) soweit dies nach nationalem Recht zulässig ist, die Befugnis, bestehende Datenverkehrsaufzeichnungen im Besitz eines Telekommunikationsbetreibers anzufordern, wenn ein hinreichender Grund zu der Annahme eines Verstoßes besteht und wenn diese Aufzeichnungen für die Untersuchung eines Verstoßes gegen diese Verordnung erforderlich sein könnten;

f) die Befugnis, das Einfrieren oder die Sicherung von Vermögenswerten oder beides zu beantragen,

g) die Befugnis, eine Sache zwecks strafrechtlicher Ermittlungen weiterzuverweisen,

h) in Ermangelung anderer verfügbarer Mittel zur Einstellung oder Verhinderung eines Verstoßes gegen diese Verordnung und um die Gefahr eines ernsthaften Schadens für die Interessen der Verbraucher zu vermeiden, soweit dies nach nationalem Recht zulässig ist und gegebenenfalls im Einklang mit Artikel 9 der Verordnung (EU) 2022/2065 steht, die Befugnis, jede der folgenden Maßnahmen zu ergreifen, einschließlich der Aufforderung an Dritte oder eine andere Behörde, diese umzusetzen:

   i) anzuordnen, dass Inhalte von Online-Schnittstellen entfernt werden oder der Zugang zu einer Online-Schnittstelle beschränkt wird oder dass den Verbrauchern beim Zugriff auf die Online-Schnittstelle ein ausdrücklicher Warnhinweis angezeigt wird,

   ii) anzuordnen, dass Hostingdiensteanbieter den Zugang zu einer Online-Schnittstelle löschen oder sperren,

   iii) anzuordnen, dass Register oder Registrierungsstellen für Domänennamen einen vollqualifizierten Domänennamen entfernen und der betreffenden zuständigen Behörde seine Registrierung gestatten;

i) die Befugnis, ein Angebot von Zahlungsdiensten zu untersagen, wenn die zuständigen Behörden feststellen, dass gegen diese Verordnung verstoßen wurde, oder ein hinreichender Grund zu der Annahme besteht, dass ein Verstoß gegen diese Verordnung stattfinden wird,

j) die Befugnis, Marketingmitteilungen auszusetzen oder zu verbieten, wenn ein hinreichender Grund zu der Annahme besteht, dass gegen diese Verordnung verstoßen wurde,

k) die Befugnis, die Erbringung von Zahlungsdiensten zu untersagen, wenn die zuständigen Behörden feststellen, dass gegen diese Verordnung verstoßen wurde,

l) wenn Grund zu der Annahme besteht, dass eine Person Zahlungsdienste ohne die erforderliche Zulassung oder Registrierung erbringt, die Befugnis, die sofortige Einstellung der Tätigkeit ohne vorherige Ankündigung oder Fristsetzung anzuordnen,

m) die Befugnis, Bekanntmachungen zu veröffentlichen.

Erweisen sich die von der zuständigen Behörde für die Zwecke des Unterabsatzes 1 Buchstaben m veröffentlichten Informationen als falsch oder die zugrunde liegenden Umstände als unrichtig, so unterrichtet die zuständige Behörde die Öffentlichkeit in gleicher Weise über diesen Umstand wie zuvor die betreffenden Informationen veröffentlicht wurden.

(6) Die EBA veröffentlicht auf ihrer Website eine Liste der gemäß den Absätzen 1 und 2 benannten zuständigen Behörden.

(7) Sind nach dem Recht eines Mitgliedstaats gemäß Artikel 106 Absätze 1 und 2 strafrechtliche Sanktionen für Verstöße gegen diese Verordnung vorgesehen, 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 aufgrund derlei mutmaßlicher Verstöße und über das Ergebnis solcher Verfahren, einschließlich einer rechtskräftigen Entscheidung, einzuholen;

b) diese Informationen anderen zuständigen Behörden und der EBA bereitzustellen, damit diese ihrer Verpflichtung nachkommen können, für die Zwecke dieser Verordnung untereinander und mit der EBA zusammenzuarbeiten.

(8) Die Durchführung und Ausübung der in diesem Artikel festgelegten Befugnisse müssen verhältnismäßig sein und im Einklang mit dem Unionsrecht und dem nationalen Recht, einschließlich der geltenden Verfahrensgarantien und der Grundsätze der Charta, stehen. Die in Anwendung dieser Verordnung ergriffenen Ermittlungs- und Durchsetzungsmaßnahmen müssen der Art und dem tatsächlichen oder potenziellen Gesamtschaden des Verstoßes angemessen sein.

Artikel 102

Berufsgeheimnis

(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 103 ausgetauschten Informationen unterliegen sowohl aufseiten der Behörde, die die Informationen weitergibt, als auch aufseiten der Behörde, die sie empfängt, der beruflichen Geheimhaltungspflicht.

(3) Die Artikel 53 und 61 der Richtlinie 2013/36/EU sind entsprechend anwendbar.

(4) Der vorliegende Artikel schließt den Informationsaustausch zwischen den zuständigen Behörden und den Steuerbehörden desselben Mitgliedstaats gemäß dem nationalen Recht nicht aus. Stammen die Informationen aus einem anderen Mitgliedstaat, so dürfen sie nur mit ausdrücklicher Zustimmung der zuständigen Behörden, die sie offengelegt haben, auf diese Weise ausgetauscht werden.

Artikel 103

Zuständigkeit und Zusammenarbeit der zuständigen Behörden

(1) Im Falle eines Verstoßes oder mutmaßlichen Verstoßes 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 diesem Falle sind die Behörden des Aufnahmemitgliedstaats zuständig.

(2) Im Falle von Verstößen oder mutmaßlichen Verstößen gegen die Titel II und III durch technische Dienstleister, Betreiber von Zahlverfahren, Zahlungssystembetreiber, abwickelnde Stellen, Geldautomatenbetreiber, 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, einschließlich in grenzüberschreitenden Fällen, arbeiten die zuständigen Behörden untereinander im Einklang mit dem Unionsrecht und dem nationalen Recht zusammen, indem sie Informationen austauschen und die gegenseitige Amtshilfe mit anderen zuständigen Behörden sicherstellen, deren Unterstützung für die wirksame Durchsetzung von verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen benötigt wird.

(4) Die Behörden anderer betroffener Sektoren arbeiten mit den zuständigen Behörden zusammen, damit verwaltungsrechtliche Sanktionen und verwaltungsrechtliche Maßnahmen effektiv durchgesetzt werden.

ABSCHNITT 4

STREITBEILEGUNGSVERFAHREN UND SANKTIONEN

Artikel 104

Streitbeilegung

(1) Die Zahlungsdienstleister schaffen angemessene und wirksame Beschwerdeverfahren und wenden diese an, um Beschwerden von Zahlungsdienstnutzern in Bezug auf die Rechte und Pflichten gemäß den Titeln II und III abzuhelfen. 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 beantworten Beschwerden der Zahlungsdienstnutzer in Papierform oder bei entsprechender Vereinbarung zwischen Zahlungsdienstleister und Zahlungsdienstnutzer auf einem anderen dauerhaften Datenträger. In dieser Antwort, die innerhalb einer angemessenen Frist, spätestens aber innerhalb von 15 Geschäftstagen nach Eingang der Beschwerde zu erfolgen hat, ist auf alle angesprochenen Fragen einzugehen. Kann der Zahlungsdienstleister in Ausnahmefällen aus Gründen, die er nicht zu verantworten hat, nicht innerhalb von 15 Geschäftstagen antworten, so versendet er ein vorläufiges Antwortschreiben, in dem die Gründe für die Verzögerung der Beantwortung der Beschwerde sowie die Frist, innerhalb derer der Zahlungsdienstnutzer die endgültige Antwort erhalten wird, klar angegeben sind. 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 in den Titeln II und III festgelegten Rechte und Pflichten 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 105

Alternative Streitbeilegungsverfahren

(1) Die Mitgliedstaaten richten angemessene, unabhängige, unparteiische, transparente und wirksame alternative Streitbeilegungsverfahren zur Beilegung von Streitigkeiten zwischen Zahlungsdienstnutzern und Zahlungsdienstleistern über die Rechte und Pflichten gemäß den Titeln II und III ein. Diese Verfahren werden nach Maßgabe der einschlägigen Vorschriften des Unionsrechts und des nationalen Rechts und entsprechend den in der Richtlinie 2013/11/EU enthaltenen Qualitätsanforderungen festgelegt, wobei gegebenenfalls auf bestehende Einrichtungen zurückgegriffen wird. Alternative Streitbeilegungsverfahren sind auf Zahlungsdienstleister anwendbar.

(2) Die Teilnahme von Zahlungsdienstleistern an alternativen Streitbeilegungsverfahren für Verbraucher ist verpflichtend, es sei denn, der Mitgliedstaat weist gegenüber der Kommission nach, dass andere Mechanismen gleichermaßen wirksam sind.

(3) Die Absätze 1 und 2 berühren nicht das Recht der Zahlungsdienstnutzer, nach geltendem nationalen Recht ein Verfahren vor einem Gericht zur Anfechtung des strittigen Zahlungsvorgangs der Zahlungsdienstleister einzuleiten.

(4) Die in Absatz 1 genannten Einrichtungen arbeiten bei der Beilegung grenzüberschreitender Streitigkeiten über die die Rechte und Pflichten gemäß den Titeln II und III wirksam zusammen.

(5) Die Mitgliedstaaten benennen im Einklang mit Artikel 18 der Richtlinie 2013/11/EU eine zuständige Behörde, die die in den Artikeln 19 und 20 der genannten Richtlinie festgelegten Aufgaben in Bezug auf AS-Stellen in ihrem Hoheitsgebiet wahrnimmt, die für die Beilegung von Streitigkeiten über die Rechte und Pflichten gemäß den Titeln II und III der vorliegenden Verordnung zuständig sind.

(6) Die in Absatz 5 genannten zuständigen Behörden teilen der Kommission gemäß Artikel 20 der Richtlinie 2013/11/EU mit, welche AS-Stelle(n) in ihrem Hoheitsgebiet für die Beilegung von Streitigkeiten über die Rechte und Pflichten gemäß den Titeln II und III der vorliegenden Verordnung zuständig ist bzw. sind.

(7) Die Kommission macht eine Liste der ihr gemäß Absatz 6 gemeldeten AS-Stellen öffentlich zugänglich und aktualisiert diese Liste jedes Mal, wenn Änderungen mitgeteilt werden.

Die Mitgliedstaaten machen einen Hyperlink zur Website der Kommission, auf der die in Unterabsatz 1 genannten Informationen abrufbar sind, öffentlich zugänglich.

Artikel 106

Verwaltungsrechtliche Sanktionen und verwaltungsrechtliche Maßnahmen

(1) Unbeschadet der Aufsichtsbefugnisse der gemäß der Richtlinie (EU) 2026/…[+] 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 verwaltungsrechtliche Maßnahmen, die bei Verstößen gegen diese Verordnung anwendbar sind, und stellen sicher, dass diese umgesetzt werden. Diese verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Die Mitgliedstaaten können beschließen, für Verstöße gegen diese Verordnung, die Sanktionen nach nationalem Strafrecht unterliegen, keine Vorschriften über verwaltungsrechtliche Sanktionen oder Maßnahmen zu erlassen. In diesen Fällen teilen diese Mitgliedstaaten der Kommission die einschlägigen geltenden strafrechtlichen Bestimmungen und alle nachfolgenden Änderungen dieser Bestimmungen gemäß Artikel 113 mit.

