Leitlinien 06/2020 zum Zusammenspiel zwischen der zweiten Zahlungsdiensterichtlinie und der DSGVO

Version 2.0

Angenommen am 15. Dezember 2020

Versionsverlauf

Version 2.0	15.12.2020	Annahme der Leitlinien nach öffentlicher Konsultation
Version 1.0	17.7.2020	Annahme der Leitlinien für die öffentliche Konsultation

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss —

gestützt auf Artikel 70 Absatz 1 Buchstabe e der 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, im Folgenden „DSGVO“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und Protokoll 37 in der durch den Beschluss Nr. 154/2018 des Gemeinsamen EWR-Ausschusses vom 6. Juli 2018 geänderten Fassung[1],

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

in Erwägung nachstehender Gründe:

(1) Die Datenschutz-Grundverordnung enthält ein einheitliches Regelwerk für die Verarbeitung personenbezogener Daten in der gesamten EU.

(2) Mit der zweiten Zahlungsdiensterichtlinie (Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 23. Dezember 2015, im Folgenden „PSD2“) wird die Richtlinie 2007/64/EG aufgehoben, während gleichzeitig neue Vorschriften zur Gewährleistung der Rechtsklarheit für Verbraucher, Einzelhändler und Unternehmen in der Zahlungskette und zur Modernisierung des rechtlichen Rahmens des Marktes für Zahlungsdienste enthalten sind.[2] Die Mitgliedstaaten hatten die PSD2 vor dem 13. Januar 2018 in nationales Recht umzusetzen.

(3) Ein wesentliches Merkmal der PSD2 ist die Einführung eines Rechtsrahmens für neue Zahlungsauslösedienste und Kontoinformationsdienste. Durch die PSD2 werden diese neuen Zahlungsdienstleister in die Lage versetzt, für die Erbringung der genannten Dienste Zugang zu Zahlungskonten betroffener Personen zu erhalten.

(4) In Bezug auf den Datenschutz erfolgt jede Verarbeitung personenbezogener Daten für die Zwecke der PSD2, einschließlich der Bereitstellung von Informationen über die Verarbeitung, gemäß Artikel 94 Absatz 1 PSD2 im Einklang mit der DSGVO[3] und der Verordnung (EU) 2018/1725.

(5) In Erwägungsgrund 89 der PSD2 heißt es, dass insbesondere bei der Verarbeitung personenbezogener Daten für die Zwecke der PSD2 der genaue Zweck der Verarbeitung angegeben, die entsprechende Rechtsgrundlage genannt und die Sicherheitsanforderungen der DSGVO umgesetzt werden sollten; darüber hinaus sollten die Grundsätze der Notwendigkeit, Verhältnismäßigkeit, Beschränkung auf den Zweck und die Angemessenheit der Frist für die Speicherung zu achten sein. Ferner sollte in allen im Rahmen der PSD2 entwickelten und eingesetzten Datenverarbeitungssystemen der Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen eingebaut sein.[4]

[1] Soweit in diesen Leitlinien auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.
[2] Erwägungsgrund 6 der PSD2.
[3] Da die PSD2 aus der Zeit vor der DSGVO stammt, verweist sie noch auf die Richtlinie 95/46/EG. Nach Artikel 94 DSGVO gelten Verweise auf die aufgehobene Richtlinie 95/46/EG als Verweise auf die DSGVO.
[4] Erwägungsgrund 89 der PSD2.

(6) In Erwägungsgrund 93 der PSD2 heißt es, dass die Zahlungsauslösedienstleister und die Kontoinformationsdienstleister einerseits und der kontoführende Zahlungsdienstleister andererseits die erforderlichen Datenschutz- und die Sicherheitsanforderungen beachten sollten, die in dieser Richtlinie festgelegt sind, oder auf die in dieser Richtlinie verwiesen wird, oder die in den Entwürfen für technische Regulierungsstandards enthalten sind —

HAT FOLGENDE LEITLINIEN ANGENOMMEN:

1. EINLEITUNG

1. Mit der zweiten Zahlungsdiensterichtlinie (im Folgenden „PSD2“) wurde eine Reihe von Neuerungen im Bereich der Zahlungsdienste eingeführt. Auch wenn durch die Anwendung der PSD2 neue Möglichkeiten für die Verbraucher entstehen und die Transparenz in diesem Bereich erhöht wird, wirft die Anwendung der PSD2 gewisse Fragen und Bedenken in Bezug auf die Notwendigkeit auf, dass die betroffenen Personen die volle Kontrolle über ihre personenbezogenen Daten behalten. Die Datenschutz-Grundverordnung (im Folgenden „DSGVO“) ist auf die Verarbeitung personenbezogener Daten anwendbar, was Verarbeitungstätigkeiten im Zusammenhang mit Zahlungsdiensten im Sinne der PSD2 einschließt.[5] Daher müssen Verantwortliche, die in dem unter die PSD2 fallenden Bereich tätig sind, stets die Einhaltung der Anforderungen der DSGVO einschließlich der Datenschutzgrundsätze gemäß Artikel 5 DSGVO sowie der einschlägigen Bestimmungen der e-Datenschutz-Richtlinie[6] sicherstellen. Obwohl die PSD2[7] und die technischen Regulierungsstandards für eine starke Kundenauthentifizierung und für gemeinsame und sichere offene Standards für die Kommunikation (im Folgenden „technische Regulierungsstandards“[8]) bestimmte Bestimmungen zum Datenschutz und zur Datensicherheit enthalten, ist Unsicherheit hinsichtlich der Auslegung dieser Bestimmungen und des Zusammenspiels zwischen dem allgemeinen Datenschutzrahmen und der PSD2 entstanden.

2. Am 5. Juli 2018 verfasste der Europäische Datenschutzausschuss (EDSA) ein Schreiben zur PSD2, in dem er Sachverhalte zum Schutz personenbezogener Daten im Zusammenhang mit der PSD2 klarstellte, insbesondere mit Blick auf die Verarbeitung personenbezogener Daten von Nichtvertragsparteien („silent party data“) durch Kontoinformationsdienstleister und Zahlungsauslösedienstleister, die Verfahren für die Erteilung und den Widerruf der Zustimmung, die technischen Regulierungsstandards und die Zusammenarbeit zwischen kontoführenden Zahlungsdienstleistern im Rahmen von Sicherheitsmaßnahmen. Im Rahmen der Vorarbeiten zu diesen Leitlinien wurden Beiträge von Interessenträgern sowohl in Schriftform als auch im Rahmen einer einschlägigen Veranstaltung gesammelt, um die dringendsten Herausforderungen zu ermitteln.

[5] Artikel 1 Absatz 1 DSGVO.
[6] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).
[7] Artikel 94 der Zahlungsdiensterichtlinie usw.
[8] 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 (Text von Bedeutung für den EWR), C/2017/7782 (ABl. L 69 vom 13.3.2011, S. 23), abrufbar unter hhttps://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R0389&from=DE.

3. Mit diesen Leitlinien sollen weitere Orientierungshilfen zu Datenschutzaspekten im Zusammenhang mit der PSD2 gegeben werden, insbesondere in Bezug auf das Verhältnis zwischen den einschlägigen Bestimmungen der DSGVO und der PSD2. Der Schwerpunkt dieser Leitlinien liegt auf der Verarbeitung personenbezogener Daten durch Kontoinformationsdienstleister und Zahlungsauslösedienstleister. Demgemäß werden in diesem Dokument die Bedingungen für die Gewährung des Zugangs zu Zahlungskontoinformationen durch kontoführende Zahlungsdienstleister und für die Verarbeitung personenbezogener Daten durch Zahlungsinformationsdienstleister und Kontoinformationsdienstleister behandelt, darunter die Anforderungen und Garantien in Bezug auf die Verarbeitung personenbezogener Daten durch Zahlungsinformationsdienstleister und Kontoinformationsdienstleister für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, insbesondere wenn diese Daten im Zusammenhang mit der Bereitstellung eines Kontoinformationsdienstes[9] erhoben wurden. Zudem werden in diesem Dokument verschiedene Konzepte der ausdrücklichen Zustimmung im Rahmen der PSD2 und der DSGVO, die Verarbeitung von Daten von Nichtvertragsparteien („silent party data"), die Verarbeitung besonderer Kategorien personenbezogener Daten durch Zahlungsinformationsdienstleister und Kontoinformationsdienstleister sowie die Anwendung der wichtigsten Datenschutzgrundsätze der DSGVO einschließlich Datenminimierung, Transparenz, Rechenschaftspflicht und Sicherheitsmaßnahmen behandelt. Die PSD2 umfasst bereichsübergreifende Verantwortlichkeiten u. a. in den Bereichen Verbraucherschutz und Wettbewerbsrecht. Etwaige Überlegungen zu diesen Rechtsbereichen würden gleichwohl über den Umfang dieser Leitlinien hinausgehen.

4. Um die Lektüre der Leitlinien zu erleichtern, sind nachstehend die wichtigsten Begriffsbestimmungen dieses Dokuments dargelegt.

1.1 Begriffsbestimmungen

„*Kontoinformationsdienst*" bezeichnet einen Online-Dienst zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten, das/die ein Zahlungsdienstnutzer entweder bei einem anderen Zahlungsdienstleister oder bei mehr als einem Zahlungsdienstleister hält;

„*kontoführender Zahlungsdienstleister*" bezeichnet einen Zahlungsdienstleister, der für einen Zahler ein Zahlungskonto bereitstellt und führt;

„*Datenminimierung*" ist ein Grundsatz des Datenschutzes, wonach personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen;

„Zahler" bezeichnet eine natürliche oder juristische Person, die Inhaber eines Zahlungskontos ist und die einen Zahlungsauftrag von diesem Zahlungskonto gestattet oder – falls kein Zahlungskonto vorhanden ist – eine natürliche oder juristische Person, die den Auftrag für einen Zahlungsvorgang erteilt;

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

[9] Ein Kontoinformationsdienst ist ein Online-Dienst zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten, das bzw. die ein Zahlungsdienstnutzer entweder bei einem anderen Zahlungsdienstleister oder bei mehr als einem Zahlungsdienstleister unterhält.

