Rat der
Europäischen Union

Brüssel, den 30. August 2022
(OR. en)

11972/22

EF 255
ECOFIN 821
DELACT 153

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	22. August 2022
Empfänger:	Generalsekretariat des Rates
Nr. Komm.dok.:	C(2022) 5517 final
Betr.:	DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION vom 3.8.2022 zur Änderung der in der Delegierten Verordnung (EU) 2018/389 festgelegten technischen Regulierungsstandards im Hinblick auf die 90-tägige Ausnahme für den Kontozugriff

Die Delegationen erhalten in der Anlage das Dokument C(2022) 5517 final.

Anl.: C(2022) 5517 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 3.8.2022
C(2022) 5517 final

DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION

vom 3.8.2022

zur Änderung der in der Delegierten Verordnung (EU) 2018/389 festgelegten technischen Regulierungsstandards im Hinblick auf die 90-tägige Ausnahme für den Kontozugriff

(Text von Bedeutung für den EWR)

BEGRÜNDUNG

1. KONTEXT DES DELEGIERTEN RECHTSAKTS

Mit Artikel 98 Absatz 1 der Richtlinie (EU) 2015/2366 (Zahlungsdiensterichtlinie, im Folgenden „PSD2“) erhielt die Europäische Bankenaufsichtsbehörde (EBA) den Auftrag, Entwürfe technischer Regulierungsstandards (im Folgenden „RTS“) für eine starke Kundenauthentifizierung und gemeinsame und sichere offene Standards für die Kommunikation (RTS zu „SCA“ und „CSC“) auszuarbeiten. In den RTS sollte eine Reihe von Anforderungen festgelegt werden, u. a. für eine starke Kundenauthentifizierung und für Ausnahmen davon. Die daraufhin von der EBA ausgearbeiteten RTS zu SCA und CSC wurden von der Kommission am 27. November 2017 angenommen und im EU-Amtsblatt als Delegierte Verordnung (EU) 2018/389 der Kommission veröffentlicht; diese gilt seit dem 14. September 2019.

Nach Artikel 98 Absatz 5 PSD2 hat die EBA die technischen Regulierungsstandards regelmäßig zu überprüfen und – soweit erforderlich – zu aktualisieren, um unter anderem der Innovation und den technologischen Entwicklungen Rechnung zu tragen. Die Kommission ist demnach befugt, die RTS gemäß den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010 in der durch die Verordnung (EU) 2019/2175 zur Errichtung der EBA geänderten Fassung zu erlassen. Nach Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1093/2010 muss die Kommission innerhalb von drei Monaten nach Erhalt der Standardentwürfe entscheiden, ob sie diese billigt. Aus Gründen des Unionsinteresses kann die Kommission Standardentwürfe auch nur teilweise oder in geänderter Form erlassen.

2. KONSULTATIONEN VOR ANNAHME DES RECHTSAKTS

Gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1093/2010 führte die EBA eine öffentliche Konsultation zu dem der Kommission vorgelegten RTS-Änderungsentwurf durch. Am 28. Oktober 2021 wurde ein Konsultationspapier auf der Website der EBA veröffentlicht; die Konsultation endete am 25. November 2021. Die EBA holte zu ihrem RTS-Änderungsentwurf die Stellungnahme der nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 eingesetzten Interessengruppe Bankensektor ein und übermittelte eine Erläuterung, wie die Ergebnisse der Konsultationen in den endgültigen der Kommission vorgelegten RTS-Änderungsentwurf eingeflossen sind.

Gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1093/2010 übermittelte die EBA der Kommission für ihren endgültigen Entwurf auch eine Folgenabschätzung samt einer Kosten-Nutzen-Analyse. Diese ist abrufbar unter https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2, S. 20-24 des Abschlussberichts über den RTS-Änderungsentwurf.