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

(3) Gelten die in Absatz 1 genannten nationalen Vorschriften für Zahlungsdienstleister und andere juristische Personen, so sind im Falle eines Verstoßes und vorbehaltlich der im nationalen Recht festgelegten Bedingungen die verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen auf die Mitglieder des Leitungsorgans der betreffenden Zahlungsdienstleister und juristischen Personen sowie auf andere natürliche Personen anwendbar, die als verantwortlich für einen Verstoß gegen diese Verordnung 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 Befugnis der zuständigen Behörden zum Abschluss von Vergleichsvereinbarungen oder zur Eröffnung von beschleunigten Durchsetzungsverfahren lässt die Pflichten der Mitgliedstaaten nach Absatz 1 unberührt.

Die Absätze 1, 3 und 4 des vorliegenden Artikels gelten für die in Artikel 107 genannten verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen.

Artikel 107

Verwaltungsrechtliche Sanktionen und verwaltungsrechtliche Maßnahmen für bestimmte Verstöße

(1) Unbeschadet des Artikels 106 Absatz 2 regeln die nationalen Rechts- und Verwaltungsvorschriften die in Absatz 2 des vorliegenden Artikels genannten verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen, wenn gegen die folgenden Bestimmungen verstoßen wird:

a) die in Artikel 33 festgelegten Vorschriften für den Zugang zu Konten bei einem Kreditinstitut,

b) die Vorschriften für Kontoinformationsdienste und Zahlungsauslösedienste gemäß Titel III Kapitel 3,

c) die Verpflichtung zur Organisation oder Anwendung von Mechanismen für die Betrugsprävention, einschließlich der starken Kundenauthentifizierung gemäß den Artikeln 91, 93 und 94,

d) die Pflicht zur Erfüllung der Anforderungen an die Gebührentransparenz durch Geldautomatenbetreiber oder andere Bargeldvertriebsstellen gemäß Artikel 20 Absatz 3 Buchstabe b,

e) die Nichteinhaltung der Frist für die Entschädigung der Zahlungsdienstnutzer gemäß Artikel 57 Absatz 2, Artikel 58 Unterabsatz 1, Artikel 60 Absatz 3 und Artikel 66 Absatz 2 durch die Zahlungsdienstleister.

(2) Im Falle der in Absatz 1 genannten Verstöße müssen die anwendbaren verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen Folgendes beinhalten:

a) Geldbußen:

i) bei juristischen Personen mit einem Höchstbetrag von mindestens 10 % des jährlichen Gesamtumsatzes im Sinne des Absatzes 3,

ii) bei natürlichen Personen mit einem Höchstbetrag von mindestens 3 000 000 EUR oder in den Mitgliedstaaten, deren Währung nicht der Euro ist, dem Gegenwert in der Landeswährung am … [Tag des Inkrafttretens dieser Verordnung],

iii) mit einem Höchstbetrag von mindestens dem doppelten Betrag der durch den Verstoß erzielten Gewinne oder vermiedenen Verluste, sofern sich diese Gewinne oder Verluste beziffern lassen, selbst wenn eine solche Geldbuße im Falle juristischer Personen die unter Ziffer i bzw. im Falle natürlicher Personen die unter Ziffer ii festgelegten Höchstbeträge übersteigt,

b) eine öffentliche Bekanntgabe der für den Verstoß verantwortlichen natürlichen oder juristischen Person und der Art des Verstoßes;

c) eine Anordnung, wonach die für den Verstoß verantwortliche natürliche oder juristische Person das rechtswidrige Verhalten abzustellen und künftig davon abzusehen hat;

d) ein vorübergehendes Verbot für jedes Mitglied 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 des vorliegenden Artikels und in Artikel 108 Absatz 1 der vorliegenden Verordnung genannte jährliche Gesamtumsatz entspricht den Nettoumsatzerlösen im Sinne des Artikels 2 Nummer 5 der Richtlinie 2013/34/EU ausweislich des zum letzten Bilanzstichtag verfügbaren Jahresabschlusses, für den die Mitglieder des Verwaltungs-, Leitungs- und Aufsichtsorgans einer 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 Einnahmen ausweislich des zum letzten Bilanzstichtag verfügbaren konsolidierten Abschlusses 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 verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen sowie andere Arten von Sanktionsbefugnissen neben den in Absatz 2 genannten vorzusehen.

Artikel 108

Zwangsgelder

(1) Die zuständigen Behörden sind befugt, bei anhaltenden Verstößen gegen diese Verordnung oder gegen Entscheidungen, die von einer zuständigen Behörde gemäß dieser Verordnung erlassen wurden, Zwangsgelder gegen natürliche oder juristische Personen zu verhängen.

Die Zwangsgelder müssen wirksam und verhältnismäßig sein und einen Betrag beinhalten, der täglich zu entrichten ist, bis die Einhaltung der Vorschriften wiederhergestellt ist. Sie werden für einen Zeitraum von höchstens sechs Monaten ab dem in der Entscheidung über das Zwangsgeld genannten Zeitpunkt verhängt.

Die zuständigen Behörden sind befugt, als Zwangsgelder mindestens bis zu 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 107 Absatz 3 genannten jährlichen Gesamtumsatz, geteilt durch 365. Wird ein Zwangsgeld gegen ein Kreditinstitut verhängt, so entspricht der durchschnittliche Tagesumsatz dem in Artikel 66 Absatz 3 und Artikel 67 Absatz 3 der Richtlinie 2013/36/EU genannten jährlichen Gesamtumsatz, geteilt durch 365.

(2) Die Mitgliedstaaten können höhere als die in Absatz 1 festgelegten Zwangsgelder vorsehen.

Artikel 109

Faktoren, die bei der Festlegung verwaltungsrechtlicher Sanktionen und verwaltungsrechtlicher Maßnahmen zu berücksichtigen sind

(1) Die zuständigen Behörden berücksichtigen alle relevanten Faktoren und Umstände, um sicherzustellen, dass Art und Umfang der verwaltungsrechtlichen Sanktionen oder verwaltungsrechtlichen Maßnahmen, die sie bei Verstößen gegen diese Verordnung verhängen, verhältnismäßig sind, darunter

a) die Schwere und Dauer des Verstoßes,

b) den Grad an Verantwortlichkeit 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 jeweils für den Verstoß verantwortlich ist, ablesen lässt,

d) die Größenordnung der durch den Verstoß von der dafür verantwortlichen natürlichen oder juristischen Person erzielten Gewinne oder vermiedenen Verluste, soweit sie sich bestimmen lassen,

e) die Verluste, die Dritten durch den Verstoß entstanden sind, soweit sie sich bestimmen lassen,

f) die strafrechtlichen Sanktionen, die zuvor aufgrund desselben Verstoßes gegen die für diesen Verstoß verantwortliche natürliche oder juristische Person verhängt wurden,

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) die früheren Verstöße der 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) die Abhilfemaßnahmen oder Handlungen der für den Verstoß verantwortlichen natürlichen oder juristischen Person, die darauf abzielen, eine Wiederholung des Verstoßes zu verhindern.

(2) Zuständige Behörden, die nach Artikel 106 Absatz 4 Vergleichsvereinbarungen oder beschleunigte Durchsetzungsverfahren nutzen, passen die in den Artikeln 106 und 107 festgelegten einschlägigen verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen sowie die in Artikel 108 festgelegten Zwangsgelder an den betreffenden Fall an, um die Verhältnismäßigkeit der verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen sicherzustellen.

Artikel 110

Rechtsbehelf

(1) Gegen die gemäß dieser Verordnung ergangenen Entscheidungen der zuständigen Behörden zur Verhängung von verwaltungsrechtlichen Sanktionen oder verwaltungsrechtlichen Maßnahmen können Rechtsbehelfe eingelegt werden.

(2) Ist nach dieser Verordnung eine Frist festgelegt, innerhalb deren eine zuständige Behörde tätig werden muss, so kann ein Rechtsbehelf eingelegt werden, wenn die Behörde nicht innerhalb dieser Frist tätig wird.

Artikel 111

Öffentliche Bekanntmachung von verwaltungsrechtlichen Sanktionen und verwaltungsrechtlichen Maßnahmen

(1) Die zuständigen Behörden veröffentlichen auf ihrer Website alle Entscheidungen zur Verhängung von verwaltungsrechtlichen Sanktionen oder verwaltungsrechtlichen Maßnahmen gegen juristische und natürliche Personen aufgrund von Verstößen gegen diese Verordnung sowie gegebenenfalls alle Vergleichsvereinbarungen. Die öffentliche Bekanntmachung beinhaltet eine kurze Beschreibung des Verstoßes, der verhängten verwaltungsrechtlichen Sanktion oder verwaltungsrechtlichen Maßnahme oder gegebenenfalls eine Erklärung über die Vergleichsvereinbarung. Ist eine natürliche Person Gegenstand einer Entscheidung, mit der eine verwaltungsrechtliche Sanktion oder verwaltungsrechtliche Maßnahme verhängt wird, oder Partei einer Vergleichsvereinbarung, so wird die Identität dieser natürlichen Person nicht veröffentlicht.

Nachdem die natürliche oder juristische Person, die Gegenstand einer Entscheidung oder Partei einer Vergleichsvereinbarung gemäß Unterabsatz 1 ist, von der betreffenden Entscheidung in Kenntnis gesetzt bzw. die Vergleichsvereinbarung unterzeichnet wurde, veröffentlichen die zuständigen Behörden umgehend die Entscheidung oder die Vergleichsvereinbarung.

(2) Abweichend von Absatz 1 des vorliegenden Artikels kann die zuständige nationale Behörde in Fällen, in denen sie 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 107 Absatz 2 Buchstabe b genannten öffentlichen Bekanntgaben oder in Artikel 107 Absatz 2 Buchstabe d genannten vorübergehenden Verboten –, die Identität der Personen oder andere personenbezogene Daten veröffentlichen, sofern sie diese Entscheidung begründet und sich die öffentliche Bekanntmachung auf die personenbezogenen Daten beschränkt, die zwingend erforderlich sind, um die Stabilität der Finanzmärkte zu schützen oder die wirksame Durchsetzung dieser Verordnung zu gewährleisten.

(3) Wird die Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion oder verwaltungsrechtlichen Maßnahme vor der einschlägigen Justiz- oder einer sonstigen Behörde angefochten, veröffentlichen die zuständigen Behörden auch die Informationen über diese Anfechtung und alle weiteren Informationen über das Ergebnis der Anfechtung unverzüglich auf ihrer offiziellen Website, soweit juristische Personen davon betroffen sind. Betrifft die angefochtene Entscheidung eine natürliche Person und kommt die abweichende Regelung nach Absatz 2 nicht zur Anwendung, so 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 mindestens fünf Jahre lang auf ihren offiziellen Websites verbleiben. Enthält die öffentliche Bekanntmachung personenbezogene Daten, so bleiben diese nur so lange auf der offiziellen Website einer zuständigen Behörde einsehbar, wie dies nach den geltenden Datenschutzbestimmungen erforderlich ist.

Artikel 112

Überwachung von Verfahren, Sanktionen und Maßnahmen

(1) Die zuständigen Behörden melden der EBA anonymisiert und in aggregierter Form regelmäßig

a) die eingeleiteten, ausgesetzten oder abgeschlossenen Verwaltungsverfahren, die zur Verhängung von verwaltungsrechtlichen Sanktionen oder verwaltungsrechtlichen Maßnahmen aufgrund von Verstößen gegen diese Verordnung geführt haben,

b) die Zwangsgelder, die gemäß Artikel 108 aufgrund laufender Verstöße gegen diese Verordnung verhängt worden sind,

c) falls anwendbar, die Vergleichsvereinbarungen und beschleunigten Durchsetzungsverfahren sowie deren Ergebnis, unabhängig von ihrer öffentlichen Bekanntmachung, gemäß Artikel 106 Absatz 4,

d) die von den Justizbehörden gemäß Artikel 101 Absatz 7 Buchstabe a gemeldeten strafrechtlichen Verfahren, die zu einer Verurteilung geführt haben, und die damit verbundenen Sanktionen,

e) etwaige Anfechtungen von Entscheidungen zur Verhängung von strafrechtlichen oder verwaltungsrechtlichen Sanktionen oder verwaltungsrechtlichen Maßnahmen für Verstöße gegen diese Verordnung und das Ergebnis einer solchen Anfechtung.

