EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

22. August 2023

Stellungnahme 39/2023

zu dem Vorschlag für eine Zahlungsdiensteverordnung im Binnenmarkt und dem Vorschlag für eine Richtlinie über Zahlungsdienste und E-Geld-Dienste im Binnenmarkt

edps.europa.eu

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 52 Absatz 2 der Verordnung (EU) 2018/1725 im „Hinblick auf die Verarbeitung personenbezogener Daten […] sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Datenschutz, von den Organen und Einrichtungen der Union geachtet werden", und er ist gemäß Artikel 52 Absatz 3 „für die Beratung der Organe und Einrichtungen der Union und der betroffenen Personen in allen Fragen der Verarbeitung personenbezogener Daten" zuständig.

Am 5. Dezember 2019 wurde Wojciech Rafał Wiewiórowski für einen Zeitraum von fünf Jahren zum Europäischen Datenschutzbeauftragten ernannt.

*Gemäß **Artikel 42 Absatz 1** der Verordnung 2018/1725 konsultiert die Kommission den Europäischen Datenschutzbeauftragten „[n]ach der Annahme von Vorschlägen für einen Gesetzgebungsakt, für Empfehlungen oder Vorschläge an den Rat nach Artikel 218 AEUV sowie bei der Ausarbeitung von delegierten Rechtsakten und Durchführungsrechtsakten, die Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten haben".*

Diese Stellungnahme bezieht sich auf den Vorschlag für eine Zahlungsdiensteverordnung im Binnenmarkt[1] und den Vorschlag für eine Richtlinie über Zahlungsdienste und E-Geld-Dienste im Binnenmarkt[2]. Die vorliegende Stellungnahme schließt künftige zusätzliche Bemerkungen oder Empfehlungen des EDSB nicht aus, insbesondere wenn weitere Probleme festgestellt oder neue Informationen bekannt werden. Diese Stellungnahme greift etwaigen künftigen Maßnahmen, die der EDSB in Ausübung seiner Befugnisse gemäß der Verordnung (EU) 2018/1725 ergreifen mag, nicht vor. Die Stellungnahme beschränkt sich auf die Bestimmungen der Vorschläge, die unter dem Gesichtspunkt des Datenschutzes relevant sind.

[1] COM(2023) 367 final.
[2] COM(2023) 366 final.

Zusammenfassung

Am 28. Juni 2023 legte die Europäische Kommission zwei Vorschläge vor: einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/21 (der „Vorschlag für eine Zahlungsdiensteverordnung“) und einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste und E-Geld-Dienste im Binnenmarkt und zur Änderung der Richtlinie 98/26/EG und zur Aufhebung der Richtlinien 2015/2366/EU und 2009/110/EG (der „Vorschlag für eine dritte Zahlungsdiensterichtlinie“) – zusammen „die Vorschläge“.

Bei Zahlungsdiensten werden häufig personenbezogene Daten verarbeitet, die sensible Informationen über eine betroffene Person enthalten können. Der EDSB begrüßt daher die Bemühungen, die unternommen wurden, um die Vereinbarkeit mit der Datenschutz-Grundverordnung („DSGVO“) zu gewährleisten. Er unterstreicht zudem die Notwendigkeit einer klaren Unterscheidung zwischen den „Erlaubnissen“ gemäß den Vorschlägen und der Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen der Datenschutz-Grundverordnung.

Eines der Ziele der Vorschläge besteht darin, den Anbietern von Zahlungssystemen und Zahlungsdiensten die Möglichkeit zu geben, besondere Kategorien personenbezogener Daten im öffentlichen Interesse des reibungslosen Funktionierens des Binnenmarktes für Zahlungsdienste zu verarbeiten. Da die Verarbeitung solcher Daten einen schwerwiegenden Eingriff in das Recht auf Achtung des Privatlebens und den Schutz personenbezogener Daten darstellen kann, ist es wichtig, dass die Rechtsvorschriften präzise genug sind, um den objektiven Zusammenhang zwischen jeder Datenkategorie in einem bestimmten Zahlungskontext und dem zu erreichenden Ziel des öffentlichen Interesses aufzuzeigen.

Der EDSB begrüßt, dass die Vorschläge kontoführende Zahlungsdienstleister dazu verpflichten würden, dem Nutzer ein Dashboard zur Verfügung zu stellen, mit dem er die von ihm erteilten Erlaubnisse überwachen und verwalten kann. Um das Risiko einer unrechtmäßigen Weitergabe personenbezogener Daten durch kontoführende Zahlungsdienstleister weiter zu verringern, empfiehlt der EDSB,

◦ sicherzustellen, dass im Dashboard auf den/die speziell benannten Zahlungsdienst(e) verwiesen wird, für den/die der Nutzer seine Erlaubnis erteilt hat;

◦ zu gewährleisten, dass Zugangsverlangen auf das für die Erbringung der erbetenen Dienstleistung erforderliche Maß beschränkt bleiben;

◦ Klarheit in Bezug auf die Rechtsgrundlage von Zugangsverlangen zu gewährleisten,

◦ dem kontoführenden Zahlungsdienstleister zu gestatten, die vom Zahlungsdienstnutzer erteilte Erlaubnis zu überprüfen oder geeignete alternative Garantien in den Vorschlag für eine Zahlungsdiensteverordnung aufzunehmen.

Schließlich empfiehlt der EDSB, eine enge Zusammenarbeit zwischen den gemäß dem Vorschlag zuständigen Behörden und den Datenschutzaufsichtsbehörden sicherzustellen, um eine einheitliche Anwendung und Durchsetzung der Vorschläge und des EU-Datenschutzrechts zu gewährleisten. Der EDSB empfiehlt daher, in Artikel 93 Absatz 3 des Vorschlags für eine

Zahlungsdiensteverordnung ausdrücklich auf die für die Überwachung und Durchsetzung des Datenschutzrechts zuständigen Aufsichtsbehörden zu verweisen.

Inhalt

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, Einrichtungen und sonstigen Stellen der Union und zum freien Datenverkehr[3], insbesondere auf Artikel 42 Absatz 1 –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

1. Am 28. Juni 2023 legte die Europäische Kommission zwei Vorschläge vor: einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt und zur Änderung der Verordnung (EU) Nr. 1093/21 (der „Vorschlag für eine Zahlungsdiensteverordnung“)[4] und einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste und E-Geld-Dienste im Binnenmarkt und zur Änderung der Richtlinie 98/26/EG und zur Aufhebung der Richtlinien 2015/2366/EU und 2009/110/EG (der „Vorschlag für eine dritte Zahlungsdiensterichtlinie“)[5] – zusammen „die Vorschläge“.

2. Dem Vorschlag für eine Zahlungsdiensteverordnung und dem Vorschlag für eine dritte Zahlungsdiensterichtlinie sind jeweils drei Anhänge beigefügt (insgesamt sechs Anhänge), in denen die Arten der Zahlungsdienste (Anhang I) sowie die Art der E-Geld-Dienste (Anhang II) beschrieben werden, die in den Anwendungsbereich der Vorschläge fallen. Schließlich enthält Anhang III eine Entsprechungstabelle, die zeigt, welche Bestimmungen der Richtlinien (EU) 2015/2366 und 2009/110/EG welchen Bestimmungen der Vorschläge entsprechen.

3. Der EDSB stellt fest, dass die von den Vorschlägen abgedeckten Arten von Diensten im Wesentlichen die gleichen zu sein scheinen wie die Dienste, die von der 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 („zweite Zahlungsdiensterichtlinie“ bzw. „PSD2“)[6] erfasst werden.

4. Die spezifischen Zielsetzungen des Vorschlags für eine Zahlungsdiensteverordnung lauten[7]:

    a. Stärkung des Nutzerschutzes und des Vertrauens in den Zahlungsverkehr, insbesondere durch die Verbesserung der Anwendung einer starken

[3] ABl. L 295 vom 21.11.2018, S. 39.
[4] COM(2023) 367 final.
[5] COM(2023) 366 final.
[6] 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).
[7] COM(2023) 367 final, S. 5-6.