3. RECHTLICHE ASPEKTE DES DELEGIERTEN RECHTSAKTS

Mit dem endgültigen RTS-Änderungsentwurf wird eine neue Bestimmung in die Delegierte Verordnung (EU) 2018/389 der Kommission aufgenommen, die eine Ausnahme von der starken Kundenauthentifizierung verbindlich vorschreibt. Demnach dürfen Kontoführer keine starke Kundenauthentifizierung verlangen, wenn Kunden über einen Kontoinformationsdienstleister auf ihre Zahlungskontoinformationen zugreifen und bestimmte Bedingungen erfüllt sind, die darauf abzielen, den Schutz und die Sicherheit der Daten des Zahlungsdienstnutzers zu gewährleisten. Zu diesen Bedingungen zählt, dass der

Umfang der Daten begrenzt sein muss, dass der kontoführende Zahlungsdienstleister („ASPSP“) die starke Kundenauthentifizierung beim erstmaligen Zugriff verlangen und regelmäßig erneuern muss und dass der kontoführende Zahlungsdienstleister jederzeit beschließen kann, doch eine starke Kundenauthentifizierung zu verlangen, wenn objektive und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugang dies rechtfertigen. Gleichzeitig schränkt der RTS-Änderungsentwurf den Anwendungsbereich der in Artikel 10 der Delegierten Verordnung (EU) 2018/389 der Kommission enthaltene Kann-Bestimmung, wonach eine Ausnahme gewährt werden darf, auf die Fälle ein, in denen der Kunde direkt auf die Kontoinformationen zugreift. Darüber hinaus verlängert der RTS-Änderungsentwurf den Zeitabstand für die Erneuerung der starken Kundenauthentifizierung bei Anwendung der vorgenannten Ausnahmen von 90 Tagen auf 180 Tage. Zahlungsdienstleister, die sowohl eine dedizierte Schnittstelle als auch einen Notfallmechanismus anbieten, sind nicht verpflichtet, die SCA-Ausnahme bei ihrem Notfallmechanismus zu implementieren, sofern sie die SCA-Ausnahme bei den direkten Kundenkanälen nicht anwenden.

DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION

vom 3.8.2022

zur Änderung der in der Delegierten Verordnung (EU) 2018/389 festgelegten technischen Regulierungsstandards im Hinblick auf die 90-tägige Ausnahme für den Kontozugriff

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG[1], insbesondere auf Artikel 98 Absatz 4 Unterabsatz 2,

in Erwägung nachstehender Gründe:

(1) Artikel 10 der Delegierten Verordnung (EU) 2018/389 der Kommission[2] sieht eine Ausnahme von der in Artikel 97 der Richtlinie (EU) 2015/2366 verankerten Pflicht zur starken Kundenauthentifizierung vor, wenn ein Zahlungsdienstnutzer nur auf seinen Kontostand und die jüngsten Vorgänge auf seinem Zahlungskonto zugreift, ohne dass dabei sensible Zahlungsdaten offengelegt werden. In diesem Fall dürfen Zahlungsdienstleister beim Zugriff auf Kontoinformationen von der starken Kundenauthentifizierung absehen, sofern beim erstmaligen Zugriff auf die Kontoinformationen und anschließend mindestens alle 90 Tage eine starke Kundenauthentifizierung verlangt wird.

(2) Die Nutzung dieser Ausnahme hat in der Praxis zu einer überaus unterschiedlichen Anwendung der Delegierten Verordnung (EU) 2018/389 geführt, wobei die starke Kundenauthentifizierung von manchen kontoführenden Zahlungsdienstleistern alle 90 Tage verlangt wird, von anderen dagegen in kürzeren Zeitabständen und von manchen, die die Ausnahme gar nicht anwenden, bei jedem Kontozugriff eine starke Kundenauthentifizierung verlangt wird. Diese Unterschiedlichkeit hat bei der Nutzung von Kontoinformationsdiensten zu unerwünschten Reibungen in der „Customer Journey“ und zu negativen Auswirkungen auf die Dienste von Kontoinformationsdienstleistern geführt.

(3) Um ein angemessenes Gleichgewicht zwischen den Zielen der Richtlinie (EU) 2015/2366, d.h. zwischen der Erhöhung der Sicherheit, der Erleichterung von Innovationen und der Förderung des Wettbewerbs im Binnenmarkt sicherzustellen, ist

[1] ABl. L 337 vom 23.12.2015, S. 35.