(2) Macht die zuständige Behörde eine verwaltungsrechtliche Sanktion oder eine verwaltungsrechtliche Maßnahme gemäß Artikel 111 öffentlich bekannt, so meldet sie diese gleichzeitig der EBA.

(3) Bis zum … [45 Monate nach dem Tag des Inkrafttretens dieser Verordnung] und danach 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 113

Mitteilung der Durchführungsmaßnahmen

Die Mitgliedstaaten teilen der Kommission bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die Rechts- und Verwaltungsvorschriften, einschließlich aller einschlägigen strafrechtlichen Bestimmungen, mit, die sie gemäß diesem Kapitel erlassen haben. Sie teilen der Kommission alle nachfolgenden Änderungen dieser Vorschriften sowie alle Rechts- und Verwaltungsvorschriften, die sie zu einem späteren Zeitpunkt nach diesem Kapitel erlassen, umgehend mit.

Kapitel 9

Produktinterventionsbefugnisse der EBA

Artikel 114

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 ein bestimmtes Merkmal eines solchen Dienstes oder Instruments in der Union vorübergehend verbieten oder beschränken. Ein solches Verbot oder eine solche Beschränkung kann in von der EBA festgelegten Fällen zur Anwendung kommen oder von der EBA festgelegten Ausnahmen unterliegen.

(2) Die EBA fasst einen Beschluss nach Absatz 1 nur dann, wenn alle folgenden Bedingungen erfüllt sind:

a) die vorgeschlagene Maßnahme richtet sich an eine signifikante Zahl von Zahlungsdienstnutzern oder gegen eine Bedrohung für die geordnete Funktionsweise oder die Integrität der Zahlungs- oder E-Geld-Märkte oder die Stabilität dieser Märkte oder eines Teils dieser Märkte in der Union;

b) die nach dem Unionsrecht auf den jeweiligen Zahlungsdienst 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 des vorliegenden Absatzes genannten Bedingungen erfüllt, kann die EBA das in Absatz 1 genannte Verbot oder die in Absatz 1 genannte Beschränkung vorsorglich verhängen, bevor ein Zahlungsdienst angeboten oder an Zahlungsdienstnutzer vertrieben wird.

(3) Bei Maßnahmen gemäß diesem Artikel stellt die EBA sicher, dass:

a) die Maßnahme keine nachteiligen Auswirkungen auf die Effizienz des Zahlungsmarkts oder des E-Geld-Markts oder auf Zahlungsdienstleister hat, die gemessen am Nutzen der Maßnahme unverhältnismäßig sind,

b) die Maßnahme kein Risiko der Aufsichtsarbitrage schafft, und

c) die Maßnahme nach Konsultationen der jeweils zuständigen nationalen Behörde ergriffen wurde.

(4) Bevor die EBA beschließt, Maßnahmen nach diesem Artikel zu ergreifen, unterrichtet sie die jeweils zuständigen Behörden über die von ihr vorgeschlagene Maßnahme.

(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 nach der Bekanntmachung anzugeben, ab dem die Maßnahmen 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 eine Handlung, die nach Wirksamwerden der Maßnahmen vorgenommen wird.

(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 nicht alle drei Monate verlängert, endet die Gültigkeit.

(7) Eine gemäß diesem Artikel beschlossene Maßnahme der EBA geht allen etwaigen früheren Maßnahmen einer zuständigen Behörde vor.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 115 delegierte Rechtsakte zu erlassen, um diese Verordnung durch die Festlegung der Kriterien und Faktoren zu ergänzen, die von der EBA zu berücksichtigen sind, wenn diese ermittelt, ob eine signifikante Zahl von Zahlungsdienstnutzern oder eine Bedrohung für die geordnete Funktionsweise oder die Integrität der Zahlungs- oder E-Geld-Märkte oder die Stabilität dieser Märkte oder eines Teils dieser Märkte in der Union vorliegt.

Zu den Kriterien und Faktoren, die in von der Kommission erlassenen delegierten Rechtsakten festgelegt werden, gehören:

a) der Komplexitätsgrad eines Zahlungsdienstes oder -instruments und der Bezug zu der Art von Nutzern, einschließlich Verbrauchern, denen sie angeboten werden,

b) der Risikogehalt eines Zahlungsdienstes oder -instruments für die Verbraucher,

c) die mögliche Nutzung des Zahlungsdienstes oder -instruments durch Betrüger,

d) die Größenordnung oder der Grad der Nutzung des Zahlungsdienstes oder -instruments,

e) der Innovationsgehalt eines Zahlungsdienstes oder -instruments.

TITEL IV
DELEGIERTE RECHTSAKTE

Artikel 115

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 den Artikeln 32, 63, 71 und 114 wird der Kommission auf unbestimmte Zeit ab dem … [Tag des Inkrafttretens dieser Verordnung] übertragen.

(3) Die Befugnisübertragung gemäß den Artikeln 32, 63, 71 und 114 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 über den Widerruf 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 den Artikeln 32, 63, 71 und 114 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 116

Günstigere Erstattungsansprüche und strengere Betrugsbekämpfungsmaßnahmen

(1) Die Mitgliedstaaten oder Zahlungsdienstleister können den Zahlungsdienstnutzern günstigere Erstattungsansprüche für autorisierte Überweisungen im Sinne der Artikel 58 und 60 einräumen und strengere Betrugsbekämpfungsmaßnahmen vorsehen, die über die in Artikel 87 Absatz 1 und Artikel 90 festgelegten hinausgehen.

(2) Die Mitgliedstaaten teilen der Kommission bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] die gesetzlichen Bestimmungen mit, die sie nach Absatz 1 erlassen. Sie teilen der Kommission alle nachfolgenden Änderungen dieser gesetzlichen Bestimmungen sowie alle gesetzlichen Bestimmungen, die sie zu einem späteren Zeitpunkt nach Absatz 1 erlassen, umgehend mit.

Artikel 117

Überprüfungsklausel

(1) Die Kommission legt dem Europäischen Parlament, dem Rat, der EZB und dem Europäischen Wirtschafts- und Sozialausschuss bis zum … [18 Monate nach dem Tag des Inkrafttretens dieser Verordnung] einen Bericht über die Praktiken bei Kartenzahlverfahren, abwickelnden Stellen, Zahlungsdienstleistern, die Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, und insbesondere über Folgendes vor:

a) die Entwicklung ihrer Gebühren im Europäischen Wirtschaftsraum (EWR), einschließlich:

i) der Gebühren, die die Kartenzahlverfahren und abwickelnden Stellen den Zahlungsdienstleistern, die Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, berechnen, aufgeschlüsselt nach wichtigen Transaktionskategorien, je Mitgliedstaat;

ii) der Gebühren, die die Zahlungsdienstleister, die Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, den gewerblichen Zahlungsdienstnutzern berechnen;

b) der Bedingungen für die Anwendung neuer Vorschriften und die damit verbundenen Gebühren, wie z. B. der Fristen für die Mitteilung dieser Vorschriften und Gebühren durch die Kartenzahlverfahren und abwickelnden Stellen;

c) der Kommunikation der Kartenzahlverfahren an die Zahlungsdienstleister, die Dienstleistungen zur Annahme und Abrechnung von Zahlungsvorgängen erbringen, und an die abwickelnden Stellen in Bezug auf die Vorschriften und Gebühren sowie den Zeitplan für deren Umsetzung;

d) der Fähigkeit der Emittenten und Erwerber, über die von den Kartenzahlverfahren vorgeschlagenen Vorschriften und Gebühren zu verhandeln;

e) des Wettbewerbsverhaltens der Kartenzahlverfahren auf den Erwerbs- und Ausgabemärkten.

Gegebenenfalls fügt die Kommission diesem Bericht einen Gesetzgebungsvorschlag bei.

Eine nichtvertrauliche Fassung des Berichts, einschließlich aggregierter Informationen über die Gebührenentwicklung, wird der Öffentlichkeit zugänglich gemacht.

(2) Die Kommission legt dem Europäischen Parlament, dem Rat, der EZB und dem Europäischen Wirtschafts- und Sozialausschuss bis zum … [drei Jahre nach dem Tag des Inkrafttretens dieser Verordnung] einen Bericht zur Bewertung folgender Aspekte vor:

a) des Anwendungsbereichs dieser Verordnung, insbesondere im Hinblick auf Zahlungssysteme, Zahlverfahren und technische Dienstleister;

b) ob es angesichts der von virtuellen IBANs ausgehenden Risiken und Herausforderungen, einschließlich aus der Perspektive der Strafverfolgung zur Bekämpfung von Geldwäsche oder Terrorismusfinanzierung, und ihrer Vorteile erforderlich ist, weitere Maßnahmen zur Regulierung virtueller IBANs auf Unionsebene einzuführen;

c) der Angemessenheit und der Auswirkungen der in den Titeln II und III dieser Verordnung festgelegten Vorschriften in Bezug auf Zahlungsvorgänge mit E-Geld-Token;

d) ob es angesichts der Entwicklungen wünschenswert ist, die Anforderungen dieser Verordnung in Bezug auf die Überprüfung des Zahlungsempfängers und das Open Banking auf Zahlungsvorgänge mit E-Geld-Token anzuwenden.

Gegebenenfalls fügt die Kommission diesem Bericht einen Gesetzgebungsvorschlag bei.

(3) Die Kommission legt dem Europäischen Parlament, dem Rat, der EZB und dem Europäischen Wirtschafts- und Sozialausschuss bis zum … [fünf Jahre nach dem Tag des Inkrafttretens dieser Verordnung] einen Bericht zur Überprüfung folgender Aspekte vor:

a) der Auswirkungen der in Artikel 28 enthaltenen Bestimmungen über Aufschläge, einschließlich der Wirkungen auf die Verbraucher, die Händler und den Wettbewerb, mit einer Einschätzung, ob eine weitere Harmonisierung erforderlich ist; und

b) der Auswirkungen der von den Betreibern von Zahlverfahren oder von Zahlungsdienstleistern verwalteten Erstattungsmechanismen, die für vom Zahlungsempfänger ausgelöste Zahlungsvorgänge, mit Ausnahme von Lastschriften, gelten, sowie die Wirkungen dieser Erstattungsmechanismen auf die Verbraucher, die Händler und den Wettbewerb;

c) der Auswirkungen der in Artikel 61 enthaltenen Bestimmungen in Bezug auf die Verpflichtungen, die den Anbietern interpersoneller Kommunikationsdienste auferlegt werden, insbesondere ob diese Verpflichtungen die Wirksamkeit der Zusammenarbeit zwischen den Anbietern interpersoneller Kommunikationsdienste und den Zahlungsdienstleistern gemäß Artikel 61 verbessern;

d) der Auswirkungen der in Artikel 61 enthaltenen Bestimmungen in Bezug auf die Verpflichtungen, die den Hostingdiensteanbietern und den Anbietern sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen auferlegt werden, insbesondere ob diese Verpflichtungen die Wirksamkeit der Zusammenarbeit zwischen den Hostingdiensteanbietern und den Zahlungsdienstleistern gemäß den Artikeln 61 und 62 und das Recht der Zahlungsdienstleister auf Abhilfe gemäß Artikel 82 verbessern.

Auf der Grundlage der in Unterabsatz 1 Buchstaben c und d genannten Bewertungen legt die Kommission fest, ob es erforderlich ist, weitere Maßnahmen zur Regelung der Beteiligung der Anbieter elektronischer Kommunikationsdienste, der Hostingdiensteanbieter, der Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen sowie der Zahlungsdienstleister an der Sicherheit von Zahlungsvorgängen auf Unionsebene einzuführen.