„*Zahlungskonto*“ bezeichnet ein auf den Namen eines oder mehrerer Zahlungsdienstnutzer(s) lautendes Konto, das für die Ausführung von Zahlungsvorgängen genutzt wird;

„*Zahlungsauslösedienstleister*“ bezeichnet den Anbieter eines Dienstes, der auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto auslöst;

„Zahlungsdienstleister“ bezeichnet eine Stelle im Sinne des Artikels 1 Absatz 1 PSD2[10] oder eine natürliche oder juristische Person, für die die Ausnahme gemäß Artikel 32 oder 33 PSD2 gilt;

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

„personenbezogene Daten“ bezeichnen alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

„*Datenschutz durch Technik*“ bezeichnet technische und organisatorische Maßnahmen, die in ein Produkt oder eine Dienstleistung eingebettet sind und mit denen die Datenschutzgrundsätze wirksam umgesetzt und die notwendigen Garantien in die Verarbeitung integriert werden sollen, um die Anforderungen der DSGVO zu erfüllen und die Rechte betroffener Personen zu schützen;

„*datenschutzfreundliche Voreinstellungen*“ bezeichnen geeignete technische und organisatorische Maßnahmen, die in ein Produkt oder eine Dienstleistung integriert werden und sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden;

„*technische Regulierungsstandards*“ verweist auf die Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen

[10] In Artikel 1 Absatz 1 PSD2 heißt es, dass mit der PSD2 die Regeln festgelegt werden, nach denen die Mitgliedstaaten die folgenden Kategorien von *Zahlungsdienstleistern* unterscheiden:
(a) Kreditinstitute im Sinne des Artikels 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates, einschließlich deren Zweigstellen im Sinne des Artikels 4 Absatz 1 Nummer 17 der genannten Verordnung, sofern sich diese Zweigstellen innerhalb der Union befinden, unabhängig davon, ob sich die Hauptverwaltungen dieser Zweigstellen innerhalb der Union befinden oder im Einklang mit Artikel 47 der Richtlinie 2013/36/EU und nationalem Recht außerhalb der Union;
(b) E-Geld-Institute im Sinne des Artikels 2 Nummer 1 der Richtlinie 2009/110/EG, einschließlich deren Zweigniederlassungen gemäß Artikel 8 der genannten Richtlinie und dem nationalen Recht, sofern sich die Zweigniederlassungen innerhalb der Union befinden und die Hauptverwaltung des E-Geld-Instituts, dem sie angehören, sich außerhalb der Union befindet und nur insofern, als die von diesen Zweigniederlassungen erbrachten Zahlungsdienste mit der Ausgabe von E-Geld in Zusammenhang stehen;
(c) Postscheckämter, die nach nationalem Recht zur Erbringung von Zahlungsdiensten berechtigt sind;
(d) Zahlungsinstitute;
(e) die Europäische Zentralbank (EZB) und die nationalen Zentralbanken, wenn sie nicht in ihrer Eigenschaft als Währungsbehörden oder andere Behörden handeln;
(f) die Mitgliedstaaten oder ihre regionalen oder lokalen Gebietskörperschaften, wenn sie nicht in ihrer Eigenschaft als Behörden handeln.

Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation;

„Drittanbieter“ bezieht sich sowohl auf Zahlungsauslösedienstleister als auch auf Kontoinformationsdienstleister.

1.2 Dienstleistungen im Rahmen der PSD2

5. Mit der PSD2 werden zwei neue Arten von Zahlungsdiensten (Zahlungsdienstleister) eingeführt: Zahlungsauslösedienstleister und Kontoinformationsdienstleister. Anhang 1 der PSD2 enthält die acht Zahlungsdienste, die unter die PSD2 fallen.

6. Zahlungsauslösedienstleister erbringen einen Dienst, der auf Antrag des Zahlungsdienstnutzers einen Zahlungsauftrag in Bezug auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto auslöst.[11] Ein Zahlungsauslösedienstleister kann einen kontoführenden Zahlungsdienstleister (in der Regel eine Bank) auffordern, eine Transaktion im Auftrag des Zahlungsdienstnutzers einzuleiten. Der (Zahlungsdienst-)Nutzer kann eine natürliche Person (betroffene Person) oder eine juristische Person sein.

7. Kontoinformationsdienstleister erbringen einen Online-Dienst zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten, das/die ein Zahlungsdienstnutzer entweder bei einem anderen Zahlungsdienstleister oder bei mehr als einem Zahlungsdienstleister hält.[12] Nach Erwägungsgrund 28 PSD2 erhält der Zahlungsdienstnutzer in Echtzeit einen Gesamtüberblick über seine finanzielle Situation zu einem bestimmten Zeitpunkt.

8. Im Rahmen von Kontoinformationsdiensten könnten verschiedene Arten von Diensten angeboten werden, wobei der Schwerpunkt auf unterschiedlichen Merkmalen und Zwecken liegt. So bieten einige Anbieter den Nutzern unter Umständen Dienstleistungen wie Finanzplanung und Ausgabenüberwachung an. Die Verarbeitung personenbezogener Daten im Rahmen dieser Dienstleistungen fällt unter die PSD2. Dienste, bei denen auch die Kreditwürdigkeit des Zahlungsdienstnutzers bewertet wird oder Prüfungsdienstleistungen auf der Grundlage der Erhebung von Informationen über einen Kontoinformationsdienst durchgeführt werden, fallen nicht in den Anwendungsbereich der PSD2, sondern dementsprechend unter die DSGVO. Darüber hinaus fallen auch andere Konten als Zahlungskonten (z. B. Sparkonten, Investitionen) nicht unter die PSD2. Für die Verarbeitung personenbezogener Daten ist die DSGVO in jedem Fall der anwendbare Rechtsrahmen.

Beispiel 1:

HappyPayments ist ein Anbieter eines Online-Dienstes, der die Bereitstellung von Informationen zu einem oder mehreren Zahlungskonten über eine mobile App beinhaltet, um einen Überblick über die Finanzlage zu gewähren (Kontoinformationsdienst). Hierdurch erhält der Zahlungsdienstnutzer einen Überblick über die Salden und jüngsten Transaktionen auf zwei oder mehreren Zahlungskonten bei verschiedenen Banken. Wenn er dies wünscht, kann ein Zahlungsdienstnutzer auch Ausgaben und Einnahmen nach unterschiedlichen Typologien (Gehalt, Freizeit, Energie/Strom, Hypothek usw.) kategorisieren lassen, was dem Zahlungsdienstnutzer bei der Finanzplanung hilft. Darüber hinaus bietet HappyPayments über diese App einen Dienst an, um Zahlungen direkt über das/die von den Nutzern benannte(n) Zahlungskonto/-konten auszulösen (Zahlungsauslösedienst).

[11] Artikel 4 Nummer 15 PSD2.
[12] Artikel 4 Nummer 16 PSD2.

9. Für die Erbringung dieser Dienste werden mit der PSD2 die rechtlichen Bedingungen geregelt, unter denen Zahlungsauslösedienstleister und Kontoinformationsdienstleister auf Zahlungskonten zugreifen können, um dem Zahlungsdienstnutzer einen Dienst zu erbringen.

10. In Artikel 66 Absatz 1 und Artikel 67 Absatz 1 PSD2 ist festgelegt, dass der Zahlungsdienstnutzer das Recht hat, auf Zahlungs- und Kontoinformationsdienste zuzugreifen und diese zu nutzen. Dies bedeutet, dass der Zahlungsdienstnutzer bei der Ausübung dieses Rechts völlig frei bleiben sollte und nicht gezwungen werden darf, von diesem Recht Gebrauch zu machen.

11. Der Zugang zu Zahlungskonten und die Nutzung von Zahlungskontoinformationen sind teilweise in den Artikeln 66 und 67 PSD2 geregelt, die Garantien für den Schutz (personenbezogener) Daten enthalten. In Artikel 66 Absatz 3 Buchstabe f PSD2 heißt es, dass der Zahlungsauslösedienstleister vom Zahlungsdienstnutzer keine anderen als die für das Erbringen des Zahlungauslösedienstes erforderlichen Daten verlangen darf, während in Artikel 66 Absatz 3 Buchstabe g PSD2 vorgesehen ist, dass der Zahlungsauslösedienstleister Daten nicht für andere Zwecke als für das Erbringen des vom Zahler ausdrücklich geforderten Zahlungsauslösedienstes verwenden, darauf zugreifen und speichern darf. Darüber hinaus ist der Zugang von Kontoinformationsdienstleistern auf Informationen von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen gemäß Artikel 67 Absatz 2 Buchstabe d PSD2 beschränkt, während in Artikel 67 Absatz 2 Buchstabe f der PSD2 festgelegt ist, dass Kontoinformationsdienstleister Daten im Einklang mit den Datenschutzvorschriften nicht für andere Zwecke als für den vom Zahlungsdienstnutzer ausdrücklich geforderten Kontoinformationsdienst verwenden, darauf zugreifen oder speichern dürfen. In den Datenschutzvorschriften wird betont, dass personenbezogene Daten im Rahmen von Kontoinformationsdiensten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen. Daher sollte ein Kontoinformationsdienstleister im Vertrag klar angeben, für welche spezifischen Zwecke personenbezogene Kontodaten im Zusammenhang mit dem von ihm bereitgestellten Kontoinformationsdienst verarbeitet werden. Der Vertrag sollte gemäß Artikel 5 DSGVO auf rechtmäßige Weise, nach Treu und Glauben und in nachvollziehbarer Weise verfasst werden und auch anderen Bestimmungen des Verbraucherschutzes entsprechen.

12. Je nach den besonderen Umständen könnte es sich bei den Zahlungsdienstleistern um einen Verantwortlichen oder Auftragsverarbeiter im Sinne der DSGVO handeln. Die für die Verarbeitung Verantwortlichen sind in diesen Leitlinien die Zahlungsdienstleister, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden. Weitere Orientierungshilfen hierzu finden sich in den Leitlinien 07/2020 des EDSA zu den Konzepten des Verantwortlichen und des Auftragsverarbeiters in der DSGVO (Guidelines 07/2020 on the concepts of controller and processor in the GDPR).

2 RECHTMÄßIGE GRÜNDE UND WEITERVERARBEITUNG IM RAHMEN DER PSD2

2.1 Rechtmäßige Gründe für die Verarbeitung

13. Nach der DSGVO müssen die für die Verarbeitung Verantwortlichen eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten vorweisen. Artikel 6 Absatz 1 DSGVO enthält eine erschöpfende und abschließende Liste von sechs Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Rahmen der DSGVO.[13] Es obliegt dem für die Verarbeitung Verantwortlichen, die geeignete Rechtsgrundlage festzulegen und sicherzustellen, dass alle Bedingungen für diese Rechtsgrundlage erfüllt sind. Die Klärung der Frage, welche Rechtsgrundlage in einer bestimmten Situation am besten geeignet ist, hängt von den Umständen ab, unter denen die Verarbeitung erfolgt, einschließlich des Zwecks der Verarbeitung und der Beziehung zwischen dem für die Verarbeitung Verantwortlichen und der betroffenen Person.

2.2 Artikel 6 Absatz 1 Buchstabe b DSGVO (Verarbeitung ist für die Erfüllung eines Vertrags erforderlich)

14. Zahlungsdienste werden auf der Grundlage eines Vertrags zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister erbracht. Erwägungsgrund 87 der PSD2 besagt, dass diese *„Richtlinie ... nur die vertraglichen Verpflichtungen und Verantwortlichkeiten zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister zum Gegenstand haben [sollte]*“. Die wichtigste Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Erbringung von Zahlungsdienstleistungen liefert Artikel 6 Absatz 1 Buchstabe b; dies bedeutet, dass die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen.