[2] 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).

es notwendig, die Anwendung der in Artikel 10 der Delegierten Verordnung (EU) 2018/389 vorgesehenen Ausnahme für den Fall, dass über einen Kontoinformationsdienstleister auf die Kontoinformationen zugegriffen wird, zu präzisieren. So sollte die starke Kundenauthentifizierung Zahlungsdienstleistern in einem solchen Fall nicht freigestellt sein, sondern sollte die Ausnahme verbindlich vorgeschrieben werden, sofern Bedingungen erfüllt sind, die darauf abzielen, den Schutz und die Sicherheit der Daten der Zahlungsdienstnutzer zu gewährleisten.

(4) Die Ausnahme sollte nur für den Zugriff auf den Kontostand und die jüngsten Zahlungsvorgänge auf einem Zahlungskonto gelten, bei dem keine sensiblen Zahlungsdaten offengelegt werden. Die Ausnahme sollte nur dann gelten, wenn die Zahlungsdienstleister beim erstmaligen Zugriff über den jeweiligen Kontoinformationsdienstleister bereits eine starke Kundenauthentifizierung verlangt haben, und sollte regelmäßig erneuert werden.

(5) Um den Schutz und die Sicherheit der Daten der Zahlungsdienstnutzer zu gewährleisten, sollten Zahlungsdienstleister jederzeit eine starke Kundenauthentifizierung verlangen dürfen, wenn sie objektiv gerechtfertigte und gebührend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugriff haben. Dies könnte der Fall sein, wenn die Transaktionsüberwachungsmechanismen des kontoführenden Zahlungsdienstleisters ein erhöhtes Risiko eines nicht autorisierten oder betrügerischen Zugriffs erkennen. Um eine einheitliche Anwendung der Ausnahme zu gewährleisten, sollten die kontoführenden Zahlungsdienstleister die Gründe für die Durchführung einer starken Kundenauthentifizierung in solchen Fällen dokumentieren und gegenüber ihrer zuständigen nationalen Behörde auf Verlangen gebührend rechtfertigen.

(6) Greift der Zahlungsdienstnutzer direkt auf die Kontoinformationen zu, sollte es den Zahlungsdienstleistern weiterhin freigestellt sein, ob sie eine starke Kundenauthentifizierung verlangen. Grund dafür ist, dass in solchen Fällen, im Gegensatz zum Zugriff über einen Kontoinformationsdienstleister, keine besonderen Probleme beobachtet wurden, die eine Änderung der in Artikel 10 der Delegierten Verordnung (EU) 2018/389 vorgesehenen Ausnahme erforderlich machen würden.

(7) Um gleiche Wettbewerbsbedingungen für alle Zahlungsdienstleister zu gewährleisten und im Einklang mit dem Ziel der Richtlinie (EU) 2015/2366, die Entwicklung benutzerfreundlicher und innovativer Dienstleistungen zu ermöglichen, ist es verhältnismäßig, für die Erneuerung der starken Kundenauthentifizierung denselben Zeitraum von 180 Tagen sowohl für den direkten Zugriff auf Kontoinformationen beim kontoführenden Zahlungsdienstleister als auch für den Zugriff über einen Kontoinformationsdienstleister vorzusehen. Die Erneuerung der starken Kundenauthentifizierung mit der aktuellen Häufigkeit könnte zu unerwünschten Reibungen in der „Customer Journey“ führen und verhindern, dass Kontoinformationsdienstleister ihre Dienste anbieten und Nutzer diese Dienste in Anspruch nehmen.