Gegebenenfalls fügt die Kommission diesem Bericht einen Gesetzgebungsvorschlag bei.

(4) Die Kommission legt dem Europäischen Parlament, dem Rat, der EZB und dem Europäischen Wirtschafts- und Sozialausschuss bis zum … [sieben Jahre nach dem Tag des Inkrafttretens dieser Verordnung] 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 über die Geschäftstätigkeit von Kontoinformationsdiensten und Zahlungsauslösediensten und insbesondere der Vorschriften über dedizierte Schnittstellen und der zugehörigen Ausnahmeregelungen gemäß den Artikeln 39 und 40 auf den Wettbewerb und die Nutzung von Open Banking;

b) die Auswirkungen der Vorschriften nach Artikel 35, wonach der Zugang von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern zu Schnittstellen ohne vertragliche Vereinbarung und kostenfrei möglich sein muss;

c) die Angemessenheit und die Auswirkungen der Vorschriften über die Betrugsprävention und die Abhilfe bei Betrug im Falle sowohl autorisierter als auch nicht autorisierter Zahlungsvorgänge unter Berücksichtigung der Arten und Trends betrügerischen Verhaltens;

d) die Angemessenheit und die Auswirkungen der Vorschriften über das Ausmaß der Situationen, in denen ein Verbraucher nach Artikel 60 ein Recht auf Erstattung autorisierter Zahlungsvorgänge hat.

Gegebenenfalls fügt die Kommission diesem Bericht einen Gesetzgebungsvorschlag bei.

Artikel 118

Übergangsbestimmungen

Abweichend von der Richtlinie (EU) 2015/2366 gilt bis zum … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung] Folgendes:

a) die folgenden Zahlungsvorgänge sind von der Anwendung der Richtlinie (EU) 2015/2366 ausgenommen:

   i) Zahlungsvorgänge, die ohne zwischengeschaltete Stellen ausschließlich mit E-Geld-Token unmittelbar vom Zahler an den Zahlungsempfänger erfolgen;

   ii) Zahlungsvorgänge, die von einem Anbieter von Kryptowerte-Dienstleistungen ausgeführt werden, der zwischen einem Käufer und einem Verkäufer vermittelt, wenn E-Geld-Token im Tausch gegen andere E-Geld-Token oder Kryptowerte entgegengenommen werden, sowie der Tausch von E-Geld-Token gegen Geldbeträge, einschließlich E-Geld-Token, oder gegen Kryptowerte, die von einem Anbieter von Kryptowerte-Dienstleistungen durchgeführt wird, der im eigenen Namen als Käufer oder Verkäufer dieser E-Geld-Token handelt;

   iii) Zahlungsvorgänge, die zwischen Anbietern von Kryptowerte-Dienstleistungen oder ihren Zweigniederlassungen auf eigene Rechnung ausgeführt werden;

b) in Bezug auf Zahlungsvorgänge mit E-Geld-Token, die über den Distributed Ledger abgewickelt werden, teilen die Zahlungsdienstleister in Fällen, in denen sie aufgrund von ihnen nicht zuzurechnenden Umständen nicht in der Lage sind, den in Artikel 45 Absatz 1 Buchstaben b und c, Artikel 52 Absatz 2 Buchstabe e, Artikel 52 Absatz 3 Buchstabe a und Artikel 56 der Richtlinie (EU) 2015/2366 festgelegten Pflichten nachzukommen, die darin genannten Informationen so bald wie möglich, in jedem Fall aber vor der Autorisierung des Vorgangs durch den Zahler, in Form einer begründeten Schätzung mit;

c) Zahlungsdienstleister sind nicht verpflichtet, Artikel 66 Absatz 4 und Artikel 67 Absatz 3 der Richtlinie (EU) 2015/2366 in Bezug auf Zahlungsvorgänge mit E-Geld-Token anzuwenden.

Artikel 119

Änderung der Verordnung (EU) Nr. 1093/2010

Die Verordnung (EU) Nr. 1093/2010 wird wie folgt geändert:

1. Artikel 1 Absatz 2 erhält folgende Fassung:

„(2) Die Behörde handelt im Rahmen der ihr durch diese Verordnung übertragenen Befugnisse und innerhalb des Anwendungsbereichs der Richtlinie 2002/87/EG, der Richtlinie 2009/110/EG, der Verordnung (EU) Nr. 575/2013*, der Richtlinie 2013/36/EU**, der Richtlinie 2014/49/EU***, der Richtlinie 2014/92/EU****, der Verordnung (EU) 2023/1114*****, der Richtlinie (EU) 2023/2225******, der Richtlinie (EU) 2026/…*******, der Verordnung (EU) 2026/…******** 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. Die Behörde handelt ferner im Einklang mit der Verordnung (EU) Nr. 1024/2013 des Rates*********.

---

* Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1, ELI: http://data.europa.eu/eli/reg/2013/575/oj).

** 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, 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, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

*** Richtlinie 2014/49/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über Einlagensicherungssysteme (ABl. L 173 vom 12.6.2014, S. 149, ELI: http://data.europa.eu/eli/dir/2014/49/oj).

**** Richtlinie 2014/92/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten und den Zugang zu Zahlungskonten mit grundlegenden Funktionen (ABl. L 257 vom 28.8.2014, S. 214, ELI: http://data.europa.eu/eli/dir/2014/92/oj).

***** Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (ABl. L 150 vom 9.6.2023, S. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

****** Richtlinie (EU) 2023/2225 des Europäischen Parlaments und des Rates vom 18. Oktober 2023 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 2008/48/EG (ABl. L, 2023/2225, 30.10.2023, ELI: http://data.europa.eu/eli/dir/2023/2225/oj).

******* Richtlinie (EU) 2026/… des Europäischen Parlaments und des Rates vom … über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinie 98/26/EG und der Verordnung (EU) 2023/1114 sowie zur Aufhebung der Richtlinien 2009/110/EG und (EU) 2015/2366 (ABl. L …, ELI: …)+.

******** Verordnung (EU) 2026/… des Europäischen Parlaments und des Rates vom … über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 260/2012, (EU) 2017/2394 und (EU) 2021/1230 (ABl. L …, ELI: …)++.

********* Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank (ABl. L 287 vom 29.10.2013, S. 63, ELI: http://data.europa.eu/eli/reg/2013/1024/oj).“

+ ABl.: Bitte die Angaben zur in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

++ ABl.: Bitte die Angaben zur vorliegenden Verordnung einfügen.

2. Artikel 4 Nummer 2 wird wie folgt geändert:

a) Ziffer i erhält folgende Fassung:

„i) 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 vi, vii und viii werden gestrichen.

Artikel 120

Änderungen der Verordnung (EU) Nr. 260/2012

Die Verordnung (EU) Nr. 260/2012 wird wie folgt geändert:

1. In Artikel 2 wird folgende Nummer eingefügt:

„15a. ‚virtuelle IBAN‘ eine Nummer, die die unter Nummer 15 genannten, durch die ISO spezifizierten Elemente enthält und durch die Zahlungen auf ein Zahlungskonto umgeleitet werden, das durch eine IBAN, die nicht dieser Nummer entspricht, identifiziert wird;“

2. Folgender Artikel wird eingefügt:

„*Artikel 2a*
Identifikator für Zahlungskonten

Für die Zwecke dieser Verordnung gilt eine virtuelle IBAN als gültiger Identifikator für Zahlungskonten, wenn die Verwendung einer IBAN erforderlich ist.“

3. in Artikel 5c erhalten die Absätze 5 und 6 folgende Fassung:

„(5) Unbeschadet von Absatz 6 Unterabsatz 3 stellen die Zahlungsdienstleister sicher, dass die Erbringung der Empfängerüberprüfung und der unter Absatz 2 beschriebenen Dienstleistung den Zahler nicht daran hindern, die betreffende Überweisung zu autorisieren.

(6) Die Zahlungsdienstleister ermöglichen Zahlungsdienstnutzern, bei denen es sich nicht um Verbraucher handelt, auf die Empfängerüberprüfung zu verzichten, wenn sie Zahlungsaufträge über Zahlungsauslösekanäle einreichen, die auf automatisierten dedizierten Prozessen oder Protokollen beruhen und nur Zahlungsdienstnutzern zur Verfügung gestellt werden, bei denen es sich nicht um Verbraucher handelt.

Die Zahlungsdienstleister stellen sicher, dass Zahlungsdienstnutzer, bei denen es sich nicht um Verbraucher handelt und die auf die Empfängerüberprüfung verzichtet haben, jederzeit das Recht haben, diese Dienstleistung wieder in Anspruch zu nehmen.

Im Falle von Zahlungsaufträgen, die über die in Unterabsatz 1 genannten Zahlungsauslösekanäle eingereicht werden, einschließlich mehrerer, als Bündel eingereichter Zahlungsaufträge, bieten die Zahlungsdienstleister Zahlungsdienstnutzern, bei denen es sich nicht um Verbraucher handelt, die Möglichkeit, im Rahmenvertrag zu vereinbaren, dass

a) die Empfängerüberprüfung nach der Autorisierung dieser Zahlungsaufträge erbracht wird und

b) der Zahlungsdienstleister des Zahlers diese Zahlungsaufträge ohne weitere Eingaben des Zahlungsdienstnutzers nur in einem oder mehreren der folgenden Fälle ausführt:

   i) aus den Informationen, die der Zahlungsdienstleister des Zahlers vom Zahlungsdienstleister des Zahlungsempfängers erhalten hat, geht hervor, dass der vom Zahler angegebene Name des Zahlungsempfängers mit dem unter Nummer 1 Buchstabe a des Anhangs genannten Identifikator für Zahlungskonten übereinstimmt;

   ii) aus den Informationen, die der Zahlungsdienstleister des Zahlers vom Zahlungsdienstleister des Zahlungsempfängers erhalten hat, geht hervor, dass der vom Zahler angegebene Name des Zahlungsempfängers nahezu mit dem unter Nummer 1 Buchstabe a des Anhangs genannten Identifikator für Zahlungskonten übereinstimmt;

   iii) die Empfängerüberprüfung kann aus technischen Gründen nicht erbracht werden.

Die Möglichkeit für den Zahlungsdienstnutzer, bei dem es sich nicht um einen Verbraucher handelt, vertraglich zu vereinbaren, dass der Zahlungsdienstleister des Zahlers Zahlungsaufträge gemäß Unterabsatz 3 ausführt, gilt unbeschadet der Anforderung in Absatz 1 Buchstabe a, dass der Zahlungsdienstleister des Zahlers in den Fällen, in denen der vom Zahler angegebene Name des Zahlungsempfängers nahezu mit dem unter Nummer 1 Buchstabe a des Anhangs genannten, vom Zahler angegebenen Identifikator des Zahlungskontos übereinstimmt, dem Zahler den mit diesem Identifikator für Zahlungskonten verbundenen Namen des Zahlungsempfängers mitteilt.

Führt der Zahlungsdienstleister des Zahlers die Zahlungsaufträge im Einklang mit dem Rahmenvertrag gemäß Unterabsatz 3 aus, so wird dieser Zahlungsdienstleister für die Zwecke des Absatzes 8 nicht dafür haftbar gemacht, dass er der Verpflichtung, die Empfängerüberprüfung anzubieten, nicht nachgekommen ist.“

Artikel 121

Änderung der Verordnung (EU) 2017/2394

Im Anhang der Verordnung (EU) 2017/2394 wird folgende Nummer angefügt:

„31. Verordnung (EU) 2026/… des Europäischen Parlaments und des Rates vom … über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 260/2012, (EU) 2017/2394 und (EU) 2021/1230 (ABl. L …, ELI: …)[+].“

[+] ABl.: Bitte die Angaben zur vorliegenden Verordnung einfügen.

