Formelle Bemerkungen des EDSB zum Entwurf eines Vorschlags für eine delegierte Verordnung der Kommission zur Änderung der Delegierten Verordnung (EU) 2018/389 der Kommission zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für gemeinsame und sichere offene Standards für die Kommunikation

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die 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 und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[1], insbesondere auf Artikel 42 Absatz 1, –

HAT DIE FOLGENDEN FORMELLEN BEMERKUNGEN ANGENOMMEN:

1. Einleitung und Hintergrund

1. Die Europäische Kommission hat den Entwurf eines Vorschlags für eine delegierte Verordnung der Kommission zur Änderung der Delegierten Verordnung (EU) 2018/389 der Kommission zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und gemeinsame und sichere offene Standards für die Kommunikation (im Folgenden „Vorschlagsentwurf“) vorgelegt.

2. Ziel des Vorschlagsentwurfs ist die Aktualisierung der technischen Regulierungsstandards, die als Delegierte Verordnung (EU) 2018/389 der Kommission[2] (im Folgenden „Delegierte Verordnung“) angenommen wurden und seit dem 14. September 2019 gelten.

[1] ABl. L 295 vom 21.11.2018, S. 39.

[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 gemeinsame und sichere offene Standards für die Kommunikation (ABl. L 69 vom 13.3.2018, S. 23).

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

3. Die bestehenden technischen Regulierungsstandards wurden gemäß Artikel 98 Absatz 1 der Richtlinie (EU) 2015/2366[3] (im Folgenden „PSD2“) angenommen, dem zufolge die Europäische Bankenaufsichtsbehörde („EBA“) technische Regulierungsstandards für eine starke Kundenauthentifizierung und gemeinsame und sichere offene Standards für die Kommunikation ausarbeitet. Gemäß Artikel 98 Absatz 5 der PSD2 müssen die technischen Regulierungsstandards regelmäßig überprüft und aktualisiert werden.

4. Mit den vorliegenden formellen Bemerkungen des EDSB wird ein Konsultationsersuchen der Europäischen Kommission vom 2. Mai 2022 gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 (im Folgenden „EU-DSVO“)[4] beantwortet.

5. Diese formellen Bemerkungen schließen künftige zusätzliche Bemerkungen des EDSB nicht aus, insbesondere, falls weitere Probleme festgestellt oder neue Informationen verfügbar werden sollten, beispielsweise infolge der Annahme einschlägiger Durchführungsrechtsakte oder delegierter Rechtsakte.[5]

6. Diese formellen Bemerkungen lassen etwaige künftige Maßnahmen des EDSB in Ausübung seiner Befugnisse gemäß Artikel 58 der Verordnung (EU) 2018/1725 unberührt und beschränken sich auf die Bestimmungen des Vorschlags, die unter dem Blickwinkel des Datenschutzes relevant sind.

---

[3] 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). Siehe auch die Stellungnahme des Europäischen Datenschutzbeauftragten zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2006/48/EG und 2009/110/EG und zur Aufhebung der Richtlinie 2007/64/EG, sowie für eine Verordnung des Europäischen Parlaments und des Rates über Interbankenentgelte für kartengebundene Zahlungsvorgänge.

[4] 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).

[5] Für den Fall anderer Durchführungsrechtsakte oder delegierter Rechtsakte mit Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten möchte der EDSB daran erinnern, dass er auch zu diesen Rechtsakten konsultiert werden muss. Gleiches gilt für künftige Änderungen, mit denen neue oder geltende Bestimmungen, die direkt oder indirekt die Verarbeitung personenbezogener Daten betreffen, eingeführt oder geändert würden.

2. Bemerkungen

2.1. Neue Ausnahmen von der Anwendung der starken Kundenauthentifizierung (SCA)

7. Der EDSB stellt fest, dass mit Artikel 1 des Vorschlagsentwurfs, der Artikel 10 der Delegierten Verordnung durch einen neuen Artikel 10 ersetzen würde, eine Änderung der Ausnahme von der SCA eingeführt wird, die für den Fall gilt, dass ein Kunde einen kontoführenden Zahlungsdienstleister (im Folgenden „ASPSP") nutzt, um direkt auf seine Zahlungskontoinformationen zuzugreifen, und dass der Zugang online auf eines oder beide der folgenden Elemente beschränkt ist, 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.
   In diesem Fall wird die Frist für die obligatorische Verlängerung der SCA durch den geänderten Artikel 10 von 90 Tagen auf 180 Tage verlängert, seit der Zahlungsdienstnutzer zuletzt auf sein Zahlungskonto und seine SCA zugegriffen hat.[6]

8. Mit Artikel 1 Absatz 2 des Vorschlagsentwurfs würde ein neuer Artikel 10a in die delegierte Verordnung aufgenommen, der den Zugang eines Kunden zu den Zahlungskontoinformationen über einen Kontoinformationsdienstleister („AISP") zum Gegenstand hat. In diesem Fall wenden die Zahlungsdienstleister die SCA nicht an, wenn ein Kunde einen AISP nutzt, um auf seine Zahlungskontoinformationen zuzugreifen, und dieser Zugriff auf eines oder beide der folgenden Elemente im Internet beschränkt ist, 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.

9. Auch in diesem Fall (Zugang über AISP) verlängert sich die Frist für die obligatorische Verlängerung der SCA von 90 Tagen auf 180 Tage, nachdem der Zahlungsdienstnutzer zuletzt online auf sein Zahlungskonto zugegriffen hat und eine SCA erfolgt ist.
   Der EDSB stellt ferner fest, dass Zahlungsdienstleistern im Falle des Zugriffs über einen AISP gestattet werden soll, eine SCA anzuwenden, wenn ein Zahlungsdienstnutzer online auf das Zahlungskonto zugreift und dem Zahlungsdienstleister sachlich gerechtfertigte und hinreichend nachgewiesene

[6] Siehe Artikel 10 Absatz 2 Buchstabe b.

Gründe für die Vermutung eines nicht autorisierten oder betrügerischen Zugriffs auf das Zahlungskonto vorliegen.[7]
Darüber hinaus ist es ASPSP, die die Zugangsschnittstelle[8] anbieten, gestattet, die SCA für die Zwecke des Notfallmechanismus anzuwenden, wenn die Zugangsschnittstelle nicht im Einklang mit Artikel 32 der Delegierten Verordnung funktioniert, die Schnittstelle ungeplant nicht verfügbar ist und eine Systemstörung vorliegt.[9]

10. Der EDSB erinnert daran, dass in den „Leitlinien des EDSA zum Zusammenspiel zwischen der zweiten Zahlungsdiensterichtlinie und der DSGVO“[10] betont wird, dass Dienstleister hohen Standards genügen sollten, einschließlich starker Mechanismen für die Kundenauthentifizierung und hoher Sicherheitsstandards für die technische Ausrüstung.

11. Der EDSB stellt fest, dass der Vorschlagsentwurf auf einer umfassenden öffentlichen Konsultation beruht, bei der sich eine Vielzahl von Interessenträgern positiv zu den eingeführten Änderungen geäußert hat, wie in der Folgenabschätzung der EBA[11] dokumentiert.

12. Der EDSB stimmt der Bewertung der EBA zu, wonach die mit dem Vorschlagsentwurf eingeführten Änderungen das richtige Gleichgewicht zwischen Nutzererfahrung und dem hohen Sicherheitsniveau, das für Zahlungsdienste erforderlich ist, herstellen.[12] Daher spricht der EDSB diesbezüglich keine weiteren Empfehlungen aus.

[7] Siehe Artikel 10a Absatz 3.
[8] Schnittstelle gemäß Artikel 31 der Delegierten Verordnung.
[9] Siehe Artikel 10a Absatz 4.
[10] EDSA Leitlinien 06/2020 zum Zusammenspiel zwischen der zweiten Zahlungsdiensterichtlinie und der DSGVO, Version 2.0, angenommen am 15. Dezember 2022, Ziffer 71, S. 26.
[11] Abschlussbericht der EBA, Entwurf technischer Regulierungsstandards zur Änderung der Delegierten Verordnung (EU) 2018/389 der Kommission zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und gemeinsame und sichere offene Standards für die Kommunikation, EBA/RTS/2022/03, 5. April 2022 (im Folgenden „EBA-Abschlussbericht“).
[12] Abschlussbericht der EBA, Ziffer 17, S. 9. Insbesondere zur Ausnahme von der SCA für AISP, siehe Ziffer 20, S. 9; zur Änderung der Häufigkeit der Verlängerung der SCA, siehe Ziffer 27, S. 11.

2.2. Fehlender Verweis auf diese Konsultation in einem Erwägungsgrund des Vorschlagsentwurfs

13. Der EDSB stellt fest, dass ein Verweis auf diese Konsultation in keinem Erwägungsgrund des Vorschlags zu finden ist. Der EDSB empfiehlt daher, einen solchen Verweis in einen Erwägungsgrund des Vorschlagsentwurfs aufzunehmen.

Brüssel, den 7. Juni 2022

(elektronisch unterzeichnet)
Wojciech Rafał Wiewiórowski