Kundenauthentifizierung, die Schaffung einer Rechtsgrundlage für den Austausch von Informationen über Betrug, die Ausweitung der Überprüfung der internationalen Kontonummer (IBAN) auf alle Überweisungen und die Verbesserung der Nutzerrechte und -informationen;

b. Verbesserung der Wettbewerbsfähigkeit von Open-Banking-Diensten durch: i) die Verpflichtung der kontoführenden Zahlungsdienstleister, eine dedizierte Datenzugangsschnittstelle und „Erlaubnis-Dashboards" einzurichten, um den Nutzern die Verwaltung ihrer gewährten Open-Banking-Zugangserlaubnisse zu ermöglichen, und ii) die Festlegung detaillierterer Spezifikationen für Mindestanforderungen an Open-Banking-Datenschnittstellen;

c. Verbesserung der Durchsetzung und Umsetzung des Rechtsrahmens für Zahlungsdienste in den Mitgliedstaaten, insbesondere durch die Ersetzung der zweiten Zahlungsdiensterichtlinie durch eine unmittelbar geltende Verordnung („Vorschlag für eine Zahlungsdiensteverordnung"), mit der unklare Aspekte der zweiten Zahlungsdiensterichtlinie präzisiert werden, und durch die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden und anderen Behörden;

d. Verbesserung des (direkten oder indirekten) Zugangs zu Zahlungssystemen und Bankkonten für Nicht-Banken-Zahlungsdienstleister, einschließlich Zahlungsauslösedienstleistern (PISP) und Kontoinformationsdienstleistern (AISP).

5. Die Vorschläge werden in Verbindung mit dem Vorschlag für eine Verordnung über den Zugang zu Finanzdaten („FiDA-Vorschlag")[8] vorgelegt, der u. a. den Zugang zu anderen Finanzdaten als Zahlungskontodaten betrifft, die in den Anwendungsbereich der Vorschläge fallen, die Gegenstand dieser Stellungnahme sind[9].

6. Im Wesentlichen würde der Vorschlag für eine Zahlungsdiensteverordnung:

   a. Anforderungen an die Transparenz der Bedingungen und Informationsanforderungen für Zahlungsdienste festlegen[10];

   b. Rechte und Pflichten in Bezug auf die Erbringung und Nutzung von Zahlungsdiensten festlegen, einschließlich Vorschriften über Datenzugangsschnittstellen für Kontoinformationsdienste und Zahlungsauslösedienste[11] und über das Datenzugangsmanagement durch Zahlungsdienstnutzer[12]; Vorschriften über den Datenschutz[13]; Vorschriften über Mechanismen für die Meldung und Überwachung von Betrugsfällen und den Austausch von Betrugsdaten[14]; Vorschriften über die starke Kundenauthentifizierung[15]; Vorschriften über Durchsetzungsverfahren, zuständige Behörden und Sanktionen[16]; Vorschriften über Interventionsbefugnisse der Europäischen Bankenaufsichtsbehörde (EBA)[17].

[8] COM(2023) 360 final.
[9] COM(2023) 367 final, S. 4.
[10] Artikel 4 bis 26 des Vorschlags für eine Zahlungsdiensteverordnung.
[11] Artikel 35 bis 38 des Vorschlags für eine Zahlungsdiensteverordnung.
[12] Artikel 43 des Vorschlags für eine Zahlungsdiensteverordnung.
[13] Artikel 80 des Vorschlags für eine Zahlungsdiensteverordnung.
[14] Artikel 82 bis 84 des Vorschlags für eine Zahlungsdiensteverordnung.
[15] Artikel 85 bis 86 des Vorschlags für eine Zahlungsdiensteverordnung.
[16] Kapitel 8 des Vorschlags für eine Zahlungsdiensteverordnung.
[17] Kapitel 9 des Vorschlags für eine Zahlungsdiensteverordnung.

7. Der Vorschlag für eine dritte Zahlungsdiensterichtlinie stützt sich weitgehend auf Titel II der derzeitigen zweiten Zahlungsdiensterichtlinie über „Zahlungsdienstleister", der nur für Zahlungsinstitute gilt. Der Vorschlag aktualisiert und präzisiert die Bestimmungen über Zahlungsinstitute und führt E-Geld-Institute als eine Unterkategorie von Zahlungsinstituten ein. Er enthält zudem Bestimmungen über Bargeldabhebungsdienste, die von Einzelhändlern oder unabhängigen Geldautomatenbetreibern angeboten werden[18].

8. Mit der vorliegenden Stellungnahme des EDSB wird das Konsultationsersuchen der Europäischen Kommission vom 29. Juni 2023 gemäß Artikel 42 Absatz 1 der EU-DSVO beantwortet. Der EDSB begrüßt den Verweis auf diese Konsultation in Erwägungsgrund 147 des Vorschlags für eine Zahlungsdiensteverordnung und Erwägungsgrund 77 des Vorschlags für eine dritte Zahlungsdiensteverordnung. In diesem Zusammenhang stellt der EDSB erfreut fest, dass er bereits informell gemäß Erwägungsgrund 60 der EU-DSVO zu den Vorschlägen konsultiert wurde.

2. Allgemeine Bemerkungen

9. Der EDSB erkennt an, wie wichtig es ist, den Schutz der Nutzer und das Vertrauen in den Zahlungsverkehr zu stärken. Er unterstützt ferner das Ziel, die Durchsetzung und Umsetzung des Rechtsrahmens für Zahlungsdienste in den Mitgliedstaaten zu verbessern, sowie das Ziel, die Wettbewerbsfähigkeit von Open-Banking-Dienstleistungen zu verbessern.

10. In der Begründung des Vorschlags für eine Zahlungsdiensteverordnung wird darauf hingewiesen, dass sich dieser Vorschlag besonders auf das Grundrecht auf Datenschutz auswirkt[19]. Es wird ferner betont, dass die Verarbeitung personenbezogener Daten im Einklang mit der Datenschutz-Grundverordnung („DSGVO")[20] stehen muss, die direkt auf alle vom Vorschlag für eine Zahlungsdiensteverordnung betroffenen Zahlungsdienste Anwendung findet.[21]

11. Der EDSB begrüßt Erwägungsgrund 97 des Vorschlags für eine Zahlungsdiensteverordnung, in dem es insbesondere heißt, dass bei der Verarbeitung personenbezogener Daten die DSGVO eingehalten werden sollte, einschließlich der Grundsätze der Zweckbindung, der Datenminimierung und der Speicherbegrenzung. Er begrüßt ferner die ausdrückliche Bestätigung, dass die Aufsichtsbehörden im Rahmen der DSGVO und der EU-DSVO für die Überwachung der Verarbeitung personenbezogener Daten im Zusammenhang mit dem Vorschlag für eine Zahlungsdiensteverordnung zuständig sein sollten. Der EDSB begrüßt zudem Erwägungsgrund 99 der Vorschlags für eine Zahlungsdiensteverordnung, in dem präzisiert wird, dass die Bereitstellung von

[18] COM(2023) 367 final, S. 7.
[19] COM(2023) 367 final, S. 8.
[20] 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.
[21] COM(2023) 367 final, S. 8.

Informationen an natürliche Personen über die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO und der EU-DSVO erfolgen sollte.

12. Der EDSB stellt fest, dass der Vorschlag für eine Zahlungsdiensteverordnung darauf abzielt, die Kohärenz mit dem FiDA-Vorschlag zu gewährleisten. In diesem Zusammenhang verweist der EDSB auf die Empfehlungen in seiner Stellungnahme zum FiDA-Vorschlag, insbesondere in Bezug auf den Begriff „Erlaubnis", auf den sowohl im Vorschlag für eine Zahlungsdiensteverordnung als auch im FiDA-Vorschlag Bezug genommen wird.

3. Rolle der „Erlaubnisse"

13. Der EDSB begrüßt, dass der Vorschlag für eine Zahlungsdiensteverordnung darauf abzielt, einige der Wechselwirkungen zwischen der zweiten Zahlungsdiensterichtlinie und dem EU-Datenschutzrahmen anzugehen. Eine solche Wechselwirkung, die auch in den Leitlinien des EDSB zu diesem Thema[22] erwähnt wird, betrifft die Unterscheidung zwischen der „ausdrücklichen Zustimmung" im Rahmen der zweiten Zahlungsdiensterichtlinie einerseits und der „Einwilligung" bzw. der „ausdrücklichen Einwilligung" gemäß der Datenschutz-Grundverordnung andererseits.

14. Der EDSB merkt an, dass in Erwägungsgrund 69 des Vorschlags für eine Zahlungsdiensteverordnung festgelegt ist, dass die Erlaubnis nicht ausschließlich als „Einwilligung" oder „ausdrückliche Einwilligung" im Sinne der Verordnung (EU) 2016/679 ausgelegt werden sollte. Der EDSB ist der Ansicht, dass das Wort „ausschließlich" eine gewisse Unsicherheit mit sich bringt und keine klare Unterscheidung zwischen „Erlaubnis" (die sich auf die Annahme der gewerblichen Dienstleistung durch den Verbraucher bezieht) einerseits und „Einwilligung" (gemäß Artikel 6 Absatz 1 Buchstabe a der DSGVO) oder „ausdrückliche Zustimmung" (gemäß Artikel 9 Absatz 2 Buchstabe a der DSGVO) andererseits ermöglicht. Erwägungsgrund 69 sollte daher so geändert werden, dass deutlich wird, dass die Erlaubnis nicht als „Einwilligung" oder „ausdrückliche Einwilligung" oder „für die Erfüllung eines Vertrags erforderlich" im Sinne der Verordnung (EU) 2016/679 ausgelegt werden sollte.