Artikel 122

Änderungen der Verordnung (EU) 2021/1230

Die Verordnung (EU) Nr. 2021/1230 wird wie folgt geändert:

1. Artikel 4 Absatz 1 erhält folgende Fassung:

„(1) In Bezug auf die Informationspflichten im Hinblick auf Währungsumrechnungsentgelte und den anwendbaren Wechselkurs gemäß Artikel 5 Absatz 2, Artikel 13 Absatz 1 und Artikel 20 Absatz 3 der Verordnung (EU) 2026/… des Europäischen Parlaments und des Rates[*+] drücken Zahlungsdienstleister und Parteien, die Währungsumrechnungen an einem Geldautomaten oder an der Verkaufsstelle gemäß Artikel 5 Absatz 2 der genannten Verordnung erbringen, die gesamten Währungsumrechnungsentgelte als monetärer Betrag in der Währung des Kontos des Zahlers und als prozentualen Aufschlag auf den aggregierten durchschnittlichen Devisenmarktkurs nach Artikel 5 Absatz 3 der genannten Verordnung aus. Dieser Aufschlag und alle sonstigen anfallenden Gebühren sind dem Zahler vor Auslösung des Zahlungsvorgangs offenzulegen.

---

[*] Verordnung (EU) 2026/… des Europäischen Parlaments und des Rates vom … über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 260/2012, (EU) 2017/2394 und (EU) 2021/1230 (ABl. L …, ELI: …)[++].“

[+] ABl.: Bitte die Nummer der vorliegenden Verordnung einfügen.

[++] ABl.: Bitte die Angaben zur vorliegenden Verordnung einfügen.

2. Artikel 5 Absatz 1 erhält folgende Fassung:

„(1) Wird eine Währungsumrechnung vom Zahlungsdienstleister des Zahlers im Zusammenhang mit einer Überweisung im Sinne von Artikel 3 Nummer 53 der Verordnung (EU) 2026/…[+] angeboten, die direkt online über die Website oder über die mobile Banking-Anwendung des Zahlungsdienstleisters ausgelöst wird, so informiert der Zahlungsdienstleister den Zahler im Hinblick auf Artikel 13 Absatz 1 und Artikel 20 Absatz 3 der genannten Verordnung vor Auslösung des Zahlungsvorgangs in einer klaren, neutralen und verständlichen Weise über die geschätzten Währungsumrechnungsentgelte und alle sonstigen anfallenden Gebühren, die für die Überweisung gelten. Die geschätzten Entgelte für die Währungsumrechnung im Zusammenhang mit Überweisungen werden als monetärer Betrag in der Währung des Kontos des Zahlers und als prozentualer Aufschlag auf den aggregierten durchschnittlichen Devisenmarktkurs nach Artikel 5 Absatz 3 der genannten Verordnung ausgedrückt.“

Artikel 123

Entsprechungstabelle

Bezugnahmen auf die Richtlinien 2009/110/EG und (EU) 2015/2366 gelten als Bezugnahmen auf die Richtlinie (EU) 2026/…[++] oder die vorliegende Verordnung und sind nach Maßgabe der Entsprechungstabelle im Anhang der vorliegenden Verordnung zu lesen.

[+] ABl.: Bitte die Nummer der vorliegenden Verordnung einfügen.

[++] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

Artikel 124

Inkrafttreten und Geltungsbeginn

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem … [21 Monate nach dem Tag des Inkrafttretens dieser Verordnung].

Die Artikel 51 und 58 gelten jedoch ab dem … [27 Monate nach dem Tag des Inkrafttretens dieser Verordnung].

Die Artikel 92 und 118 gelten ab dem … [Tag des Inkrafttretens dieser Verordnung].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu … am …

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident/Die Präsidentin	*Der Präsident/Die Präsidentin*

ANHANG

Entsprechungstabelle

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 1 Absatz 1	Artikel 1 Absatz 1	–	Artikel 2 Absatz 1
Artikel 1 Absatz 1 Buchstabe a	Artikel 1 Absatz 1 Buchstabe a	–	Artikel 2 Absatz 1 Buchstabe a
Artikel 1 Absatz 1 Buchstabe b	Artikel 1 Absatz 1 Buchstabe b	–	–
Artikel 1 Absatz 1 Buchstabe c	Artikel 1 Absatz 1 Buchstabe c	–	Artikel 2 Absatz 1 Buchstabe b
Artikel 1 Absatz 1 Buchstabe d	–	–	Artikel 2 Absatz 1 Buchstabe c
Artikel 1 Absatz 1 Buchstabe e	Artikel 1 Absatz 1 Buchstabe d	–	Artikel 2 Absatz 1 Buchstabe d
Artikel 1 Absatz 1 Buchstabe f	Artikel 1 Absatz 1 Buchstabe e	–	Artikel 2 Absatz 1 Buchstabe e
–	Artikel 1 Absatz 2	Artikel 1 Absatz 1	–
–	Artikel 1 Absatz 3	Artikel 1 Absatz 2	–
Artikel 1 Absatz 2	–	–	Artikel 1 Absatz 1
Artikel 2 Absatz 1	–	–	Artikel 2 Absatz 1
Artikel 2 Absatz 2	–	–	Artikel 2 Absatz 4
Artikel 2 Absatz 3	–	–	Artikel 2 Absatz 5
Artikel 2 Absatz 4	–	–	Artikel 2 Absatz 6
Artikel 2 Absatz 5	–	–	Artikel 2 Absatz 7
Artikel 3 Buchstabe a	–	–	Artikel 2 Absatz 3 Buchstabe a
Artikel 3 Buchstabe b	–	–	Artikel 2 Absatz 3 Buchstabe c
Artikel 3 Buchstabe c	–	–	Artikel 2 Absatz 3 Buchstabe p
Artikel 3 Buchstabe d	–	–	Artikel 2 Absatz 3 Buchstabe d
Artikel 3 Buchstabe e	–	–	Artikel 2 Absatz 3 Buchstabe e
Artikel 3 Buchstabe f	–	–	Artikel 2 Absatz 3 Buchstabe q
Artikel 3 Buchstabe g	–	–	Artikel 2 Absatz 3 Buchstabe g

[+] ABl.: Bitte die Nummer der in Dokument ST 8535/26 (2023/0209 (COD)) enthaltenen Richtlinie einfügen.

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 3 Buchstabe h	–	–	Artikel 2 Absatz 3 Buchstabe h
Artikel 3 Buchstabe i	–	–	Artikel 2 Absatz 3 Buchstabe i
Artikel 3 Buchstabe j	–	–	–
Artikel 3 Buchstabe k	Artikel 1 Absatz 4	–	Artikel 2 Absatz 3 Buchstabe k
Artikel 3 Buchstabe l	Artikel 1 Absatz 5	–	Artikel 2 Absatz 3 Buchstabe l
Artikel 3 Buchstabe m	–	–	Artikel 2 Absatz 3 Buchstabe m
Artikel 3 Buchstabe n	–	–	Artikel 2 Absatz 3 Buchstabe o
Artikel 3 Buchstabe o	–	–	–
Artikel 4 Nummern 1 und 2	–	–	Artikel 3 Nummern 15 und 16
Artikel 4 Nummer 3	–	–	Artikel 3 Nummer 1
Artikel 4 Nummer 4	–	–	Artikel 3 Nummer 13
Artikel 4 Nummer 5	–	–	Artikel 3 Nummer 8
Artikel 4 Nummer 6	–	–	Artikel 3 Nummer 12
Artikel 4 Nummer 7	–	–	Artikel 3 Nummer 20
Artikel 4 Nummern 8 und 9	–	–	Artikel 3 Nummern 5 und 6
Artikel 4 Nummer 10	–	–	Artikel 3 Nummer 3
Artikel 4 Nummer 11	–	–	Artikel 3 Nummer 2
Artikel 4 Nummer 12	–	–	Artikel 3 Nummer 35
Artikel 4 Nummer 13	–	–	Artikel 3 Nummer 11
Artikel 4 Nummern 14, 15 und 16	–	–	Artikel 3 Nummern 42, 43 und 44
Artikel 4 Nummer 17	–	–	Artikel 3 Nummer 37
Artikel 4 Nummern 18 und 19	–	–	Artikel 3 Nummern 45 und 46
Artikel 4 Nummer 20	–	–	Artikel 3 Nummer 4

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 4 Nummer 21	–	–	Artikel 3 Nummer 33
Artikel 4 Nummer 22	–	–	Artikel 3 Nummer 41
Artikel 4 Nummern 23 und 24	–	–	Artikel 3 Nummern 52 und 53
Artikel 4 Nummer 25	–	–	Artikel 3 Nummer 7
Artikel 4 Nummern 26, 27 und 28	–	–	Artikel 3 Nummern 55, 56 und 57
Artikel 4 Nummern 29 bis 33	–	–	Artikel 3 Nummern 59 bis 63
Artikel 4 Nummer 34	–	–	Artikel 3 Nummer 34
Artikel 4 Nummer 35	–	–	Artikel 3 Nummer 39
Artikel 4 Nummer 36	–	–	Artikel 3 Nummer 32
Artikel 4 Nummer 37	–	–	Artikel 3 Nummer 64
Artikel 4 Nummern 38, 39 und 40	–	–	Artikel 3 Nummern 17, 18 und 19
Artikel 4 Nummern 41 und 42	–	–	–
Artikel 4 Nummer 43	–	–	Artikel 3 Nummer 31
Artikel 4 Nummern 44 und 45	–	–	Artikel 3 Nummern 50 und 51
Artikel 4 Nummer 46	–	Artikel 2 Nummer 2	–
Artikel 4 Nummer 47	–	–	–
Artikel 4 Nummer 48	–	–	–
–	Artikel 2 Nummer 1	–	–
–	Artikel 2 Nummer 2	–	Artikel 3 Nummer 30
–	Artikel 2 Nummer 3	–	–
–	Artikel 2 Nummer 4	Artikel 2 Nummer 3	–

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 5 Absatz 1	Artikel 3 Absatz 1	Artikel 3 Absatz 3	–
–	Artikel 3 Absatz 2	Artikel 9 Absatz 7	–
Artikel 5 Absatz 2	–	Artikel 3 Absatz 5	–
Artikel 5 Absatz 3	–	Artikel 35 Absatz 4	–
Artikel 5 Absätze 4 und 5	–	–	–
Artikel 5 Absatz 6	–	Artikel 3 Absätze 6 und 7	–
Artikel 5 Absatz 7	–	–	–
Artikel 6 Absatz 1	Artikel 3 Absatz 3	Artikel 4 Absatz 1	–
–	Artikel 3 Absatz 4	Artikel 19	–
Artikel 6 Absatz 2	–	Artikel 4 Absatz 2	–
Artikel 6 Absatz 3	–	Artikel 4 Absatz 3	–
Artikel 6 Absatz 4	–	Artikel 4 Absatz 4	–
Artikel 7	Artikel 4	Artikel 5	–
Artikel 8 Absatz 1	Artikel 5 Absatz 1	Artikel 6 Absatz 1	–
Artikel 8 Absatz 2	Artikel 5 Absatz 6	Artikel 6 Absatz 2	–
Artikel 8 Absatz 3	Artikel 5 Absatz 7	Artikel 6 Absatz 3	–
Artikel 9 Absatz 1	–	Artikel 7 Absätze 1 und 2	–
Artikel 9 Absatz 2	–	Artikel 7 Absatz 3	–
Artikel 9 Absatz 3	–	Artikel 7 Absatz 5	–
–	Artikel 5 Absatz 2	Artikel 8 Absätze 2 und 3	–
–	Artikel 5 Absatz 3	Artikel 8 Absatz 2	–
–	Artikel 5 Absatz 4	Artikel 8 Absatz 4	–
–	Artikel 5 Absätze 5, 6 und 7	–	–
Artikel 10 Absatz 1	–	Artikel 9 Absätze 1 und 2	–