(8) Kontoführende Zahlungsdienstleister, die eine dedizierte Schnittstelle anbieten und einen Notfallmechanismus nach Maßgabe von Artikel 33 Absatz 4 der Delegierten Verordnung (EU) 2018/389 eingerichtet haben, sollten nicht verpflichtet werden, die neue verbindlich vorgeschriebene Ausnahme in ihren direkten Kundenschnittstellen für den Notfallmechanismus zu implementieren, sofern sie die in Artikel 10 der Delegierten Verordnung (EU) 2018/389 vorgesehene Ausnahme nicht auf ihre direkten Kundenschnittstellen anwenden. Es wäre unverhältnismäßig, kontoführende

Zahlungsdienstleister, die eine dedizierte Schnittstelle anbieten, bei der sie die neue verbindlich vorgeschriebene Ausnahme implementieren müssen, dazu zu verpflichten, diese Ausnahme auch bei ihren direkten Kundenschnittstellen für den Notfallmechanismus zu implementieren.

(9) Um sicherzustellen, dass die Zahlungsdienstleister ausreichend Zeit haben, um an ihren Systemen die erforderlichen Veränderungen vorzunehmen, sollten die kontoführenden Zahlungsdienstleister den Zahlungsdienstleistern die Veränderungen, die sie an den technischen Spezifikationen ihrer Schnittstellen vorgenommen haben, um dieser Verordnung nachzukommen, mindestens zwei Monate, bevor diese Veränderungen implementiert werden, zur Verfügung stellen.

(10) Die Delegierte Verordnung (EU) 2018/389 sollte daher entsprechend geändert werden.

(11) Die vorliegende Verordnung beruht auf dem Entwurf technischer Regulierungsstandards, der der Kommission von der Europäischen Bankenaufsichtsbehörde übermittelt wurde.

(12) Die Europäische Bankenaufsichtsbehörde hat zu diesem Entwurf öffentliche Konsultationen durchgeführt, die damit verbundenen potenziellen Kosten- und Nutzeneffekte analysiert und die Stellungnahme der nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlament und des Rates[3] eingesetzten Interessengruppe Bankensektor eingeholt.

(13) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 konsultiert und hat am 7. Juni 2022 eine förmliche Stellungnahme abgegeben.

(14) Um einen reibungslosen Übergang zu den in dieser Verordnung festgelegten neuen Anforderungen zu ermöglichen, sollte es Zahlungsdienstleistern, die die Ausnahme nach Artikel 10 der Delegierten Verordnung (EU) 2018/389 vor dem Geltungsbeginn der vorliegenden Verordnung angewandt haben, gestattet werden, diese Ausnahme noch für einen Zeitraum von bis zu 90 Tagen ab der letzten starken Kundenauthentifizierung anzuwenden –

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1
Änderung der Delegierten Verordnung (EU) 2018/389

Die Delegierte Verordnung (EU) 2018/389 wird wie folgt geändert:

1. Artikel 10 erhält folgende Fassung:

[3] 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).

„Artikel 10

Zugriff auf Zahlungskontoinformationen direkt beim kontoführenden Zahlungsdienstleister

(1) Zahlungsdienstleister dürfen unter Einhaltung der in Artikel 2 festgelegten Anforderungen davon absehen, eine starke Kundenauthentifizierung zu verlangen, wenn ein Zahlungsdienstnutzer direkt auf seine Zahlungskontoinformationen online zugreift und sich dieser Zugriff auf eine der folgenden Online-Abfragen beschränkt, ohne dass sensible Zahlungsdaten offengelegt werden:

a) Kontostand eines oder mehrerer bezeichneter Zahlungskonten;

b) Zahlungsvorgänge, die in den vergangenen 90 Tagen über ein oder mehrere bezeichnete Zahlungskonten ausgeführt wurden.

(2) Abweichend von Absatz 1 dürfen Zahlungsdienstleister nicht von der Durchführung einer starken Kundenauthentifizierung befreit werden, wenn eine der folgenden Bedingungen erfüllt ist:

a) Der Zahlungsdienstnutzer greift zum ersten Mal online auf die in Absatz 1 genannten Informationen zu.

b) Mehr als 180 Tage sind verstrichen, seitdem der Zahlungsdienstnutzer letztmals auf die in Absatz 1 Buchstabe b genannten Informationen online zugegriffen hat und eine starke Kundenauthentifizierung verlangt wurde.“