15. Der EDSB empfiehlt ferner – ähnlich wie in Erwägungsgrund 10 des FiDA-Vorschlags –, klarzustellen, dass Zahlungsauslösedienstleister und Kontoinformationsdienstleister einen rechtmäßigen Grund für die Verarbeitung personenbezogener Daten gemäß der DSGVO sicherstellen müssen[23]. Ebenso empfiehlt der EDSB, zu präzisieren, dass die Erteilung der Erlaubnis durch einen Zahlungsdienstnutzer insbesondere die Verpflichtungen der Datennutzer gemäß Artikel 6 und Artikel 9 der Datenschutz-Grundverordnung[24] unberührt lässt.

---

[22] Leitlinien 06/2020 des EDSA zum Zusammenspiel zwischen der zweiten Zahlungsdiensterichtlinie und der DSGVO, angenommen am 15. Dezember 2020, Absatz 44.

[23] In Erwägungsgrund 10 des FiDA-Vorschlags heißt es, dass ein Datennutzer über eine gültige Rechtsgrundlage für die Verarbeitung gemäß der Verordnung (EU) 2016/679 verfügen sollte, wenn personenbezogene Daten verarbeitet werden.

[24] Siehe in diesem Sinne auch Erwägungsgrund 48 des FiDA-Vorschlags, wonach die Erteilung der Erlaubnis durch einen Kunden nicht die Pflichten der Datennutzer gemäß Artikel 6 der Verordnung (EU) 2016/679 berührt. *Personenbezogene Daten, die zur Verfügung gestellt und an einen Datennutzer weitergegeben werden, sollten nur dann für Dienste verarbeitet werden, die von einem Datennutzer bereitgestellt werden, wenn eine gültige Rechtsgrundlage gemäß Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 besteht und gegebenenfalls die Anforderungen des Artikels 9 der genannten Verordnung in Bezug auf die Verarbeitung besonderer Datenkategorien erfüllt sind.*

4. Überprüfung der Erlaubnis durch den kontoführenden Zahlungsdienstleister

16. Der EDSB stellt fest, dass Zahlungsauslösedienstleister und Kontoinformationsdienstleister gemäß Artikel 43 Absatz 4 Buchstabe b der Vorschlags für eine Zahlungsdiensteverordnung verpflichtet wären, kontoführende Zahlungsdienstleister in Echtzeit über eine neue, von einem Zahlungsdienstnutzer erteilte Erlaubnis zu informieren.

17. Der EDSB ist jedoch darüber besorgt, dass Artikel 44 Absatz 1 Buchstabe c und Artikel 49 Absatz 4 des Vorschlags für eine Zahlungsdiensteverordnung die kontoführenden Zahlungsdienstleister daran hindern würden, die Erlaubnis zu überprüfen, die der Zahlungsdienstnutzer Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern erteilt hat, damit sie auf seine Zahlungskontoinformationen zugreifen können. Obwohl der Begriff „Erlaubnis" nicht als „Einwilligung" oder „ausdrückliche Einwilligung" im Sinne der DSGVO ausgelegt werden sollte, kann ein Verbot, die vom Nutzer erteilte Erlaubnis zu überprüfen, dazu führen, dass kontoführende Zahlungsdienstleister personenbezogene Daten an Dritte weitergeben, die *keine* angemessene Rechtsgrundlage gemäß der DSGVO sichergestellt haben (oder mehr personenbezogene Daten weitergeben als vom Nutzer beabsichtigt).

18. Jeder für die Verarbeitung Verantwortliche hat die Pflicht, sicherzustellen, dass personenbezogene Daten nicht in einer Weise weiterverarbeitet werden, die mit den Zwecken, für die sie ursprünglich erhoben wurden, unvereinbar ist. Jede Weitergabe durch einen für die Verarbeitung Verantwortlichen bedarf einer Rechtsgrundlage und einer Bewertung der Vereinbarkeit, unabhängig davon, ob es sich bei dem Empfänger um einen eigenständig für die Verarbeitung Verantwortlichen oder einen gemeinsam für die Verarbeitung Verantwortlichen handelt.[25] Daher fordert der EDSB den Mitgesetzgeber auf, das für kontoführende Zahlungsdienstleister geltende Verbot einer Überprüfung der Erlaubnis gemäß Artikel 44 Absatz 1 Buchstabe c und Artikel 49 Absatz 4 der Vorschlags für eine Zahlungsdiensteverordnung zu überdenken. Insbesondere empfiehlt der EDSB, entweder (i) das für kontoführende Zahlungsdienstleister geltende Verbot einer Überprüfung der Datenzugangserlaubnis gemäß Artikel 44 Absatz 1 Buchstabe c und Artikel 49 Absatz 4 des Vorschlags für eine Zahlungsdiensteverordnung zu streichen oder (ii) geeignete Garantien einzuführen, um die Zahlungsdienstnutzer vor dem Risiko einer möglichen unrechtmäßigen Weitergabe personenbezogener Daten durch kontoführende Zahlungsdienstleister zu schützen, das dieses Verbot mit sich bringen könnte.

5. Starke Kundenauthentifizierungsverfahren und Verwendung personalisierter Sicherheitsmerkmale

19. Im Jahr 2014 empfahl die Europäische Zentralbank („EZB"), dass zwischen den TPPs [Drittanbietern] und dem kontoführenden Zahlungsdienstleister keine gemeinsamen Zugangsdaten ausgetauscht werden sollten; der TPP sollte den Zahler entweder auf sichere Weise an seinen kontoführenden Zahlungsdienstleister weiterleiten oder seine eigenen

[25] Leitlinien 07/2020 des EDSA zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, 7. Juli 2021, S. 45 (Absatz 167 und Fußnote 76).

Sicherheitsmerkmale vergeben. Beide Optionen sollten Teil einer standardisierten europäischen Schnittstelle für den Zugang zu Zahlungskonten sein, die entwickelt werden müsse.[26] Im Jahr 2016 erklärte die Interessengruppe Bankensektor der EBA (Banking Stakeholder Group) ferner: Um die Verbraucher zu schützen, das Risiko zu verringern und Betrug zu vermeiden, empfehlen wir, dass die PSC [personalisierten Sicherheitsmerkmale] nicht direkt von TPP [Drittanbietern] abgerufen werden.[27]

20. Der EDSB stellt fest, dass Artikel 86 Absatz 2 des Vorschlags für eine Zahlungsdiensteverordnung es Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern erlauben würde, sich auf die Authentifizierungsverfahren zu „verlassen", die der kontoführende Zahlungsdienstleister dem Zahlungsdienstnutzer zur Verfügung stellt. Gleichzeitig würden Zahlungsauslösedienstleister daran gehindert, „sensible Zahlungsdaten", zu denen auch „personalisierte Sicherheitsmerkmale" gehören, „zu speichern" (Artikel 46 Absatz 2 Buchstabe a), und Kontoinformationsdienstleister würden daran gehindert, derartige Daten „anzufordern" (Artikel 47 Absatz 2 Buchstabe a).[28]

21. Der EDSB ist der Auffassung, dass eine etwaige Weitergabe der Sicherheitsmerkmale, die der Zahlungsdienstnutzer zur Authentifizierung beim kontoführenden Zahlungsdienstleister verwendet, an Zahlungsdienstleister und Kontoinformationsdienstleister unnötige Risiken mit sich bringen würde[29] und daher ausgeschlossen werden sollte. Um mögliche Unklarheiten zu vermeiden, empfiehlt der EDSB, Artikel 46 Absatz 2 Buchstabe a und Artikel 47 Absatz 2 Buchstabe a des Vorschlags für eine Zahlungsdiensteverordnung dahingehend zu ändern, dass Zahlungsauslösedienstleister und Kontoinformationsdienstleister nicht auf die vom kontoführenden Zahlungsdienstleister zur Verfügung gestellten personalisierten Sicherheitsmerkmale zugreifen dürfen (und sie nicht nur „nicht speichern" oder „nicht anfordern" dürfen).

22. Artikel 89 Absatz 1 würde die EBA verpflichten, Entwürfe technischer Regulierungsstandards auszuarbeiten, um die Anforderungen an eine starke Kundenauthentifizierung zu präzisieren. Die EBA wäre auch verpflichtet, die Anforderungen festzulegen, die Sicherheitsmaßnahmen erfüllen müssen, damit die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der

---

[26] ECB Final Recommendations for the security of payment account access services following public consultation (Endgültige Empfehlungen der EZB zur Sicherheit der Zugangsdienste für Zahlungskonten nach öffentlicher Konsultation), Mai 2014, Seite 5.