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 10 Absatz 2	–	Artikel 9 Absatz 4	–
–	Artikel 7 Absatz 1	Artikel 9 Absatz 4	–
–	Artikel 7 Absätze 2, 3 und 4	–	–
Artikel 11 Absatz 1	–	Artikel 13 Absatz 1	–
Artikel 11 Absatz 2	–	Artikel 13 Absatz 2	–
Artikel 11 Absatz 3	–	Artikel 13 Absatz 4	–
Artikel 11 Absatz 4	–	Artikel 13 Absatz 5	–
Artikel 11 Absatz 5	–	Artikel 13 Absatz 5	–
Artikel 11 Absatz 6	–	Artikel 13 Absatz 6	–
Artikel 11 Absatz 7	–	Artikel 13 Absatz 6 Buchstabe b	–
Artikel 11 Absatz 8	–	Artikel 13 Absatz 6 Buchstabe c	–
Artikel 11 Absatz 9	–	Artikel 13 Absatz 7	–
Artikel 12	–	Artikel 14	–
Artikel 13 Absatz 1	–	Artikel 16 Absatz 1	–
Artikel 13 Absatz 2	–	Artikel 16 Absatz 2	–
Artikel 13 Absatz 3	–	Artikel 16 Absatz 3	–
Artikel 14 Absatz 1	–	Artikel 17 Absatz 1	–
Artikel 14 Absatz 2	–	Artikel 17 Absätze 2 und 3	–
Artikel 14 Absatz 3	–	Artikel 17 Absatz 4	–
Artikel 14 Absatz 4	–	Artikel 17 Absatz 5	–
Artikel 15 Absatz 1	–	Artikel 18 Absätze 1 und 2	–
Artikel 15 Absatz 2	–	Artikel 18 Absatz 3	–
Artikel 15 Absatz 3	–	Artikel 18 Absatz 4	–
Artikel 15 Absatz 4	–	Artikel 18 Absatz 5	–

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 15 Absatz 5	–	Artikel 18 Absatz 6	–
Artikel 16	–	Artikel 15	–
Artikel 17 Absatz 1	–	Artikel 11 Absatz 1	–
Artikel 17 Absatz 2	–	Artikel 11 Absatz 2	–
Artikel 17 Absatz 3	–	Artikel 11 Absatz 3	–
Artikel 17 Absatz 4	–	Artikel 11 Absatz 4	–
Artikel 18 Absatz 1	Artikel 6 Absatz 1 Buchstabe a	Artikel 10 Absatz 1	–
Artikel 18 Absatz 1 Buchstabe a	Artikel 6 Absatz 1 Buchstabe c	Artikel 10 Absatz 1 Buchstabe a	–
Artikel 18 Absatz 1 Buchstabe b	Artikel 6 Absatz 1 Buchstabe d	Artikel 10 Absatz 1 Buchstabe b	–
Artikel 18 Absatz 1 Buchstabe c	Artikel 6 Absatz 1 Buchstabe e	Artikel 10 Absatz 1 Buchstabe c	–
Artikel 18 Absatz 2	Artikel 6 Absatz 4	Artikel 10 Absatz 2	–
Artikel 18 Absatz 3	Artikel 6 Absatz 4	Artikel 10 Absatz 3	–
Artikel 18 Absatz 4	Artikel 6 Absatz 1 Buchstabe b	Artikel 10 Absatz 4	–
Artikel 18 Absatz 5	Artikel 6 Absätze 2 und 4	Artikel 10 Absatz 5	–
–	Artikel 6 Absatz 3	Artikel 10 Absatz 6	–
Artikel 18 Absatz 6	–	Artikel 10 Absatz 7	–
Artikel 19 Absatz 1	–	Artikel 19 Absatz 1	–
Artikel 19 Absatz 2	–	Artikel 19 Absatz 2	–
Artikel 19 Absatz 3	–	Artikel 19 Absatz 3	–
Artikel 19 Absatz 4	–	Artikel 19 Absatz 4	–
Artikel 19 Absatz 5	–	Artikel 19 Absatz 5	–
Artikel 19 Absatz 6	–	Artikel 21 Absatz 1	–
Artikel 19 Absatz 7	–	Artikel 19 Absatz 6, Artikel 20 Absatz 2	–

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 19 Absatz 8	–	Artikel 19 Absatz 7, Artikel 21 Absatz 2	–
Artikel 20 Absatz 1	–	Artikel 22 Absatz 1	–
Artikel 20 Absatz 2	–	Artikel 22 Absatz 2	–
Artikel 21	–	Artikel 12	–
Artikel 22 Absatz 1	–	Artikel 23 Absatz 1	–
Artikel 22 Absatz 2	–	Artikel 23 Absatz 2	–
Artikel 22 Absatz 3	–	Artikel 23 Absatz 3	–
Artikel 22 Absatz 4	–	Artikel 23 Absatz 4	–
Artikel 22 Absatz 5	–	Artikel 23 Absatz 5	–
Artikel 23 Absatz 1	–	Artikel 24 Absatz 1	–
Artikel 23 Absatz 1 Buchstabe a	–	Artikel 24 Absatz 1 Buchstabe a	–
Artikel 23 Absatz 1 Buchstabe b	–	Artikel 24 Absatz 1 Buchstabe b	–
Artikel 23 Absatz 1 Buchstabe c	–	Artikel 24 Absatz 1 Buchstabe c	–
Artikel 23 Absatz 1 Buchstabe d	–	Artikel 24 Absatz 1 Buchstabe d	–
Artikel 23 Absatz 2	–	Artikel 24 Absatz 2	–
Artikel 23 Absatz 3	–	Artikel 23 Absatz 3	–
Artikel 24 Absatz 1	–	Artikel 25 Absatz 1	Artikel 102 Absatz 1
Artikel 24 Absatz 2	–	Artikel 25 Absatz 2	Artikel 102 Absatz 2
Artikel 24 Absatz 3	–	Artikel 25 Absatz 3	Artikel 102 Absatz 3
Artikel 25 Absatz 1	–	Artikel 26 Absatz 1	–
Artikel 25 Absatz 2	–	Artikel 26 Absatz 2	–
Artikel 26 Absatz 1	–	Artikel 27 Absatz 1	–

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 26 Absatz 2	–	Artikel 27 Absatz 2	–
Artikel 27 Absatz 1	–	Artikel 28 Absatz 1	–
Artikel 27 Absatz 2	–	Artikel 28 Absatz 2	–
Artikel 28 Absatz 1	–	Artikel 29 Absatz 1	–
Artikel 28 Absatz 2	–	Artikel 29 Absatz 2	–
Artikel 28 Absatz 3	–	Artikel 29 Absatz 3	–
Artikel 28 Absatz 4	–	Artikel 29 Absatz 4	–
Artikel 28 Absatz 5	–	Artikel 29 Absatz 5	–
Artikel 29 Absatz 1	–	Artikel 30 Absatz 1	–
Artikel 29 Absatz 2	–	Artikel 30 Absatz 2	–
Artikel 29 Absatz 3	–	Artikel 30 Absatz 3	–
Artikel 29 Absatz 4	–	Artikel 30 Absatz 4	–
Artikel 29 Absatz 5	–	Artikel 30 Absatz 5	–
Artikel 29 Absatz 6	–	–	–
Artikel 30 Absatz 1	–	Artikel 31 Absatz 1	–
Artikel 30 Absatz 2	–	Artikel 31 Absatz 2	–
Artikel 30 Absatz 3	–	Artikel 31 Absatz 3	–
Artikel 30 Absatz 4	–	Artikel 31 Absatz 4	–
Artikel 31 Absatz 1	–	Artikel 32 Absatz 1	–
Artikel 31 Absatz 2	–	Artikel 32 Absatz 2	–
–	Artikel 8 Absätze 1, 2 und 3	–	–
Artikel 32 Absatz 1 Buchstabe a	–	Artikel 33 Absatz 1 Buchstabe a	–
–	Artikel 9 Absatz 1 Buchstabe a	Artikel 33 Absatz 1 Buchstabe b	–

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 32 Absatz 1 Buchstabe b	Artikel 9 Absatz 1 Buchstabe b	Artikel 33 Absatz 1 Buchstabe c	–
Artikel 32 Absatz 2	Artikel 9 Absatz 2	Artikel 33 Absatz 3	–
Artikel 32 Absatz 3	Artikel 9 Absatz 3	Artikel 33 Absatz 4	–
Artikel 32 Absatz 4	Artikel 9 Absatz 4	Artikel 33 Absatz 5	–
Artikel 32 Absatz 5	Artikel 9 Absätze 5, 6 und 7	Artikel 33 Absätze 6 und 7	–
Artikel 32 Absatz 6	Artikel 9 Absatz 8	Artikel 33 Absatz 8	–
Artikel 33 Absatz 1	–	Artikel 35Absatz 1 bis 5	–
Artikel 33 Absatz 2	–	Artikel 3 Absatz 2	Artikel 47 Absatz 2
Artikel 34	Artikel 9 Absatz 9	Artikel 34	–
–	Artikel 10	Artikel 45 Absätze 2 und 4	–
–	Artikel 11 Absatz 1	–	Artikel 30 Absatz 1
–	Artikel 11 Absatz 2	–	Artikel 30 Absatz 2
–	Artikel 11 Absatz 3	–	Artikel 30 Absatz 3
–	Artikel 11 Absatz 4	–	Artikel 30 Absatz 4
–	Artikel 11 Absatz 5	–	Artikel 30 Absatz 5
–	Artikel 11 Absatz 6	–	Artikel 30 Absatz 6
–	Artikel 11 Absatz 7	–	Artikel 30 Absatz 7
–	Artikel 12	–	Artikel 30 Absatz 8
Artikel 35 Absatz 1	–	–	Artikel 31 Absätze 1, 2 und 4
Artikel 35 Absatz 2	–	–	Artikel 31 Absätze 3, 5 und 6
Artikel 36	–	–	Artikel 33

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 37 Absatz 1	–	–	Artikel 99
Artikel 37 Absatz 2	–	Artikel 38 Absatz 1	–
Artikel 37 Absatz 3	–	Artikel 38 Absatz 2	–
Artikel 37 Absatz 4	–	Artikel 38 Absatz 3	–
Artikel 37 Absatz 5	–	Artikel 38 Absatz 4	–
Artikel 38 Absatz 1	–	–	Artikel 4 Absatz 1
Artikel 38 Absatz 2	–	–	Artikel 4 Absatz 2
Artikel 38 Absatz 3	–	–	–
Artikel 39	–	–	–
Artikel 40 Absatz 1	–	–	Artikel 8 Absatz 1
Artikel 40 Absatz 2	–	–	Artikel 8 Absatz 2
Artikel 40 Absatz 3	–	–	Artikel 8 Absatz 3
Artikel 41	–	–	Artikel 9
Artikel 42 Absatz 1	–	–	Artikel 10
Artikel 42 Absatz 2	–	–	–
Artikel 43 Absatz 1	–	–	Artikel 11 Absatz 1
Artikel 43 Absatz 2	–	–	Artikel 11 Absatz 2
Artikel 44 Absatz 1	–	–	Artikel 12 Absatz 1
Artikel 44 Absatz 2	–	–	Artikel 12 Absatz 2
Artikel 44 Absatz 3	–	–	Artikel 12 Absatz 3
Artikel 45 Absatz 1 Buchstabe a	–	–	Artikel 13 Absatz 1 Buchstabe a
Artikel 45 Absatz 1 Buchstabe b	–	–	Artikel 13 Absatz 1 Buchstabe b
Artikel 45 Absatz 1 Buchstabe c	–	–	Artikel 13 Absatz 1 Buchstabe d
Artikel 45 Absatz 1 Buchstabe d	–	–	Artikel 13 Absatz 1 Buchstabe e