15. Die Zahlungsdienste im Rahmen der PSD2 sind in Anhang 1 der PSD2 definiert. Die Erbringung dieser Dienste im Sinne der PSD2 ist eine Voraussetzung für den Abschluss eines Vertrags, in dem

[13] Gemäß Artikel 6 ist die Verarbeitung nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

(a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

(b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

(c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

(d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

(e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

(f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

die Parteien Zugang zu den Zahlungskontodaten des Zahlungsdienstnutzers haben. Diese Zahlungsdienstleister müssen auch zugelassene Betreiber sein. In Bezug auf Zahlungsauslösedienste und Kontoinformationsdienste im Rahmen der PSD2 können Verträge Bedingungen enthalten, die auch Bedingungen für zusätzliche Dienste vorschreiben, die nicht durch die PSD2 geregelt sind. In den *Leitlinien 2/2019 des EDSA für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen* wird klargestellt, dass Verantwortliche bewerten müssen, welche Verarbeitung personenbezogener Daten für die Erfüllung des Vertrags objektiv erforderlich ist. In diesen Leitlinien wird darauf hingewiesen, dass die Begründung der Erforderlichkeit von der Art der Dienstleistung, den gegenseitigen Perspektiven und Erwartungen der Vertragsparteien, dem genauen Grundgedanken des Vertrags und den wesentlichen Elementen des Vertrags abhängt.

16. Ebenso wird in den Leitlinien 2/2019 des EDSA klargestellt, dass im Lichte von Artikel 7 Absatz 4 DSGVO zwischen Verarbeitungstätigkeiten, die für die Erfüllung eines Vertrags erforderlich sind, und Klauseln, die die Erbringung der Dienstleistung von bestimmten Verarbeitungstätigkeiten abhängig machen, die für die Erfüllung des Vertrags tatsächlich nicht erforderlich sind, unterschieden wird. Ein „für die Erfüllung erforderlich“ erfordert eindeutig mehr als eine Vertragsbedingung.[14] Der Verantwortliche sollte nachweisen können, inwieweit der Hauptgegenstand des Vertrags mit der betroffenen Person tatsächlich nicht erfüllt werden kann, wenn die spezifische Verarbeitung der fraglichen personenbezogenen Daten nicht erfolgt. Die bloße Bezugnahme oder Erwähnung der Verarbeitung von Daten in einem Vertrag reicht nicht aus, um die fragliche Verarbeitung in den Anwendungsbereich von Artikel 6 Absatz 1 Buchstabe b DSGVO zu bringen.

17. In Artikel 5 Absatz 1 Buchstabe b der DSGVO ist der Grundsatz der Zweckbindung vorgesehen, wonach personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Bei der Beantwortung der Frage, ob Artikel 6 Absatz 1 Buchstabe b eine geeignete Rechtsgrundlage für einen Online-(Zahlungs-)Dienst darstellt, sollte das spezifische Ziel, der Zweck oder die Zielsetzung der Dienstleistung berücksichtigt werden.[15] Die Zwecke der Verarbeitung müssen im Einklang mit den Verpflichtungen des Verantwortlichen zu Zweckbindung und Transparenz klar festgelegt und der betroffenen Person mitgeteilt werden. Die Prüfung der Erforderlichkeit beinhaltet das Erfordernis einer kombinierten, faktengestützten Bewertung der Verarbeitung „mit Blick auf das angestrebte Ziel und im Hinblick auf die Frage, ob sie im Vergleich zu anderen Optionen für das Erreichen desselben Ziels weniger eingreifend ist“. Artikel 6 Absatz 1 Buchstabe b gilt nicht für eine Verarbeitung, die nützlich, aber für die Erbringung der vertraglichen Dienstleistung oder für die Einleitung entsprechender vorvertraglicher Schritte auf Anfrage der betroffenen Person objektiv nicht erforderlich ist, selbst wenn sie für andere Geschäftszwecke des Verantwortlichen erforderlich ist.[16]

18. In den Leitlinien 2/2019 des EDSA wird klargestellt, dass die Kategorien personenbezogener Daten oder die Arten von Verarbeitungsvorgängen, die der Verantwortliche ausführen muss, um einen Vertrag im Sinne von Artikel 6 Absatz 1 Buchstabe b zu erfüllen, in Verträgen nicht künstlich

[14] Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, EDSA, S. 8.
[15] Ebenda.
[16] Ebenda, Seite 7.

erweitert werden können.[17] In diesen Leitlinien werden auch Fälle behandelt, in denen betroffene Personen, die vielleicht nur an einem Dienst interessiert sind, vor der Entscheidung „Alles oder nichts“ stehen. Dies könnte geschehen, wenn ein Verantwortlicher mehrere getrennte Dienste oder Elemente eines Dienstes mit unterschiedlichen grundlegenden Funktionen, Merkmalen oder Beweggründen in einem Vertrag bündeln will. Besteht der Vertrag aus mehreren eigenständigen Dienstleistungen oder Elementen eines Dienstes, die sinnvollerweise tatsächlich unabhängig voneinander erbracht werden können, ist die Anwendbarkeit von Artikel 6 Absatz 1 Buchstabe b für jeden dieser Dienste gesondert zu beurteilen, wobei zu prüfen ist, was objektiv erforderlich ist, um den einzelnen Dienst, den die betroffene Person aktiv verlangt oder für den sie sich angemeldet hat, zu erbringen.[18]

19. Die Verantwortlichen müssen im Einklang mit den oben genannten Leitlinien prüfen, was für die Erfüllung des Vertrags objektiv erforderlich ist. Wenn die Verantwortlichen nicht nachweisen können, dass die Verarbeitung der personenbezogenen Zahlungskontodaten für die gesonderte Erbringung jedes einzelnen dieser Dienste objektiv erforderlich ist, ist Artikel 6 Absatz 1 Buchstabe b DSGVO keine gültige Rechtsgrundlage für die Verarbeitung. In diesen Fällen sollte der Verantwortliche eine andere Rechtsgrundlage für die Verarbeitung in Erwägung ziehen.

2.3 Schutzmaßnahmen gegen Betrug

20. Nach Artikel 94 Absatz 1 PSD2 gestatten die Mitgliedstaaten die Verarbeitung personenbezogener Daten durch Zahlungssysteme und Zahlungsdienstleister, sofern das zur Verhütung, Ermittlung und Feststellung von Betrugsfällen im Zahlungsverkehr notwendig ist. Die Verarbeitung personenbezogener Daten, die zur Verhinderung von Betrug unbedingt erforderlich ist, könnte ein berechtigtes Interesse des betreffenden Zahlungsdienstleisters darstellen, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.[19] Verarbeitungstätigkeiten zum Zwecke der Betrugsprävention sollten im Einklang mit dem Grundsatz der Rechenschaftspflicht auf einer sorgfältigen Einzelfallbewertung durch den Verantwortlichen beruhen. Darüber hinaus können die Verantwortlichen zur Verhinderung von Betrug besonderen rechtlichen Verpflichtungen unterliegen, die die Verarbeitung personenbezogener Daten erforderlich machen.

2.4 Weiterverarbeitung (Kontoinformationsdienstleister und Zahlungsauslösedienstleister)

21. In Artikel 6 Absatz 4 DSGVO sind die Bedingungen für die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, festgelegt. Eine solche Weiterverarbeitung kann insbesondere dann erfolgen, wenn sie auf Unionsrecht oder dem Recht der Mitgliedstaaten beruht, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, wenn die betroffene Person ihre Einwilligung gegeben hat oder wenn die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist.

22. Artikel 66 Absatz 3 Buchstabe g und Artikel 67 Absatz 2 Buchstabe f PSD2 sind sorgfältig zu berücksichtigen. Wie vorstehend erwähnt, ist in Artikel 66 Absatz 3 Buchstabe g PSD2 vorgesehen, dass der Zahlungsauslösedienstleister Daten nicht für andere Zwecke als für das Erbringen des vom Zahler ausdrücklich geforderten Zahlungauslösedienstes verwenden, darauf zugreifen und

[17] Ebenda, Seite 10.
[18] Ebenda, Seite 11.
[19] Erwägungsgrund 47 der DSGVO.

speichern darf. In Artikel 67 Absatz 2 Buchstabe f PSD2 heißt es, dass der Kontoinformationsdienstleister im Einklang mit den Datenschutzvorschriften Daten nicht für andere Zwecke als für den vom Zahlungsdienstnutzer ausdrücklich geforderten Kontoinformationsdienst verwenden, darauf zugreifen oder speichern darf.

23. Folglich werden die Möglichkeiten der Verarbeitung für andere Zwecke durch Artikel 66 Absatz 3 Buchstabe g und Artikel 67 Absatz 2 Buchstabe f PSD2 erheblich eingeschränkt; dies bedeutet, dass die Verarbeitung für einen anderen Zweck nicht erlaubt ist, sofern die betroffene Person keine Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a DSGVO gegeben hat oder die Verarbeitung auf keiner Rechtsvorschrift der Union oder der Mitgliedstaaten beruht, der der Verantwortliche gemäß Artikel 6 Absatz 4 DSGVO unterliegt. Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder einer Rechtsvorschrift der Union oder der Mitgliedstaaten, so geht aus den Einschränkungen nach Artikel 66 Absatz 3 Buchstabe g und Artikel 67 Absatz 2 Buchstabe f PSD2 klar hervor, dass jeder andere Zweck nicht mit dem Zweck vereinbar ist, zu dem die personenbezogenen Daten ursprünglich erhoben wurden. Die Prüfung der Vereinbarkeit nach Artikel 6 Absatz 4 DSGVO kann zu keiner Rechtsgrundlage für die Verarbeitung führen.

24. Nach Artikel 6 Absatz 4 DSGVO ist eine Weiterverarbeitung auf der Grundlage einer Rechtsvorschrift der Union oder der Mitgliedstaaten möglich. Beispielsweise sind alle Zahlungsauslösedienstleister und Kontoinformationsdienstleister Verpflichtete im Sinne von Artikel 3 Nummer 2 Buchstabe a der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung. Daher sind diese Verpflichteten gezwungen, die in der Richtlinie festgelegten Sorgfaltspflichten gegenüber Kunden anzuwenden. Die im Zusammenhang mit einem PSD2-Dienst verarbeiteten personenbezogenen Daten werden daher auf der Grundlage mindestens einer rechtlichen Verpflichtung des Diensteanbieters weiterverarbeitet.[20]

25. Wie unter Randnummer 20 dargelegt, besagt Artikel 6 Absatz 4 DSGVO, dass die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, auf der Einwilligung der betroffenen Person beruhen könnte, wenn alle Bedingungen für die Einwilligung im Sinne der DSGVO erfüllt sind. Wie oben dargelegt, muss der Verantwortliche nachweisen, dass es möglich ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (Erwägungsgrund 42 der DSGVO).