[27] Draft BSG response to EBA/DP/2015/03 on future draft regulatory technical standards on strong customer authentication and secure communication under the revised payment services directive (psd2) (Entwurf einer Antwort der Interessengruppe Bankensektor auf EBA/DP/2015/03 zu künftigen Entwürfen technischer Regulierungsstandards für eine starke Kundenauthentifizierung und sichere Kommunikation im Rahmen der überarbeiteten [zweiten] Zahlungsdiensterichtlinie), Seite 2.

[28] Gemäß Artikel 3 Absatz 38 der Vorschlags für eine Zahlungsdiensteverordnung bezeichnet der Ausdruck „sensible Zahlungsdaten" Daten, die zur Begehung von Betrug verwendet werden können, einschließlich personalisierter Sicherheitsmerkmale.

[29] Die Speicherung der Sicherheitsmerkmale des Zahlungsdienstnutzers an mehreren Speicherorten würde die Angriffsfläche und damit das Risiko eines unbefugten Zugriffs (z. B. aufgrund einer Verletzung des Schutzes personenbezogener Daten) erhöhen. Darüber hinaus würde der Zugriff auf die Anmeldedaten des Zahlungsdienstnutzers das Risiko einer unbefugten Datenverarbeitung erhöhen, da die Sicherheitsmerkmale von Kontoinformationsdienstleistern oder Zahlungsauslösedienstleistern zur Umgehung der zulässigen Nutzung der dedizierten Datenzugangsschnittstelle verwendet werden könnten (indem sich zum Beispiel ein Kontoinformationsdienstleister mit der Webschnittstelle des kontoführenden Zahlungsdienstleisters verbindet). Darüber hinaus würde es gegen bewährte Sicherheitspraktiken und -standards verstoßen, wenn es dem Zahlungsdienstnutzer gestattet würde, die von ihnen für die Authentifizierung beim kontoführenden Zahlungsdienstleister verwendeten Sicherheitsmerkmale an Dritte weiterzugeben. So ist beispielsweise in ISO 27002:2022 unter den Verantwortlichkeiten der Nutzer die Verpflichtung aufgeführt, vertrauliche „*geheime Authentifizierungsinformationen wie Passwörter*" zu schützen, während gleichzeitig darauf hingewiesen wird, dass „*personenbezogene geheime Authentifizierungsinformationen nicht an andere weitergegeben werden dürfen.*"

Zahlungsdienstnutzer geschützt sind.[30] Der Kommission soll die Befugnis übertragen werden, die von der EBA entwickelten Standards gemäß den Artikeln 10 bis 14 der Verordnung (EU) Nr. 1093/2010 anzunehmen. In diesem Zusammenhang erinnert der EDSB die Kommission an ihre Verpflichtung gemäß Artikel 42 Absatz 1 EU-DSVO, den EDSB bei der Ausarbeitung delegierter Rechtsakte, die sich auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten auswirken würden, zu konsultieren.

23. Schließlich empfiehlt der EDSB auch eine Präzisierung der Definition des Begriffs „sensible Zahlungsdaten" in Artikel 3 Absatz 38 des Vorschlags für eine Zahlungsdiensteverordnung (die im weitesten Sinne als Daten bezeichnet werden, die zur Begehung von Betrug verwendet werden können, einschließlich personalisierter Sicherheitsmerkmale), indem die Kategorien personenbezogener Daten, die unter diese Definition fallen, genauer spezifiziert werden.

6. Besondere Kategorien personenbezogener Daten

24. Bei Finanztransaktionen können sensible Informationen über eine einzelne betroffene Person offengelegt werden, einschließlich in Bezug auf besondere Kategorien personenbezogener Daten[31]. Artikel 80 des Vorschlags für eine Zahlungsdiensteverordnung besagt in Verbindung mit Erwägungsgrund 98 desselben Vorschlags, dass es Zahlungssystemen und Zahlungsdienstleistern – vorbehaltlich angemessener Garantien für die Grundrechte und Grundfreiheiten natürlicher Personen – gestattet sein muss, besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der DSGVO und Artikel 10 Absatz 1 der EU-DSVO zu verarbeiten, soweit dies für die Erbringung von Zahlungsdiensten und die Einhaltung von in dieser Verordnung vorgesehenen Verpflichtungen im öffentlichen Interesse des reibungslosen Funktionierens des Binnenmarkts für Zahlungsdienste erforderlich ist. Artikel 80 enthält auch eine (nicht erschöpfende) Liste solcher Garantien.

25. Artikel 9 Absatz 2 Buchstabe g der DSGVO, der eine Ausnahme vom Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 DSGVO aus Gründen eines wesentlichen öffentlichen Interesses zulässt, ist an eine Reihe von Bedingungen geknüpft und sollte eng ausgelegt werden[32]. Diese Bedingungen sind: (i) die Verarbeitung personenbezogener Daten muss für den festgelegten Zweck erforderlich sein; (ii) sie muss auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats erfolgen; und (iii) das Unionsrechts oder des Rechts des Mitgliedstaats selbst

[30] Artikel 89 Absatz 1 Buchstaben a und c des Vorschlags für eine Zahlungsdiensteverordnung; Artikel 89 Absatz 2 Buchstabe b des Vorschlags für eine Zahlungsdiensteverordnung sieht vor, dass die EBA bei der Ausarbeitung der technischen Regulierungsstandards der Notwendigkeit Rechnung trägt, die Sicherheit der Gelder und personenbezogenen Daten der Zahlungsdienstnutzer zu gewährleisten.

[31] Siehe Leitlinien des EDSA zum Zusammenspiel zwischen der zweiten Zahlungsdiensterichtlinie und der DSGVO, angenommen am 15. Dezember 2020, Rn. 52. Siehe auch Urteil des Gerichtshofs vom 1. August 2022, *OT gegen Vyriausioji tarnybinės etikos komisija*, C-184/20, ECLI:EU:C:2022:601, Randnrn. 117-128, und Urteil des Gerichtshofs vom 4. Juli 2023, *Meta Platforms u. a. (Allgemeine Nutzungsbedingungen eines sozialen Netzwerks)*, C-252/21, ECLI:EU:C:2023:537, Randnrn. 69-73.

[32] Siehe Urteil des Gerichtshofs vom 4. Juli 2023, *Meta Platforms u. a. (Allgemeine Nutzungsbedingungen eines sozialen Netzwerks)*, C-252/21, ECLI:EU:C:2023:537, Randnrn. 93: „[...] *die in Art. 6 Abs. 1 Unterabs. 1 Buchst. b bis f DSGVO vorgesehenen Rechtfertigungsgründe [sind] eng auszulegen, da sie dazu führen können, dass eine Verarbeitung personenbezogener Daten trotz fehlender Einwilligung der betroffenen Person rechtmäßig ist (vgl. in diesem Sinne Urteil vom 24. Februar 2022, Valsts ieņēmumu dienests [Verarbeitung personenbezogener Daten für steuerliche Zwecke], C-175/20, EU:C:2022:124, Rn. 73 und die dort angeführte Rechtsprechung)*", sowie Randnrn. 133-134.

muss in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen[33].

26. Der EDSB ist der Auffassung, dass Artikel 80 des Vorschlags für eine Zahlungsdiensteverordnung nicht den Anforderungen der Notwendigkeit und Verhältnismäßigkeit genügt. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der Europäischen Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Sie müssen sich auf das absolut Notwendige beschränken, und die den Eingriff enthaltende Regelung muss klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen[34]. Die strikte Einhaltung der Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit ist besonders wichtig, wenn es um die Verarbeitung besonderer Kategorien personenbezogener Daten geht, da die Verarbeitung solcher Daten einen schweren Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen kann. Angesichts der Schwere des Eingriffs, der sich aus der Verarbeitung besonderer Datenkategorien ergibt, ist es wichtig, dass die Rechtsvorschriften hinreichend präzise sind, um den objektiven Zusammenhang zwischen den einzelnen Datenkategorien in einem bestimmten Zahlungskontext und dem zu erreichenden Ziel des öffentlichen Interesses aufzuzeigen.

27. Um den Erfordernissen der Notwendigkeit und Verhältnismäßigkeit Rechnung zu tragen, sollten in dem Vorschlag für eine Verordnung für eine Zahlungsdiensteverordnung:

    a. die besonderen Zwecke der Verarbeitung näher beschreiben, indem die Art(en) der Zahlungsdienste[35] angegeben werden, für die die Zahlungssysteme und Zahlungsdienstleister berechtigt wären, besondere Kategorien personenbezogener Daten zu verarbeiten; zudem sollte angegeben werden, um welche besonderen Kategorien personenbezogener Daten es sich dabei handeln würde[36]. Der Vorschlag für eine Zahlungsdiensteverordnung sollte (in einem Erwägungsgrund) auch Begründungen dafür enthalten, warum die Verarbeitung der besonderen Kategorien personenbezogener Daten

---

[33] Siehe auch Stellungnahme 33/2023 des EDSB zu dem Vorschlag für eine Verordnung in Fragen betreffend den Schutz Erwachsener vom 18. Juli 2023, Absätze 14-15.

[34] Urteil des Gerichtshofs vom 22. Juni 2021, *Latvijas Republikas Saeima (Strafpunkte)*, C-439/19, EU:C:2021:504, Rn. 105.

[35] Wenngleich es sich bei den Arten von Diensten, auf die sich der Vorschlag für eine Zahlungsdiensteverordnung bezieht, im Wesentlichen um dieselben zu handeln scheint wie die in der zweiten Zahlungsdiensterichtlinie, wird in Erwägungsgrund 26 auch betont, dass ein neues Geschäftsmodell, das auf Open Banking basiert, eine Änderung der Definition der Kontoinformationsdienste erfordert, damit klar ersichtlich wird, dass die vom zugelassenen Kontoinformationsdienstleister zusammengestellten Informationen an einen Dritten übermittelt werden können, damit dieser Dritte mit Erlaubnis des Endnutzers einen anderen Dienst für den Endnutzer erbringen kann.

[36] Siehe auch Leitlinien des EDSA zum Zusammenspiel zwischen der zweiten Zahlungsdiensterichtlinie und der DSGVO, angenommen am 15. Dezember 2020, Rn. 56 [Hervorhebung hinzugefügt]: *„Zahlungsdienste dürfen besondere Kategorien personenbezogener Daten aus Gründen eines erheblichen öffentlichen Interesses nur dann verarbeiten, wenn alle Bedingungen von Artikel 9 Absatz 2 Buchstabe g DSGVO erfüllt sind. Dies bedeutet, dass die Verarbeitung der besonderen Kategorien personenbezogener Daten Gegenstand einer spezifischen Ausnahme von Artikel 9 Absatz 1 DSGVO im Unionsrecht oder im Recht der Mitgliedstaaten sein muss. Gegenstand dieser Bestimmung muss die Verhältnismäßigkeit in Bezug auf das angestrebte Ziel der Verarbeitung sein, während sie gleichzeitig geeignete und spezifische Maßnahmen zum Schutz der Grundrechte und Interessen der betroffenen Person enthalten muss. Darüber hinaus muss in dieser Bestimmung im Unionsrecht oder im Recht der Mitgliedstaaten der Wesensgehalt des Rechts auf Datenschutz gewahrt werden. Schließlich muss auch nachgewiesen werden, dass die Verarbeitung der besonderen Datenkategorien aus Gründen des erheblichen öffentlichen Interesses, einschließlich systemischer Interessen, erforderlich ist. Nur wenn alle diese Bedingungen vollständig erfüllt sind, könnte diese Ausnahmeregelung auf bestimmte Arten von Zahlungsdiensten anwendbar sein.“*

für den betreffenden Dienst unbedingt erforderlich ist und nicht vermieden werden kann (d. h. die Vermeidung der Verarbeitung dieser Daten wäre unmöglich); und

b. klar angegeben werden, welche besonderen Kategorien personenbezogener Daten für die Erreichung des spezifischen Zwecks erforderlich wären und für wen (welche genaue Art von Wirtschaftsbeteiligten) diese Rechtsgrundlage gelten würde.

28. Der EDSB ist der Ansicht, dass in einigen Fällen – etwa im Hinblick auf die Multi-Faktor-Authentifizierung des Zahlungsdienstnutzers –, in denen es möglich ist, nicht biometrische Authentifizierungsmittel zu verwenden, die (ausdrückliche) Einwilligung der betroffenen Person eine besser geeignete Grundlage für die Verarbeitung sensibler Daten im Einklang mit Artikel 6 und 9 der DSGVO darstellen kann.

29. Was die nach Artikel 9 Absatz 2 Buchstabe g der DSGVO erforderlichen Garantien betrifft, so begrüßt der EDSB die nicht erschöpfende Liste von Garantien in Artikel 80 des Vorschlags für eine Zahlungsdiensteverordnung. Der EDSB empfiehlt jedoch, auch einen Verweis auf die Anforderungen für die Registrierung in Bezug auf die Protokollierung von Anmeldevorgängen (um zu überprüfen, ob ein unrechtmäßiger Zugang stattgefunden hat) in den Text aufzunehmen.

7. Bereitstellung dedizierter Zugangsschnittstellen

30. Der EDSB stellt fest, dass Artikel 35 Absatz 6 des Vorschlags für eine Zahlungsdiensteverordnung über die Einrichtung einer Testeinrichtung durch kontoführende Zahlungsdienstleister für ihre dedizierte Schnittstelle die Weitergabe sensibler Zahlungsdaten oder sonstiger personenbezogener Daten über die Einrichtung verbietet. Der EDSB begrüßt diese Präzisierung, da personenbezogene Daten im Einklang mit den Grundsätzen der Datenminimierung und des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen grundsätzlich auch nicht beim Testen einer Funktion verarbeitet werden sollten.[37]

8. Datenzugangsmanagement

31. Der EDSB begrüßt Artikel 43, wonach kontoführende Zahlungsdienstleister dem Zahlungsdienstnutzer ein Dashboard zur Verfügung stellen müssen, das die Überwachung und Verwaltung der Erlaubnisse ermöglicht, die er Kontoinformationsdienstleistern oder Zahlungsdienstleistern für mehrere und wiederkehrende Zahlungen erteilt hat. Im Hinblick auf die Informationen, die die kontoführenden Zahlungsdienstleister den Zahlungsdienstnutzern über das Dashboard[38] zur Verfügung stellen müssen, begrüßt der

[37] Artikel 5 Absatz 1 Buchstabe c und Artikel 25 Absatz 1 der DSGVO.

[38] Gemäß Artikel 43 Absatz 2 der Vorschlags für eine Zahlungsdiensteverordnung müssen dem Zahlungsdienstnutzer über das Dashboard folgende Informationen bereitgestellt werden:
(i) der Name des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters, dem Zugang gewährt wurde;
(ii) das Kundenkonto, zu dem der Zugang gewährt wurde;
(iii) der Zweck der Erlaubnis;
(iv) die Gültigkeitsdauer der Erlaubnis;
(v) die Kategorien offengelegter Daten.

EDSB insbesondere den Verweis auf die Kategorien offengelegter Daten[39]. Dieser Zusatz trägt dazu bei, dass der Zahlungsdienstnutzer, bei dem es sich um eine betroffene Person im Sinne der DSGVO handelt, einen wirksamen Überblick und eine wirksame Kontrolle über die Ströme personenbezogener Daten erhält. Der EDSB empfiehlt jedoch, in Artikel 43 Absatz 2 Buchstabe a einen Verweis auf den/die benannte(n) Dienst(e) aufzunehmen, für die die Erlaubnis erteilt wird[40].

32. In Bezug auf die spezifischen Pflichten der Zahlungsauslösedienstleister und der Kontoinformationsdienstleister begrüßt der EDSB insbesondere die Einschränkung, dass die Zahlungsauslösedienstleister und die Kontoinformationsdienstleister personenbezogene Daten nur für die Erbringung des Zahlungsauslöse- bzw. Kontoinformationsdienstes verarbeiten dürfen, für den der Zahlungsdienstnutzer ihm seine Erlaubnis erteilt hat[41]. Der EDSB stellt jedoch fest, dass die Anforderung nach Artikel 46 Absatz 2 Buchstabe b, wonach Zahlungsauslösedienstleister vom Zahlungsdienstnutzer nur die Daten anfordern können, die für die Erbringung des (Zahlungsauslöse-)Dienstes erforderlich sind, in Artikel 47 Absatz 2 betreffend die Pflichten der Kontoinformationsdienstleister nicht sinngemäß enthalten ist. Er empfiehlt daher, eine entsprechende Bestimmung in Artikel 47 Absatz 2 des Vorschlags für eine Zahlungsdiensteverordnung einzufügen.

33. Der EDSB nimmt ferner positiv zur Kenntnis, dass der kontoführende Zahlungsdienstleister dem Zahlungsdienstnutzer über das Dashboard eine Übersicht über jede bestehende Erlaubnis in Bezug auf den/die Kontoinformationsdienst(e) oder Zahlungsauslösedienst(e) mit folgenden Angaben zur Verfügung stellen muss: Name des Zahlungsauslösedienstleisters oder Kontoinformationsdienstleisters, dem der Zugang gewährt wurde; Kundenkonto, zu dem der Zugang gewährt wurde; Zweck der Erlaubnis; Kategorien offengelegter Daten und Gültigkeitsdauer der Erlaubnis[42]. Um sicherzustellen, dass kontoführende Zahlungsdienstleister in der Lage sind, den Zahlungsdienstnutzern alle in Artikel 43 Absatz 2 des Vorschlags für eine Zahlungsdiensteverordnung genannten Informationen zu übermitteln, empfiehlt der EDSB, dass Zahlungsauslösedienstleister und Kontoinformationsdienstleister gemäß Artikel 43 Absatz 4 Buchstabe b verpflichtet werden, auch den kontoführenden Zahlungsdienstleister über das Kundenkonto zu informieren, zu dem Zugang beantragt wird.

34. Darüber hinaus empfiehlt der EDSB, dass Artikel 43 Absatz 4 Buchstabe b des Vorschlags für eine Zahlungsdiensteverordnung vorschreibt, dass Zahlungsauslösedienstleister und Kontoinformationsdienstleister die kontoführenden Zahlungsdienstleister über die Rechtsgrundlage gemäß Artikel 6 Absatz 1 der DSGVO und (falls zutreffend) die Ausnahme gemäß Artikel 9 Absatz 2 der DSGVO informieren, auf die sie sich stützen würden, um auf die (besonderen Kategorien von) personenbezogenen Daten des Zahlungsdienstnutzers zuzugreifen. Dies würde dazu beitragen, dass kontoführende Zahlungsdienstleister keinen Zugang zu personenbezogenen Daten gewähren, wenn keine geeignete DSGVO-Rechtsgrundlage vorliegt[43].

Siehe auch Erwägungsgrund 65 des Vorschlags für eine Zahlungsdiensteverordnung.

[39] Artikel 43 Absatz 2 Buchstabe v des Vorschlags für eine Zahlungsdiensteverordnung.

[40] Entspricht Artikel 8 Absatz 2 Buchstabe a Ziffer ii des FiDA-Vorschlags.

[41] Siehe Artikel 46 Absatz 2 Buchstabe c und Artikel 47 Absatz 2 Buchstabe b des Vorschlags für eine Zahlungsdiensteverordnung.

[42] Artikel 43 Absatz 2 Buchstabe a des Vorschlags für eine Zahlungsdiensteverordnung.

[43] Siehe auch Absätze 17 und 18 der vorliegenden Stellungnahme.

35. Der EDSB begrüßt die in Artikel 43 Absatz 3 des Vorschlags für eine Zahlungsdiensteverordnung enthaltene Anforderung, dass das Dashboard auf der Benutzeroberfläche leicht auffindbar sein sollte und dass die im Dashboard angezeigten Informationen für den Zahlungsdienstnutzer klar, genau und leicht verständlich sind. In Erwägungsgrund 65 des Vorschlags für eine Zahlungsdiensteverordnung heißt es weiter, dass das Dashboard die Kunden in die Lage versetzen sollte, ihre Berechtigungen auf informierte und unparteiische Weise zu verwalten, und ihnen ein hohes Maß an Kontrolle darüber geben sollte, wie ihre personenbezogenen und nicht personenbezogenen Daten verwendet werden.

36. Vor allem in einem sensiblen Bereich, wie z. B. bei Zahlungsdiensten, sind die Verbraucher möglicherweise nicht über die Folgen der Weitergabe ihrer personenbezogenen Daten an Zahlungsdienstleister informiert[44]. Der EDSB empfiehlt daher, dass im Vorschlag für eine Zahlungsdiensteverordnung, insbesondere in Artikel 43 Buchstabe b, festgelegt wird, dass das Dashboard nicht in einer Weise konzipiert werden sollte, die die Zahlungsdienstnutzer auf unangemessene Weise dazu beeinflussen würde, Erlaubnisse zu erteilen oder zu widerrufen.

9. Transaktionsüberwachungsmechanismen und Weitergabe von betrugsbezogenen Daten

37. Mit Artikel 83 der Vorschlags für eine Zahlungsdiensteverordnung würden Zahlungsdienstleister verpflichtet, über Mechanismen für die Transaktionsüberwachung zu verfügen, die es Zahlungsdienstleistern unter anderem ermöglichen, potenziell betrügerische Zahlungsvorgänge – einschließlich Transaktionen mit Beteiligung von Zahlungsauslösedienstleistern – zu verhindern und aufzudecken[45].

38. In Artikel 83 Absatz 2 der Vorschlags für eine Zahlungsdiensteverordnung ist festgelegt, dass die Mechanismen für die Transaktionsüberwachung auf der Analyse früherer Zahlungsvorgänge und des Online-Zugangs zu Zahlungskonten beruhen würden. Zudem werden dort die zu diesem Zweck erforderlichen Daten festgelegt, nämlich: (a) Informationen über den Zahlungsdienstnutzer, einschließlich der Umgebungs- und Verhaltensmerkmale, die für den Zahlungsdienstnutzer bei normaler Verwendung der personalisierten Sicherheitsmerkmale typisch sind; (b) Informationen über das Zahlungskonto, einschließlich der Historie der Zahlungstransaktionen; (c) Transaktionsinformationen, einschließlich des Transaktionsbetrags und der

[44] The Finance Innovation Lab, „Open Finance and Vulnerability – A Policy Discussion Paper", Juli 2021, Seite 9: „*Terms and conditions around data sharing are difficult to understand and time consuming to read. Researchers at the LSE have found that this makes determining 'informed consent' in financial services very difficult. Contracts often involve complex data chains, which cede control of data to many more firms than is at first apparent. This can result in data sharing impacting access to multiple services. There is therefore a real danger that people will fail to understand the full implications of allowing access to open finance data.*" („Die Bedingungen für die Weitergabe von Daten sind schwer verständlich, und das Lesen ist zeitaufwändig. Forscher der London School of Economics haben herausgefunden, dass dies die genaue Bestimmung einer ‚Einwilligung in voller Kenntnis der Sachlage' bei Finanzdienstleistungen sehr schwierig macht. Verträge enthalten oft komplexe Datenketten, mit denen die Kontrolle über die Daten an viel mehr Unternehmen abgetreten wird, als auf den ersten Blick ersichtlich ist. Dies kann dazu führen, dass die Datenweitergabe den Zugang zu mehreren Dienstleistungen beeinträchtigt. Es besteht daher die reale Gefahr, dass die Menschen die volle Tragweite des Zugangs zu Daten des offenen Finanzwesens nicht verstehen."); siehe zudem Seite 10: „*There is a risk that data sharing becomes a prerequisite for accessing essential financial services.*" („Es besteht die Gefahr, dass die Weitergabe von Daten zu einer Voraussetzung für den Zugang zu wesentlichen Finanzdienstleistungen wird.")

[45] Artikel 83 Absatz 1 Buchstabe c des Vorschlags für eine Zahlungsdiensteverordnung.

Kundenkennung des Zahlungsempfängers; (d) Sitzungsdaten, einschließlich des IP-Adressbereichs des Geräts, von dem aus auf das Zahlungskonto zugegriffen wurde.

39. Artikel 83 Absatz 3 legt außerdem fest, dass die Transaktionsüberwachungsmechanismen mindestens die folgenden Risikofaktoren berücksichtigen sollten: (a) Listen der missbräuchlich verwendeten oder gestohlenen Authentifizierungselemente; (b) der Betrag jedes Zahlungsvorgangs; (c) bekannte Betrugsszenarien bei der Erbringung von Zahlungsdienstleistungen; (d) Anzeichen für eine Malware-Infektion in einer Phase des Authentifizierungsverfahrens; (e) ungewöhnliche Nutzung des Geräts oder der Software (falls das Zugangsgerät oder die Software vom Zahlungsdienstleister bereitgestellt wird).

40. Der EDSB begrüßt, dass der Vorschlag darauf abzielt, die Kategorien von Daten, die für die Zwecke der Transaktionsüberwachungsmechanismen verwendet werden können, erschöpfend festzulegen. Er stellt jedoch fest, dass bestimmte Kategorien personenbezogener Daten nach wie vor sehr weit gefasst sind, wenn man bedenkt, dass in der Begründung der Standort des Zahlungsdienstnutzers, der Zeitpunkt der Transaktion, das verwendete Gerät, die Ausgabegewohnheiten und der für den Kauf genutzt Online-Shop als Umgebungs- und Verhaltensmerkmale genannt werden.[46]

41. Der EDSB stellt ferner fest, dass Zahlungsdienstleister bereits Datenverarbeitungstätigkeiten zum Zwecke der Betrugsüberwachung auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f der DSGVO (berechtigte Interessen) ausführen.[47] Diese Rechtsgrundlage verlangt von den für die Verarbeitung Verantwortlichen – wie den Zahlungsdienstleistern – eine sorgfältige Abwägung. Um sich auf Artikel 6 Absatz 1 Buchstabe f der DSGVO berufen zu können, müssen drei kumulative Bedingungen erfüllt sein: (i) die Wahrnehmung eines berechtigten Interesses durch den für die Verarbeitung Verantwortlichen oder durch den oder die Dritten, denen die Daten übermittelt werden, (ii) die Erforderlichkeit der Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses und (iii) die Bedingung, dass die Grundrechte und Grundfreiheiten der betroffenen Person in Bezug auf den Datenschutz nicht überwiegen.[48] Mit den neuen Bestimmungen gemäß Artikel 83 des Vorschlag für eine Zahlungsdiensteverordnung würde jedoch eine gesetzliche Verpflichtung für Zahlungsdienstleister geschaffen, solche Verarbeitungstätigkeiten im Sinne von Artikel 6 Absatz 1 Buchstabe c der DSGVO durchzuführen. Zwar sollte die Verarbeitung nach wie vor auf die aufgeführten Datenkategorien „beschränkt" werden, doch verlangt der Vorschlag von den Zahlungsdienstleistern nicht, dass sie vor der Verarbeitung personenbezogener Daten von Zahlungsdienstnutzern zu Zwecken der Betrugsüberwachung eine Abwägung gemäß dem Vorschlag für eine Zahlungsdiensteverordnung vornehmen.

42. Da der Vorschlag für eine Zahlungsdiensteverordnung eine rechtliche Verpflichtung zur Verarbeitung personenbezogener Daten vorsehen würde, sollten die Grenzen dieser Verarbeitung klar definiert werden. Dies erfordert eine klare Bestimmung der Kategorien personenbezogener Daten, die Zahlungsdienstleister im Rahmen der Mechanismen für die Transaktionsüberwachung verarbeiten dürfen. In diesem Zusammenhang empfiehlt der EDSB, eine klare und umfassende Definition der in Artikel 83 Absatz 2 Buchstabe a des

[46] COM(2023) 367 final, S. 13.
[47] Siehe Verweis auf die Betrugsbekämpfung in Erwägungsgrund 47 der DSGVO als eines der möglichen berechtigten Interessen, die durch Artikel 6 Absatz 1 Buchstabe f der DSGVO geschützt werden.
[48] S. Urteil des Gerichtshofs vom 29. Juli 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, Rn. 95.

Vorschlags genannten Informationen über den Zahlungsdienstnutzer festzulegen. Darüber hinaus empfiehlt der EDSB, ausdrücklich festzulegen, dass die Verarbeitung der in Absatz 2 aufgeführten Datenkategorien nur in dem Maß durchgeführt werden darf, das erforderlich ist, um die in Artikel 83 Absatz 1 des Vorschlags für eine Zahlungsdiensteverordnung genannten Zwecke zu erreichen. Schließlich empfiehlt er die Festlegung angemessener Höchst-Speicherfristen für die gemäß Artikel 83 erhobenen personenbezogenen Daten[49].

43. Der EDSB begrüßt, dass den Vereinbarungen über den Informationsaustausch zwischen Zahlungsdienstleistern eine Datenschutz-Folgenabschätzung (DSFA) im Sinne von Artikel 35 der DSGVO vorausgehen muss, die von den an der Vereinbarung beteiligten Zahlungsdienstleistern gemeinsam durchzuführen ist[50], sowie gegebenenfalls eine vorherige Konsultation gemäß Artikel 36 der DSGVO. Gleichzeitig stellt der EDSB fest, dass der Begriff „Vereinbarung über den Informationsaustausch" im Vorschlag für eine Zahlungsdiensteverordnung nicht definiert ist, und empfiehlt, in Artikel 3 der Vorschlags für eine Zahlungsdiensteverordnung eine Begriffsbestimmung aufzunehmen.

44. Der EDSB begrüßt, dass die Verarbeitung personenbezogener Daten gemäß der Vereinbarung über den Informationsaustausch nicht zur Beendigung der Beziehung zwischen dem Kunden und dem Zahlungsdienstleister führen oder seine künftige Annahme bei einem anderen Zahlungsdienstleister beeinträchtigen kann[51]. Dies ist eine wichtige Garantie im Hinblick auf die möglichen Auswirkungen auf die betroffene Person, die von der Verarbeitung personenbezogener Daten im Rahmen von Transaktionsüberwachungsmechanismen betroffen ist. Der EDSB empfiehlt jedoch, in dem Vorschlag für eine Zahlungsdiensteverordnung ausdrücklich – allgemeiner – vorzusehen, dass *jede* Verarbeitung personenbezogener Daten zum Zwecke der Einhaltung der rechtlichen Verpflichtungen zur Betrugsbekämpfung gemäß Artikel 83 (nicht nur gemäß Artikel 83 Absatz 4) ausschließlich zum spezifischen Zweck der Betrugsprävention erfolgen darf und nicht zu einer Beendigung der Beziehung zwischen dem Kunden und dem Zahlungsdienstleister führen oder die Annahme des Zahlungsdienstnutzers bei einem anderen Zahlungsdienstleister beeinträchtigen kann.

45. Der EDSB stellt fest, dass die technischen Anforderungen an die Mechanismen für die Transaktionsüberwachung in Entwürfen technischer Regulierungsstandards festgelegt würden, die von der EBA ausgearbeitet und von der Kommission im Wege eines Durchführungsrechtsakts angenommen würden[52]. In diesem Zusammenhang erinnert der EDSB die Kommission an ihre Verpflichtung gemäß Artikel 42 Absatz 1 der EU-DSVO, den EDSB bei der Ausarbeitung von Durchführungsrechtsakten, die sich auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten auswirken würden, zu konsultieren.

10. Zuständige Behörden

46. Gemäß Artikel 91 Absatz 2 des Vorschlags für eine Zahlungsdiensteverordnung müssen die Mitgliedstaaten zuständige Behörden benennen, die die wirksame Einhaltung des Vorschlags für eine Zahlungsdiensteverordnung sicherstellen und überwachen. Bei diesen

[49] Siehe auch Erwägungsgrund 102 des Vorschlags für eine Zahlungsdiensteverordnung.
[50] Artikel 83 Absatz 4 des Vorschlags für eine Zahlungsdiensteverordnung.
[51] Artikel 83 Absatz 6 des Vorschlags für eine Zahlungsdiensteverordnung.
[52] Artikel 89 Absatz 1 Buchstabe g und Artikel 89 Absatz 2 des Vorschlags für eine Zahlungsdiensteverordnung.

Behörden würde es sich entweder um a) Behörden oder b) Stellen handeln, die nach nationalem Recht oder von Behörden anerkannt sind, die nach nationalem Recht ausdrücklich zu diesem Zweck ermächtigt sind, einschließlich nationaler Zentralbanken. Artikel 93 Absatz 3 sieht vor, dass die zuständigen Behörden bei der Ausübung ihrer Ermittlungs- und Sanktionsbefugnisse, auch in grenzüberschreitenden Fällen, zusammenarbeiten und die gegenseitige Amtshilfe gegenüber den anderen betroffenen Behörden sicherstellen.

47. In Erwägungsgrund 130 der Vorschlags für eine Zahlungsdiensteverordnung wird zu Recht betont, dass die Wirksamkeit des Rechtsrahmens für Zahlungsdienste von der Zusammenarbeit zwischen den zuständigen Behörden, einschließlich der für den Datenschutz zuständigen nationalen Behörden, abhängt[53]. Der EDSB ist der Auffassung, dass eine solche Zusammenarbeit dazu beitragen würde, die Einheitlichkeit zwischen der Anwendung und Durchsetzung des Vorschlags für eine Zahlungsdiensteverordnung und dem EU-Datenschutzrecht sicherzustellen.

48. Damit eine klare Rechtsgrundlage für den Austausch einschlägiger Informationen gewährleistet ist, empfiehlt der EDSB, dass die für die Überwachung und Durchsetzung des Datenschutzrechts zuständigen Aufsichtsbehörden in Artikel 93 Absatz 3 des Vorschlags für eine Zahlungsdiensterichtlinie ausdrücklich genannt werden.

11. Bekanntmachung verwaltungsrechtlicher Sanktionen und Maßnahmen

49. Artikel 101 Absatz 1 des Vorschlags für eine Zahlungsdiensterichtlinie sieht vor, dass im Zusammenhang mit der Veröffentlichung von Entscheidungen über die Verhängung einer verwaltungsrechtlichen Sanktion oder Verwaltungsmaßnahme gegen juristische und natürliche Personen wegen Verstößen gegen diese Verordnung und gegebenenfalls von Vergleichsvereinbarungen auf ihrer Website die Identität der natürlichen Person, die Gegenstand der Entscheidung über die Verhängung einer verwaltungsrechtlichen Sanktion oder Verwaltungsmaßnahme ist, nicht veröffentlicht würde. Nur abweichend von Artikel 101 Absatz 1 kann die zuständige nationale Behörde in Fällen, in denen sie die Veröffentlichung der Identität oder anderer personenbezogener Daten natürlicher Personen für erforderlich hält, auch die Identität der betreffenden Person veröffentlichen.[54]

50. Der EDSB ist der Ansicht, dass die Veröffentlichung personenbezogener Daten mit den Entscheidungen der zuständigen Behörden in der Tat die Ausnahme darstellen sollte, über die nach einer Einzelfallprüfung zu entscheiden ist. Damit bliebe den zuständigen Behörden die Möglichkeit, im Falle schwerer Verstöße und wenn eine starke abschreckende Wirkung erforderlich ist, die betreffenden personenbezogenen Daten nach Einzelfallprüfung zu veröffentlichen. Der EDSB merkt an, dass die Veröffentlichung personenbezogener Daten von Personen, die wegen eines Verstoßes gegen die Verordnung sanktioniert wurden, nur in ordnungsgemäß begründeten Ausnahmefällen erfolgen sollte, da die allgemeine

[53] Siehe auch Erwägungsgrund 76 des Vorschlags für eine dritte Zahlungsdiensterichtlinie: *Die Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie muss im Einklang mit der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725 erfolgen. Daher sind die Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725 für die Überwachung der Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie zuständig.*

[54] Artikel 101 Absatz 2 des Vorschlags für eine Zahlungsdiensteverordnung. Siehe auch Erwägungsgrund 136 des Vorschlags für eine Zahlungsdiensteverordnung.

Veröffentlichung derartiger personenbezogener Daten als schwerer Eingriff in die in den Artikeln 7 und 8 der Charta verankerten Grundrechte angesehen werden könnte.

51. Schließlich begrüßt der EDSB, dass in Artikel 101 Absatz 4 des Vorschlags für eine Zahlungsdiensteverordnung im Einklang mit dem Grundsatz der Speicherbegrenzung[55] festgelegt ist, dass personenbezogene Daten, die in der Veröffentlichung enthalten sind, nur dann auf der offiziellen Website der zuständigen Behörde zu speichern sind, wenn eine jährliche Überprüfung ergibt, dass die Veröffentlichung dieser Daten zum Schutz der Stabilität der Finanzmärkte oder zur Gewährleistung einer wirksamen Durchsetzung des Vorschlags für eine Zahlungsdiensteverordnung nach wie vor erforderlich ist, auf jeden Fall aber nicht länger als fünf Jahre.

12. Schlussfolgerungen

52. Vor diesem Hintergrund empfiehlt der EDSB:

(1) eine klare Unterscheidung zwischen dem Begriff „Erlaubnis" und der Rechtsgrundlage für die Verarbeitung im Rahmen der DSGVO vorzunehmen, indem in Erwägungsgrund 62 der Vorschlags für eine Zahlungsdiensteverordnung klargestellt wird, dass die „Erlaubnis" nicht als „Zustimmung" oder „ausdrückliche Zustimmung" im Sinne der Verordnung (EU) 2016/679 ausgelegt werden sollte;

(2) in einem Erwägungsgrund klarzustellen, dass die Erteilung einer Erlaubnis durch den Zahlungsdienstnutzer insbesondere die Pflichten von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern gemäß den Artikeln 6 und 9 der Verordnung (EU) 2016/679 unberührt lässt;

(3) das für kontoführende Zahlungsdienstleister geltende Verbot der Überprüfung der Erlaubnis gemäß Artikel 49 Absatz 4 der Vorschlags für eine Zahlungsdiensteverordnung zu überdenken oder im verfügenden Teil der Vorschläge geeignete alternative Garantien einzuführen, um die Zahlungsdienstnutzer vor der Gefahr einer möglichen unrechtmäßigen Weitergabe personenbezogener Daten durch kontoführende Zahlungsdienstleister zu schützen, die dieses Verbot mit sich bringen könnte;

(4) Artikel 46 Absatz 2 Buchstabe a und Artikel 47 Absatz 2 Buchstabe a der Vorschlags für eine Zahlungsdiensteverordnung dahingehend zu ändern, dass festgelegt wird, dass Zahlungsauslösedienstleister und Kontoinformationsdienstleister keinen Zugang zu personalisierten Sicherheitsmerkmalen haben;

(5) den Begriff „sensible Zahlungsdaten" in Artikel 3 Absatz 38 des Vorschlags für eine Zahlungsdiensteverordnung zu präzisieren, insbesondere durch die Festlegung der Arten personenbezogener Daten, die unter diese Definition fallen;

(6) anzugeben, für welche(n) bestimmte(n) Art(en) benannter Zahlungsdienste die Zahlungssysteme und der Zahlungsdienstleister zur Verarbeitung (welcher Kategorien)

[55] Artikel 5 Absatz 1 Buchstabe c der DSGVO.

besonderer Kategorien personenbezogener Daten in Artikel 80 der Vorschlags für eine Zahlungsdiensteverordnung berechtigt wären;

(7) (in einem Erwägungsgrund) zu begründen, warum die Verarbeitung der besonderen Kategorien personenbezogener Daten für die benannten Zahlungsdienste in Artikel 80 des Vorschlags für eine Zahlungsdiensteverordnung notwendig und verhältnismäßig ist und nicht mit alternativen technischen Mitteln vermieden werden kann;

(8) einen Verweis auf die Registrierung in Bezug auf die Protokollierung von Anmeldevorgängen (um zu überprüfen, ob ein unrechtmäßiger Zugang stattgefunden hat) in Artikel 80 des Vorschlags für eine Zahlungsdiensteverordnung aufzunehmen;

(9) in Artikel 43 Absatz 2 Buchstabe a einen Verweis auf den/die bezeichneten Zahlungsdienst(e) aufzunehmen, für den/die der Zahlungsdienstnutzer die Erlaubnis erteilt hat;

(10) in Artikel 47 Absatz 2 in Bezug auf die Pflichten von Kontoinformationsdienstleistern die Anforderung gemäß Artikel 46 Absatz 2 Buchstabe b aufzunehmen, wonach Zahlungsdienstleister vom Zahlungsdienstnutzer nur die Daten anfordern können, die für die Erbringung der angeforderten Dienstleistung erforderlich sind;

(11) von Zahlungsdienstleistern und Kontoinformationsdienstleistern gemäß Artikel 43 Absatz 4 Buchstabe b zu verlangen, kontoführende Zahlungsdienstleister über das Kundenkonto, zu dem Zugang beantragt wird, und über die Rechtsgrundlage gemäß Artikel 6 Absatz 1 der DSGVO und (gegebenenfalls) über die Ausnahme gemäß Artikel 9 Absatz 2 der DSGVO, auf die sie sich für den Zugang zu den personenbezogenen Daten des Zahlungsdienstnutzers verlassen würden, zu informieren;

(12) dass in Artikel 43 Buchstabe b, festgelegt wird, dass das Dashboard nicht in einer Weise konzipiert werden sollte, die die Zahlungsdienstnutzer ermutigen oder auf unangemessene Weise dazu beeinflussen würde, Erlaubnisse zu erteilen oder zu widerrufen;

(13) eindeutig die Kategorien personenbezogener Daten festzulegen, die Zahlungsdienstleister im Rahmen von Transaktionsüberwachungsmechanismen verarbeiten dürfen (insbesondere durch die Festlegung einer Definition des Begriffs „Informationen über den Zahlungsdienstnutzer" gemäß Artikel 83 Absatz 2 Buchstabe a);

(14) angemessene Speicherfristen für die gemäß Artikel 83 erhobenen personenbezogenen Daten festzulegen;

(15) eine Definition des Begriffs „Vereinbarung über den Informationsaustausch" in Artikel 3 der Vorschläge über eine Zahlungsdiensteverordnung aufzunehmen;

(16) in dem Vorschlag für eine Zahlungsdiensteverordnung ausdrücklich vorzusehen, dass jede Verarbeitung personenbezogener Daten zum Zwecke der Einhaltung der rechtlichen Verpflichtungen zur Betrugsbekämpfung gemäß Artikel 83 ausschließlich zu diesem spezifischen Zweck erfolgen darf und nicht zu einer Beendigung der Beziehung zwischen dem Kunden und dem Zahlungsdienstleister führen oder die Annahme des Zahlungsdienstnutzers bei einem anderen Zahlungsdienstleister beeinträchtigen darf;

(17) in Artikel 93 Absatz 3 des Vorschlags für eine Zahlungsdiensteverordnung die für die Überwachung und Durchsetzung des Datenschutzrechts zuständigen Aufsichtsbehörden ausdrücklich zu benennen.

Brüssel, 22. August 2023

Wojciech Rafał WIEWIÓROWSKI

i.A. Leonardo CERVERA NAVAS
Generalsekretär