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 45 Absatz 2 Buchstabe a	–	–	Artikel 13 Absatz 2 Buchstabe a
Artikel 45 Absatz 2 Buchstabe b	–	–	Artikel 13 Absatz 2 Buchstabe b
Artikel 45 Absatz 3	–	–	Artikel 13 Absatz 3
Artikel 46	–	–	Artikel 14
Artikel 47	–	–	Artikel 15
Artikel 48	–	–	Artikel 16
Artikel 49	–	–	Artikel 17
Artikel 50	–	–	Artikel 18
Artikel 51 Absatz 1	–	–	Artikel 19 Absatz 1
Artikel 51 Absatz 2	–	–	Artikel 19 Absatz 2
Artikel 51 Absatz 3	–	–	Artikel 19 Absatz 3
Artikel 52 Absatz 1 Buchstabe a	–	–	Artikel 20 Absatz 1 Buchstabe a
Artikel 52 Absatz 1 Buchstabe b	–	–	Artikel 20 Absatz 1 Buchstabe b
Artikel 52 Absatz 2 Buchstabe a	–	–	Artikel 20 Absatz 2 Buchstabe a
Artikel 52 Absatz 2 Buchstabe b	–	–	Artikel 20 Absatz 2 Buchstabe b
Artikel 52 Absatz 2 Buchstabe c	–	–	Artikel 20 Absatz 2 Buchstabe c
Artikel 52 Absatz 2 Buchstabe d	–	–	Artikel 20 Absatz 2 Buchstabe d
Artikel 52 Absatz 2 Buchstabe e	–	–	Artikel 20 Absatz 2 Buchstabe e
Artikel 52 Absatz 2 Buchstabe f	–	–	Artikel 20 Absatz 2 Buchstabe g
Artikel 52 Absatz 2 Buchstabe g	–	–	Artikel 20 Absatz 2 Buchstabe h
Artikel 52 Absatz 3 Buchstabe a	–	–	Artikel 20 Absatz 3 Buchstabe a

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 52 Absatz 3 Buchstabe b	–	–	Artikel 20 Absatz 3 Buchstabe c
Artikel 52 Absatz 3 Buchstabe c	–	–	Artikel 20 Absatz 3 Buchstabe d
Artikel 52 Absatz 4 Buchstabe a	–	–	Artikel 20 Absatz 4 Buchstabe a
Artikel 52 Absatz 4 Buchstabe b	–	–	Artikel 20 Absatz 4 Buchstabe b
Artikel 52 Absatz 4 Buchstabe c	–	–	Artikel 20 Absatz 4 Buchstabe c
Artikel 52 Absatz 4 Buchstabe d	–	–	Artikel 20 Absatz 4 Buchstabe d
Artikel 52 Absatz 5 Buchstabe a	–	–	Artikel 20 Absatz 5 Buchstabe a
Artikel 52 Absatz 5 Buchstabe b	–	–	Artikel 20 Absatz 5 Buchstabe b
Artikel 52 Absatz 5 Buchstabe c	–	–	Artikel 20 Absatz 5 Buchstabe c
Artikel 52 Absatz 5 Buchstabe d	–	–	Artikel 20 Absatz 5 Buchstabe d
Artikel 52 Absatz 5 Buchstabe e	–	–	Artikel 20 Absatz 5 Buchstabe e
Artikel 52 Absatz 5 Buchstabe f	–	–	Artikel 20 Absatz 5 Buchstabe g
Artikel 52 Absatz 5 Buchstabe g	–	–	Artikel 20 Absatz 5 Buchstabe h
Artikel 52 Absatz 6 Buchstabe a	–	–	Artikel 20 Absatz 6 Buchstabe a
Artikel 52 Absatz 6 Buchstabe b	–	–	Artikel 20 Absatz 6 Buchstabe b
Artikel 52 Absatz 6 Buchstabe c	–	–	Artikel 20 Absatz 6 Buchstabe c
Artikel 52 Absatz 7 Buchstabe a	–	–	Artikel 20 Absatz 7 Buchstabe a
Artikel 52 Absatz 7 Buchstabe b	–	–	Artikel 20 Absatz 7 Buchstabe b
Artikel 53	–	–	Artikel 21

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 54 Absatz 1	–	–	Artikel 22 Absatz 1
Artikel 54 Absatz 2	–	–	Artikel 22 Absatz 3
Artikel 54 Absatz 3	–	–	Artikel 22 Absatz 4
Artikel 55 Absatz 1	–	–	Artikel 23 Absatz 1
Artikel 55 Absatz 2	–	–	Artikel 23 Absatz 2
Artikel 55 Absatz 3	–	–	Artikel 23 Absatz 3
Artikel 55 Absatz 4	–	–	Artikel 23 Absatz 4
Artikel 55 Absatz 5	–	–	Artikel 23 Absatz 5
Artikel 55 Absatz 6	–	–	Artikel 23 Absatz 6
Artikel 56	–	–	Artikel 24
Artikel 57 Absatz 1	–	–	Artikel 25 Absatz 1
Artikel 57 Absatz 2	–	–	Artikel 25 Absatz 2
Artikel 57 Absatz 3	–	–	Artikel 25 Absatz 3
Artikel 58 Absatz 1	–	–	Artikel 26 Absatz 1
Artikel 58 Absatz 2	–	–	Artikel 26 Absatz 2
Artikel 58 Absatz 3	–	–	Artikel 26 Absatz 3
Artikel 59 Absatz 1	–	–	Artikel 5 Absatz 1
Artikel 59 Absatz 2	–	–	Artikel 5 Absatz 2
Artikel 60 Absatz 1	–	–	Artikel 6 Absatz 1
Artikel 60 Absatz 2	–	–	Artikel 6 Absatz 2
Artikel 60 Absatz 3	–	–	Artikel 6 Absatz 3
Artikel 61 Absatz 1	–	–	Artikel 27 Absatz 1
Artikel 61 Absatz 2	–	–	Artikel 27 Absatz 2
Artikel 61 Absatz 3	–	–	Artikel 27 Absatz 3
Artikel 61 Absatz 4	–	–	–

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 62 Absatz 1	–	–	Artikel 28 Absatz 1
Artikel 62 Absatz 2	–	–	Artikel 28 Absatz 2
Artikel 62 Absatz 3	–	–	Artikel 28 Absatz 5
Artikel 62 Absatz 4	–	–	Artikel 28 Absatz 3
Artikel 62 Absatz 5	–	–	Artikel 28 Absatz 4
Artikel 63 Absatz 1	–	–	Artikel 29 Absätze 1 und 2
Artikel 63 Absatz 2	–	–	–
Artikel 63 Absatz 3	–	–	Artikel 29 Absatz 3
Artikel 64 Absatz 1	–	–	Artikel 50 Absatz 1
Artikel 64 Absatz 2 Unterabsatz 1	–	–	Artikel 50 Absatz 6 Unterabsatz 1
Artikel 64 Absatz 2 Unterabsatz 2	–	–	Artikel 50 Absatz 4
Artikel 64 Absatz 3	–	–	Artikel 50 Absatz 7
Artikel 64 Absatz 4	–	–	Artikel 50 Absatz 6 Unterabsatz 2
Artikel 65 Absatz 1	–	–	–
Artikel 65 Absatz 2	–	–	–
Artikel 65 Absatz 3	–	–	–
Artikel 65 Absatz 4	–	–	–
Artikel 65 Absatz 5	–	–	–
Artikel 65 Absatz 6	–	–	–
Artikel 66 Absatz 1	–	–	Artikel 34 Absatz 1
Artikel 66 Absatz 2	–	–	Artikel 41; Artikel 50
Artikel 66 Absatz 3	–	–	Artikel 47
Artikel 66 Absatz 4	–	–	Artikel 41
Artikel 66 Absatz 5	–	–	Artikel 35

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 67 Absatz 1	–	–	Artikel 34 Absatz 2
Artikel 67 Absatz 2	–	–	Artikel 48 Absätze 1 und 2
Artikel 67 Absatz 3	–	–	Artikel 42 Absatz 1
Artikel 67 Absatz 4	–	–	Artikel 35
Artikel 68 Absatz 1	–	–	Artikel 52 Absatz 1
Artikel 68 Absatz 2	–	–	Artikel 52 Absatz 4
Artikel 68 Absatz 3	–	–	Artikel 52 Absatz 5
Artikel 68 Absatz 4	–	–	Artikel 52 Absatz 5
Artikel 68 Absatz 5	–	–	Artikel 43 Absatz 1
Artikel 68 Absatz 6	–	–	Artikel 43 Absatz 2
Artikel 69 Absatz 1 Buchstabe a	–	–	Artikel 53 Absatz 1 Buchstabe a
Artikel 69 Absatz 1 Buchstabe b	–	–	Artikel 53 Absatz 1 Buchstabe b
Artikel 69 Absatz 2	–	–	Artikel 53 Absatz 2
Artikel 70 Absatz 1 Buchstabe a	–	–	Artikel 54 Absatz 1 Buchstabe a
Artikel 70 Absatz 1 Buchstabe b	–	–	Artikel 54 Absatz 1 Buchstabe b
Artikel 70 Absatz 1 Buchstabe c	–	–	Artikel 54 Absatz 1 Unterabsatz 1 Buchstabe c und Unterabsatz 2
Artikel 70 Absatz 1 Buchstabe d	–	–	Artikel 54 Absatz 1 Unterabsatz 1 Buchstabe d
Artikel 70 Absatz 1 Buchstabe e	–	–	Artikel 54 Absatz 1 Unterabsatz 1 Buchstabe e

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 70 Absatz 2	–	–	Artikel 54 Absatz 2
Artikel 71 Absatz 1	–	–	Artikel 55 Absatz 1
Artikel 71 Absatz 2	–	–	Artikel 55 Absatz 2
Artikel 72 Absatz 1	–	–	Artikel 56 Absatz 1
Artikel 72 Absatz 2	–	–	Artikel 56 Absatz 2
Artikel 73 Absatz 1	–	–	Artikel 57 Absatz 1, Absatz 2 Buchstabe b und Absatz 3
Artikel 73 Absatz 2	–	–	Artikel 57 Absatz 4
Artikel 73 Absatz 2 Unterabsatz 2	–	–	Artikel 57 Absatz 5
Artikel 73 Absatz 3	–	–	Artikel 57 Absatz 6
Artikel 74 Absatz 1	–	–	Artikel 63 Absatz 1
Artikel 74 Absatz 1 Unterabsatz 2 Buchstabe a	–	–	Artikel 63 Absatz 1 Unterabsatz 2 Buchstabe a
Artikel 74 Absatz 1 Unterabsatz 2 Buchstabe b	–	–	Artikel 63 Absatz 1 Unterabsatz 2 Buchstabe b
Artikel 74 Absatz 1 Unterabsatz 3	–	–	Artikel 63 Absatz 2
Artikel 74 Absatz 1 Unterabsatz 4	–	–	Artikel 63 Absatz 1 Unterabsatz 3
Artikel 74 Absatz 2	–	–	Artikel 63 Absatz 3
Artikel 74 Absatz 3	–	–	Artikel 63 Absatz 5
Artikel 75 Absatz 1	–	–	Artikel 64 Absatz 1
Artikel 75 Absatz 2	–	–	Artikel 64 Absatz 4
Artikel 76 Absatz 1 Unterabsatz 1 Buchstabe a	–	–	Artikel 65 Absatz 1 Unterabsatz 1 Buchstabe a

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 76 Absatz 1 Unterabsatz 1 Buchstabe b	–	–	Artikel 65 Absatz 1 Unterabsatz 1 Buchstabe b
Artikel 76 Absatz 1 Unterabsatz 2	–	–	Artikel 65 Absatz 1 Unterabsatz 2
Artikel 76 Absatz 1 Unterabsatz 3	–	–	Artikel 65 Absatz 1 Unterabsatz 3
Artikel 76 Absatz 1 Unterabsatz 4	–	–	Artikel 65 Absatz 1 Unterabsatz 4
Artikel 76 Absatz 2	–	–	Artikel 65 Absatz 2
Artikel 76 Absatz 3 Buchstabe a	–	–	Artikel 65 Absatz 3 Buchstabe a
Artikel 76 Absatz 3 Buchstabe b	–	–	Artikel 65 Absatz 3 Buchstabe b
Artikel 76 Absatz 4	–	–	Artikel 65 Absatz 4
Artikel 77 Absatz 1	–	–	Artikel 66 Absatz 1
Artikel 77 Absatz 2	–	–	Artikel 66 Absatz 2
Artikel 78 Absatz 1	–	–	Artikel 67 Absatz 1
Artikel 78 Absatz 2	–	–	Artikel 67 Absatz 2
Artikel 79 Absatz 1	–	–	Artikel 68 Absatz 3
Artikel 79 Absatz 2	–	–	Artikel 68 Absatz 1
Artikel 79 Absatz 3	–	–	Artikel 68 Absatz 5
Artikel 80 Absatz 1	–	–	Artikel 69 Absatz 1
Artikel 80 Absatz 2	–	–	Artikel 69 Absatz 2
Artikel 80 Absatz 3	–	–	Artikel 69 Absatz 3
Artikel 80 Absatz 4	–	–	Artikel 69 Absatz 4
Artikel 80 Absatz 5	–	–	Artikel 69 Absatz 5
Artikel 81 Absatz 1	–	–	Artikel 70 Absatz 1
Artikel 81 Absatz 2	–	–	Artikel 70 Absatz 2

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 81 Absatz 3	–	–	Artikel 70 Absatz 3
Artikel 82 Absatz 1	–	–	Artikel 72 Absatz 1
Artikel 82 Absatz 2	–	–	Artikel 72 Absatz 2
Artikel 83 Absatz 1	–	–	Artikel 73 Absatz 1
Artikel 83 Absatz 2	–	–	Artikel 73 Absatz 2
Artikel 83 Absatz 3	–	–	Artikel 73 Absatz 8
Artikel 84	–	–	Artikel 74 Absatz 1
Artikel 85	–	–	Artikel 75
Artikel 86	–	–	Artikel 76 Absatz 1
Artikel 87 Absatz 1	–	–	Artikel 77 Absatz 1
Artikel 87 Absatz 2	–	–	Artikel 77 Absatz 2
Artikel 87 Absatz 3	–	–	Artikel 77 Absatz 3
Artikel 88 Absatz 1	–	–	Artikel 78 Absatz 1
Artikel 88 Absatz 2	–	–	Artikel 78 Absatz 2 Unterabsatz 1
Artikel 88 Absatz 3 Unterabsatz 1	–	–	Artikel 78 Absatz 2 Unterabsatz 2
Artikel 88 Absatz 3 Unterabsatz 2	–	–	Artikel 78 Absatz 2 Unterabsatz 3
Artikel 88 Absatz 4	–	–	Artikel 78 Absatz 3
Artikel 88 Absatz 5	–	–	Artikel 78 Absatz 4
Artikel 89 Absatz 1	–	–	Artikel 79 Absatz 1
Artikel 89 Absatz 2	–	–	Artikel 79 Absatz 2
Artikel 89 Absatz 3	–	–	Artikel 79 Absatz 3
Artikel 90 Absatz 1	–	–	Artikel 80 Absatz 1
Artikel 90 Absatz 2	–	–	Artikel 80 Absatz 2

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 91	–	–	Artikel 81
Artikel 92 Absatz 1	–	–	Artikel 82 Absatz 1
Artikel 92 Absatz 2	–	–	Artikel 82 Absatz 3
Artikel 93	–	–	Artikel 83
Artikel 94 Absatz 1 und 2	–	–	Artikel 84
Artikel 95 Absatz 1	–	–	Artikel 85 Absatz 1
Artikel 95 Absatz 1 Unterabsatz 2 Buchstabe a	–	–	Artikel 85 Absatz 1 Unterabsatz 2 Buchstabe a
Artikel 95 Absatz 1 Unterabsatz 2 Buchstabe b	–	–	Artikel 85 Absatz 1 Unterabsatz 2 Buchstabe b
Artikel 95 Absatz 1 Unterabsatz 2 Buchstabe c	–	–	Artikel 85 Absatz 1 Unterabsatz 2 Buchstabe c
Artikel 95 Absatz 1 Unterabsatz 2 Buchstabe d	–	–	Artikel 85 Absatz 1 Unterabsatz 2 Buchstabe c
Artikel 95 Absatz 2	–	–	–
Artikel 95 Absatz 3	–	–	–
Artikel 95 Absatz 4	–	–	–
Artikel 95 Absatz 5	–	–	Artikel 85 Absatz 2
Artikel 96 Absatz 1	–	–	–
Artikel 96 Absatz 2	–	–	–
Artikel 96 Absatz 3	–	–	–
Artikel 96 Absatz 4	–	–	–
Artikel 96 Absatz 5	–	–	–
Artikel 96 Absatz 6	–	–	Artikel 86
Artikel 96 Absatz 7	–	–	–

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 97 Absatz 1	–	–	Artikel 91 Absatz 1
Artikel 97 Absatz 1 Buchstabe a	–	–	Artikel 91 Absatz 1 Buchstabe a
Artikel 97 Absatz 1 Buchstabe b	–	–	Artikel 91 Absatz 1 Buchstabe b
Artikel 97 Absatz 1 Buchstabe c	–	–	Artikel 91 Absatz 1 Buchstabe c
Artikel 97 Absatz 2	–	–	Artikel 91 Absätze 6 und 7
Artikel 97 Absatz 3	–	–	Artikel 91 Absatz 8
Artikel 97 Absatz 4	–	–	Artikel 93 Absatz 1
Artikel 97 Absatz 5	–	–	Artikel 93 Absatz 2
Artikel 98 Absatz 1	–	–	Artikel 97 Absatz 1
Artikel 98 Absatz 1 Buchstabe a	–	–	Artikel 97 Absatz 1 Unterabsatz 1 Buchstabe a
Artikel 98 Absatz 1 Buchstabe b	–	–	Artikel 97 Absatz 1 Unterabsatz 1 Buchstabe b
Artikel 98 Absatz 1 Buchstabe c	–	–	Artikel 97 Absatz 1 Unterabsatz 1 Buchstabe c
Artikel 98 Absatz 1 Buchstabe d	–	–	Artikel 97 Absatz 1 Unterabsatz 1 Buchstabe e
Artikel 98 Absatz 2	–	–	Artikel 97 Absatz 2
Artikel 98 Absatz 2 Buchstabe a	–	–	Artikel 97 Absatz 2 Unterabsatz 1 Buchstabe a
Artikel 98 Absatz 2 Buchstabe b	–	–	Artikel 97 Absatz 2 Unterabsatz 1 Buchstabe b

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 98 Absatz 2 Buchstabe c	–	–	Artikel 97 Absatz 2 Unterabsatz 1 Buchstabe c
Artikel 98 Absatz 2 Buchstabe d	–	–	Artikel 97 Absatz 2 Unterabsatz 1 Buchstabe d
Artikel 98 Absatz 2 Buchstabe e	–	–	Artikel 97 Absatz 2 Unterabsatz 1 Buchstabe e
Artikel 98 Absatz 3	–	–	Artikel 91 Absatz 9
Artikel 98 Absatz 3 Buchstabe a	–	–	Artikel 91 Absatz 9 Unterabsatz 1 Buchstabe a
Artikel 98 Absatz 3 Buchstabe b	–	–	Artikel 91 Absatz 9 Unterabsatz 1 Buchstabe b
Artikel 98 Absatz 3 Buchstabe c	–	–	Artikel 91 Absatz 9 Unterabsatz 1 Buchstabe c
Artikel 98 Absatz 4	–	–	Artikel 97 Absatz 2 Unterabsätze 2 und 3
Artikel 98 Absatz 5	–	–	Artikel 97 Absatz 3
Artikel 99 Absatz 1	–	–	Artikel 100 Absatz 1
Artikel 99 Absatz 2	–	–	Artikel 100 Absatz 2
Artikel 100 Absatz 1	–	–	Artikel 101 Absatz 1
Artikel 100 Absatz 2	–	–	Artikel 101 Absätze 2 und 5
Artikel 100 Absatz 3	–	–	Artikel 101 Absatz 3 Buchstaben a und b

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 100 Absätze 4 und 5	–	–	Artikel 103 Absatz 1
Artikel 100 Absatz 5	–	–	Artikel 101 Absatz 1 Unterabsatz 1
Artikel 100 Absatz 6	–	–	Artikel 100 Absatz 3
Artikel 101 Absatz 1	–	–	Artikel 104 Absatz 1
Artikel 101 Absatz 2	–	–	Artikel 104 Absatz 2
Artikel 101 Absatz 3	–	–	Artikel 104 Absatz 3
Artikel 101 Absatz 4	–	–	Artikel 104 Absatz 4
Artikel 102 Absatz 1	–	–	Artikel 105 Absatz 1
Artikel 102 Absatz 2	–	–	Artikel 105 Absatz 4
Artikel 103 Absatz 1	–	–	Artikel 106 Absatz 1
Artikel 103 Absatz 2	–	–	Artikel 111
Artikel 104b	–	Artikel 39	Artikel 63 Absatz 6
Artikel 105 Absatz 1	–	Artikel 40 Absatz 1	Artikel 115 Absatz 1
Artikel 105 Absatz 2	–	Artikel 40 Absatz 2	Artikel 115 Absatz 2
Artikel 105 Absatz 3	–	Artikel 40 Absatz 3	Artikel 115 Absatz 3
Artikel 105 Absatz 4	–	Artikel 40 Absatz 5	Artikel 115 Absatz 5
Artikel 105 Absatz 5	–	Artikel 46 Absatz 6	Artikel 115 Absatz 6
Artikel 106	–	–	–
–	Artikel 13	–	Artikel 100; Artikel 106 Absatz 1; Artikel 103 Absatz 1; Artikel 105 Absätze 1 und 4
–	Artikel 14 Absätze 1 und 2	Artikel 39	–
–	Artikel 15 Absätze 1 und 2	Artikel 40	–
Artikel 107 Absatz 1	Artikel 16 Absatz 1	Artikel 41 Absatz 1	–

Richtlinie (EU) 2015/2366	Richtlinie 2009/110/EG	Richtlinie (EU) 2026/…[+]	Vorliegende Verordnung
Artikel 107 Absatz 2	–	Artikel 41 Absatz 2	–
Artikel 107 Absatz 3	Artikel 16 Absatz 2	Artikel 41 Absatz 3	–
Artikel 108	Artikel 17	Artikel 42	Artikel 117
Artikel 109 Absatz 1	–	–	–
Artikel 109 Absatz 2	–	–	–
Artikel 109 Absatz 3	–	–	–
Artikel 109 Absatz 4	–	–	–
Artikel 109 Absatz 5	–	–	–
–	Artikel 18 Absatz 1	–	–
–	Artikel 18 Absatz 2	–	–
–	Artikel 18 Absatz 3	–	–
–	Artikel 18 Absatz 4	–	–
Artikel 114	Artikel 21	Artikel 48	–
Artikel 115 Absatz 1	Artikel 22 Absatz 1	Artikel 49 Absatz 1	–
Artikel 115 Absatz 2	–	Artikel 49 Absatz 1 Unterabsätze 2 und 3	–
Artikel 115 Absatz 3	Artikel 22 Absatz 2	Artikel 49 Absatz 2	–
Artikel 115 Absatz 4	–	–	–
Artikel 115 Absatz 5	–	–	–
Artikel 115 Absatz 6	–	–	–
Artikel 116	Artikel 23	Artikel 50	Artikel 124
Artikel 117	Artikel 24	Artikel 51	–
Anhang I	–	Anhang I	–
Anhang II	–	Anhang II	Anhang