2.5 Rechtmäßiger Grund für die Gewährung des Zugangs zum Konto (kontoführender Zahlungsdienstleister)

26. Wie in Randnummer 10 erwähnt, können Zahlungsdienstnutzer von ihrem Recht Gebrauch machen, Zahlungsauslöse- und Kontoinformationsdienste in Anspruch zu nehmen. Die den Mitgliedstaaten in Artikel 66 Absatz 1 und Artikel 67 Absatz 1 PSD2 auferlegten Pflichten sollten in nationales Recht umgesetzt werden, um die wirksame Anwendung des Rechts des Zahlungsdienstnutzers auf Nutzung der vorgenannten Zahlungsdienste zu gewährleisten. Die wirksame Anwendung solcher Rechte wäre ohne eine entsprechende Verpflichtung des kontoführenden Zahlungsdienstleisters (in der Regel eine Bank), dem Zahlungsdienstleister unter der Voraussetzung, dass er alle Voraussetzungen für den Zugang zum Konto des

[20] Es sei darauf hingewiesen, dass eine gründliche Prüfung der Frage, ob die Richtlinie zur Bekämpfung der Geldwäsche den Anforderungen von Artikel 6 Absatz 4 DSGVO entspricht, den Rahmen dieses Dokuments übersteigt.

Zahlungsdienstnutzers erfüllt hat, Zugang zu dem Konto zu gewähren, nicht möglich. Darüber hinaus ist in Artikel 66 Absatz 5 und Artikel 67 Absatz 4 PSD2 eindeutig festgelegt, dass das Erbringen von Zahlungsauslösediensten und Kontoinformationsdiensten nicht vom Bestehen einer vertraglichen Beziehung zu diesem Zweck zwischen den Zahlungsauslösedienstleistern bzw. Kontoinformationsdienstleistern und den kontoführenden Zahlungsdienstleistern abhängt.

27. Die Verarbeitung personenbezogener Daten durch den kontoführenden Zahlungsdienstleister, die darin besteht, den vom Zahlungsauslösedienstleister und dem Kontoinformationsdienstleister verlangten Zugang zu den personenbezogenen Daten zu gewähren, um dem Zahlungsdienstnutzer ihre Zahlungsdienste zu erbringen, beruht auf einer rechtlichen Verpflichtung. Zur Erreichung der Ziele der PSD2 müssen kontoführende Zahlungsdienstleister die personenbezogenen Daten für die Dienste von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern bereitstellen, was eine notwendige Voraussetzung dafür ist, dass Zahlungsauslösedienstleister und Kontoinformationsdienstleister ihre Dienste erbringen und somit die in Artikel 66 Absatz 1 und Artikel 67 Absatz 1 PSD2 vorgesehenen Rechte gewährleisten. Daher ist in diesem Fall Artikel 6 Absatz 1 Buchstabe c DSGVO als anwendbare Rechtsgrundlage heranzuziehen.

28. Da in der DSGVO festgelegt ist, dass eine Verarbeitung auf der Grundlage einer rechtlichen Verpflichtung eindeutig durch Unionsrecht oder das Recht der Mitgliedstaaten festgelegt sein sollte (siehe Artikel 6 Absatz 3 DSGVO), sollte sich die Verpflichtung der kontoführenden Zahlungsdienstleister, Zugang zu gewähren, aus den nationalen Rechtsvorschriften zur Umsetzung der PSD2 ergeben.

3 AUSDRÜCKLICHE EINWILLIGUNG

3.1 Einwilligung nach der DSGVO

29. Nach der DSGVO ist die Einwilligung eine der sechs Rechtsgrundlagen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten. Gemäß Artikel 4 Nummer 11 DSGVO ist unter Einwilligung der betroffenen Person „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“, zu verstehen. Diese vier Bedingungen – d. h. freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich – sind für die Wirksamkeit der Einwilligung von wesentlicher Bedeutung. Gemäß den Leitlinien 05/2020 des EDSA zur Einwilligung gemäß Verordnung 2016/679 kann die Einwilligung nur dann eine angemessene Grundlage für die Rechtmäßigkeit darstellen, wenn die betroffene Person die Kontrolle und eine echte Wahl erhält, die angebotenen Bedingungen anzunehmen bzw. ohne Nachteile abzulehnen. Wenn ein Verantwortlicher um Einwilligung ersucht, muss er prüfen, ob alle Voraussetzungen für das Einholen einer wirksamen Einwilligung erfüllt sind. Wird die Einwilligung unter vollumfänglicher Einhaltung der DSGVO eingeholt, gibt sie den betroffenen Personen die Kontrolle darüber, ob die sie betreffenden personenbezogenen Daten verarbeitet werden oder nicht. Andernfalls wird die Kontrolle der betroffenen Person illusorisch, und dann ist die Einwilligung eine unwirksame Grundlage für die Verarbeitung, was die Verarbeitung rechtswidrig macht.[21]

30. Die DSGVO enthält auch weitere Garantien in Artikel 7, wonach der Verantwortliche nachweisen können muss, dass zum Zeitpunkt der Verarbeitung eine gültige Einwilligung vorgelegen hat. Außerdem muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, sodass es von den anderen Sachverhalten klar zu unterscheiden ist. Darüber hinaus muss die betroffene Person über das Recht belehrt werden, dass sie ihre Einwilligung jederzeit genauso einfach widerrufen kann, wie sie die Einwilligung erteilt hat.

31. Gemäß Artikel 9 DSGVO ist die Einwilligung eine der Ausnahmen vom allgemeinen Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten. In diesem Fall muss die Einwilligung der betroffenen Person jedoch „ausdrücklich“ sein.[22]

32. Nach den Leitlinien 05/2020 des EDSA zur Einwilligung gemäß Verordnung 2016/679 bezieht sich der Begriff „ausdrücklich“ gemäß der DSGVO darauf, wie die betroffene Person ihre Einwilligung zum Ausdruck bringt. Dies bedeutet, dass die betroffene Person eine ausdrückliche Einwilligung für bestimmte Verarbeitungszwecke abgeben soll. Ein offensichtlicher Weg zum Einholen einer ausdrücklichen Einwilligung wäre, dass die Einwilligung in einer schriftlichen Erklärung ausdrücklich bestätigt wird. Der Verantwortliche könnte gegebenenfalls sicherstellen, dass die Erklärung von der betroffenen Person unterzeichnet wird, um alle möglichen Zweifel und einen möglicherweise fehlenden Nachweis für die Zukunft aus dem Weg zu räumen.

33. Unter keinen Umständen kann aus möglicherweise mehrdeutigen Erklärungen oder Handlungen eine Einwilligung abgeleitet werden. Ein Verantwortlicher muss auch beachten, dass eine

[21] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Rn. 3.

[22] Siehe auch Stellungnahme 15/2011 zur Definition von Einwilligung (WP 187), S. 6–8, und/oder Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG (WP 217), S. 9, 10, 13 und 14.

Einwilligung nicht durch denselben Vorgang erteilt werden kann, mit dem einem Vertrag oder den allgemeinen Geschäftsbedingungen einer Dienstleistung zugestimmt wird.

3.2 Zustimmung nach der PSD2

34. Der EDSA stellt fest, dass der rechtliche Rahmen für die ausdrückliche Zustimmung komplex ist, da sowohl die PSD2 als auch die DSGVO das Konzept der „ausdrücklichen Zustimmung bzw. Einwilligung“ enthalten. Dies wirft die Frage auf, ob die in Artikel 94 Absatz 2 PSD2 genannte „ausdrückliche Zustimmung“ in gleicher Weise ausgelegt werden sollte wie die ausdrückliche Einwilligung gemäß der DSGVO.

3.2.1 Ausdrückliche Zustimmung gemäß Artikel 94 Absatz 2 PSD2

35. Die PSD2 enthält eine Reihe spezifischer Vorschriften für die Verarbeitung personenbezogener Daten, insbesondere Artikel 94 Absatz 1 PSD2, in dem festgelegt ist, dass die Verarbeitung personenbezogener Daten für die Zwecke der PSD2 im Einklang mit dem EU-Datenschutzrecht erfolgen muss. Darüber hinaus ist in Artikel 94 Absatz 2 PSD2 festgeschrieben, dass Zahlungsdienstleister die für das Erbringen ihrer Zahlungsdienste notwendigen personenbezogenen Daten nur mit der ausdrücklichen Zustimmung des Zahlungsdienstnutzers abrufen, verarbeiten und speichern dürfen. Gemäß Artikel 33 Absatz 2 PSD2 gilt diese Anforderung der ausdrücklichen Zustimmung des Zahlungsdienstnutzers nicht für Kontoinformationsdienstleister. Gleichwohl benötigen Kontoinformationsdienstleister nach Artikel 67 Absatz 2 Buchstabe a PSD2 für die Erbringung ihrer Dienstleistungen weiterhin die ausdrückliche Zustimmung.

36. Wie bereits erwähnt, ist die Liste der Rechtsgrundlagen für die Verarbeitung im Rahmen der DSGVO abschließend. Gemäß Randnummer 14 liefert Artikel 6 Absatz 1 Buchstabe b DSGVO prinzipiell die Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Erbringung von Zahlungsdienstleistungen; dies bedeutet, dass die Verarbeitung für die Erfüllung eines Vertrags, dessen Partei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Daraus folgt, dass Artikel 94 Absatz 2 PSD2 nicht als zusätzliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten angesehen werden kann. Angesichts der vorstehenden Ausführungen ist der EDSA der Auffassung, dass dieser Absatz einerseits in Übereinstimmung mit dem geltenden Rechtsrahmen für den Datenschutz und andererseits in einer Weise ausgelegt werden sollte, die seine praktische Wirksamkeit bewahrt. Daher sollte die ausdrückliche Zustimmung nach Artikel 94 Absatz 2 PSD2 als zusätzliche vertragliche Anforderung[23] betrachtet werden, die sich auf den Zugang zu personenbezogenen Daten und deren anschließende Verarbeitung und Speicherung zum Zwecke der Erbringung von Zahlungsdiensten bezieht; dementsprechend ist sie nicht identisch mit der (ausdrücklichen) Einwilligung nach der DSGVO.

37. Die „ausdrückliche Zustimmung“ im Sinne von Artikel 94 Absatz 2 PSD2 ist eine vertragliche Zustimmung. Dies bedeutet, dass Artikel 94 Absatz 2 PSD2 dahingehend auszulegen ist, dass betroffene Personen beim Abschluss eines Vertrags mit einem Zahlungsdienstleister gemäß der PSD2 umfassend über die spezifischen Kategorien personenbezogener Daten, die verarbeitet werden, unterrichtet werden müssen. Außerdem müssen sie auf den spezifischen Zweck (Zahlungsdienst) hingewiesen werden, zu dem ihre personenbezogenen Daten verarbeitet werden, und sie müssen diesen Klauseln ausdrücklich zustimmen. Solche Klauseln sollen sich

[23] Schreiben des EDSA zur PSD2-Richtlinie vom 5. Juli 2018, S. 4.

deutlich von den anderen im Vertrag behandelten Sachverhalten unterscheiden und müssen von der betroffenen Person ausdrücklich akzeptiert werden.

38. Von zentraler Bedeutung für den Begriff „ausdrückliche Zustimmung“ im Sinne von Artikel 94 Absatz 2 PSD2 ist der Zugang zu personenbezogenen Daten zur anschließenden Verarbeitung und Speicherung dieser Daten für die Erbringung von Zahlungsdiensten. Dies bedeutet, dass der Zahlungsdienstleister[24] die personenbezogenen Daten noch nicht verarbeitet, sondern Zugang zu personenbezogenen Daten benötigt, die unter der Verantwortung eines anderen Verantwortlichen verarbeitet wurden. Schließt ein Zahlungsdienstnutzer beispielsweise einen Vertrag mit einem Zahlungsauslösedienstleister, muss Letzterer Zugang zu personenbezogenen Daten des Zahlungsdienstnutzers erhalten, die unter der Verantwortung des kontoführenden Zahlungsdienstleisters verarbeitet werden. Gegenstand der ausdrücklichen Zustimmung nach Artikel 94 Absatz 2 PSD2 ist die Erlaubnis, Zugang zu diesen personenbezogenen Daten zu erhalten, um diese personenbezogenen Daten, die für die Erbringung des Zahlungsdienstes notwendig sind, verarbeiten und speichern zu können. Wenn die betroffene Person ausdrücklich zustimmt, ist der kontoführende Zahlungsdienstleister verpflichtet, Zugang zu den angegebenen personenbezogenen Daten zu gewähren.

39. Obwohl die Zustimmung nach Artikel 94 Absatz 2 PSD2 keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten ist, bezieht sich diese Zustimmung speziell auf personenbezogene Daten und den Datenschutz und gewährleistet Transparenz und ein gewisses Maß an Kontrolle für den Zahlungsdienstnutzer.[25] Wenngleich die wesentlichen Bedingungen für die Zustimmung nach Artikel 94 Absatz 2 PSD2 in der PSD2 nicht festgelegt sind, sollte sie, wie oben dargelegt, in Übereinstimmung mit dem anwendbaren Rechtsrahmen des Datenschutzes und in einer Weise ausgelegt werden, die ihre praktische Wirksamkeit bewahrt.

40. In Bezug auf die von den Verantwortlichen bereitzustellenden Informationen und das Transparenzgebot heißt es in den Leitlinien für Transparenz der Artikel-29-Datenschutzgruppe: *Bei dem in diesen Bestimmungen skizzierten Transparenzgrundsatz stellt die Tatsache einen zentralen Erwägungsfaktor dar, dass die betroffene Person den Umfang und die Folgen der Verarbeitung im Vorfeld ermitteln kann und nicht später von der Art und Weise überrascht werden sollte, in der ihre personenbezogenen Daten verwendet worden sind.*[26]

41. Darüber hinaus müssen personenbezogene Daten gemäß dem Grundsatz der Zweckbindung für festgelegte, eindeutige und legitime Zwecke erhoben werden (Artikel 5 Absatz 1 Buchstabe b DSGVO). Werden personenbezogene Daten für mehr als einen Zweck erhoben, so sollten die Verantwortlichen nicht nur einen einzigen umfassenden Zweck ermitteln, um verschiedene Weiterverarbeitungsvorgänge zu rechtfertigen, die tatsächlich nur entfernt mit dem eigentlichen ursprünglichen Zweck zusammenhängen[27]. Der EDSA hat – zuletzt im Zusammenhang mit Verträgen über Online-Dienste – auf das Risiko hingewiesen, dass allgemeine Bedingungen für die Verarbeitung in die Verträge aufgenommen werden, und erklärt, dass der Zweck der Erhebung klar und konkret festgelegt werden sollte: Er muss hinreichend detailliert besagen, welche Art der Verarbeitung zu dem bestimmten Zweck gehört bzw. nicht dazu gehört, und es muss ermöglicht

[24] Dies gilt für die Dienste 1 bis 7 des Anhangs der PSD2.
[25] Artikel 94 Absatz 2 PSD2 fällt unter Kapitel 4 „Datenschutz“.
[26] Artikel-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, Rn. 10 (angenommen am 11. April 2018) – vom EDSA gebilligt.
[27] Article 29 Working Party Opinion 03/2013 on purpose limitation (WP 203) (Artikel-29-Datenschutzgruppe, Stellungnahme 03/2013 zur Zweckbindung (WP 203)), S. 16.

werden, dass die Einhaltung des Rechts bewertet und die Anwendung von Datenschutzgarantien sichergestellt werden kann.[28]

42. Wird dies im Zusammenhang mit dem zusätzlichen Erfordernis der ausdrücklichen Zustimmung gemäß Artikel 94 Absatz 2 PSD2 betrachtet, bedeutet dies, dass die Verantwortlichen betroffenen Personen spezifische und ausdrückliche Informationen über die spezifischen Zwecke zur Verfügung stellen müssen, die von dem Verantwortlichen ermittelt wurden und die Verarbeitung und Speicherung der personenbezogenen Daten und den Zugriff darauf betreffen. Gemäß Artikel 94 Absatz 2 PSD2 müssen die betroffenen Personen diesen spezifischen Zwecken ausdrücklich zustimmen.

43. Darüber hinaus weist der EDSA, wie oben in Randnummer 10 ausgeführt, darauf hin, dass der Zahlungsdienstnutzer frei entscheiden können muss, den Dienst zu nutzen oder nicht, und nicht dazu gezwungen werden kann. Daher muss die Zustimmung nach Artikel 94 Absatz 2 PSD2 auch eine freiwillig erteilte Zustimmung sein.

3.3 Schlussfolgerung

44. Die ausdrückliche Zustimmung im Rahmen der PSD2 unterscheidet sich von der (ausdrücklichen) Einwilligung der DSGVO. Die ausdrückliche Zustimmung gemäß Artikel 94 Absatz 2 PSD2 ist eine zusätzliche Anforderung vertraglicher Natur. Benötigt ein Zahlungsdienstleister für die Erbringung eines Zahlungsdienstes Zugang zu personenbezogenen Daten, ist die ausdrückliche Zustimmung des Zahlungsdienstnutzers gemäß Artikel 94 Absatz 2 PSD2 erforderlich.

[28] Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, Rn. 16 (Version der öffentlichen Konsultation) und Stellungnahme 03/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung (WP 203) (Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203)), S. 15–16.

4 VERARBEITUNG VON DATEN VON NICHTVERTRAGSPARTEIEN („SILENT PARTY DATA“)

4.1 Daten von Nichtvertragsparteien

45. Ein Aspekt des Datenschutzes, der sorgfältig geprüft werden muss, betrifft die Verarbeitung sogenannter Daten von Nichtvertragsparteien. Im Zusammenhang mit diesem Dokument sind Daten von Nichtvertragsparteien personenbezogene Daten einer betroffenen Person, die zwar nicht Nutzer eines bestimmten Zahlungsdienstleisters ist, deren personenbezogene Daten jedoch von diesem bestimmten Zahlungsdienstleister für die Erfüllung eines Vertrags zwischen dem Zahlungsdienstleister und dem Zahlungsdienstnutzer verarbeitet werden. Dies ist beispielsweise der Fall, wenn ein Zahlungsdienstnutzer, d. h. die betroffene Person A, die Dienste eines Kontoinformationsdienstleisters in Anspruch nimmt, und die betroffene Person B eine Reihe von Zahlungsvorgängen auf das Zahlungskonto der betroffenen Person A ausgeführt hat. In diesem Fall gilt die betroffene Person B als Nichtvertragspartei, und die personenbezogenen Daten (wie die Kontonummer der betroffenen Person B und der Geldbetrag dieser Vorgänge) in Bezug auf die betroffene Person B werden als Daten von Nichtvertragsparteien betrachtet.

4.2 Berechtigtes Interesse des Verantwortlichen

46. Nach Artikel 5 Absatz 1 Buchstabe b DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Darüber hinaus ist in der DSGVO festgelegt, dass jede Verarbeitung personenbezogener Daten sowohl notwendig als auch verhältnismäßig sein und mit den Datenschutzgrundsätzen, wie den Grundsätzen der Zweckbindung und der Datenminimierung, im Einklang stehen muss.

47. Gemäß der DSGVO kann die Verarbeitung von Daten von Nichtvertragsparteien erlaubt sein, wenn diese Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist (Artikel 6 Absatz 1 Buchstabe f DSGVO). Eine solche Verarbeitung kann jedoch nur erfolgen, „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“.

48. Somit kann das berechtigte Interesse eines Verantwortlichen oder eines Dritten an der Erfüllung des Vertrags mit dem Zahlungsdienstnutzer eine Grundlage für die Rechtmäßigkeit der Verarbeitung von Daten von Nichtvertragsparteien durch Zahlungsauslösedienstleister und Kontoinformationsdienstleister im Zusammenhang mit der Erbringung von Zahlungsdiensten im Rahmen der PSD2 sein. Die Notwendigkeit, personenbezogene Daten von Nichtvertragsparteien zu verarbeiten, ist beschränkt und wird durch die vernünftigen Erwartungen dieser betroffenen Personen bestimmt. Im Zusammenhang mit der Erbringung von Zahlungsdiensten, die unter die PSD2 fallen, müssen wirksame und geeignete Maßnahmen ergriffen werden, damit die Interessen oder Grundrechte und Grundfreiheiten der Nichtvertragsparteien nicht außer Acht gelassen werden; außerdem muss sichergestellt sein, dass den vernünftigen Erwartungen dieser betroffenen Personen an die Verarbeitung ihrer personenbezogenen Daten entsprochen wird. In diesem Zusammenhang muss der Verantwortliche (Kontoinformationsdienstleister oder Zahlungsauslösedienstleister) die erforderlichen Garantien für die Verarbeitung schaffen, um die Rechte der betroffenen Personen zu schützen. In diesem Rahmen muss unter anderem mit technischen Maßnahmen sichergestellt werden, dass Daten von Nichtvertragsparteien nicht zu einem anderen Zweck verarbeitet werden als zu dem, zu dem die personenbezogenen Daten ursprünglich von Zahlungsauslösedienstleistern und Kontoinformationsdienstleistern erhoben

wurden. Soweit machbar, sollten auch Verschlüsselungstechniken oder andere Techniken angewandt werden, um ein angemessenes Maß an Sicherheit und Datenminimierung zu erreichen.

4.3 Weiterverarbeitung personenbezogener Daten von Nichtvertragsparteien

49. Wie in Randnummer 29 ausgeführt, könnten personenbezogene Daten, die im Zusammenhang mit einem von der PSD2 regulierten Zahlungsdienst verarbeitet werden, auf der Grundlage rechtlicher Verpflichtungen des Diensteanbieters weiterverarbeitet werden. Diese rechtlichen Verpflichtungen könnten personenbezogene Daten der Nichtvertragspartei betreffen.

50. In Bezug auf die Weiterverarbeitung von Daten von Nichtvertragsparteien auf der Grundlage eines berechtigten Interesses vertritt der EDSA die Auffassung, dass diese Daten zu keinem Zweck verwendet werden dürfen, der von dem abweicht, zu dem die Daten ursprünglich erhoben wurden, und der nicht mit Unionsrecht oder dem Recht der Mitgliedstaaten vereinbar ist. Die Einholung der Einwilligung der Nichtvertragspartei ist rechtlich nicht machbar, da personenbezogene Daten der Nichtvertragspartei erhoben oder verarbeitet werden müssten, um die Einwilligung der betroffenen Person zu erhalten, wofür nach Artikel 6 DSGVO keine Rechtsgrundlage gefunden werden kann. Die Prüfung der Vereinbarkeit nach Artikel 6 Absatz 4 DSGVO kann auch keine Grundlage für die Verarbeitung zu anderen Zwecken (z. B. Direktwerbung) bieten. Die Rechte und Freiheiten dieser betroffenen Personen, die als Nichtvertragspartei beteiligt sind, werden nicht gewahrt, wenn der neue Verantwortliche die personenbezogenen Daten für andere Zwecke verwendet, wobei der Kontext, in dem die personenbezogenen Daten erhoben wurden, berücksichtigt wird, insbesondere das Fehlen jeglicher Beziehung zu den betroffenen Personen, die Nichtvertragsparteien sind[29], das Fehlen eines Zusammenhangs zwischen einem anderen Zweck und dem Zweck, zu dem die personenbezogenen Daten ursprünglich erhoben wurden (d. h. die Tatsache, dass Zahlungsdienstleister lediglich Daten von Nichtvertragsparteien benötigen, um einen Vertrag mit der anderen Vertragspartei zu erfüllen), die Art der betreffenden personenbezogenen Daten[30], der Umstand, dass betroffene Personen nicht in der Lage sind, vernünftigerweise eine weitere Verarbeitung zu erwarten oder zu wissen, welcher Verantwortliche ihre personenbezogenen Daten verarbeiten kann, und angesichts der rechtlichen Beschränkungen für die Verarbeitung gemäß Artikel 66 Absatz 3 Buchstabe g und Artikel 67 Absatz 2 Buchstabe f PSD2.

[29] Nach Erwägungsgrund 87 der PSD2 hat die PSD2 nur „die vertraglichen Verpflichtungen und Verantwortlichkeiten zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister zum Gegenstand". Daher fallen Daten von Nichtvertragsparteien nicht in den Anwendungsbereich der PSD2.

[30] Besondere Sorgfalt sollte bei der Verarbeitung personenbezogener Finanzdaten gelten, da davon ausgegangen werden kann, dass die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen gemäß den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) mit sich bringt.

5 VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN IM RAHMEN DER PSD2

5.1 Besondere Kategorien personenbezogener Daten

51. Nach Artikel 9 Absatz 1 DSGVO ist die Verarbeitung „personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“ untersagt.

52. Es sollte betont werden, dass elektronische Zahlungen in einigen Mitgliedstaaten bereits allgegenwärtig sind und von vielen Menschen im Alltag gegenüber Bargeld bevorzugt werden. Gleichzeitig können durch Finanztransaktionen sensible Informationen über eine einzelne betroffene Person offengelegt werden, einschließlich solcher, die sich auf besondere Kategorien personenbezogener Daten beziehen. Je nach den Transaktionsdaten können politische Meinungen und religiöse Überzeugungen beispielsweise durch Spenden an politische Parteien oder Organisationen, Kirchen oder Gemeinden offengelegt werden. Die Mitgliedschaft in einer Gewerkschaft kann aus der Abbuchung eines jährlichen Mitgliedsbeitrags vom Bankkonto einer Person abgeleitet werden. Personenbezogene Gesundheitsdaten können aus der Analyse medizinischer Rechnungen gewonnen werden, die von einer betroffenen Person an eine medizinische Fachkraft (z. B. einen Psychiater) gezahlt werden. Ebenso können Informationen über bestimmte Käufe Hinweise zum Sexualleben oder der sexuellen Orientierung einer Person offenlegen. Wie aus diesen Beispielen hervorgeht, können selbst einzelne Transaktionen besondere Kategorien personenbezogener Daten enthalten. Darüber hinaus könnten Kontoinformationsdienste auf Profiling im Sinne von Artikel 4 Absatz 4 DSGVO zurückgreifen. Wie bereits in den Leitlinien der Artikel-29-Datenschutzgruppe zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 (vom EDSA gebilligt) dargelegt, können durch „Profiling [...] Daten besonderer Kategorien erzeugt werden, indem aus Daten, die an sich keine besondere Datenkategorien bilden, dies aber in Kombination mit anderen Daten tun, Daten abgeleitet werden.“[31] Dies bedeutet, dass sich aus der Summe von Finanztransaktionen verschiedene Arten von Verhaltensmustern herauslesen lassen, was auch besondere Kategorien personenbezogener Daten umfassen kann. Daher ist es sehr wahrscheinlich, dass ein Diensteanbieter, der Informationen über Finanztransaktionen betroffener Personen verarbeitet, auch besondere Kategorien personenbezogener Daten verarbeitet.

53. In Bezug auf den Begriff „sensible Zahlungsdaten“ stellt der EDSA Folgendes fest: Die Definition sensibler Zahlungsdaten in der PSD2 unterscheidet sich erheblich von der gängigen Verwendung des Begriffs „sensible personenbezogene Daten“ im Kontext der DSGVO und des Datenschutz(rechts). Während „sensible Zahlungsdaten“ in der PSD2 als „Daten, einschließlich personalisierter Sicherheitsmerkmale, die für betrügerische Handlungen verwendet werden können“, definiert werden, wird in der DSGVO betont, dass besondere Kategorien personenbezogener Daten, die nach Artikel 9 DSGVO ihrem Wesen nach hinsichtlich der

[31] Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP251rev.01, S. 16.

Grundrechte und Grundfreiheiten besonders sensibel sind, wie z. B. besondere Kategorien personenbezogener Daten, besonders geschützt werden müssen.[32] In diesem Zusammenhang wird empfohlen, zumindest die Art der personenbezogenen Daten, die verarbeitet werden, genau zu erfassen und zu kategorisieren. Höchstwahrscheinlich wird eine Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO erforderlich sein, was bei dieser Erfassung hilfreich ist. Weitere Orientierungshilfen zu Datenschutz-Folgenabschätzungen finden sich in den Leitlinien der Artikel-29-Arbeitsgruppe zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (vom EDSA gebilligt).

5.2 Mögliche Ausnahmeregelungen

54. Das Verbot nach Artikel 9 DSGVO ist nicht absolut. Insbesondere in Anbetracht dessen, dass Ausnahmen von Artikel 9 Absatz 2 Buchstaben b bis f und Buchstaben h bis j DSGVO offensichtlich nicht auf die Verarbeitung personenbezogener Daten im Zusammenhang mit der PSD2 anwendbar sind, könnten die beiden folgenden Ausnahmen in Artikel 9 Absatz 2 DSGVO in Betracht gezogen werden:

a) Das Verbot gilt nicht, wenn die betroffene Person ausdrücklich in die Verarbeitung dieser personenbezogenen Daten für einen oder mehrere festgelegte Zwecke eingewilligt hat (Artikel 9 Absatz 2 Buchstabe a DSGVO).

b) Das Verbot ist nicht anwendbar, wenn die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist (Artikel 9 Absatz 2 Buchstabe g DSGVO).

55. Es sei darauf hingewiesen, dass die Liste der Ausnahmen in Artikel 9 Absatz 2 DSGVO abschließend ist. Die Möglichkeit, dass in den personenbezogenen Daten, die für die Erbringung einer der unter die PSD2 fallenden Dienste verarbeitet werden, besondere Kategorien personenbezogener Daten enthalten sind, muss vom Diensteanbieter eingeräumt werden. Da das Verbot von Artikel 9 Absatz 1 DSGVO auf diese Diensteanbieter anwendbar ist, müssen Letztere sicherstellen, dass eine der Ausnahmen nach Artikel 9 Absatz 2 DSGVO auf sie anwendbar ist. Zu beachten ist, dass in Fällen, in denen der Dienstleister nicht nachweisen kann, dass eine der Ausnahmen erfüllt ist, das Verbot von Artikel 9 Absatz 1 Anwendung findet.

5.3 Erhebliches öffentliches Interesse

56. 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

[32] So werden beispielsweise in Erwägungsgrund 10 der DSGVO besondere Kategorien personenbezogener Daten als „sensible Daten“ bezeichnet.

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.

5.4 Ausdrückliche Einwilligung

57. In Fällen, in denen die Ausnahmeregelung gemäß Artikel 9 Absatz 2 Buchstabe g DSGVO nicht anwendbar ist, scheint die Einholung einer ausdrücklichen Einwilligung – im Einklang mit den Bedingungen für eine gültige Einwilligung in der DSGVO – die einzige mögliche rechtmäßige Ausnahme für die Verarbeitung besonderer Kategorien personenbezogener Daten durch Drittanbieter zu sein. In den Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 des EDSA heißt es[33]: „Nach Artikel 9 Absatz 2 ist ‚für die Erfüllung eines Vertrags erforderlich' nicht als eine Ausnahme von dem allgemeinen Verbot anzusehen, besondere Kategorien von Daten zu verarbeiten. Deshalb sollten Verantwortliche und Mitgliedstaaten, die mit dieser Situation umgehen, die spezifischen Ausnahmen in Artikel 9 Absatz 2 Buchstaben b bis j prüfen." Wenn sich Dienstleister auf Artikel 9 Absatz 2 Buchstabe a DSGVO berufen, müssen sie sicherstellen, dass sie vor Beginn der Verarbeitung die ausdrückliche Einwilligung erhalten haben. Bei der ausdrücklichen Einwilligung gemäß Artikel 9 Absatz 2 Buchstabe a DSGVO müssen alle Anforderungen der DSGVO erfüllt sein.

5.5 Keine geeignete Ausnahme

58. Wie bereits erwähnt, ist das Verbot von Artikel 9 Absatz 1 anwendbar, wenn der Dienstleister nicht nachweisen kann, dass eine der Ausnahmen zutrifft. In diesem Fall könnten technische Maßnahmen ergriffen werden, um die Verarbeitung besonderer Kategorien personenbezogener Daten zu verhindern, indem beispielsweise die Verarbeitung bestimmter Datenpunkte verhindert wird. In diesem Zusammenhang können Zahlungsdienstleister die technischen Möglichkeiten prüfen, um bestimmte Kategorien personenbezogener Daten auszuschließen und einen selektiven Zugang zu gewähren, was die Verarbeitung besonderer Kategorien personenbezogener Daten im Zusammenhang mit Daten von Nichtvertragsparteien durch Drittanbieter verhindern würde.

[33] Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, EDSA, Rn. 99.

6 DATENMINIMIERUNG, SICHERHEIT, TRANSPARENZ, RECHENSCHAFTSPFLICHT UND PROFILING

6.1 Datenminimierung und Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

59. Der Grundsatz der Datenminimierung ist in Artikel 5 Absatz 1 Buchstabe c DSGVO verankert: „Personenbezogene Daten müssen ... dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“. Nach dem Grundsatz der Datenminimierung sollten Verantwortliche im Wesentlichen nicht mehr personenbezogene Daten verarbeiten als zur Erreichung des betreffenden spezifischen Zwecks erforderlich. Wie in Kapitel 2 ausgeführt, richten sich die Menge und die Art der personenbezogenen Daten, die für die Erbringung des Zahlungsdienstes erforderlich sind, nach dem Ziel und dem gegenseitigen Verständnis über den vertraglichen Zweck.[34] Die Datenminimierung ist auf jede Verarbeitung anwendbar (z. B. jegliche Erhebungen oder Anforderungen personenbezogener Daten sowie jegliche Zugriffe auf diese Daten). In den Leitlinien 4/2019 des EDSA zum Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen heißt es, dass Verarbeiter und Technologieanbieter auch als Schlüsselfaktoren für den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen anerkannt sind; ebenso sollten sie sich darüber im Klaren sein, dass die für die Verarbeitung Verantwortlichen verpflichtet sind, personenbezogene Daten nur mit Systemen und Technologien zu verarbeiten, die einen integrierten Datenschutz aufweisen.[35]

60. Artikel 25 DSGVO enthält die Verpflichtungen zur Anwendung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Diese Verpflichtungen sind für den Grundsatz der Datenminimierung von besonderer Bedeutung. In dem Artikel ist festgelegt, dass Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen ergreifen müssen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen. Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Diese Maßnahmen können Verschlüsselung, Pseudonymisierung und andere technische Maßnahmen umfassen.

61. Bei der Anwendung der Verpflichtung nach Artikel 25 DSGVO sind der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen, die mit der Verarbeitung verbunden sind. Weitere Klarstellungen zu dieser Verpflichtung finden sich in den oben genannten Leitlinien 4/2019 des

[34] Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, EDSA, Rn. 32.
[35] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), S. 29.

EDSA zu Artikel 25 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Guidelines 4/2019 on Article 25 Data Protection by Design and by Default).

6.2 Maßnahmen zur Datenminimierung

62. Der Drittanbieter, der für die Erbringung der angeforderten Dienste auf Zahlungskontodaten zugreift, muss auch dem Grundsatz der Datenminimierung Rechnung tragen und darf nur personenbezogene Daten erheben, die für die Erbringung der vom Zahlungsdienstnutzer angeforderten spezifischen Zahlungsdienste erforderlich sind. Der Zugang zu personenbezogenen Daten sollte grundsätzlich auf das für die Erbringung von Zahlungsdiensten erforderliche Maß beschränkt werden. Wie in Kapitel 2 dargelegt, sind kontoführende Zahlungsdienstleister gemäß der PSD2 verpflichtet, auf Verlangen des Zahlungsdienstnutzers Informationen über Zahlungsdienstnutzer auszutauschen, wenn der Zahlungsdienstnutzer einen Zahlungsauslösedienst oder einen Kontoinformationsdienst nutzen möchte.

63. Sind nicht alle Zahlungskontodaten für die Vertragserfüllung erforderlich, sollte der Kontoinformationsdienstleister eine Auswahl der relevanten Datenkategorien vornehmen, bevor die Daten erhoben werden. So können beispielsweise Datenkategorien, die möglicherweise nicht erforderlich sind, die Identität der Nichtvertragspartei und die Daten der Transaktion enthalten. Außerdem muss die IBAN des Bankkontos der Nichtvertragspartei unter Umständen nicht angezeigt werden, sofern dies nicht im Recht eines Mitgliedstaats oder im Unionsrecht vorgeschrieben ist.

64. In diesem Zusammenhang könnte im Rahmen der Umsetzung geeigneter Datenschutzvorkehrungen nach Artikel 24 Absatz 2 DSGVO die mögliche Anwendung technischer Maßnahmen erwogen werden, die Drittanbieter bei der Erfüllung ihrer Verpflichtung unterstützen, nur auf die für die Erbringung ihrer Dienste erforderlichen personenbezogenen Daten zuzugreifen und diese auszulesen. In diesem Zusammenhang empfiehlt der EDSA die Nutzung digitaler Instrumente, um Kontoinformationsdienstleister bei der Erfüllung ihrer Verpflichtung zu unterstützen, nur personenbezogene Daten zu erheben, die für die Zwecke, zu denen sie verarbeitet werden, erforderlich sind. Benötigt beispielsweise ein Dienstleister für die Erbringung seiner Leistung nicht die Transaktionsmerkmale (im Beschreibungsfeld der Transaktionsbelege), könnte ein digitales Auswahlinstrument es Drittanbietern ermöglichen, dieses Feld von den gesamten Verarbeitungsvorgängen des Drittanbieters auszuschließen.

Beispiel 2:

HappyPayments, der Kontoinformationsdienstleister aus Beispiel 1, möchte sicherstellen, dass er nur die personenbezogenen Zahlungskontodaten verarbeitet, an denen seine Nutzer interessiert sind. Der Zugang zu mehr Zahlungskontodaten wäre für die Erbringung des Dienstes nicht erforderlich. Daher ermöglicht er den Nutzern, die spezifischen Arten von Informationen auszuwählen, an denen sie interessiert sind.

Nutzer A wünscht einen Überblick über seine Ausgaben in den letzten zwei Monaten. Dementsprechend fordert er für seine beiden Bankkonten, die bei verschiedenen kontoführenden Zahlungsdienstleistern geführt werden, die Angaben zu allen Transaktionen der letzten beiden Monate, den Transaktionsbetrag, das Ausführungsdatum sowie den Namen des Begünstigten an und kreuzt die entsprechenden Felder in der Benutzeroberfläche von HappyPayments an.

HappyPayments fordert dann von den jeweiligen kontoführenden Zahlungsdienstleistern nur die Informationen an, die den von Nutzer A angekreuzten Feldern entsprechen und in den letzten zwei Monaten angefallen sind. Informationen wie der „Verwendungszweck“ der Überweisung oder sogar die IBAN werden nicht verlangt, da Nutzer A diese Informationen nicht angefordert hat.

Um HappyPayments die Erfüllung seiner Verpflichtungen in Bezug auf die Datenminimierung zu ermöglichen, erlauben die kontoführenden Zahlungsdienstleister HappyPayments, bestimmte Felder für eine Reihe von Daten anzufordern.

65. In diesem Zusammenhang ist auch darauf hinzuweisen, dass kontoführende Zahlungsdienstleister laut PSD2 nur Zugang zu Zahlungskontoinformationen gewähren dürfen. Im Rahmen der PSD2 gibt es keine Rechtsgrundlage für die Gewährung des Zugangs zu personenbezogenen Daten anderer Konten wie Sparkonten, Hypotheken oder Anlagekonten. Dementsprechend muss gemäß der PSD2 mit technischen Maßnahmen sichergestellt werden, dass der Zugang auf die erforderlichen Zahlungskontoinformationen beschränkt wird.

66. Der Dienstleister muss nicht nur so wenige Daten wie möglich erheben, sondern auch begrenzte Speicherfristen anwenden. Personenbezogene Daten sollten vom Dienstleister nicht länger gespeichert werden, als dies für die vom Zahlungsdienstnutzer gewünschten Zwecke erforderlich ist.

67. Erfordert der Vertrag zwischen der betroffenen Person und dem Kontoinformationsdienstleister die Übermittlung personenbezogener Daten an Dritte, dürfen nur die personenbezogenen Daten übermittelt werden, die für die Erfüllung des Vertrags erforderlich sind. Betroffene Personen sollten auch darüber unterrichtet werden, dass und welche personenbezogenen Daten an Dritte übermittelt werden.

6.3 Sicherheit

68. Der EDSA hat bereits betont, dass die Verletzung in Bezug auf personenbezogene Finanzdaten *„mit ernsthaften Konsequenzen für den Alltag des Betroffenen“* einhergeht, und nennt als Beispiel die Gefahr von Zahlungsbetrug.[36]

69. Betrifft eine Datenschutzverletzung Finanzdaten, so kann die betroffene Person erheblichen Risiken ausgesetzt sein. Je nachdem, welche Informationen von der Datenschutzverletzung betroffen sind, können betroffene Personen dem Risiko des Identitätsdiebstahls, des Diebstahls der Gelder auf ihren Konten und anderer Vermögenswerte ausgesetzt sein. Darüber hinaus ist nicht auszuschließen, dass die Offenlegung von Transaktionsdaten mit erheblichen Datenschutzrisiken verbunden ist, da Transaktionsdaten Hinweise auf alle Aspekte des Privatlebens einer betroffenen Person enthalten können. Gleichzeitig sind Finanzdaten für Kriminelle ohne Frage wertvoll und daher ein attraktives Ziel.

70. Als für die Verarbeitung Verantwortliche sind Zahlungsdienstleister verpflichtet, geeignete Maßnahmen zum Schutz der personenbezogenen Daten betroffener Personen zu ergreifen (Artikel 24 Absatz 1 DSGVO). Je höher die Risiken im Zusammenhang mit der Verarbeitung durch den für die Verarbeitung Verantwortlichen sind, desto strenger sind die anzuwendenden Sicherheitsstandards. Da die Verarbeitung von Finanzdaten mit einer Vielzahl schwerwiegender Risiken verbunden ist, sollten die Sicherheitsmaßnahmen entsprechend streng sein.

71. Dienstleister sollten hohen Standards genügen, einschließlich strenger Mechanismen für die Kundenauthentifizierung und hoher Sicherheitsstandards für die technische Ausrüstung.[37] Weitere

[36] Leitlinien der Artikel-29-Datenschutzgruppe zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP248 rev.01 – vom EDSA gebilligt.
[37] Siehe hierzu die technischen Regulierungsstandards.

Verfahren wie die Überprüfung von Verarbeitern auf Sicherheitsstandards und die Umsetzung von Verfahren zum Schutz vor unbefugtem Zugriff sind auch wichtig.

6.4 Transparenz und Rechenschaftspflicht

72. Transparenz und Rechenschaftspflicht sind zwei Grundprinzipien der DSGVO.

73. In Bezug auf Transparenz (Artikel 5 Absatz 1 Buchstabe a DSGVO) ist in Artikel 12 DSGVO festgelegt, dass Verantwortliche geeignete Maßnahmen treffen müssen, um die in den Artikeln 13 und 14 DSGVO genannten Informationen zu übermitteln. Außerdem müssen die Informationen oder Mitteilungen über die Verarbeitung personenbezogener Daten präzise, transparent, verständlich und leicht zugänglich sein. Die Informationen sind in einer klaren und einfachen Sprache schriftlich „oder in anderer Form, gegebenenfalls auch elektronisch“ zu übermitteln. Die vom EDSA gebilligten Leitlinien für Transparenz gemäß der Verordnung 2016/679 der Artikel-29-Datenschutzgruppe enthalten spezielle Anweisungen für die Einhaltung des Grundsatzes der Transparenz in digitalen Umgebungen.

74. Die oben genannten Leitlinien für Transparenz gemäß der Verordnung 2016/679 besagen, dass Artikel 11 DSGVO als eine Möglichkeit ausgelegt werden sollte, ohne Behinderung der Ausübung der Rechte betroffener Personen eine echte Datenminimierung durchzusetzen, und dass die Wahrnehmung der Rechte betroffener Personen mithilfe der von der betroffenen Person zur Verfügung gestellten zusätzlichen Informationen ermöglicht werden muss. Darüber hinaus treten ggfs. Situationen auf, in denen der Verantwortliche personenbezogene Daten verarbeitet, die keine Identifizierung der betroffenen Person erfordern (zum Beispiel bei pseudonymisierten Daten). In solchen Fällen kann auch Artikel 11 Absatz 1 relevant sein, da es dort heißt, dass der Verantwortliche nicht verpflichtet ist, zur bloßen Einhaltung der DSGVO zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

75. Für die Dienste im Rahmen der PSD2 ist Artikel 13 DSGVO auf die von der betroffenen Person erhobenen personenbezogenen Daten anwendbar, während Artikel 14 auf das Szenario anwendbar ist, in dem die personenbezogenen Daten nicht von der betroffenen Person selbst erlangt wurden.

76. Die betroffene Person muss insbesondere über den Zeitraum, in dem die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, über die Kriterien zur Bestimmung dieses Zeitraums und gegebenenfalls über die berechtigten Interessen, die von dem für die Verarbeitung Verantwortlichen oder einem potenziellen Dritten verfolgt werden, unterrichtet werden. Beruht die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a DSGVO oder auf einer ausdrücklichen Einwilligung gemäß Artikel 9 Absatz 2 Buchstabe a DSGVO, so muss die betroffene Person darüber informiert werden, dass sie das Recht hat, diese Einwilligung jederzeit zu widerrufen.

77. Der für die Verarbeitung Verantwortliche unterrichtet die betroffene Person über die besonderen Umstände, unter denen die personenbezogenen Daten verarbeitet werden. Falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, was bei Kontoinformationsdienstleistern wahrscheinlich der Fall sein wird, müssen die Informationen spätestens zum Zeitpunkt der ersten Mitteilung an die betroffene Person übermittelt werden.[38] Sofern personenbezogene Daten einem anderen Empfänger offengelegt

[38] Artikel 14 Absatz 3 Buchstabe b DSGVO.

werden sollen, müssen die Informationen spätestens zum Zeitpunkt der ersten Offenlegung der personenbezogenen Daten übermittelt werden.

78. In Bezug auf Online-Zahlungsdienste wird in den oben genannten Leitlinien klargestellt, dass von den Verantwortlichen ein Mehrebenen-Ansatz verfolgt werden kann, in dessen Rahmen sie sich für einen Einsatz kombinierter Verfahren entscheiden, um Transparenz zu gewährleisten. Um Informationsermüdung zu vermeiden und die Wirksamkeit der Information sicherzustellen, wird insbesondere der Einsatz von Mehrebenen-Datenschutzerklärungen/-hinweisen empfohlen, um die verschiedenen Kategorien von Informationen, die der betroffenen Person zur Verfügung gestellt werden müssen, zu verknüpfen – anstelle einer Darstellung dieser gesamten Informationen auf dem Bildschirm in Form eines einzigen Hinweises.

79. Ebenso wird in den vorgenannten Leitlinien klargestellt, dass die für die Verarbeitung Verantwortlichen sich dafür entscheiden können, zusätzliche Instrumente zu verwenden, um der betroffenen Person Informationen zur Verfügung zu stellen, z. B. Datenschutz-Dashboards. Ein Datenschutz-Dashboard stellt eine zentrale Anlaufstelle dar, über welche die betroffenen Personen die „Datenschutzinformationen" einsehen und ihre Datenschutzpräferenzen verwalten können, indem sie ihre Einwilligung zu der Nutzung ihrer Daten auf gewisse Weise durch den besagten Dienst geben oder dieser widersprechen.[39] Ein Datenschutz-Dashboard könnte einen Überblick über die Drittanbieter geben, die die ausdrückliche Einwilligung der betroffenen Personen erhalten haben, und könnte sachdienliche Informationen über Art und Menge der personenbezogenen Daten, auf die die Drittanbieter zugegriffen haben, bieten. Grundsätzlich kann ein kontoführender Zahlungsdienstleister dem Nutzer die Möglichkeit bieten, eine spezifische ausdrückliche Einwilligung gemäß der PSD2[40] durch die Übersicht zu widerrufen, was eine Verweigerung des Zugangs zu seinen Zahlungskonten für einen oder mehrere Drittanbieter nach sich zöge. Ebenso könnte der Nutzer einen kontoführenden Zahlungsdienstleister auffordern, einem oder mehreren bestimmten Drittanbietern[41] den Zugang zu seinem Zahlungskonto/seinen Zahlungskonten zu verwehren, da der Nutzer das Recht besitzt, einen Kontoinformationsdienst (nicht) zu nutzen. Wenn Datenschutz-Dashboards verwendet werden, um eine ausdrückliche Einwilligung zu erteilen oder zu widerrufen, sollten sie rechtmäßig konzipiert und angewandt werden und insbesondere verhindern, dass Hindernisse für das Recht der Drittanbieter zur Erbringung von Dienstleistungen im Einklang mit der PSD2 geschaffen werden. In diesem Zusammenhang und im Einklang mit den anwendbaren Bestimmungen der PSD2 hat ein Drittanbieter die Möglichkeit, erneut die ausdrückliche Einwilligung des Nutzers einzuholen, nachdem diese Einwilligung widerrufen wurde.

80. Nach den Grundsätzen der Rechenschaftspflicht muss der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, um sicherzustellen und nachweisen zu können, dass die Verarbeitung gemäß der DSGVO und insbesondere gemäß den wichtigsten

[39] Gemäß den vom EDSA gebilligten Leitlinien der Artikel-29-Datenschutzgruppe für Transparenz gemäß der Verordnung 2016/679 sind Datenschutz-Dashboards insbesondere dann nützlich, wenn die betreffenden Personen den gleichen Dienst auf einer Vielzahl verschiedene Geräte nutzen, da sie so unabhängig davon, wie sie den Dienst nutzen, Zugang zu und die Kontrolle über ihre personenbezogenen Daten haben. Die Möglichkeit für die betroffenen Personen, ihre Datenschutzeinstellungen über ein Datenschutz-Dashboard manuell anzupassen, kann auch die Personalisierung von Datenschutzerklärungen/-hinweisen insofern erleichtern, als dann nur noch jeweils die Verarbeitungsarten aufgegriffen werden, die bei einer bestimmten betroffenen Person tatsächlich zum Tragen kommen.

[40] Siehe hierzu beispielsweise die „ausdrückliche Zustimmung" gemäß Artikel 67 Absatz 2 Buchstabe a PSD2.

[41] Siehe hierzu ebenfalls die Stellungnahme EBA/OP/2020/10 der EBA, Rn. 45.

Datenschutzgrundsätzen nach Artikel 5 Absatz 1 erfolgt. Diese Maßnahmen sollten die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen und im Bedarfsfall überprüft und angepasst werden.[42]

6.5 Profiling

81. Die Verarbeitung personenbezogener Daten durch Zahlungsdienstleister kann ein „Profiling" im Sinne von Artikel 4 Nummer 4 DSGVO beinhalten. Kontoinformationsdienstleister könnten beispielsweise die automatisierte Verarbeitung personenbezogener Daten heranziehen, um bestimmte personenbezogene Aspekte im Zusammenhang mit einer natürlichen Person zu bewerten. Je nach den Merkmalen des Dienstes könnten die persönlichen finanziellen Verhältnisse einer betroffenen Person bewertet werden. Kontoinformationsdienste, die auf Wunsch der Nutzer bereitgestellt werden, können eine umfassende Auswertung personenbezogener Zahlungskontodaten beinhalten.

82. Der für die Verarbeitung Verantwortliche muss die betroffene Person auch über das Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling, unterrichten. In diesen Fällen muss der für die Verarbeitung Verantwortliche aussagekräftige Informationen über die involvierte Logik sowie über die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person bereitstellen (Artikel 13 Absatz 2 Buchstabe f, Artikel 14 Absatz 2 Buchstabe g und Erwägungsgrund 60).[43] Ebenso hat die betroffene Person nach Artikel 15 DSGVO das Recht, von dem Verantwortlichen Informationen über das Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling, die involvierte Logik und die Folgen für die betroffene Person zu verlangen und zu erhalten, und unter bestimmten Umständen ein Recht auf Widerspruch gegen Profiling, unabhängig davon, ob ausschließlich automatisierte, auf Profiling beruhende Entscheidungen im Einzelfall getroffen werden.[44]

83. Darüber hinaus ist in diesem Zusammenhang auch das Recht der betroffenen Person relevant, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie in Artikel 22 DSGVO vorgesehen. Diese Norm schließt unter bestimmten Umständen auch die Notwendigkeit ein, dass die für die Verarbeitung Verantwortlichen geeignete Maßnahmen ergreifen, um die Rechte der betroffenen Person zu schützen, wie etwa die spezifische Unterrichtung der betroffenen Person und das Recht auf Eingreifen einer Person in die Entscheidungsfindung, und ihren Standpunkt darzulegen und die Entscheidung anzufechten. Wie auch in Erwägungsgrund 71 DSGVO ausgeführt, bedeutet dies unter anderem, dass betroffene Personen das Recht haben, keiner Entscheidung unterworfen zu werden, wie etwa der automatischen Ablehnung eines Online-Kreditantrags ohne jegliches menschliche Eingreifen.[45]

84. Eine automatisierte Entscheidungsfindung, einschließlich Profiling, die besondere Kategorien personenbezogener Daten umfasst, ist nur unter folgenden kumulativen Bedingungen zulässig (Artikel 22 Absatz 4 DSGVO):

[42] Artikel 5 Absatz 2 und Artikel 24 DSGVO.
[43] Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01 – vom EDSA gebilligt.
[44] Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP251rev.01.
[45] Erwägungsgrund 71 der DSGVO.

- Es gilt eine Ausnahme nach Artikel 22 Absatz 2, und
- es findet Artikel 9 Absatz 2 Buchstabe a oder g der DSGVO Anwendung. In beiden Fällen muss der Verantwortliche angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person treffen.[46]

85. Die in diesen Leitlinien festgelegten Anforderungen an die Weiterverarbeitung sind ebenfalls zu beachten. Die vom EDSA gebilligten Klarstellungen und Anweisungen zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, die in den Leitlinien der Artikel-29-Datenschutzgruppe zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 enthalten sind, sind im Zusammenhang mit Zahlungsdiensten uneingeschränkt relevant und sollten daher gebührend berücksichtigt werden.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)

[46] Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP251rev.01, Seite 26–27.