2. Folgender Artikel 10a wird eingefügt:

„Artikel 10a

Zugriff auf Zahlungskontoinformationen über einen Kontoinformationsdienstleister

(1) Zahlungsdienstleister dürfen keine starke Kundenauthentifizierung verlangen, wenn ein Zahlungsdienstnutzer über einen Kontoinformationsdienstleister online auf sein Zahlungskonto zugreift und sich dieser Zugriff auf eine der folgenden Online-Abfragen beschränkt, ohne dass sensible Zahlungsdaten offengelegt werden:

a) Kontostand eines oder mehrerer bezeichneter Zahlungskonten;

b) Zahlungsvorgänge, die in den vergangenen 90 Tagen über ein oder mehrere bezeichnete Zahlungskonten ausgeführt wurden.

(2) Abweichend von Absatz 1 verlangen Zahlungsdienstleister eine starke Kundenauthentifizierung, wenn eine der folgenden Bedingungen erfüllt ist:

a) Der Zahlungsdienstnutzer greift zum ersten Mal über den Kontoinformationsdienstleister online auf die in Absatz 1 genannten Informationen zu.

b) Mehr als 180 Tage sind verstrichen, seitdem der Zahlungsdienstnutzer letztmals über den Kontoinformationsdienstleister auf die in Absatz 1

Buchstabe b genannten Informationen online zugegriffen hat und eine starke Kundenauthentifizierung verlangt wurde.

(3) Abweichend von Absatz 1 ist es Zahlungsdienstleistern gestattet, eine starke Kundenauthentifizierung zu verlangen, wenn ein Zahlungsdienstnutzer über einen Kontoinformationsdienstleister online auf sein Zahlungskonto zugreift und der Zahlungsdienstleister sachlich gerechtfertigte und hinreichend nachgewiesene Gründe im Zusammenhang mit einem nicht autorisierten oder betrügerischen Zugriff auf das Zahlungskonto hat. In einem solchen Fall werden die Gründe für die Durchführung einer starken Kundenauthentifizierung vom Zahlungsdienstleister dokumentiert und gegenüber seiner zuständigen nationalen Behörde auf Verlangen gebührend gerechtfertigt.

(4) Kontoführende Zahlungsdienstleister, die eine dedizierte Schnittstelle im Sinne von Artikel 31 anbieten, sind nicht verpflichtet, die in Absatz 1 vorgesehene Ausnahme für die Zwecke des in Artikel 33 Absatz 4 genannten Notfallmechanismus zu implementieren, wenn sie die in Artikel 10 vorgesehene Ausnahme bei der direkten Schnittstelle für die Authentifizierung und Kommunikation mit ihren Zahlungsdienstnutzern nicht anwenden.“

3. In Artikel 30 wird folgender Absatz 4a eingefügt:

„(4a) Abweichend von Absatz 4 stellen kontoführende Zahlungsdienstleister den in diesem Artikel genannten Zahlungsdienstleistern die Veränderungen, die sie an den technischen Spezifikationen ihrer Schnittstellen vorgenommen haben, um Artikel 10a nachzukommen, mindestens zwei Monate, bevor diese Veränderungen implementiert werden, zur Verfügung.“

Artikel 2
Übergangsbestimmungen

(1) Zahlungsdienstleister, die die in Artikel 10 der Delegierten Verordnung (EU) 2018/389 vorgesehene Ausnahme vor dem ... [OP, bitte Datum einfügen: 7 Monate nach Inkrafttreten dieser Verordnung] angewandt haben, dürfen diese Ausnahme bei Zugriffsanfragen über einen Kontoinformationsdienstleister solange weiter anwenden, bis die Geltungsdauer der betreffenden Ausnahme endet.

(2) Abweichend von Absatz 1 unterliegt jede neue starke Kundenauthentifizierung, die bei Zugriffsanfragen über einen Kontoinformationsdienstleister durchgeführt wird, bevor die in Absatz 1 genannte Geltungsdauer der Ausnahme endet, dem mit dieser Verordnung eingeführten Artikel 10a.

Artikel 3
Inkrafttreten und Geltungsbeginn

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem … [OP: Bitte Datum 7 Monate nach Inkrafttreten dieser Verordnung einfügen].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 3.8.2022

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN