Sammlung der Rechtsprechung

URTEIL DES GERICHTSHOFS (Große Kammer)

16. Juli 2020*

„Vorlage zur Vorabentscheidung – Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten – Charta der Grundrechte der Europäischen Union – Art. 7, 8 und 47 – Verordnung (EU) 2016/679 – Art. 2 Abs. 2 – Anwendungsbereich – Übermittlungen personenbezogener Daten zu gewerblichen Zwecken in Drittländer – Art. 45 – Angemessenheitsbeschluss der Kommission – Art. 46 – Datenübermittlung vorbehaltlich geeigneter Garantien – Art. 58 – Befugnisse der Aufsichtsbehörden – Verarbeitung der übermittelten Daten für Zwecke der nationalen Sicherheit durch die Behörden eines Drittlands – Beurteilung der Angemessenheit des im Drittland gebotenen Schutzniveaus – Beschluss 2010/87/EU – Standardschutzklauseln für die Übermittlung personenbezogener Daten in Drittländer – Angemessene Garantien seitens des Verantwortlichen – Gültigkeit – Durchführungsbeschluss (EU) 2016/1250 – Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes – Gültigkeit – Beschwerde einer natürlichen Person, deren Daten aus der Europäischen Union in die Vereinigten Staaten übermittelt wurden“

In der Rechtssache C-311/18

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom High Court (Hoher Gerichtshof, Irland) mit Entscheidung vom 4. Mai 2018, beim Gerichtshof eingegangen am 9. Mai 2018, in dem Verfahren

Data Protection Commissioner

gegen

Facebook Ireland Ltd,

Maximillian Schrems,

Beteiligte:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

erlässt

* Verfahrenssprache: Englisch.

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten K. Lenaerts, der Vizepräsidentin R. Silva de Lapuerta, des Kammerpräsidenten A. Arabadjiev, der Kammerpräsidentin A. Prechal, der Kammerpräsidenten M. Vilaras, M. Safjan, S. Rodin und P. G. Xuereb, der Kammerpräsidentin L. S. Rossi, des Kammerpräsidenten I. Jarukaitis sowie der Richter M. Ilešič, T. von Danwitz (Berichterstatter) und D. Šváby,

Generalanwalt: H. Saugmandsgaard Øe,

Kanzler: C. Strömholm, Verwaltungsrätin,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 9. Juli 2019,

unter Berücksichtigung der Erklärungen

– des Data Protection Commissioner, vertreten durch D. Young, Solicitor, B. Murray und M. Collins, SC, sowie C. Donnelly, BL,

– der Facebook Ireland Ltd, vertreten durch P. Gallagher und N. Hyland, SC, A. Mulligan und F. Kieran, BL, sowie P. Nolan, C. Monaghan, C. O'Neill und R. Woulfe, Solicitors,

– von Herrn Schrems, vertreten durch Rechtsanwalt H. Hofmann, E. McCullough, J. Doherty und S. O'Sullivan, SC, sowie G. Rudden, Solicitor,

– von The United States of America, vertreten durch E. Barrington, SC, S. Kingston, BL, sowie S. Barton und B. Walsh, Solicitors,

– des Electronic Privacy Information Centre, vertreten durch S. Lucey, Solicitor, G. Gilmore und A. Butler, BL, sowie C. O'Dwyer, SC,

– der BSA Business Software Alliance Inc., vertreten durch B. Van Vooren und K. Van Quathem, advocaten,

– von Digitaleurope, vertreten durch N. Cahill, Barrister, J. Cahir, Solicitor, und M. Cush, SC,

– Irlands, vertreten durch A. Joyce und M. Browne als Bevollmächtigte im Beistand von D. Fennelly, BL,

– der belgischen Regierung, vertreten durch J.-C. Halleux und P. Cottin als Bevollmächtigte,

– der tschechischen Regierung, vertreten durch M. Smolek, J. Vláčil, O. Serdula und A. Kasalická als Bevollmächtigte,

– der deutschen Regierung, vertreten durch J. Möller, D. Klebs und T. Henze als Bevollmächtigte,

– der französischen Regierung, vertreten durch A.-L. Desjonquères als Bevollmächtigte,

– der niederländischen Regierung, vertreten durch C. S. Schillemans, M. K. Bulterman und M. Noort als Bevollmächtigte,

– der österreichischen Regierung, vertreten durch J. Schmoll und G. Kunnert als Bevollmächtigte,

– der polnischen Regierung, vertreten durch B. Majczyna als Bevollmächtigten,

– der portugiesischen Regierung, vertreten durch L. Inez Fernandes, A. Pimenta und C. Vieira Guerra als Bevollmächtigte,

– der Regierung des Vereinigten Königreichs, vertreten durch S. Brandon als Bevollmächtigten im Beistand von J. Holmes, QC, und C. Knight, Barrister,

– des Europäischen Parlaments, vertreten durch M. J. Martínez Iglesias und A. Caiola als Bevollmächtigte,

– der Europäischen Kommission, vertreten durch D. Nardi, H. Krämer und H. Kranenborg als Bevollmächtigte,

– des Europäischen Datenschutzausschusses (EDSA), vertreten durch A. Jelinek und K. Behn als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 19. Dezember 2019

folgendes

Urteil

1 Das Vorabentscheidungsersuchen betrifft im Wesentlichen

– die Auslegung von Art. 3 Abs. 2 erster Gedankenstrich, der Art. 25 und 26 sowie von Art. 28 Abs. 3 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31) im Licht von Art. 4 Abs. 2 EUV sowie der Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta),

– die Auslegung und die Gültigkeit des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46 (ABl. 2010, L 39, S. 5) in der durch den Durchführungsbeschluss (EU) 2016/2297 der Kommission vom 16. Dezember 2016 (ABl. 2016, L 344, S. 100) geänderten Fassung (im Folgenden: SDK-Beschluss) sowie

– die Auslegung und die Gültigkeit des Durchführungsbeschlusses (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (ABl. 2016, L 207, S. 1, im Folgenden: DSS-Beschluss).

2 Dieses Ersuchen ergeht im Rahmen eines Rechtsstreits zwischen dem Data Protection Commissioner (Datenschutzbeauftragter, Irland) (im Folgenden: Commissioner) auf der einen Seite und der Facebook Ireland Ltd sowie Herrn Maximillian Schrems auf der anderen Seite wegen einer Beschwerde von Herrn Schrems in Bezug auf die Übermittlung seiner personenbezogenen Daten durch Facebook Ireland an die Facebook Inc. in den Vereinigten Staaten.

Rechtlicher Rahmen

Richtlinie 95/46

3 Art. 3 („Anwendungsbereich“) der Richtlinie 95/46 bestimmte in Abs. 2:

„Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

– die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;

…“

4 Art. 25 der Richtlinie bestimmte:

„(1) Die Mitgliedstaaten sehen vor, dass die Übermittlung personenbezogener Daten … in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; …

…

(6) Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

Die Mitgliedstaaten treffen die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.“

5 Art. 26 Abs. 2 und 4 der Richtlinie sah vor:

„(2) Unbeschadet des Absatzes 1 kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland genehmigen, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben.

…

(4) Befindet die Kommission nach dem Verfahren des Artikels 31 Absatz 2, dass bestimmte Standardvertragsklauseln ausreichende Garantien gemäß Absatz 2 bieten, so treffen die Mitgliedstaaten die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.“

6 Art. 28 Abs. 3 der Richtlinie bestimmte:

„Jede Kontrollstelle verfügt insbesondere über:

– Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;

– wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;

– das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.

…“

DSGVO

7 Die Richtlinie 95/46 wurde durch die 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 (Datenschutz-Grundverordnung) (ABl. 2016, L 119, S. 1, berichtigt im ABl. 2016, L 314, S. 72, und im ABl. 2018, L 127, S. 2, im Folgenden: DSGVO) aufgehoben und ersetzt.

8 In den Erwägungsgründen 6, 10, 101, 103, 104, 107 bis 109, 114, 116 und 141 der DSGVO heißt es:

„(6) Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert und dürfte den Verkehr personenbezogener Daten innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei ein hohes Datenschutzniveau zu gewährleisten ist.

…

(10) Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden. Hinsichtlich der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, sollten die Mitgliedstaaten die Möglichkeit haben, nationale Bestimmungen, mit denen die Anwendung der

Vorschriften dieser Verordnung genauer festgelegt wird, beizubehalten oder einzuführen. In Verbindung mit den allgemeinen und horizontalen Rechtsvorschriften über den Datenschutz zur Umsetzung der Richtlinie 95/46/EG gibt es in den Mitgliedstaaten mehrere sektorspezifische Rechtsvorschriften in Bereichen, die spezifischere Bestimmungen erfordern. Diese Verordnung bietet den Mitgliedstaaten zudem einen Spielraum für die Spezifizierung ihrer Vorschriften, auch für die Verarbeitung besonderer Kategorien von personenbezogenen Daten (im Folgenden ‚sensible Daten'). Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

…

(101) Der Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und in Drittländer und internationale Organisationen ist für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Das durch diese Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen sollte jedoch bei der Übermittlung personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weiterübermittelt werden. In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig. Eine Datenübermittlung könnte nur stattfinden, wenn die in dieser Verordnung festgelegten Bedingungen zur Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vorbehaltlich der übrigen Bestimmungen dieser Verordnung von dem Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.

…

(103) Die Kommission darf mit Wirkung für die gesamte Union beschließen, dass ein bestimmtes Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet, und auf diese Weise in Bezug auf das Drittland oder die internationale Organisation, das bzw. die für fähig gehalten wird, ein solches Schutzniveau zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen. In derartigen Fällen dürfen personenbezogene Daten ohne weitere Genehmigung an dieses Land oder diese internationale Organisation übermittelt werden. Die Kommission kann, nach Abgabe einer ausführlichen Erklärung, in der dem Drittland oder der internationalen Organisation eine Begründung gegeben wird, auch entscheiden, eine solche Feststellung zu widerrufen.

(104) In Übereinstimmung mit den Grundwerten der Union, zu denen insbesondere der Schutz der Menschenrechte zählt, sollte die Kommission bei der Bewertung des Drittlands oder eines Gebiets oder eines bestimmten Sektors eines Drittlands berücksichtigen, inwieweit dort die Rechtsstaatlichkeit gewahrt ist, der Rechtsweg gewährleistet ist und die internationalen Menschenrechtsnormen und -standards eingehalten werden und welche allgemeinen und sektorspezifischen Vorschriften, wozu auch die Vorschriften über die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit sowie die öffentliche Ordnung und das Strafrecht zählen, dort gelten. Die Annahme eines Angemessenheitsbeschlusses in Bezug auf ein Gebiet oder einen bestimmten Sektor eines Drittlands sollte unter Berücksichtigung eindeutiger und objektiver Kriterien wie bestimmter Verarbeitungsvorgänge und des

Anwendungsbereichs anwendbarer Rechtsnormen und geltender Rechtsvorschriften in dem Drittland erfolgen. Das Drittland sollte Garantien für ein angemessenes Schutzniveau bieten, das dem innerhalb der Union gewährleisteten Schutzniveau der Sache nach gleichwertig ist, insbesondere in Fällen, in denen personenbezogene Daten in einem oder mehreren spezifischen Sektoren verarbeitet werden. Das Drittland sollte insbesondere eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten und Mechanismen für eine Zusammenarbeit mit den Datenschutzbehörden der Mitgliedstaaten vorsehen, und den betroffenen Personen sollten wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe eingeräumt werden.

…

(107) Die Kommission kann feststellen, dass ein Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation kein angemessenes Datenschutzniveau mehr bietet. Die Übermittlung personenbezogener Daten an dieses Drittland oder an diese internationale Organisation sollte daraufhin verboten werden, es sei denn, die Anforderungen dieser Verordnung in Bezug auf die Datenübermittlung vorbehaltlich geeigneter Garantien, einschließlich verbindlicher interner Datenschutzvorschriften und auf Ausnahmen für bestimmte Fälle werden erfüllt. In diesem Falle sollten Konsultationen zwischen der Kommission und den betreffenden Drittländern oder internationalen Organisationen vorgesehen werden. Die Kommission sollte dem Drittland oder der internationalen Organisation frühzeitig die Gründe mitteilen und Konsultationen aufnehmen, um Abhilfe für die Situation zu schaffen.

(108) Bei Fehlen eines Angemessenheitsbeschlusses sollte der Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. Diese geeigneten Garantien können darin bestehen, dass auf verbindliche interne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder von einer Aufsichtsbehörde genehmigte Vertragsklauseln zurückgegriffen wird. Diese Garantien sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden; dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen einschließlich des Rechts auf wirksame verwaltungsrechtliche oder gerichtliche Rechtsbehelfe sowie des Rechts auf Geltendmachung von Schadenersatzansprüchen in der Union oder in einem Drittland. Sie sollten sich insbesondere auf die Einhaltung der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten, die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen beziehen. …

(109) Die dem Verantwortlichen oder dem Auftragsverarbeiter offenstehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde festgelegten Standard-Datenschutzklauseln zurückzugreifen, sollte den Verantwortlichen oder den Auftragsverarbeiter weder daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen, wie zum Beispiel Verträgen zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, zu verwenden, noch ihn daran hindern, ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen oder die Grundrechte und Grundfreiheiten der betroffenen Personen beschneiden. Die Verantwortlichen und die Auftragsverarbeiter sollten ermutigt werden, mit vertraglichen Verpflichtungen, die die Standard-Schutzklauseln ergänzen, zusätzliche Garantien zu bieten.

…

(114) In allen Fällen, in denen kein Kommissionsbeschluss zur Angemessenheit des in einem Drittland bestehenden Datenschutzniveaus vorliegt, sollte der Verantwortliche oder der Auftragsverarbeiter auf Lösungen zurückgreifen, mit denen den betroffenen Personen durchsetzbare und wirksame Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten in der Union nach der Übermittlung dieser Daten eingeräumt werden, damit sie weiterhin die Grundrechte und Garantien genießen können.

…

(116) Wenn personenbezogene Daten in ein anderes Land außerhalb der Union übermittelt werden, besteht eine erhöhte Gefahr, dass natürliche Personen ihre Datenschutzrechte nicht wahrnehmen können[, um] sich insbesondere gegen die unrechtmäßige Nutzung oder Offenlegung dieser Informationen zu schützen. Ebenso kann es vorkommen, dass Aufsichtsbehörden Beschwerden nicht nachgehen oder Untersuchungen nicht durchführen können, die einen Bezug zu Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats haben. Ihre Bemühungen um grenzüberschreitende Zusammenarbeit können auch durch unzureichende Präventiv- und Abhilfebefugnisse, widersprüchliche Rechtsordnungen und praktische Hindernisse wie Ressourcenknappheit behindert werden. …

…

(141) Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts eine Beschwerde einzureichen und gemäß Artikel 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht oder wenn die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, eine Beschwerde teilweise oder ganz abweist oder ablehnt oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist. …“

9 Art. 2 Abs. 1 und 2 der DSGVO sieht vor:

„(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,

c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“

10 Art. 4 der DSGVO bestimmt:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck:

…

2. ‚Verarbeitung' jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

…

7. ‚Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

8. ‚Auftragsverarbeiter' eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

9. ‚Empfänger' eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

…"

11 In Art. 23 der DSGVO heißt es:

„(1) Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

…

(2) Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf

a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,

b) die Kategorien personenbezogener Daten,

c) den Umfang der vorgenommenen Beschränkungen,

d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung,

e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,

f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,

g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und

h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist."

12 Kapitel V („Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen") der DSGVO enthält ihre Art. 44 bis 50. Art. 44 („Allgemeine Grundsätze der Datenübermittlung") lautet:

„Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird."

13 Art. 45 („Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses") der DSGVO sieht in den Abs. 1 bis 3 vor:

„(1) Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere das Folgende:

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art – auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten – sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten. In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b des vorliegenden Artikels genannte Aufsichtsbehörde bzw. genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen."

14 Art. 46 („Datenübermittlung vorbehaltlich geeigneter Garantien") der DSGVO bestimmt in den Abs. 1 bis 3:

„(1) Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in

a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,

b) verbindlichen internen Datenschutzvorschriften gemäß Artikel 47,

c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden,

d) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 genehmigt wurden,

e) genehmigten Verhaltensregeln gemäß Artikel 40 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder

f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

(3) Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können die geeigneten Garantien gemäß Absatz 1 auch insbesondere bestehen in

a) Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, oder

b) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen."

15 Art. 49 („Ausnahmen für bestimmte Fälle") der DSGVO lautet:

„(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

a) [D]ie betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,

b) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,

c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,

d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,

e) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,

f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,

g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 – einschließlich der verbindlichen internen Datenschutzvorschriften – gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht

wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 13 und 14 mitgeteilten Informationen.

(2) Datenübermittlungen gemäß Absatz 1 Unterabsatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

(3) Absatz 1 Unterabsatz 1 Buchstaben a, b und c und … Absatz 1 Unterabsatz 2 gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.

(4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.

(5) Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit.

(6) Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Absatzes 1 Unterabsatz 2 des vorliegenden Artikels in der Dokumentation gemäß Artikel 30.“

16 Art. 51 Abs. 1 der DSGVO bestimmt:

„Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden ‚Aufsichtsbehörde‘).“

17 Gemäß Art. 55 Abs. 1 der DSGVO ist „[j]ede Aufsichtsbehörde … für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig“.

18 Art. 57 Abs. 1 der DSGVO sieht vor:

„Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

a) die Anwendung dieser Verordnung überwachen und durchsetzen;

…

f) sich mit Beschwerden einer betroffenen Person … befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

…“

19 In Art. 58 Abs. 2 und 4 der DSGVO heißt es:

„(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

…

f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,

…

j) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

…

(4) Die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta.“

20 Art. 64 Abs. 2 der DSGVO lautet:

„Jede Aufsichtsbehörde, der Vorsitz des [Europäischen Datenschutzausschusses (EDSA)] oder die Kommission können beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten, insbesondere wenn eine zuständige Aufsichtsbehörde den Verpflichtungen zur Amtshilfe gemäß Artikel 61 oder zu gemeinsamen Maßnahmen gemäß Artikel 62 nicht nachkommt.“

21 In Art. 65 Abs. 1 der DSGVO heißt es:

„Um die ordnungsgemäße und einheitliche Anwendung dieser Verordnung in Einzelfällen sicherzustellen, erlässt der Ausschuss in den folgenden Fällen einen verbindlichen Beschluss:

…

c) wenn eine zuständige Aufsichtsbehörde in den in Artikel 64 Absatz 1 genannten Fällen keine Stellungnahme des Ausschusses einholt oder der Stellungnahme des Ausschusses gemäß Artikel 64 nicht folgt. In diesem Fall kann jede betroffene Aufsichtsbehörde oder die Kommission die Angelegenheit dem Ausschuss vorlegen.“

22 Art. 77 („Recht auf Beschwerde bei einer Aufsichtsbehörde“) der DSGVO lautet:

„(1) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

(2) Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 78.“

23 Art. 78 („Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde“) der DSGVO sieht in den Abs. 1 und 2 vor:

„(1) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

(2) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Recht[s]behelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die nach den Artikeln 55 und 56 zuständige Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 77 erhobenen Beschwerde in Kenntnis gesetzt hat.“

24 Art. 94 der DSGVO bestimmt:

„(1) Die Richtlinie [95/46] wird mit Wirkung vom 25. Mai 2018 aufgehoben.

(2) Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie [95/46] eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.“

25 Art. 99 der DSGVO lautet:

„(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018.“

SDK-Beschluss

26 Der elfte Erwägungsgrund des SDK-Beschlusses lautet:

„Die Kontrollstellen der Mitgliedstaaten spielen eine Schlüsselrolle in diesem Vertragsmechanismus, weil sie sicherstellen, dass personenbezogene Daten nach der Übermittlung angemessen geschützt werden. In Ausnahmefällen, in denen Datenexporteure es ablehnen oder nicht in der Lage sind, dem Datenimporteur angemessene Anweisungen zu geben, und in denen eine hohe Wahrscheinlichkeit besteht, dass den betroffenen Personen ein schwerwiegender Schaden entsteht, sollten die Standardvertragsklauseln es den Kontrollstellen ermöglichen, Datenimporteure und Unterauftragsverarbeiter einer Prüfung zu unterziehen und gegebenenfalls Entscheidungen zu treffen,

denen Datenimporteure und Unterauftragsverarbeiter Folge leisten müssen. Die Kontrollstellen sollten befugt sein, eine Datenübermittlung oder eine Reihe von Datenübermittlungen auf der Grundlage der Standardvertragsklauseln zu untersagen oder zurückzuhalten; dies gilt für jene Ausnahmefälle, für die feststeht, dass sich eine Übermittlung auf Vertragsbasis wahrscheinlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die den betroffenen Personen angemessenen Schutz bieten sollen."

27 Art. 1 des SDK-Beschlusses bestimmt:

„Die Standardvertragsklauseln im Anhang gelten als angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte nach Artikel 26 Absatz 2 der Richtlinie [95/46]."

28 Gemäß Art. 2 Abs. 2 des SDK-Beschlusses „gilt [dieser] für die Übermittlung personenbezogener Daten durch für die Verarbeitung Verantwortliche, die in der Europäischen Union niedergelassen sind, an Empfänger außerhalb der Europäischen Union, die ausschließlich als Auftragsverarbeiter fungieren".

29 In Art. 3 des SDK-Beschlusses heißt es:

„Für die Zwecke dieses Beschlusses gelten die folgenden Begriffsbestimmungen:

…

c) der Begriff ‚Datenexporteur' bezeichnet den für die Verarbeitung Verantwortlichen, der die personenbezogenen Daten übermittelt;

d) der Begriff ‚Datenimporteur' bezeichnet den in einem Drittland niedergelassenen Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur nach dessen Anweisungen und den Vorschriften dieses Beschlusses personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung in dessen Auftrag zu verarbeiten, und der nicht dem System eines Drittlands unterliegt, das ein angemessenes Schutzniveau im Sinne von Artikel 25 Absatz 1 der Richtlinie [95/46] bietet;

…

f) der Begriff ‚anwendbares Datenschutzrecht' bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre im Hinblick auf die Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, für den für die Verarbeitung Verantwortlichen gelten;

…"

30 In seiner ursprünglichen Fassung, die vor dem Inkrafttreten des Durchführungsbeschlusses 2016/2297 galt, sah Art. 4 des SDK-Beschlusses vor:

„(1) Unbeschadet ihrer Befugnisse, tätig zu werden, um die Einhaltung nationaler Vorschriften gemäß den Kapiteln II, III, V und VI der Richtlinie [95/46] zu gewährleisten, können die zuständigen Kontrollstellen in den Mitgliedstaaten ihre Befugnisse ausüben und zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung in Drittländer verbieten oder aussetzen, wenn

a) feststeht, dass der Datenimporteur oder Unterauftragsverarbeiter nach den für ihn geltenden Rechtsvorschriften Anforderungen unterliegt, die ihn zwingen, vom anwendbaren Datenschutzrecht in einem Maß abzuweichen, das über die Beschränkungen hinausgeht, die im

Sinne von Artikel 13 der Richtlinie [95/46] für eine demokratische Gesellschaft erforderlich sind, und dass sich diese Anforderungen wahrscheinlich sehr nachteilig auf die Garantien auswirken würden, die das anwendbare Datenschutzrecht und die Standardvertragsklauseln bieten,

b) eine zuständige Behörde festgestellt hat, dass der Datenimporteur oder ein Unterauftragsverarbeiter die Standardvertragsklauseln im Anhang nicht eingehalten hat, oder

c) eine hohe Wahrscheinlichkeit besteht, dass die im Anhang enthaltenen Standardvertragsklauseln derzeit oder künftig nicht eingehalten werden und die Fortsetzung der Übermittlung den betroffenen Personen einen schwerwiegenden Schaden zufügen könnte.

(2) Das Verbot oder die Aussetzung gemäß Absatz 1 wird aufgehoben, sobald die Gründe für das Verbot oder die Aussetzung nicht mehr vorliegen.

(3) Wenn die Mitgliedstaaten Maßnahmen gemäß den Absätzen 1 und 2 ergreifen, informieren sie unverzüglich die Kommission, die ihrerseits die Informationen an die anderen Mitgliedstaaten weiterleitet."

31 Der fünfte Erwägungsgrund des Durchführungsbeschlusses 2016/2297, der im Anschluss an die Verkündung des Urteils vom 6. Oktober 2015, Schrems (C-362/14, EU:C:2015:650), erlassen wurde, lautet:

„Folglich ist eine gemäß Artikel 26 Absatz 4 der Richtlinie [95/46] angenommene Entscheidung der Kommission für alle Organe der Mitgliedstaaten bindend, an die sie gerichtet ist, einschließlich ihrer unabhängigen Aufsichtsbehörden, insoweit hiermit anerkannt wird, dass die Datenübermittlungen auf der Grundlage der in diesem Artikel genannten Standardvertragsklauseln ausreichende Garantien im Sinne von Artikel 26 Absatz 2 dieser Richtlinie bieten. Dies hindert eine nationale Aufsichtsbehörde jedoch nicht daran, Datenübermittlungen zu kontrollieren und unter anderem eine Übermittlung personenbezogener Daten auszusetzen oder zu verbieten, wenn sie feststellt, dass durch die Übermittlung EU- oder nationale Datenschutzvorschriften verletzt werden, beispielsweise wenn der Datenimporteur die Standardvertragsklauseln missachtet."

32 In seiner aktuellen, aus dem Durchführungsbeschluss 2016/2297 hervorgegangenen Fassung sieht Art. 4 des SDK-Beschlusses vor:

„Wenn die zuständigen Behörden in den Mitgliedstaaten ihre Befugnisse gemäß Artikel 28 Absatz 3 der Richtlinie [95/46] ausüben und die Datenübertragungen an Drittstaaten aussetzen oder endgültig verbieten, um Privatpersonen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten zu schützen, informiert der betreffende Mitgliedstaat unverzüglich die Kommission, die ihrerseits die Informationen an die anderen Mitgliedstaaten weiterleitet."

33 Der Anhang („Standardvertragsklauseln [Auftragsverarbeiter]") des SDK-Beschlusses enthält zwölf Standardklauseln. Klausel 3 („Drittbegünstigtenklausel") des Anhangs sieht vor:

„(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des

Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

…“

34 In Klausel 4 („Pflichten des Datenexporteurs“) dieses Anhangs heißt es:

„Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

…

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder so bald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie [95/46] bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

…“

35 Klausel 5 („Pflichten des Datenimporteurs …“) des Anhangs bestimmt:

„Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

…

d) er den Datenexporteur unverzüglich informiert über

i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;
ii) jeden zufälligen oder unberechtigten Zugang und
iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

…“

36 In der Fußnote zur Überschrift von Klausel 5 heißt es:

„Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie [95/46] aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. …“

37 Klausel 6 („Haftung“) im Anhang des SDK-Beschlusses sieht vor:

„(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht …

…“

38 Klausel 8 („Zusammenarbeit mit Kontrollstellen“) des Anhangs bestimmt in Abs. 2:

„Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.“

39 In Klausel 9 („Anwendbares Recht“) des Anhangs wird klargestellt, dass für die Klauseln das Recht des Mitgliedstaats gilt, in dem der Datenexporteur niedergelassen ist.

40 In Klausel 11 („Vergabe eines Unterauftrags“) des Anhangs heißt es:

„(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs

Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss …

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

…“

41 Klausel 12 („Pflichten nach Beendigung der Datenverarbeitungsdienste“) im Anhang des SDK-Beschlusses bestimmt in Abs. 1:

„Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. …“

DSS-Beschluss

42 Mit Urteil vom 6. Oktober 2015, Schrems (C-362/14, EU:C:2015:650), hat der Gerichtshof die Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46 über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (ABl. 2000, L 215, S. 7), in der die Kommission festgestellt hatte, dass dieses Drittland ein angemessenes Schutzniveau gewährleiste, für ungültig erklärt.

43 Im Anschluss an die Verkündung dieses Urteils erließ die Kommission den DSS-Beschluss, nachdem sie zu diesem Zweck das amerikanische Recht analysiert hatte, wie im 65. Erwägungsgrund dieses Beschlusses dargelegt wird:

„Die Kommission hat die Einschränkungen und Garantien bewertet, die im amerikanischen Recht für im Rahmen des EU-US-Datenschutzschilds übermittelte Daten gelten, welche durch staatliche Einrichtungen der USA aus Gründen der nationalen Sicherheit, der Strafverfolgung oder anderer im öffentlichen Interesse liegender Ziele gesammelt und genutzt werden. Überdies hat die Regierung der USA über das Amt des Director of National Intelligence (ODNI) der Kommission gegenüber detaillierte Erklärungen abgegeben und Zusagen gemacht, die in Anhang VI dieses Beschlusses enthalten sind. In einem Schreiben, das vom Außenminister unterzeichnet wurde und diesem Beschluss als Anhang III beigefügt ist, hat sich die Regierung der USA zudem verpflichtet, eine neue Aufsichtsinstanz für Eingriffe aus Gründen der nationalen Sicherheit ins Leben zu rufen, die Ombudsperson des Datenschutzschilds (Privacy Shield Ombudsperson), die von der Intelligence Community unabhängig ist. Außerdem werden in einer Erklärung des Justizministeriums der USA, die in Anhang VII des vorliegenden Beschlusses enthalten ist, die Einschränkungen und Garantien dargelegt, die für die Sammlung und Nutzung von Daten durch staatliche Stellen für Zwecke der Strafverfolgung und andere im öffentlichen Interesse liegende Ziele gelten. Um für größere

Transparenz zu sorgen und die Rechtsverbindlichkeit dieser Zusagen zu unterstreichen, werden alle aufgeführten und diesem Beschluss beigefügten Schriftstücke im Bundesregister der USA veröffentlicht."

44 Die von der Kommission durchgeführte Analyse bezüglich dieser Einschränkungen und Garantien wird in den Erwägungsgründen 67 bis 135 des DSS-Beschlusses zusammengefasst, während ihre Schlussfolgerungen betreffend den angemessenen Rechtsschutz im Rahmen des EU-US-Datenschutzschilds in den Erwägungsgründen 136 bis 141 dieses Beschlusses dargelegt werden.

45 Im Einzelnen heißt es in den Erwägungsgründen 68, 69, 76, 77, 109, 112 bis 116, 120, 136 und 140 des DSS-Beschlusses:

„(68) Nach der Verfassung der USA fällt die Gewährleistung der nationalen Sicherheit in die Zuständigkeit des Präsidenten als Oberbefehlshaber, Staatsoberhaupt und, soweit die Auslandsaufklärung betroffen ist, Verantwortlicher für die Außenpolitik der USA … Der Kongress ist zwar befugt, ihm Beschränkungen aufzuerlegen, und hat von diesem Recht mehrfach Gebrauch gemacht, doch kann der Präsident innerhalb dieser Grenzen die Aktivitäten der amerikanischen Intelligence Community lenken, insbesondere durch Executive Orders oder Presidential Directives. … Zwei zentrale Rechtsvorschriften dieser Art sind die Executive Order 12333 (‚E.O. 12333') und die Presidential Policy Directive 28.

(69) Die am 17. Januar 2014 erlassene Presidential Policy Directive 28 (‚PPD-28') bringt eine Reihe von Einschränkungen für die ‚Signalaufklärung' mit sich … Diese Verordnung ist für die Nachrichtendienste der USA verbindlich … und bleibt auch bei einem Regierungswechsel in Kraft … Die PPD-28 ist für Personen außerhalb der USA, darunter Betroffene in der EU, von besonderer Bedeutung. …

…

(76) [Die] Prinzipien [der PPD-28] bringen den Wesensinhalt der Grundsätze der Notwendigkeit und der Verhältnismäßigkeit zum Ausdruck, auch wenn diese Begriffe nicht ausdrücklich verwendet werden. …

(77) Da es sich um eine Direktive des Präsidenten in seiner Eigenschaft als Staatsoberhaupt handelt, sind ihre Bestimmungen für die gesamte Intelligence Community verbindlich und inzwischen durch Regeln und Verfahren der Nachrichtendienste weiter ausgestaltet worden, die die allgemeinen Grundsätze in konkrete Anleitungen für die alltägliche Praxis umsetzen. …

…

(109) Hingegen autorisiert [der United States Foreign Intelligence Surveillance Court (FISC) (Gericht für die Überwachung der Auslandsgeheimdienste der Vereinigten Staaten)] nach [Section] 702 des [Foreign Intelligence Surveillance Act (FISA) (Gesetz zur Überwachung in der Auslandsaufklärung)] keine individuellen Überwachungsmaßnahmen; vielmehr genehmigt [er] Überwachungsprogramme (wie PRISM oder UPSTREAM) auf der Grundlage jährlicher Zertifizierungen, die vom [United States Attorney General (Justizminister)] und [vom] Director of National Intelligence vorgenommen werden. … Wie bereits angemerkt, enthalten die vom FISC zu bestätigenden Zertifizierungen keine Informationen über die einzelnen zu überwachenden Personen, sondern beziehen sich auf Kategorien von Auslandsaufklärungsdaten … D[er] FISC beurteilt nicht – anhand eines hinreichenden Verdachts oder sonstigen Kriteriums –, ob die Personen vorschriftsgemäß als Zielpersonen für die Beschaffung von

Auslandsaufklärungsdaten ausgewählt wurden …, sondern überprüft die Einhaltung der Bestimmung, dass ‚ein wesentlicher Zweck der Datenerhebung darin besteht, Auslandsaufklärungsdaten zu erlangen' …

…

(112) Erstens bietet der [FISA] eine Reihe von Rechtsschutzinstrumenten, die auch Nicht-US-Bürger in Anspruch nehmen können, um gegen rechtswidrige elektronische Überwachung … vorzugehen. Beispielsweise haben Privatpersonen die Möglichkeit, eine Zivilklage auf Schadenersatz gegen die Vereinigten Staaten anzustrengen, wenn Informationen, die sie betreffen, gesetzwidrig und vorsätzlich genutzt oder offengelegt wurden[,] US-Regierungsbeamte in persönlicher Eigenschaft (nach dem Grundsatz der Rechtsscheinhaftung) auf Schadenersatz zu verklagen … und die Rechtmäßigkeit der Überwachung anzufechten (und auf die Unterdrückung der Informationen hinzuwirken), sofern die US-Regierung beabsichtigt, in den Vereinigten Staaten direkt oder mittelbar aus der elektronischen Überwachung gewonnene Erkenntnisse in einem Gerichts- oder Verwaltungsverfahren gegen die betroffene Person zu verwenden oder offenzulegen …

(113) Zweitens hat die US-Regierung die Kommission auf eine Reihe zusätzlicher Möglichkeiten hingewiesen, die betroffene Personen in der EU nutzen könnten, um rechtlich gegen Regierungsbeamte wegen des rechtswidrigen Zugangs zu [personenbezogenen Daten] oder der Verarbeitung personenbezogener Daten, auch für vorgebliche Ziele der nationalen Sicherheit, vorzugehen …

(114) Darüber hinaus benannte die US-Regierung den Freedom of Information Act [(FOIA) (Informationsfreiheitsgesetz)] als Mittel, mit dem Nicht-US-Bürger Zugang zu vorhandenen Unterlagen von Bundesbehörden erlangen können, auch zu solchen, die personenbezogene Daten der betreffenden Personen enthalten … Aufgrund seines zentralen Anliegens eröffnet der FOIA einerseits keine Möglichkeit für individuellen Recht[s]schutz gegen Eingriffe in personenbezogene Daten als solche, wobei das Gesetz andererseits vom Grundsatz her Privatpersonen den Zugang zu relevanten Informationen ermöglichen könnte, die sich im Besitz von bundesweit operierenden Nachrichtendiensten befinden. …

(115) Auch wenn Privatpersonen, einschließlich Betroffene[n] in der EU, eine Reihe von Rechtsschutzinstrumenten zur Verfügung steht, wenn sie aus Gründen der nationalen Sicherheit rechtswidrig (elektronisch) überwacht wurden, steht doch fest, dass zumindest einige Rechtsgrundlagen, die US-Nachrichtendienste nutzen können (z. B. [die] E.O. 12333), [davon nicht erfasst werden]. Selbst wenn Nicht-US-Bürger im Prinzip auf gerichtliche Rechtsbehelfe zurückgreifen können, beispielsweise auf der Grundlage des FISA im Falle der Überwachung, sind die verfügbaren Klagemöglichkeiten begrenzt …, denn Klagen von Einzelpersonen (auch US-Bürgern) werden abgewiesen, wenn diese ihre ‚Klagebefugnis' nicht nachweisen können …, was den Zugang zu den ordentlichen Gerichten einschränkt …

(116) Um eine zusätzliche Rechtsschutzmöglichkeit zu schaffen, die allen Betroffenen in der EU offensteht, hat die US-Regierung beschlossen, als neue Einrichtung einen Ombudsmechanismus ins Leben zu rufen, wie er im Schreiben des US-Außenministers an die Kommission beschrieben wird, das Bestandteil von Anhang III zum vorliegenden Beschluss ist. Er basiert auf der gemäß [der] PPD-28 erfolgenden Benennung eines Senior Coordinator [(Hauptkoordinator)] (im Range eines Under-Secretary [Staatssekretärs]) im Außenministerium, der als Ansprechpartner für ausländische Regierungen fungiert, die Bedenken im Zusammenhang mit der US-Signalaufklärung vorbringen, geht aber deutlich darüber hinaus.

…

(120) [D]ie US-Regierung [sichert] zu, dafür zu sorgen, dass sich die Ombudsperson des Datenschutzschilds bei der Erfüllung ihrer Aufgaben auf die Zusammenarbeit mit anderen im amerikanischen Recht vorgesehenen unabhängigen Überwachungs- und Kontrollgremien stützen kann. … Wenn eines der Kontrollgremien Verstöße feststellt, muss die betreffende Einrichtung der Intelligence Community (z. B. ein Nachrichtendienst) die Verstöße abstellen, da die Ombudsperson nur dann in der Lage ist, der betroffenen Person eine ‚positive' Antwort zu geben (in dem Sinne, dass etwaige Verstöße abgestellt worden sind), wozu sich die US-Regierung verpflichtet hat. …

…

(136) Im Licht dieser Feststellungen geht die Kommission davon aus, dass die Vereinigten Staaten einen angemessenen Rechtsschutz für personenbezogene Daten gewährleisten, die im Rahmen des EU-US-Datenschutzschilds aus der Europäischen Union an selbstzertifizierte Organisationen in den Vereinigten Staaten übermittelt werden.

…

(140) Schließlich kommt die Kommission aufgrund der verfügbaren Informationen über die Rechtsordnung der USA, einschließlich der Erklärungen und Zusagen der US-Regierung, zu dem Schluss, dass jegliche Eingriffe in die Grundrechte von Personen, deren Daten im Rahmen des EU-US-Datenschutzschilds aus Gründen der nationalen Sicherheit, der Strafverfolgung oder für andere im öffentlichen Interesse liegende Zwecke aus der Europäischen Union in die Vereinigten Staaten übermittelt werden, sowie die deshalb den selbstzertifizierten Organisationen bei der Einhaltung der Grundsätze auferlegten Beschränkungen auf das für die Erreichung solcher legitimen Ziele absolut notwendige Maß beschränkt werden und dass damit ein wirksamer Rechtsschutz vor derartigen Eingriffen gewährleistet ist."

46 Art. 1 des DSS-Beschlusses lautet:

„(1) Im Sinne von Artikel 25 Absatz 2 der Richtlinie [95/46] gewährleisten die Vereinigten Staaten ein angemessenes Schutzniveau für personenbezogene Daten, die im Rahmen des EU-US-Datenschutzschilds aus der Europäischen Union an Organisationen in den Vereinigten Staaten übermittelt werden.

(2) Der EU-US-Datenschutzschild besteht aus den Grundsätzen, die am 7. Juli 2016 vom US-Handelsministerium herausgegeben wurden und in Anhang II aufgeführt sind, und den offiziellen Erklärungen und Zusagen, die in den Schriftstücken der Anhänge I und III bis VII enthalten sind.

(3) Im Sinne von Absatz 1 werden personenbezogene Daten im Rahmen des EU-US-Datenschutzschilds übermittelt, wenn sie aus der Europäischen Union an US-Organisationen übermittelt werden, die in der ‚Datenschutzschild-Liste' aufgeführt sind, welche in Übereinstimmung mit [den] Abschnitt[en] I und III der Grundsätze in Anhang II vom US-Handelsministerium geführt und der Öffentlichkeit zugänglich gemacht wird."

47 Anhang II („Grundsätze des EU-US-Datenschutzschilds[,] vorgelegt vom amerikanischen Handelsministerium") des DSS-Beschlusses sieht in Abschnitt I.5 vor, dass die Einhaltung dieser Grundsätze begrenzt sein kann, u. a. „insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss".

48 Anhang III des DSS-Beschlusses enthält ein Schreiben von John Kerry, dem damaligen Secretary of State (Außenminister, Vereinigte Staaten), an die Kommissarin für Justiz, Verbraucher und Gleichstellung vom 7. Juli 2016, dem als Anlage A eine mit „Ombudsstelle des EU-U.S.-Datenschutzschilds für die signalerfassende Aufklärung“ überschriebene Absichtserklärung mit folgenden Angaben beigefügt ist:

„In Anerkennung der Bedeutung des EU-U.S.-Datenschutzschilds gibt die vorstehende Absichtserklärung einen Überblick über das Verfahren zur Umsetzung eines neuen Mechanismus für die signalerfassende Aufklärung, der mit der [PPD-28] im Einklang steht.

… Präsident Obama kündigte die Veröffentlichung einer neuen Presidential Directive, der ‚PPD-28‘, an mit ‚klaren Vorschriften dazu, was wir unternehmen und was nicht, wenn es um unsere Auslandsaufklärung geht‘.

In [Section] 4 Buchstabe d der PPD-28 wird der Außenminister beauftragt, einen ‚Senior Coordinator for International Information Technology Diplomacy‘ (Senior Coordinator) zu benennen, ‚der … als Ansprechpartner für ausländische Regierungen fungiert, die Bedenken im Zusammenhang mit der Signalaufklärung der Vereinigten Staaten vorbringen‘.

…

1. … Der Senior Coordinator fungiert als Ombudsperson des Datenschutzschilds und … arbeitet eng mit den jeweiligen Beamten aus anderen Regierungsstellen zusammen, die dem geltendem Recht und der bestehenden Auslegungspraxis der Vereinigten Staaten entsprechend für die Bearbeitung von Anträgen zuständig sind. Die Ombuds[person] untersteht unmittelbar dem Außenminister, der dafür Sorge trägt, dass [sie] ihre Aufgabe objektiv und frei von unzulässiger Einflussnahme erfüllt, die sich auf die zu erteilende Antwort auswirken kann.

…“

49 Anhang VI des DSS-Beschlusses enthält ein Schreiben des Office of the Director of National Intelligence an den amerikanischen Handelsminister sowie an die International Trade Administration vom 21. Juni 2016, in dem es heißt, dass die PPD-28 es ermögliche, eine „‚Sammelerhebung‘ … einer relativ großen Menge von signalerfassenden Aufklärungsdaten unter Bedingungen [durchzuführen], in denen die Intelligence Community keinen mit einer bestimmten Zielperson verbundenen Identifikator … für eine zielgerichtete Erhebung verwenden kann“.

Ausgangsrechtsstreit und Vorlagefragen

50 Herr Schrems, ein in Österreich wohnhafter österreichischer Staatsangehöriger, nutzt seit 2008 das soziale Netzwerk Facebook (im Folgenden: Facebook).

51 Alle im Unionsgebiet wohnhaften Personen, die Facebook nutzen wollen, müssen bei ihrer Anmeldung einen Vertrag mit Facebook Ireland abschließen, einer Tochtergesellschaft der in den Vereinigten Staaten ansässigen Facebook Inc. Die personenbezogenen Daten der im Unionsgebiet wohnhaften Nutzer von Facebook werden ganz oder teilweise an Server der Facebook Inc., die sich in den Vereinigten Staaten befinden, übermittelt und dort verarbeitet.

52 Am 25. Juni 2013 legte Herr Schrems beim Commissioner eine Beschwerde ein, mit der er ihn im Wesentlichen aufforderte, Facebook Ireland die Übermittlung seiner personenbezogenen Daten in die Vereinigten Staaten zu untersagen. Dabei machte er geltend, das Recht und die Praxis der Vereinigten Staaten gewährleisteten keinen ausreichenden Schutz der in diesem Land gespeicherten

personenbezogenen Daten vor den Überwachungstätigkeiten der dortigen Behörden. Die Beschwerde wurde u. a. mit der Begründung zurückgewiesen, die Kommission habe in der Entscheidung 2000/520 festgestellt, dass die Vereinigten Staaten ein angemessenes Schutzniveau gewährleisteten.

53 Der High Court (Hoher Gerichtshof, Irland), vor dem Herr Schrems Klage gegen die Zurückweisung seiner Beschwerde erhoben hatte, befasste den Gerichtshof mit einem Vorabentscheidungsersuchen betreffend die Auslegung und die Gültigkeit der Entscheidung 2000/520. Mit Urteil vom 6. Oktober 2015, Schrems (C-362/14, EU:C:2015:650), erklärte der Gerichtshof diese Entscheidung für ungültig.

54 Im Anschluss an dieses Urteil hob das vorlegende Gericht die Entscheidung, mit der die Beschwerde von Herrn Schrems zurückgewiesen worden war, auf und verwies die Sache an den Commissioner zurück. Im Rahmen der von ihm eingeleiteten Untersuchung erklärte Facebook Ireland, ein großer Teil der personenbezogenen Daten werde auf der Grundlage der im Anhang des SDK-Beschlusses enthaltenen Standarddatenschutzklauseln an die Facebook Inc. übermittelt. Vor diesem Hintergrund forderte der Commissioner Herrn Schrems auf, seine Beschwerde umzuformulieren.

55 Mit seiner dementsprechend umformulierten, am 1. Dezember 2015 eingereichten Beschwerde machte Herr Schrems insbesondere geltend, dass die Facebook Inc. nach amerikanischem Recht verpflichtet sei, die ihr übermittelten personenbezogenen Daten amerikanischen Behörden wie der National Security Agency (NSA) und dem Federal Bureau of Investigation (FBI) zur Verfügung zu stellen. Da diese Daten im Rahmen verschiedener Überwachungsprogramme in einer mit den Art. 7, 8 und 47 der Charta unvereinbaren Weise verwendet würden, könne der SDK-Beschluss ihre Übermittlung in die Vereinigten Staaten nicht rechtfertigen. Herr Schrems forderte den Commissioner daher auf, die Übermittlung seiner personenbezogenen Daten an die Facebook Inc. zu verbieten oder auszusetzen.

56 Am 24. Mai 2016 veröffentlichte der Commissioner einen „Entscheidungsentwurf“, in dem er die vorläufigen Schlussfolgerungen seiner Untersuchung zusammenfasste. Darin äußerte er die vorläufige Auffassung, es sei zu befürchten, dass die amerikanischen Behörden die in die Vereinigten Staaten übermittelten personenbezogenen Daten von Unionsbürgern in einer mit den Art. 7 und 8 der Charta unvereinbaren Weise abfragten und verarbeiteten; insoweit biete das Recht der Vereinigten Staaten den Unionsbürgern keine mit Art. 47 der Charta vereinbaren Rechtsbehelfe. Die Standarddatenschutzklauseln im Anhang des SDK-Beschlusses seien nicht geeignet, diesem Mangel abzuhelfen, da sie den betroffenen Personen nur vertragliche Rechte gegenüber dem Datenexporteur und dem Datenimporteur einräumten, ohne die amerikanischen Behörden zu binden.

57 Der Commissioner war der Auffassung, dass die umformulierte Beschwerde von Herrn Schrems unter diesen Umständen die Frage der Gültigkeit des SDK-Beschlusses aufwerfe, und rief daher am 31. Mai 2016 unter Verweis auf die mit dem Urteil vom 6. Oktober 2015, Schrems (C-362/14, EU:C:2015:650, Rn. 65), begründete Rechtsprechung den High Court (Hoher Gerichtshof) an, damit er den Gerichtshof hierzu befragen möge. Mit Entscheidung vom 4. Mai 2018 befasste der High Court (Hoher Gerichtshof) den Gerichtshof mit dem vorliegenden Vorabentscheidungsersuchen.

58 Der High Court (Hoher Gerichtshof) fügte seinem Vorabentscheidungsersuchen ein Urteil vom 3. Oktober 2017 bei, in dem er das Ergebnis der Würdigung der ihm im nationalen Verfahren – an dem die amerikanische Regierung beteiligt gewesen war – vorgelegten Beweise dargelegt hatte.

59 In diesem Urteil, auf das im Vorabentscheidungsersuchen mehrfach Bezug genommen wird, führte das vorlegende Gericht aus, grundsätzlich sei es nicht nur berechtigt, sondern auch verpflichtet, sämtliche vor ihm geltend gemachten Tatsachen und Argumente zu prüfen, um auf deren Grundlage zu entscheiden, ob eine Vorlage zur Vorabentscheidung erforderlich sei. Jedenfalls müsse es etwaige Rechtsänderungen berücksichtigen, die zwischen der Klageerhebung und der von ihm anberaumten mündlichen Verhandlung eingetreten seien. Im Ausgangsverfahren sei seine eigene Beurteilung nicht

auf die vom Commissioner geltend gemachten Ungültigkeitsgründe beschränkt, so dass es auch von Amts wegen weitere Ungültigkeitsgründe aufwerfen und auf deren Grundlage ein Vorabentscheidungsersuchen einreichen könne.

60 Nach den Feststellungen in diesem Urteil stützen sich die nachrichtendienstlichen Tätigkeiten der amerikanischen Behörden, was die in die Vereinigten Staaten übermittelten personenbezogenen Daten anbelangt, namentlich auf Section 702 des FISA und die E.O. 12333.

61 Zu Section 702 des FISA führt das vorlegende Gericht in diesem Urteil aus, der Justizminister und der Direktor der nationalen Nachrichtendienste könnten gemäß dieser Vorschrift nach Billigung durch den FISC gemeinsam zur Beschaffung von „Informationen im Bereich der Auslandsaufklärung“ die Überwachung von Personen genehmigen, die keine amerikanischen Staatsbürger seien (im Folgenden: Nicht-US-Personen) und sich außerhalb des Hoheitsgebiets der Vereinigten Staaten aufhielten. Insbesondere diene die Vorschrift als Grundlage für die Überwachungsprogramme PRISM und UPSTREAM. Im Rahmen des PRISM-Programms seien die Anbieter von Internetdiensten verpflichtet, der NSA die gesamte Kommunikation vorzulegen, die von einem „Selektor“ versandt oder empfangen worden sei. Ein Teil davon werde auch dem FBI und der Central Intelligence Agency (CIA) (Zentraler Nachrichtendienst) übermittelt.

62 Im Rahmen des UPSTREAM-Programms seien die Telekommunikationsunternehmen, die das „backbone“ (Rückgrat) des Internets – d. h. das Netz von Kabeln, Switches und Routern – betrieben, verpflichtet, der NSA zu gestatten, die Internetverkehrsflüsse zu kopieren und zu filtern, um Zugang zu der Kommunikation zu erlangen, die von einer von einem „Selektor“ erfassten Nicht-US-Person versandt oder von ihr empfangen worden sei oder sie betreffe. Im Rahmen dieses Programms habe die NSA Zugriff sowohl auf die Metadaten als auch auf den Inhalt der betreffenden Kommunikation.

63 Die E.O. 12333 erlaube der NSA den Zugang zu Daten, die „auf dem Weg“ in die Vereinigten Staaten seien, mittels Zugriff auf die am Grund des Atlantiks verlegten Seekabel, sowie die Sammlung und Speicherung dieser Daten, bevor sie in den Vereinigten Staaten ankämen und dort den Bestimmungen des FISA unterlägen. Die auf die E.O. 12333 gestützten Tätigkeiten seien nicht gesetzlich geregelt.

64 Hinsichtlich der für nachrichtendienstliche Tätigkeiten eingeführten Beschränkungen sei hervorzuheben, dass Nicht-US-Personen nur von der PPD-28 erfasst würden, in der es lediglich heiße, dass nachrichtendienstliche Tätigkeiten „as tailored as feasible“ (so gezielt wie möglich) sein müssten. Auf der Grundlage dieser Feststellungen sei davon auszugehen, dass die Vereinigten Staaten eine massenhafte Datenverarbeitung durchführten, ohne einen Schutz zu gewährleisten, der dem durch die Art. 7 und 8 der Charta garantierten Schutz der Sache nach gleichwertig sei.

65 Was den gerichtlichen Rechtsschutz anbelange, verfügten Unionsbürger nicht über dieselben Rechtsbehelfe wie amerikanische Staatsbürger, um sich gegen die Verarbeitung personenbezogener Daten durch amerikanische Behörden zu wehren, da der Vierte Zusatzartikel zur Constitution of the United States (Verfassung der Vereinigten Staaten), der im amerikanischen Recht den wichtigsten Schutz vor illegaler Überwachung darstelle, nicht für Unionsbürger gelte. Den übrigen Rechtsbehelfen, über die sie verfügten, stünden erhebliche Hindernisse entgegen, insbesondere die übermäßig schwer zu erfüllende Obliegenheit, ihre Klagebefugnis nachzuweisen. Zudem unterlägen die auf die E.O. 12333 gestützten Tätigkeiten der NSA keiner gerichtlichen Überwachung und könnten nicht Gegenstand eines gerichtlichen Rechtsbehelfs sein. Schließlich sei, da die Ombudsperson des Datenschutzschilds kein Gericht im Sinne von Art. 47 der Charta sei, davon auszugehen, dass das amerikanische Recht den Unionsbürgern kein Schutzniveau gewährleiste, das dem Niveau, das durch das in diesem Artikel niedergelegte Grundrecht garantiert werde, der Sache nach gleichwertig sei.

66 In seinem Vorabentscheidungsersuchen weist das vorlegende Gericht außerdem darauf hin, dass sich die Parteien des Ausgangsverfahrens insbesondere darüber uneins seien, ob das Unionsrecht auf die Übermittlung personenbezogener Daten in ein Drittland, die von den Behörden dieses Drittlands u. a.

für Zwecke der nationalen Sicherheit verarbeitet werden könnten, überhaupt anwendbar sei und welche Gesichtspunkte zu berücksichtigen seien, um zu beurteilen, ob das Schutzniveau in diesem Land angemessen sei. Insbesondere sei Facebook Ireland der Auffassung, dass die Feststellungen der Kommission bezüglich der Angemessenheit des von einem Drittland gewährleisteten Schutzniveaus, wie sie im DSS-Beschluss getroffen würden, für die Aufsichtsbehörden auch im Zusammenhang mit einer Übermittlung personenbezogener Daten auf der Grundlage der Standarddatenschutzklauseln im Anhang des SDK-Beschlusses bindend seien.

67 Hinsichtlich dieser Standarddatenschutzklauseln wirft das vorlegende Gericht die Frage auf, ob der SDK-Beschluss als gültig angesehen werden könne, obwohl die Klauseln die staatlichen Behörden des betreffenden Drittlands nicht bänden und daher nicht geeignet seien, dem etwaigen Fehlen eines angemessenen Schutzniveaus in diesem Land abzuhelfen. Die den zuständigen Behörden der Mitgliedstaaten durch Art. 4 Abs. 1 Buchst. a des Beschlusses 2010/87 in seiner Fassung vor dem Inkrafttreten des Durchführungsbeschlusses 2016/2297 zuerkannte Möglichkeit des Verbots von Übermittlungen personenbezogener Daten in ein Drittland, das dem Datenimporteur Pflichten auferlege, die mit den in den Schutzklauseln enthaltenen Garantien unvereinbar seien, zeige, dass die Rechtslage im Drittland das Verbot einer Datenübermittlung rechtfertigen könne, selbst wenn sie auf der Grundlage der Standarddatenschutzklauseln im Anhang des SDK-Beschlusses erfolge, und mache somit deutlich, dass diese Klauseln unzureichend sein könnten, um einen angemessenen Schutz zu gewährleisten. Indessen sei fraglich, wie weit die Befugnis des Commissioner reiche, eine auf diese Klauseln gestützte Datenübermittlung zu verbieten. Insoweit könne eine Ermessensbefugnis nicht genügen, um angemessenen Schutz zu gewährleisten.

68 Unter diesen Umständen hat der High Court (Hoher Gerichtshof) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Findet in dem Fall, dass personenbezogene Daten aufgrund des SDK-Beschlusses von einem privaten Unternehmen aus einem Mitgliedstaat der Union zu einem gewerblichen Zweck an ein privates Unternehmen in einem Drittland übermittelt und in dem Drittland durch dessen Behörden für Zwecke der nationalen Sicherheit, aber auch der Durchführung von Gesetzen und der Außenpolitik des Drittlands weiter verarbeitet werden können, das Unionsrecht (einschließlich der Charta) ungeachtet der Bestimmungen des Art. 4 Abs. 2 EUV über die nationale Sicherheit und der Bestimmungen des Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 über die öffentliche Sicherheit, die Landesverteidigung und die Sicherheit des Staates auf die Übermittlung der Daten Anwendung?

2. a) Sind bei der Beurteilung des Vorliegens einer Verletzung der Rechte einer natürlichen Person durch die Übermittlung von Daten aus der Union in ein Drittland, die aufgrund des SDK-Beschlusses erfolgt, soweit diese für Zwecke der nationalen Sicherheit weiterverarbeitet werden können, der relevante Vergleichsmaßstab im Sinne der Richtlinie 95/46
   i) die Charta, der EU-Vertrag, der AEU-Vertrag, die Richtlinie 95/46, die am 4. November 1950 in Rom unterzeichnete Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (oder eine sonstige Bestimmung des Unionsrechts) oder
   ii) die nationalen Rechtsvorschriften eines oder mehrerer Mitgliedstaaten?
   b) Falls der relevante Vergleichsmaßstab derjenige nach Ziff. ii ist, ist in diesen auch die im Kontext der nationalen Sicherheit in einem oder mehreren Mitgliedstaaten bestehende Praxis einzubeziehen?

3. Richtet sich die Beurteilung, ob ein Drittland das nach dem Unionsrecht erforderliche Schutzniveau für in dieses Land übermittelte personenbezogene Daten im Sinne von Art. 26 der Richtlinie 95/46 gewährleistet,

a) nach den geltenden Rechtsnormen in dem Drittland, die sich aus seinen innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen ergeben, und der Praxis im Hinblick darauf, wie die Einhaltung dieser Normen sichergestellt werden soll, einschließlich der in dem Drittland geltenden Standesregeln und Sicherheitsmaßnahmen,

oder

b) nach den in Buchst. a genannten Rechtsnormen ebenso wie der Praxis der Verwaltung, Regulierung und Einhaltung von Normen sowie Schutzmaßnahmen, Verfahren, Vorgehensweisen, Kontrollmechanismen und außergerichtlichen Rechtsbehelfen, die in dem Drittland bestehen?

4. Verletzt angesichts der vom High Court (Hoher Gerichtshof) in Bezug auf das Recht der Vereinigten Staaten getroffenen Feststellungen eine Übermittlung personenbezogener Daten aus der Union in die Vereinigten Staaten, die aufgrund des SDK-Beschlusses erfolgt, die Rechte von natürlichen Personen nach Art. 7 und/oder 8 der Charta?

5. Wird angesichts der vom High Court (Hoher Gerichtshof) in Bezug auf das Recht der Vereinigten Staaten getroffenen Feststellungen bei einer Übermittlung personenbezogener Daten aus der Union in die Vereinigten Staaten, die aufgrund des SDK-Beschlusses erfolgt,
   a) durch das von den Vereinigten Staaten gewährte Schutzniveau der Wesensgehalt des durch Art. 47 der Charta garantierten Rechts einer natürlichen Person auf einen gerichtlichen Rechtsbehelf wegen einer Verletzung ihrer Datenschutzrechte geachtet?

   Falls Frage 5 a) bejaht wird:
   b) Sind die Einschränkungen, denen das Recht einer natürlichen Person auf einen gerichtlichen Rechtsbehelf nach dem Recht der Vereinigten Staaten im Kontext der nationalen Sicherheit der Vereinigten Staaten unterliegt, im Sinne von Art. 52 der Charta verhältnismäßig, und gehen sie nicht über das in einer demokratischen Gesellschaft für Zwecke der nationalen Sicherheit erforderliche Maß hinaus?

6. a) Welches Schutzniveau muss personenbezogenen Daten bei einer Übermittlung in ein Drittland, die aufgrund von Standardvertragsklauseln erfolgt, die im Einklang mit einer Feststellung der Kommission nach Art. 26 Abs. 4 der Richtlinie 95/46 angewendet werden, nach den Bestimmungen dieser Richtlinie, insbesondere ihren Art. 25 und 26 in Verbindung mit der Charta, gewährt werden?
   b) Welche Gesichtspunkte sind bei der Beurteilung zu berücksichtigen, ob das Schutzniveau, das Daten bei einer Übermittlung in ein Drittland, die aufgrund des SDK-Beschlusses erfolgt, gewährt wird, den Anforderungen der Richtlinie und der Charta entspricht?

7. Führt der Umstand, dass die Standardvertragsklauseln im Verhältnis zwischen Datenexporteur und Datenimporteur gelten und keine Bindungswirkung für nationale Behörden eines Drittlands haben, die den Datenimporteur verpflichten können, die personenbezogenen Daten, die aufgrund der im SDK-Beschluss genannten Klauseln übermittelt werden, ihren Sicherheitsbehörden zur weiteren Verarbeitung zugänglich zu machen, dazu, dass die Klauseln keine ausreichenden Garantien im Sinne von Art. 26 Abs. 2 der Richtlinie 95/46 bieten?

8. Ist eine Datenschutzbehörde in dem Fall, dass ein Datenimporteur eines Drittlands Überwachungsgesetzen unterliegt, die nach Ansicht einer Datenschutzbehörde mit den Klauseln im Anhang des SDK-Beschlusses oder den Art. 25 oder 26 der Richtlinie 95/46 und/oder der Charta unvereinbar sind, verpflichtet, von ihren Durchsetzungsbefugnissen nach Art. 28 Abs. 3 der Richtlinie 95/46 Gebrauch zu machen, um Datenübermittlungen auszusetzen, oder ist die Ausübung dieser Befugnisse im Licht des elften Erwägungsgrundes des SDK-Beschlusses lediglich auf Ausnahmefälle begrenzt, oder kann eine Datenschutzbehörde ihr Ermessen dahin ausüben, von einer Aussetzung von Datenübermittlungen abzusehen?

9. a) Stellt der DSS-Beschluss im Sinne von Art. 25 Abs. 6 der Richtlinie 95/46 eine allgemeingültige Feststellung dar, die für die Datenschutzbehörden und Gerichte der Mitgliedstaaten dahin gehend verbindlich ist, dass die Vereinigten Staaten aufgrund ihrer innerstaatlichen Rechtsvorschriften oder der von ihnen eingegangenen internationalen Verpflichtungen ein angemessenes Schutzniveau im Sinne von Art. 25 Abs. 2 der Richtlinie gewährleisten?
   b) Wenn dies nicht der Fall ist, welche Bedeutung kommt gegebenenfalls dem DSS-Beschluss bei der Beurteilung der Angemessenheit der Garantien zu, die für Daten bei einer Übermittlung in die Vereinigten Staaten, die aufgrund des SDK-Beschlusses erfolgt, gewährt werden?

10. Wird angesichts der Feststellungen des High Court (Hoher Gerichtshof) in Bezug auf das Recht der Vereinigten Staaten durch die Einrichtung der „Datenschutzschild"-Ombudsstelle nach Anlage A von Anhang III des DSS-Beschlusses in Verbindung mit der in den Vereinigten Staaten bestehenden Regelung gewährleistet, dass die Vereinigten Staaten betroffenen Personen, deren personenbezogene Daten aufgrund des SDK-Beschlusses in die Vereinigten Staaten übermittelt werden, einen Rechtsbehelf bieten, der mit Art. 47 der Charta im Einklang steht?

11. Verstößt der SDK-Beschluss gegen Art. 7, 8 und/oder 47 der Charta?

Zur Zulässigkeit des Vorabentscheidungsersuchens

69 Facebook Ireland, die deutsche Regierung und die Regierung des Vereinigten Königreichs machen geltend, das Vorabentscheidungsersuchen sei unzulässig.

70 Facebook Ireland führt zu ihrer Einrede aus, die Bestimmungen der Richtlinie 95/46, auf die sich die Vorlagefragen bezögen, seien durch die DSGVO aufgehoben worden.

71 Insoweit trifft es zwar zu, dass die Richtlinie 95/46 durch Art. 94 Abs. 1 der DSGVO mit Wirkung vom 25. Mai 2018 aufgehoben wurde, doch war sie noch in Kraft, als das am 9. Mai 2018 beim Gerichtshof eingegangene Vorabentscheidungsersuchen am 4. Mai 2018 formuliert wurde. Zudem wurden Art. 3 Abs. 2 erster Gedankenstrich, die Art. 25 und 26 sowie Art. 28 Abs. 3 der Richtlinie 95/46, auf die sich die Vorlagefragen beziehen, im Wesentlichen in Art. 2 Abs. 2 sowie in den Art. 45, 46 und 58 der DSGVO übernommen. Im Übrigen ist es die Aufgabe des Gerichtshofs, alle Bestimmungen des Unionsrechts auszulegen, die die nationalen Gerichte benötigen, um die bei ihnen anhängigen Rechtsstreitigkeiten zu entscheiden, auch wenn diese Bestimmungen in den dem Gerichtshof von diesen Gerichten vorgelegten Fragen nicht ausdrücklich genannt sind (Urteil vom 2. April 2020, Ruska Federacija, C-897/19 PPU, EU:C:2020:262, Rn. 43 und die dort angeführte Rechtsprechung). Aus diesen verschiedenen Gründen kann der Umstand, dass das vorlegende Gericht die Vorlagefragen nur unter Bezugnahme auf die Bestimmungen der Richtlinie 95/46 formuliert hat, nicht zur Unzulässigkeit seines Vorabentscheidungsersuchens führen.

72 Die deutsche Regierung führt zur Begründung ihrer Unzulässigkeitseinrede aus, zum einen habe der Commissioner hinsichtlich der Frage der Gültigkeit des SDK-Beschlusses nur Zweifel und keine abschließende Meinung geäußert, und zum anderen habe das vorlegende Gericht nicht geprüft, ob Herr Schrems ohne jeden Zweifel in die Übermittlung der fraglichen Daten eingewilligt habe, was die Beantwortung dieser Frage entbehrlich machen würde. Schließlich vertritt die Regierung des Vereinigten Königreichs die Auffassung, die Vorlagefragen seien hypothetischer Natur, da das vorlegende Gericht nicht festgestellt habe, dass die fraglichen Daten tatsächlich auf der Grundlage des SDK-Beschlusses übermittelt worden seien.

73 Nach ständiger Rechtsprechung des Gerichtshofs ist es allein Sache des nationalen Gerichts, das mit dem Rechtsstreit befasst ist und in dessen Verantwortungsbereich die zu erlassende Entscheidung fällt, anhand der Besonderheiten der Rechtssache sowohl die Erforderlichkeit einer Vorabentscheidung für

den Erlass seines Urteils als auch die Erheblichkeit der Fragen zu beurteilen, die es dem Gerichtshof vorlegt. Daher ist der Gerichtshof grundsätzlich gehalten, über ihm vorgelegte Fragen zu befinden, wenn sie die Auslegung oder die Gültigkeit einer Vorschrift des Unionsrechts betreffen. Folglich gilt für Fragen nationaler Gerichte eine Vermutung der Entscheidungserheblichkeit. Der Gerichtshof kann die Beantwortung einer Vorlagefrage eines nationalen Gerichts nur ablehnen, wenn die erbetene Auslegung ersichtlich in keinem Zusammenhang mit der Realität oder dem Gegenstand des Ausgangsrechtsstreits steht, wenn das Problem hypothetischer Natur ist oder wenn der Gerichtshof nicht über die tatsächlichen und rechtlichen Angaben verfügt, die für eine zweckdienliche Beantwortung der ihm vorgelegten Fragen erforderlich sind (Urteile vom 16. Juni 2015, Gauweiler u. a., C-62/14, EU:C:2015:400, Rn. 24 und 25, vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 45, sowie vom 19. Dezember 2019, Dobersberger, C-16/18, EU:C:2019:1110, Rn. 18 und 19).

74 Im vorliegenden Fall enthält das Vorabentscheidungsersuchen genügend tatsächliche und rechtliche Angaben, um die Tragweite der Vorlagefragen zu verstehen. Zudem und vor allem enthalten die dem Gerichtshof vorliegenden Akten keinen Anhaltspunkt dafür, dass die begehrte Auslegung des Unionsrechts in keinem Zusammenhang mit der Realität oder dem Gegenstand des Ausgangsrechtsstreits stünde oder hypothetischer Natur wäre, etwa weil die Übermittlung der fraglichen personenbezogenen Daten auf die ausdrückliche Einwilligung des Betroffenen und nicht auf den SDK-Beschluss gestützt wäre. Nach den Angaben im Vorabentscheidungsersuchen hat Facebook Ireland nämlich eingeräumt, dass sie die personenbezogenen Daten ihrer in der Union wohnhaften Nutzer an die Facebook Inc. übermittle und dass ein großer Teil dieser Transfers – deren Zulässigkeit Herr Schrems in Abrede stellt – auf der Grundlage der Standarddatenschutzklauseln im Anhang des SDK-Beschlusses erfolge.

75 Im Übrigen ist es für die Zulässigkeit des Vorabentscheidungsersuchens unerheblich, dass sich der Commissioner nicht abschließend zur Gültigkeit des SDK-Beschlusses geäußert hat, da das vorlegende Gericht der Auffassung ist, dass die Beantwortung der – die Auslegung und die Gültigkeit unionsrechtlicher Bestimmungen betreffenden – Vorlagefragen für die Entscheidung des Ausgangsrechtsstreits erforderlich sei.

76 Folglich ist das Vorabentscheidungsersuchen zulässig.

Zu den Vorlagefragen

77 Einleitend ist darauf hinzuweisen, dass das Vorabentscheidungsersuchen auf eine Beschwerde von Herrn Schrems zurückgeht, die auf eine Anordnung des Commissioner abzielt, mit der die Übermittlung seiner personenbezogenen Daten durch Facebook Ireland an die Facebook Inc. für die Zukunft ausgesetzt oder verboten wird. Auch wenn sich die Vorlagefragen auf die Bestimmungen der Richtlinie 95/46 beziehen, steht aber fest, dass der Commissioner die Beschwerde noch nicht endgültig beschieden hatte, als diese Richtlinie mit Wirkung vom 25. Mai 2018 durch die DSGVO aufgehoben und ersetzt wurde.

78 Aufgrund dieses Fehlens einer nationalen Entscheidung unterscheidet sich das Ausgangsverfahren von den Sachverhalten, die den Urteilen vom 24. September 2019, Google (Räumliche Reichweite der Auslistung) (C-507/17, EU:C:2019:772), und vom 1. Oktober 2019, Planet49 (C-673/17, EU:C:2019:801), zugrunde lagen, in denen es um Entscheidungen ging, die vor der Aufhebung der Richtlinie 95/46 ergangen waren.

79 Daher sind die Vorlagefragen anhand der Bestimmungen der DSGVO und nicht der Richtlinie 95/46 zu beantworten.

Zur ersten Frage

80 Mit seiner ersten Frage möchte das vorlegende Gericht wissen, ob Art. 2 Abs. 1 und Art. 2 Abs. 2 Buchst. a, b und d der DSGVO in Verbindung mit Art. 4 Abs. 2 EUV dahin auszulegen sind, dass eine Übermittlung personenbezogener Daten durch einen in einem Mitgliedstaat ansässigen Wirtschaftsteilnehmer an einen anderen, in einem Drittland ansässigen Wirtschaftsteilnehmer in den Anwendungsbereich dieser Verordnung fällt, wenn die Daten bei ihrer Übermittlung oder im Anschluss daran von den Behörden dieses Drittlands für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates verarbeitet werden können.

81 Hierzu ist zunächst festzustellen, dass die in Art. 4 Abs. 2 EUV enthaltene Bestimmung, wonach innerhalb der Union die nationale Sicherheit in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt, ausschließlich die Mitgliedstaaten der Union betrifft. Folglich ist diese Bestimmung im vorliegenden Fall für die Auslegung von Art. 2 Abs. 1 und Art. 2 Abs. 2 Buchst. a, b und d der DSGVO nicht maßgeblich.

82 Gemäß ihrem Art. 2 Abs. 1 gilt die DSGVO für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Nach Art. 4 Nr. 2 dieser Verordnung bezeichnet der Ausdruck „Verarbeitung“ „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“. Hierfür wird beispielhaft „die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung“ angeführt, ohne Unterscheidung danach, ob diese Vorgänge innerhalb der Union stattfinden oder eine Verknüpfung mit einem Drittland aufweisen. Darüber hinaus unterwirft die DSGVO die Übermittlung personenbezogener Daten in Drittländer bestimmten Regeln, die in ihrem Kapitel V („Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen“) festgelegt werden, und weist den Aufsichtsbehörden in dieser Hinsicht spezifische, in ihrem Art. 58 Abs. 2 Buchst. j genannte Befugnisse zu.

83 Folglich stellt die Übermittlung personenbezogener Daten aus einem Mitgliedstaat in ein Drittland als solche eine Verarbeitung personenbezogener Daten im Sinne von Art. 4 Nr. 2 der DSGVO dar, die im Hoheitsgebiet eines Mitgliedstaats vorgenommen wird. Auf eine derartige Verarbeitung findet die DSGVO gemäß ihrem Art. 2 Abs. 1 Anwendung (vgl. entsprechend, zu Art. 2 Buchst. b und Art. 3 Abs. 1 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 45 und die dort angeführte Rechtsprechung).

84 Was die Frage anbelangt, ob ein solcher Vorgang gemäß Art. 2 Abs. 2 der DSGVO als vom Anwendungsbereich dieser Verordnung ausgenommen angesehen werden kann, ist darauf hinzuweisen, dass diese Vorschrift Ausnahmen vom Anwendungsbereich der Verordnung – wie in deren Art. 2 Abs. 1 definiert – vorsieht, die eng auszulegen sind (vgl. entsprechend, zu Art. 3 Abs. 2 der Richtlinie 95/46, Urteil vom 10. Juli 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, Rn. 37 und die dort angeführte Rechtsprechung).

85 Im vorliegenden Fall fällt die fragliche Übermittlung personenbezogener Daten, da sie von Facebook Ireland an die Facebook Inc., d. h. zwischen zwei juristischen Personen, erfolgt, nicht unter Art. 2 Abs. 2 Buchst. c der DSGVO, der die Datenverarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten betrifft. Sie fällt auch nicht unter die in Art. 2 Abs. 2 Buchst. a, b und d der DSGVO genannten Ausnahmen, da die Tätigkeiten, die in dieser Vorschrift beispielhaft aufgeführt sind, allesamt spezifische Tätigkeiten des Staates oder staatlicher Stellen sind, die mit den Tätigkeitsbereichen von Privatpersonen nichts zu tun haben (vgl. entsprechend, zu Art. 3 Abs. 2 der Richtlinie 95/46, Urteil vom 10. Juli 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, Rn. 38 und die dort angeführte Rechtsprechung).

86 Indes kann die Möglichkeit, dass personenbezogene Daten, die zwischen zwei Wirtschaftsteilnehmern zu gewerblichen Zwecken übermittelt werden, bei ihrer Übermittlung oder im Anschluss daran von den Behörden des betreffenden Drittlands für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates verarbeitet werden, nicht dazu führen, dass ihre Übermittlung vom Anwendungsbereich der DSGVO ausgenommen wäre.

87 Im Übrigen wird schon aus dem Wortlaut von Art. 45 Abs. 2 Buchst. a der DSGVO deutlich, dass die etwaige Verarbeitung der betreffenden Daten durch ein Drittland für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates die Anwendbarkeit der DSGVO auf die fragliche Übermittlung nicht in Frage stellt. Diese Vorschrift verpflichtet die Kommission nämlich ausdrücklich dazu, bei der Prüfung der Angemessenheit des von einem Drittland gebotenen Schutzniveaus u. a. „die … einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art – auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten – sowie die Anwendung dieser Rechtsvorschriften“ zu berücksichtigen.

88 Demnach kann eine solche Übermittlung dem Anwendungsbereich der DSGVO nicht deshalb entzogen sein, weil die fraglichen Daten bei ihrer Übermittlung oder im Anschluss daran von den Behörden des betreffenden Drittlands für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates verarbeitet werden können.

89 Folglich ist auf die erste Frage zu antworten, dass Art. 2 Abs. 1 und 2 der DSGVO dahin auszulegen ist, dass eine zu gewerblichen Zwecken erfolgende Übermittlung personenbezogener Daten durch einen in einem Mitgliedstaat ansässigen Wirtschaftsteilnehmer an einen anderen, in einem Drittland ansässigen Wirtschaftsteilnehmer in den Anwendungsbereich dieser Verordnung fällt, ungeachtet dessen, ob die Daten bei ihrer Übermittlung oder im Anschluss daran von den Behörden des betreffenden Drittlands für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates verarbeitet werden können.

Zu den Fragen 2, 3 und 6

90 Mit seinen Fragen 2, 3 und 6 möchte das vorlegende Gericht wissen, welches Schutzniveau durch Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der DSGVO verlangt wird, wenn personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden. Insbesondere ersucht das vorlegende Gericht den Gerichtshof um nähere Angaben dazu, welche Gesichtspunkte zu berücksichtigen sind, um festzustellen, ob dieses Schutzniveau im Rahmen einer solchen Datenübermittlung gewährleistet wird.

91 In Bezug auf das erforderliche Schutzniveau ergibt sich aus einer Gesamtbetrachtung der genannten Vorschriften, dass ein Verantwortlicher oder ein Auftragsverarbeiter, falls kein gemäß Art. 45 Abs. 3 der DSGVO ergangener Angemessenheitsbeschluss vorliegt, personenbezogene Daten nur dann in ein Drittland übermitteln darf, wenn er „geeignete Garantien“ vorgesehen hat und den betroffenen Personen „durchsetzbare Rechte und wirksame Rechtsbehelfe“ zur Verfügung stehen, wobei die geeigneten Garantien u. a. in von der Kommission erlassenen Standarddatenschutzklauseln bestehen können.

92 Art. 46 der DSGVO präzisiert zwar nicht die Art der Anforderungen, die sich aus dieser Bezugnahme auf „geeignete Garantien“, „durchsetzbare Rechte“ und „wirksame Rechtsbehelfe“ ergeben. Dazu ist jedoch festzustellen, dass dieser Artikel zu Kapitel V der Verordnung gehört und daher im Licht ihres Art. 44 („Allgemeine Grundsätze der Datenübermittlung“) zu sehen ist, wonach „[a]lle Bestimmungen dieses Kapitels … anzuwenden [sind], um sicherzustellen, dass das durch diese Verordnung

gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird“. Dieses Schutzniveau muss folglich gewährleistet werden, unabhängig davon, aufgrund welcher Bestimmung dieses Kapitels eine Übermittlung personenbezogener Daten in ein Drittland erfolgt.

93 Wie der Generalanwalt in Nr. 117 seiner Schlussanträge ausgeführt hat, sollen die Bestimmungen in Kapitel V der DSGVO nämlich – im Einklang mit dem in ihrem sechsten Erwägungsgrund genannten Ziel – den Fortbestand des hohen Schutzniveaus bei der Übermittlung personenbezogener Daten in ein Drittland gewährleisten.

94 Art. 45 Abs. 1 Satz 1 der DSGVO sieht vor, dass eine Übermittlung personenbezogener Daten in ein Drittland aufgrund eines Beschlusses der Kommission zulässig sein kann, dem zufolge dieses Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Land ein angemessenes Schutzniveau bieten. Auch wenn der Ausdruck „angemessenes Schutzniveau“ nicht bedeutet, dass das betreffende Drittland ein Schutzniveau gewährleisten müsste, das mit dem in der Unionsrechtsordnung garantierten Niveau identisch ist, ist er, wie der 104. Erwägungsgrund der DSGVO bestätigt, so zu verstehen, dass verlangt wird, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder seiner internationalen Verpflichtungen tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet, das dem in der Union durch die DSGVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist. Ohne ein solches Erfordernis würde nämlich das in der vorstehenden Randnummer erwähnte Ziel missachtet (vgl. entsprechend, zu Art. 25 Abs. 6 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 73).

95 In diesem Zusammenhang besagt der 107. Erwägungsgrund der DSGVO, dass, wenn „ein Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands … kein angemessenes Datenschutzniveau mehr bietet …, [d]ie Übermittlung personenbezogener Daten an dieses Drittland … verboten werden [sollte], es sei denn, die Anforderungen dieser Verordnung in Bezug auf die Datenübermittlung vorbehaltlich geeigneter Garantien … werden erfüllt“. Hierzu wird im 108. Erwägungsgrund der DSGVO näher ausgeführt, dass, wenn kein Angemessenheitsbeschluss vorliegt, die geeigneten Garantien, die der Verantwortliche oder der Auftragsverarbeiter gemäß Art. 46 Abs. 1 der DSGVO vorsehen muss, einen „Ausgleich für den [im] Drittland bestehenden Mangel an Datenschutz“ bewirken müssen, um „sicher[zu]stellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden“.

96 Demnach müssen, wie der Generalanwalt in Nr. 115 seiner Schlussanträge ausgeführt hat, die geeigneten Garantien so beschaffen sein, dass sie für Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden – wie im Rahmen einer auf einen Angemessenheitsbeschluss gestützten Übermittlung –, ein Schutzniveau gewährleisten, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist.

97 Das vorlegende Gericht hat außerdem Zweifel daran, ob dieses Schutzniveau, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist, anhand des Unionsrechts, insbesondere der durch die Charta garantierten Rechte, und/oder anhand der in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (im Folgenden: EMRK) verankerten Grundrechte oder anhand des nationalen Rechts der Mitgliedstaaten zu bestimmen ist.

98 Hierzu ist darauf hinzuweisen, dass die in der EMRK niedergelegten Grundrechte zwar, wie Art. 6 Abs. 3 EUV bestätigt, als allgemeine Grundsätze Teil des Unionsrechts sind und dass nach Art. 52 Abs. 3 der Charta die in ihr enthaltenen Rechte, die den durch die EMRK garantierten Rechten entsprechen, die gleiche Bedeutung und Tragweite haben, wie sie ihnen in der EMRK verliehen werden; die EMRK stellt jedoch, solange die Union ihr nicht beigetreten ist, kein Rechtsinstrument

dar, das formell in die Unionsrechtsordnung übernommen wurde (Urteile vom 26. Februar 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, Rn. 44 und die dort angeführte Rechtsprechung, sowie vom 20. März 2018, Menci, C-524/15, EU:C:2018:197, Rn. 22).

99 Unter diesen Umständen hat der Gerichtshof entschieden, dass die Auslegung des Unionsrechts und die Prüfung der Gültigkeit von Unionsrechtsakten anhand der durch die Charta verbürgten Grundrechte vorzunehmen sind (vgl. entsprechend Urteil vom 20. März 2018, Menci, C-524/15, EU:C:2018:197, Rn. 24).

100 Im Übrigen entspricht es ständiger Rechtsprechung, dass die Gültigkeit unionsrechtlicher Bestimmungen und, sofern darin kein ausdrücklicher Verweis auf das nationale Recht der Mitgliedstaaten erfolgt, ihre Auslegung nicht anhand dieses nationalen Rechts zu beurteilen sind, selbst wenn es im Verfassungsrang steht, insbesondere nicht anhand der Grundrechte, wie sie in den nationalen Verfassungen der Mitgliedstaaten ausgestaltet sind (vgl. in diesem Sinne Urteile vom 17. Dezember 1970, Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, Rn. 3, vom 13. Dezember 1979, Hauer, 44/79, EU:C:1979:290, Rn. 14, sowie vom 18. Oktober 2016, Nikiforidis, C-135/15, EU:C:2016:774, Rn. 28 und die dort angeführte Rechtsprechung).

101 Angesichts dessen, dass eine Übermittlung personenbezogener Daten wie die im Ausgangsverfahren in Rede stehende, die von einem in einem Mitgliedstaat ansässigen Wirtschaftsteilnehmer zu gewerblichen Zwecken an einen in einem Drittland ansässigen Wirtschaftsteilnehmer erfolgt, in den Anwendungsbereich der DSGVO fällt, wie aus der Antwort auf die erste Frage hervorgeht, und dass diese Verordnung, wie sich aus ihrem zehnten Erwägungsgrund ergibt, namentlich darauf abzielt, innerhalb der Union ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und zu diesem Zweck für eine unionsweit gleichmäßige und einheitliche Anwendung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten dieser Personen bei der Verarbeitung personenbezogener Daten zu sorgen, muss folglich das nach Art. 46 Abs. 1 der DSGVO erforderliche Niveau des Grundrechtsschutzes auf der Grundlage der Bestimmungen dieser Verordnung im Licht der durch die Charta verbürgten Grundrechte ermittelt werden.

102 Das vorlegende Gericht möchte ferner wissen, welche Gesichtspunkte zu berücksichtigen sind, um festzustellen, ob ein angemessenes Schutzniveau besteht, wenn personenbezogene Daten auf der Grundlage gemäß Art. 46 Abs. 2 Buchst. c der DSGVO erarbeiteter Standarddatenschutzklauseln in ein Drittland übermittelt werden.

103 Zwar werden in dieser Vorschrift nicht die verschiedenen Elemente aufgezählt, die bei der Beurteilung der Angemessenheit des im Rahmen einer solchen Übermittlung einzuhaltenden Schutzniveaus zu berücksichtigen sind, doch wird in Art. 46 Abs. 1 der DSGVO klargestellt, dass den betroffenen Personen geeignete Garantien zugutekommen und durchsetzbare Rechte sowie wirksame Rechtsbehelfe zur Verfügung stehen müssen.

104 Bei der insoweit im Zusammenhang mit einer solchen Übermittlung erforderlichen Beurteilung sind insbesondere die vertraglichen Regelungen zu berücksichtigen, die zwischen dem in der Union ansässigen Verantwortlichen bzw. seinem dort ansässigen Auftragsverarbeiter und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, sowie, was einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten betrifft, die maßgeblichen Elemente der Rechtsordnung dieses Landes. In der letztgenannten Hinsicht entsprechen die Elemente, die im Kontext von Art. 46 der DSGVO zu berücksichtigen sind, denen, die in ihrem Art. 45 Abs. 2 in nicht abschließender Weise aufgezählt werden.

105 Folglich ist auf die Fragen 2, 3 und 6 zu antworten, dass Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der DSGVO dahin auszulegen sind, dass die nach diesen Vorschriften erforderlichen geeigneten Garantien, durchsetzbaren Rechte und wirksamen Rechtsbehelfe gewährleisten müssen, dass die Rechte der Personen, deren personenbezogene Daten auf der Grundlage von

Standarddatenschutzklauseln in ein Drittland übermittelt werden, ein Schutzniveau genießen, das dem in der Union durch die DSGVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist. Bei der insoweit im Zusammenhang mit einer solchen Übermittlung vorzunehmenden Beurteilung sind insbesondere die vertraglichen Regelungen zu berücksichtigen, die zwischen dem in der Union ansässigen Verantwortlichen bzw. seinem dort ansässigen Auftragsverarbeiter und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, sowie, was einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten betrifft, die maßgeblichen Elemente der Rechtsordnung dieses Landes, insbesondere die in Art. 45 Abs. 2 der DSGVO genannten Elemente.

Zur achten Frage

106 Mit seiner achten Frage möchte das vorlegende Gericht wissen, ob Art. 58 Abs. 2 Buchst. f und j der DSGVO dahin auszulegen ist, dass die zuständige Aufsichtsbehörde verpflichtet ist, eine auf Standarddatenschutzklauseln, die von der Kommission erlassen wurden, gestützte Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn sie der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht, insbesondere nach den Art. 45 und 46 der DSGVO sowie nach der Charta, erforderliche Schutz der übermittelten Daten nicht gewährleistet werden kann, oder ob der besagte Artikel dahin auszulegen ist, dass die Ausübung dieser Befugnisse auf Ausnahmefälle beschränkt ist.

107 Gemäß Art. 8 Abs. 3 der Charta sowie Art. 51 Abs. 1 und Art. 57 Abs. 1 Buchst. a der DSGVO haben die nationalen Aufsichtsbehörden die Einhaltung der Unionsvorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu überwachen. Folglich ist jede von ihnen zu der Prüfung befugt, ob bei einer Übermittlung personenbezogener Daten aus ihrem Mitgliedstaat in ein Drittland die in der DSGVO aufgestellten Anforderungen eingehalten werden (vgl. entsprechend, zu Art. 28 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 47).

108 Aus diesen Bestimmungen folgt, dass die Aufsichtsbehörden primär die Aufgabe haben, die Anwendung der DSGVO zu überwachen und für ihre Einhaltung zu sorgen. Besonders wichtig ist die Erfüllung dieser Aufgabe im Zusammenhang mit einer Übermittlung personenbezogener Daten in ein Drittland, da, wie bereits aus dem Wortlaut des 116. Erwägungsgrundes dieser Verordnung hervorgeht, „[w]enn personenbezogene Daten in ein anderes Land außerhalb der Union übermittelt werden, … eine erhöhte Gefahr [besteht], dass natürliche Personen ihre Datenschutzrechte nicht wahrnehmen können[, um] sich insbesondere gegen die unrechtmäßige Nutzung oder Offenlegung dieser Informationen zu schützen“. In diesem Fall kann es, wie im selben Erwägungsgrund hinzugefügt wird, „vorkommen, dass Aufsichtsbehörden Beschwerden nicht nachgehen oder Untersuchungen nicht durchführen können, die einen Bezug zu Tätigkeiten außerhalb der Grenzen ihres Mitgliedstaats haben“.

109 Des Weiteren ist jede Aufsichtsbehörde nach Art. 57 Abs. 1 Buchst. f der DSGVO verpflichtet, sich in ihrem Hoheitsgebiet mit Beschwerden zu befassen, die jede Person gemäß Art. 77 Abs. 1 der DSGVO einlegen kann, wenn sie der Ansicht ist, dass eine Verarbeitung sie betreffender personenbezogener Daten gegen diese Verordnung verstößt, und den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen. Die Aufsichtsbehörde muss eine solche Beschwerde mit aller gebotenen Sorgfalt bearbeiten (vgl. entsprechend, zu Art. 25 Abs. 6 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 63).

110 Nach Art. 78 Abs. 1 und 2 der DSGVO hat jede Person u. a. dann das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sich die Aufsichtsbehörde nicht mit ihrer Beschwerde befasst. Auch im 141. Erwägungsgrund der DSGVO wird auf dieses „Recht[,] gemäß Artikel 47 der Charta einen

wirksamen gerichtlichen Rechtsbehelf einzulegen“, für den Fall Bezug genommen, dass die Aufsichtsbehörde „nicht tätig wird, … obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist“.

111 Hinsichtlich der Bearbeitung von Beschwerden verleiht Art. 58 Abs. 1 der DSGVO jeder Aufsichtsbehörde weitreichende Untersuchungsbefugnisse. Ist eine solche Behörde am Ende ihrer Untersuchung der Ansicht, dass die betroffene Person, deren personenbezogene Daten in ein Drittland übermittelt wurden, dort kein angemessenes Schutzniveau genießt, ist sie nach dem Unionsrecht verpflichtet, in geeigneter Weise zu reagieren, um der festgestellten Unzulänglichkeit abzuhelfen, und zwar unabhängig davon, welchen Ursprungs und welcher Art sie ist. Zu diesem Zweck werden in Art. 58 Abs. 2 der DSGVO die verschiedenen der Aufsichtsbehörde zur Verfügung stehenden Abhilfebefugnisse aufgezählt.

112 Auch wenn es Sache der Aufsichtsbehörde ist, unter Berücksichtigung aller Umstände der fraglichen Übermittlung personenbezogener Daten das geeignete und erforderliche Mittel zu wählen, ist sie gleichwohl verpflichtet, mit aller gebotenen Sorgfalt ihre Aufgabe zu erfüllen, die darin besteht, über die umfassende Einhaltung der DSGVO zu wachen.

113 Insoweit ist die Aufsichtsbehörde, wie auch der Generalanwalt in Nr. 148 seiner Schlussanträge festgestellt hat, nach Art. 58 Abs. 2 Buchst. f und j der DSGVO verpflichtet, eine Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn sie im Licht aller Umstände dieser Übermittlung der Auffassung ist, dass die Standarddatenschutzklauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht durch andere Mittel gewährleistet werden kann, es sei denn, der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter hat die Übermittlung selbst ausgesetzt oder beendet.

114 Die in der vorstehenden Randnummer dargelegte Auslegung wird nicht durch das Vorbringen des Commissioner in Frage gestellt, wonach Art. 4 des Beschlusses 2010/87 in seiner vor dem Inkrafttreten des Durchführungsbeschlusses 2016/2297 geltenden Fassung, im Licht des elften Erwägungsgrundes dieses Beschlusses betrachtet, die Befugnis der Aufsichtsbehörden, eine Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, auf bestimmte Ausnahmefälle beschränke. In seiner aus dem Durchführungsbeschluss 2016/2297 hervorgegangenen Fassung nimmt Art. 4 des SDK-Beschlusses nämlich auf die – nunmehr auf Art. 58 Abs. 2 Buchst. f und j der DSGVO beruhende – Befugnis der Aufsichtsbehörden Bezug, eine solche Übermittlung auszusetzen oder zu verbieten, ohne die Ausübung dieser Befugnis in irgendeiner Weise auf außergewöhnliche Umstände zu beschränken.

115 Jedenfalls berechtigt die Durchführungsbefugnis, die Art. 46 Abs. 2 Buchst. c der DSGVO der Kommission für den Erlass von Standarddatenschutzklauseln einräumt, die Kommission nicht, die den Aufsichtsbehörden nach Art. 58 Abs. 2 dieser Verordnung zustehenden Befugnisse zu beschränken (vgl. entsprechend, zu Art. 25 Abs. 6 und Art. 28 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 102 und 103). Im Übrigen bestätigt der fünfte Erwägungsgrund des Durchführungsbeschlusses 2016/2297, dass der SDK-Beschluss „eine … Aufsichtsbehörde … nicht daran [hindert], Datenübermittlungen zu kontrollieren und unter anderem eine Übermittlung personenbezogener Daten auszusetzen oder zu verbieten, wenn sie feststellt, dass durch die Übermittlung EU- oder nationale Datenschutzvorschriften verletzt werden“.

116 Die Befugnisse der zuständigen Aufsichtsbehörde sind allerdings unter umfassender Beachtung eines etwaigen Beschlusses wahrzunehmen, mit dem die Kommission gemäß Art. 45 Abs. 1 Satz 1 der DSGVO feststellt, dass ein bestimmtes Drittland ein angemessenes Schutzniveau bietet. Für einen solchen Fall geht nämlich aus Art. 45 Abs. 1 Satz 2 dieser Verordnung in Verbindung mit deren 103. Erwägungsgrund hervor, dass die Übermittlung personenbezogener Daten in das betreffende Drittland keiner besonderen Genehmigung bedarf.

117 Nach Art. 288 Abs. 4 AEUV bindet ein Angemessenheitsbeschluss der Kommission in allen seinen Teilen alle Mitgliedstaaten und ist damit für alle ihre Organe verbindlich, soweit darin festgestellt wird, dass das betreffende Drittland ein angemessenes Schutzniveau gewährleistet, und die Übermittlung personenbezogener Daten im Ergebnis genehmigt wird (vgl. entsprechend, zu Art. 25 Abs. 6 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 51 und die dort angeführte Rechtsprechung).

118 Solange der Angemessenheitsbeschluss vom Gerichtshof nicht für ungültig erklärt wurde, können die Mitgliedstaaten und ihre Organe, zu denen ihre unabhängigen Aufsichtsbehörden gehören, somit zwar keine diesem Beschluss zuwiderlaufenden Maßnahmen treffen, wie etwa Rechtsakte, mit denen verbindlich festgestellt wird, dass das Drittland, auf das sich der Beschluss bezieht, kein angemessenes Schutzniveau gewährleistet (Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 52 und die dort angeführte Rechtsprechung), und mit denen infolgedessen die Übermittlung personenbezogener Daten in dieses Drittland ausgesetzt oder verboten wird.

119 Ein nach Art. 45 Abs. 3 der DSGVO ergangener Angemessenheitsbeschluss der Kommission kann Personen, deren personenbezogene Daten in ein Drittland übermittelt wurden oder werden könnten, jedoch nicht daran hindern, gemäß Art. 77 Abs. 1 der DSGVO die zuständige nationale Aufsichtsbehörde mit einer Beschwerde bezüglich des Schutzes ihrer Rechte und Freiheiten bei der Verarbeitung solcher Daten zu befassen. Desgleichen kann ein derartiger Beschluss die den nationalen Aufsichtsbehörden durch Art. 8 Abs. 3 der Charta sowie durch Art. 51 Abs. 1 und Art. 57 Abs. 1 Buchst. a der DSGVO ausdrücklich zuerkannten Befugnisse weder beseitigen noch beschränken (vgl. entsprechend, zu Art. 25 Abs. 6 und Art. 28 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 53).

120 Auch wenn die Kommission einen Angemessenheitsbeschluss erlassen hat, muss die zuständige nationale Aufsichtsbehörde, an die sich eine Person mit einer Beschwerde bezüglich des Schutzes ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten wendet, daher in völliger Unabhängigkeit prüfen können, ob bei der Übermittlung dieser Daten die in der DSGVO aufgestellten Anforderungen gewahrt werden, und gegebenenfalls Klage vor den nationalen Gerichten erheben können, damit diese, wenn sie die Zweifel der Aufsichtsbehörde an der Gültigkeit des Angemessenheitsbeschlusses teilen, um eine Vorabentscheidung über dessen Gültigkeit ersuchen (vgl. entsprechend, zu Art. 25 Abs. 6 und Art. 28 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 57 und 65).

121 Nach alledem ist auf die achte Frage zu antworten, dass Art. 58 Abs. 2 Buchst. f und j der DSGVO dahin auszulegen ist, dass die zuständige Aufsichtsbehörde, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, verpflichtet ist, eine auf Standarddatenschutzklauseln, die von der Kommission erarbeitet wurden, gestützte Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn diese Behörde im Licht aller Umstände dieser Übermittlung der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht, insbesondere nach den Art. 45 und 46 der DSGVO sowie nach der Charta, erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, es sei denn, der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter hat die Übermittlung selbst ausgesetzt oder beendet.

Zur siebten und zur elften Frage

122 Mit seinen zusammen zu prüfenden Fragen 7 und 11 befragt das vorlegende Gericht den Gerichtshof nach der Gültigkeit des SDK-Beschlusses im Hinblick auf die Art. 7, 8 und 47 der Charta.

123 Insbesondere möchte das vorlegende Gericht, wie aus dem Wortlaut der siebten Frage und den sie betreffenden Erläuterungen im Vorabentscheidungsersuchen hervorgeht, wissen, ob der SDK-Beschluss vor dem Hintergrund, dass die darin vorgesehenen Standarddatenschutzklauseln drittstaatliche Behörden nicht binden, ein angemessenes Schutzniveau für die in Drittländer übermittelten personenbezogenen Daten zu gewährleisten vermag.

124 Art. 1 des SDK-Beschlusses bestimmt, dass die Standarddatenschutzklauseln im Anhang dieses Beschlusses entsprechend den Anforderungen von Art. 26 Abs. 2 der Richtlinie 95/46 als angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen gelten. Die letztgenannte Bestimmung wurde in Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der DSGVO im Wesentlichen übernommen.

125 Während diese Klauseln für den in der Union ansässigen Verantwortlichen und den in einem Drittland ansässigen Empfänger der Übermittlung personenbezogener Daten verbindlich sind, sofern sie einen Vertrag unter Bezugnahme auf diese Klauseln geschlossen haben, steht allerdings außer Frage, dass sie die Behörden dieses Drittlands nicht binden können, da diese nicht Vertragspartei sind.

126 Demnach gibt es zwar Situationen, in denen der Empfänger einer solchen Übermittlung in Anbetracht der Rechtslage und der Praxis im betreffenden Drittland den erforderlichen Datenschutz allein auf der Grundlage der Standarddatenschutzklauseln garantieren kann, aber auch Situationen, in denen die in diesen Klauseln enthaltenen Regelungen möglicherweise kein ausreichendes Mittel darstellen, um in der Praxis den effektiven Schutz der in das betreffende Drittland übermittelten personenbezogenen Daten zu gewährleisten. So verhält es sich etwa, wenn das Recht dieses Drittlands dessen Behörden Eingriffe in die Rechte der betroffenen Personen bezüglich dieser Daten erlaubt.

127 Somit stellt sich die Frage, ob ein nach Art. 46 Abs. 2 Buchst. c der DSGVO ergangener Beschluss der Kommission zu Standarddatenschutzklauseln ungültig ist, wenn er keine Garantien enthält, die den Behörden des Drittlands, in das personenbezogene Daten auf der Grundlage dieser Klauseln übermittelt werden oder übermittelt werden könnten, entgegengehalten werden können.

128 Nach Art. 46 Abs. 1 der DSGVO darf ein Verantwortlicher oder ein Auftragsverarbeiter, falls kein Angemessenheitsbeschluss vorliegt, personenbezogene Daten an ein Drittland nur übermitteln, sofern er geeignete Garantien vorgesehen hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Nach Art. 46 Abs. 2 Buchst. c der DSGVO können diese Garantien in von der Kommission erlassenen Standarddatenschutzklauseln bestehen. Nach diesen Bestimmungen müssen aber nicht sämtliche Garantien zwangsläufig in einem Beschluss der Kommission wie dem SDK-Beschluss vorgesehen sein.

129 Insoweit unterscheidet sich ein solcher Beschluss von einem nach Art. 45 Abs. 3 der DSGVO ergangenen Angemessenheitsbeschluss, der darauf abzielt – im Anschluss an eine Untersuchung des Rechts des betreffenden Drittlands, bei der insbesondere die maßgeblichen Vorschriften im Bereich der nationalen Sicherheit und des Zugangs der Behörden zu personenbezogenen Daten berücksichtigt werden –, verbindlich festzustellen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland ein angemessenes Schutzniveau bieten, so dass der Zugang der Behörden dieses Landes zu solchen Daten ihrer Übermittlung in dieses Land nicht entgegensteht. Die Kommission darf einen solchen Angemessenheitsbeschluss also nur erlassen, wenn sie festgestellt hat, dass die einschlägigen Rechtsvorschriften des Drittlands tatsächlich alle erforderlichen Garantien bieten, so dass angenommen werden kann, dass sie ein angemessenes Schutzniveau gewährleisten.

130 Bei einem Beschluss der Kommission wie dem SDK-Beschluss, mit dem Standarddatenschutzklauseln aufgestellt werden, kann hingegen, da ein solcher Beschluss nicht ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland betrifft, aus Art. 46 Abs. 1 und Art. 46 Abs. 2

Buchst. c der DSGVO nicht abgeleitet werden, dass die Kommission verpflichtet wäre, vor seinem Erlass die Angemessenheit des Schutzniveaus zu beurteilen, das in den Drittländern geboten wird, in die personenbezogene Daten auf der Grundlage solcher Klauseln übermittelt werden könnten.

131 Insoweit ist darauf hinzuweisen, dass es gemäß Art. 46 Abs. 1 der DSGVO, falls kein Angemessenheitsbeschluss der Kommission vorliegt, Sache des in der Union ansässigen Verantwortlichen bzw. des dort ansässigen Auftragsverarbeiters ist, insbesondere geeignete Garantien vorzusehen. Die Erwägungsgründe 108 und 114 dieser Verordnung bestätigen, dass der Verantwortliche oder gegebenenfalls sein Auftragsverarbeiter, wenn die Kommission keine Entscheidung in Bezug auf die Angemessenheit des Datenschutzniveaus in einem Drittland getroffen hat, „als Ausgleich für den [im] Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen [sollte]“ und dass „[d]iese Garantien … sicherstellen [sollten], dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden; dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen … in der Union oder in einem Drittland“.

132 Da Standarddatenschutzklauseln, wie aus Rn. 125 des vorliegenden Urteils hervorgeht, aufgrund ihres Vertragscharakters naturgemäß keine drittstaatlichen Behörden binden können, während Art. 44, Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der DSGVO – ausgelegt im Licht der Art. 7, 8 und 47 der Charta –verlangen, dass das durch die DSGVO verbürgte Schutzniveau für natürliche Personen nicht beeinträchtigt wird, kann es sich als notwendig erweisen, die in den Standarddatenschutzklauseln enthaltenen Garantien zu ergänzen. Dazu heißt es im 109. Erwägungsgrund dieser Verordnung, dass „[d]ie dem Verantwortlichen … offenstehende Möglichkeit, auf die von der Kommission … festgelegten Standard-Datenschutzklauseln zurückzugreifen, … den Verantwortlichen [nicht] daran hindern [sollte], ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen“, und dass der Verantwortliche insbesondere „ermutigt werden [sollte], [durch Ergänzung der Standarddatenschutzklauseln] zusätzliche Garantien zu bieten“.

133 Somit ist davon auszugehen, dass die von der Kommission gemäß Art. 46 Abs. 2 Buchst. c DSGVO erlassenen Standarddatenschutzklauseln nur darauf abzielen, den in der Union ansässigen Verantwortlichen bzw. ihren dort ansässigen Auftragsverarbeitern vertragliche Garantien zu bieten, die in allen Drittländern einheitlich gelten, d. h. unabhängig vom dort jeweils garantierten Schutzniveau. Da diese Standarddatenschutzklauseln ihrer Natur nach keine Garantien bieten können, die über die vertragliche Verpflichtung, für die Einhaltung des unionsrechtlich verlangten Schutzniveaus zu sorgen, hinausgehen, kann es je nach der in einem bestimmten Drittland gegebenen Lage erforderlich sein, dass der Verantwortliche zusätzliche Maßnahmen ergreift, um die Einhaltung dieses Schutzniveaus zu gewährleisten.

134 Wie der Generalanwalt hierzu in Nr. 126 seiner Schlussanträge ausgeführt hat, beruht der in Art. 46 Abs. 2 Buchst. c der DSGVO vorgesehene vertragliche Mechanismus auf der Eigenverantwortlichkeit des in der Union ansässigen Verantwortlichen bzw. seines dort ansässigen Auftragsverarbeiters und, in zweiter Linie, der zuständigen Aufsichtsbehörde. Folglich obliegt es vor allem diesem Verantwortlichen bzw. seinem Auftragsverarbeiter, in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung – zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen zu gewähren.

135 Kann der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter keine hinreichenden zusätzlichen Maßnahmen ergreifen, um einen solchen Schutz zu gewährleisten, ist er – bzw. in zweiter Linie die zuständige Aufsichtsbehörde – verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auszusetzen oder zu beenden. Dies ist insbesondere dann der Fall, wenn das Recht dieses Drittlands dem Empfänger aus der Union

übermittelter personenbezogener Daten Verpflichtungen auferlegt, die den genannten Klauseln widersprechen und daher geeignet sind, die vertragliche Garantie eines angemessenen Schutzniveaus hinsichtlich des Zugangs der Behörden dieses Drittlands zu diesen Daten zu untergraben.

136 Der bloße Umstand, dass Standarddatenschutzklauseln, die wie die im Anhang des SDK-Beschlusses befindlichen in einem gemäß Art. 46 Abs. 2 Buchst. c der DSGVO ergangenen Beschluss der Kommission enthalten sind, die Behörden der Drittländer, in die möglicherweise personenbezogene Daten übermittelt werden, nicht binden, kann folglich die Gültigkeit dieses Beschlusses nicht berühren.

137 Vielmehr hängt die Gültigkeit eines solchen Beschlusses davon ab, ob er – im Einklang mit dem aus Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der DSGVO im Licht der Art. 7, 8 und 47 der Charta resultierenden Erfordernis – wirksame Mechanismen enthält, die in der Praxis gewährleisten können, dass das vom Unionsrecht verlangte Schutzniveau eingehalten wird und dass auf solche Klauseln gestützte Übermittlungen personenbezogener Daten ausgesetzt oder verboten werden, wenn gegen diese Klauseln verstoßen wird oder ihre Einhaltung unmöglich ist.

138 Was die in den Standarddatenschutzklauseln im Anhang des SDK-Beschlusses enthaltenen Garantien betrifft, geht aus Klausel 4 Buchst. a und b, Klausel 5 Buchst. a, Klausel 9 sowie Klausel 11 Abs. 1 dieses Anhangs hervor, dass sich der in der Union ansässige Verantwortliche, der Empfänger der Übermittlung personenbezogener Daten sowie der etwaige Auftragsverarbeiter dieses Empfängers gegenseitig verpflichten, zu gewährleisten, dass die Verarbeitung der Daten, einschließlich ihrer Übermittlung, im Einklang mit dem „anwendbaren Datenschutzrecht“ erfolgt ist und weiterhin erfolgen wird, d. h. gemäß der Definition in Art. 3 Buchst. f des SDK-Beschlusses, im Einklang mit den „Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre im Hinblick auf die Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, für den für die Verarbeitung Verantwortlichen gelten“. Die Bestimmungen der DSGVO – im Licht der Charta betrachtet – gehören zu diesen Vorschriften.

139 Des Weiteren verpflichtet sich der in einem Drittland ansässige Empfänger der Übermittlung personenbezogener Daten gemäß Klausel 5 Buchst. a des Anhangs des SDK-Beschlusses dazu, den in der Union ansässigen Verantwortlichen unverzüglich in Kenntnis zu setzen, falls er seine vertraglichen Pflichten nicht einhalten kann. Insbesondere versichert der Empfänger gemäß Klausel 5 Buchst. b, dass er seines Wissens keinen Gesetzen unterliegt, die die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und verpflichtet sich, dem Verantwortlichen, sobald er davon Kenntnis erhält, jede Änderung der ihn betreffenden nationalen Rechtsvorschriften mitzuteilen, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Standarddatenschutzklauseln im Anhang des SDK-Beschlusses bieten sollen. Im Übrigen ist der Empfänger der Übermittlung personenbezogener Daten zwar nach Klausel 5 Buchst. d Ziff. i berechtigt, den in der Union ansässigen Verantwortlichen nicht über rechtlich bindende Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten zu informieren, falls ihm diese Information rechtlich untersagt ist, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen. Allerdings ist er auch in diesem Fall gemäß Klausel 5 Buchst. a verpflichtet, den Verantwortlichen davon in Kenntnis zu setzen, dass er die Standarddatenschutzklauseln nicht einhalten kann.

140 In den beiden von ihr erfassten Fällen räumt Klausel 5 Buchst. a und b dem in der Union ansässigen Verantwortlichen das Recht ein, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten. In Anbetracht der Anforderungen, die sich aus Art. 46 Abs. 1 und Abs. 2 Buchst. c der DSGVO im Licht der Art. 7 und 8 der Charta ergeben, ist der Verantwortliche zur Aussetzung der Datenübermittlung und/oder zum Rücktritt vom Vertrag verpflichtet, wenn der Empfänger der

Übermittlung nicht oder nicht mehr in der Lage ist, die Standarddatenschutzklauseln einzuhalten. Unterließe der Verantwortliche dies, würde er die Pflichten verletzen, die ihm nach Klausel 4 Buchst. a des Anhangs des SDK-Beschlusses, ausgelegt im Licht der DSGVO und der Charta, obliegen.

141 Somit verpflichten Klausel 4 Buchst. a sowie Klausel 5 Buchst. a und b dieses Anhangs den in der Union ansässigen Verantwortlichen und den Empfänger der Übermittlung personenbezogener Daten, sich vor der Übermittlung personenbezogener Daten in ein Drittland zu vergewissern, dass das Recht des Bestimmungsdrittlands es dem Empfänger erlaubt, die Standarddatenschutzklauseln im Anhang des SDK-Beschlusses einzuhalten. Hinsichtlich dieser Prüfung wird in der Fußnote zu Klausel 5 klargestellt, dass zwingende Erfordernisse dieses Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft zur Gewährleistung u. a. der Sicherheit des Staates, der Landesverteidigung und der öffentlichen Sicherheit erforderlich ist, nicht den Standarddatenschutzklauseln widersprechen. Umgekehrt ist es, wie der Generalanwalt in Nr. 131 seiner Schlussanträge ausgeführt hat, als Verstoß gegen diese Klauseln anzusehen, wenn einer aus dem Recht des Bestimmungsdrittlands folgenden Verpflichtung nachgekommen wird, die über das hinausgeht, was für Zwecke wie die oben genannten erforderlich ist. Bei ihrer Beurteilung, ob eine solche Verpflichtung erforderlich ist, müssen die genannten Akteure gegebenenfalls berücksichtigen, dass das vom betreffenden Drittland gebotene Schutzniveau in einem gemäß Art. 45 Abs. 3 der DSGVO erlassenen Angemessenheitsbeschluss der Kommission für angemessen erklärt wurde.

142 Demzufolge sind der in der Union ansässige Verantwortliche und der Empfänger der Übermittlung personenbezogener Daten verpflichtet, vorab zu prüfen, ob im betreffenden Drittland das unionsrechtlich geforderte Schutzniveau eingehalten wird. Der Empfänger der Übermittlung ist nach Klausel 5 Buchst. b des Anhangs des SDK-Beschlusses gegebenenfalls verpflichtet, dem Verantwortlichen mitzuteilen, dass er die Klauseln nicht einhalten kann, woraufhin der Verantwortliche die Datenübermittlung aussetzen und/oder vom Vertrag zurücktreten muss.

143 Teilt der Empfänger der in ein Drittland erfolgenden Übermittlung personenbezogener Daten dem Verantwortlichen gemäß Klausel 5 Buchst. b des Anhangs des SDK-Beschlusses mit, dass das Recht des betreffenden Drittlands es ihm nicht erlaube, die Standarddatenschutzklauseln in diesem Anhang einzuhalten, folgt aus dessen Klausel 12, dass die bereits in dieses Drittland übermittelten Daten und deren Kopien – sämtlich – zurückgeschickt oder zerstört werden müssen. In jedem Fall sieht Klausel 6 des Anhangs eine Sanktion für den Verstoß gegen die Standarddatenschutzklauseln vor, indem sie der betroffenen Person einen Schadensersatzanspruch verschafft.

144 Zu ergänzen ist, dass sich der in der Union ansässige Verantwortliche gemäß Klausel 4 Buchst. f des Anhangs des SDK-Beschlusses verpflichtet, für den Fall, dass besondere Datenkategorien in ein Drittland, das kein angemessenes Schutzniveau bietet, übermittelt werden könnten, die betroffene Person vor oder so bald wie möglich nach der Übermittlung davon in Kenntnis zu setzen. Durch diese Mitteilung wird die betroffene Person in die Lage versetzt, die ihr durch Klausel 3 Abs. 1 dieses Anhangs zuerkannten rechtlichen Mittel gegenüber dem Verantwortlichen wahrzunehmen, damit er die beabsichtigte Übermittlung aussetzt, von dem mit dem Empfänger der Übermittlung personenbezogener Daten geschlossenen Vertrag zurücktritt oder gegebenenfalls von ihm verlangt, die bereits übermittelten Daten zurückzuschicken oder zu zerstören.

145 Wenn der Empfänger der Übermittlung personenbezogener Daten dem in der Union ansässigen Verantwortlichen gemäß Klausel 5 Buchst. b des Anhangs des SDK-Beschlusses mitteilt, dass die ihn betreffenden Rechtsvorschriften in einer Weise geändert worden seien, die sich sehr nachteilig auf die durch die Standarddatenschutzklauseln gebotenen Garantien und Pflichten auswirken könnte, muss der Verantwortliche diese Mitteilung nach Klausel 4 Buchst. g dieses Anhangs an die zuständige Aufsichtsbehörde weiterleiten, falls er trotz der Mitteilung beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben. Die Weiterleitung einer solchen Mitteilung an die Aufsichtsbehörde und deren Recht, den Empfänger der Übermittlung personenbezogener Daten gemäß Klausel 8 Abs. 2

des Anhangs einer Prüfung zu unterziehen, ermöglichen es der Aufsichtsbehörde, zu prüfen, ob die beabsichtigte Übermittlung ausgesetzt oder verboten werden muss, um ein angemessenes Schutzniveau zu wahren.

146 In diesem Zusammenhang bestätigt Art. 4 des SDK-Beschlusses im Licht des fünften Erwägungsgrundes des Durchführungsbeschlusses 2016/2297, dass der SDK-Beschluss die zuständige Aufsichtsbehörde keineswegs daran hindert, eine auf die Standarddatenschutzklauseln im Anhang dieses Beschlusses gestützte Übermittlung personenbezogener Daten in ein Drittland gegebenenfalls auszusetzen oder zu verbieten. Insoweit muss, wie sich aus der Antwort auf die achte Frage ergibt, die zuständige Aufsichtsbehörde, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, gemäß Art. 58 Abs. 2 Buchst. f und j der DSGVO eine solche Übermittlung aussetzen oder verbieten, wenn sie im Licht aller Umstände der Übermittlung der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, es sei denn, der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter hat die Übermittlung selbst ausgesetzt oder beendet.

147 Was den vom Commissioner angeführten Umstand betrifft, dass die Aufsichtsbehörden verschiedener Mitgliedstaaten unter Umständen divergierende Entscheidungen in Bezug auf Übermittlungen personenbezogener Daten in ein solches Drittland treffen könnten, ist zu ergänzen, dass, wie aus Art. 55 Abs. 1 und Art. 57 Abs. 1 Buchst. a der DSGVO hervorgeht, mit der Aufgabe, die Einhaltung dieser Verordnung zu überwachen, grundsätzlich jede Aufsichtsbehörde im Hoheitsgebiet ihres eigenen Mitgliedstaats betraut ist. Um divergierende Entscheidungen zu vermeiden, sieht Art. 64 Abs. 2 der DSGVO überdies vor, dass eine Aufsichtsbehörde, die der Auffassung ist, dass Datenübermittlungen in ein Drittland generell verboten werden müssen, eine Stellungnahme des Europäischen Datenschutzausschusses (EDSA) einholen kann, der seinerseits nach Art. 65 Abs. 1 Buchst. c der DSGVO u. a. dann einen verbindlichen Beschluss erlassen kann, wenn eine Aufsichtsbehörde seiner Stellungnahme nicht folgt.

148 Folglich sieht der SDK-Beschluss wirksame Mechanismen vor, mit denen in der Praxis gewährleistet werden kann, dass die auf die Standarddatenschutzklauseln im Anhang dieses Beschlusses gestützte Übermittlung personenbezogener Daten in ein Drittland ausgesetzt oder verboten wird, wenn der Empfänger der Übermittlung diese Klauseln nicht einhält oder nicht einhalten kann.

149 Nach alledem ist auf die siebte und die elfte Frage zu antworten, dass die Prüfung des SDK-Beschlusses anhand der Art. 7, 8 und 47 der Charta nichts ergeben hat, was seine Gültigkeit berühren könnte.

Zu den Fragen 4, 5, 9 und 10

150 Mit seiner neunten Frage möchte das vorlegende Gericht wissen, ob und inwieweit eine Aufsichtsbehörde eines Mitgliedstaats an die Feststellungen im DSS-Beschluss gebunden ist, wonach die Vereinigten Staaten ein angemessenes Schutzniveau gewährleisten. Mit seinen Fragen 4, 5 und 10 möchte es im Kern wissen, ob – in Anbetracht seiner eigenen Feststellungen zum Recht der Vereinigten Staaten – die auf die Standarddatenschutzklauseln im Anhang des SDK-Beschlusses gestützte Übermittlung personenbezogener Daten in dieses Drittland die durch die Art. 7, 8 und 47 der Charta verbürgten Rechte verletzt. Insbesondere ersucht es den Gerichtshof, sich zu der Frage zu äußern, ob die Einsetzung der in Anhang III des DSS-Beschlusses erwähnten Ombudsperson mit Art. 47 der Charta im Einklang steht.

151 Zunächst ist festzustellen, dass mit der vom Commissioner im Ausgangsverfahren erhobenen Klage zwar nur die Gültigkeit des SDK-Beschlusses in Frage gestellt wird, doch wurde sie vor dem Erlass des DSS-Beschlusses beim vorlegenden Gericht erhoben. Da es mit seiner vierten und seiner fünften Frage vom Gerichtshof allgemein wissen möchte, welcher Schutz nach den Art. 7, 8 und 47 der Charta im

Rahmen einer solchen Übermittlung zu gewährleisten ist, muss der Gerichtshof bei seiner Prüfung die Folgen berücksichtigen, die sich aus dem zwischenzeitlichen Erlass des DSS-Beschlusses ergeben. Dies gilt umso mehr, als das vorlegende Gericht mit seiner zehnten Frage explizit wissen möchte, ob der nach Art. 47 der Charta erforderliche Schutz durch die in diesem Beschluss erwähnte Ombudsperson gewährleistet wird.

152 Zudem geht aus den Angaben im Vorabentscheidungsersuchen hervor, dass Facebook Ireland im Rahmen des Ausgangsverfahrens geltend gemacht hat, der DSS-Beschluss binde den Commissioner in Bezug auf die Feststellung der Angemessenheit des von den Vereinigten Staaten gebotenen Schutzniveaus und damit hinsichtlich der Zulässigkeit einer auf die Standarddatenschutzklauseln im Anhang des SDK-Beschlusses gestützten Übermittlung personenbezogener Daten in dieses Drittland.

153 Wie sich aus Rn. 59 des vorliegenden Urteils ergibt, hat das vorlegende Gericht in seinem Urteil vom 3. Oktober 2017, das dem Vorabentscheidungsersuchen beigefügt ist, hervorgehoben, dass es die zwischen der Klageerhebung und der von ihm anberaumten mündlichen Verhandlung eingetretenen Rechtsänderungen berücksichtigen müsse. Demnach muss es offenbar bei der Entscheidung des Ausgangsrechtsstreits die aus dem Erlass des DSS-Beschlusses resultierende Veränderung der Umstände sowie etwaige verbindliche Wirkungen dieses Beschlusses berücksichtigen.

154 Die Frage der Verbindlichkeit der Feststellung im DSS-Beschluss, dass in den Vereinigten Staaten ein angemessenes Schutzniveau bestehe, ist insbesondere relevant sowohl für die Beurteilung der in den Rn. 141 und 142 des vorliegenden Urteils dargelegten Pflichten des Verantwortlichen und des Empfängers einer auf die Standarddatenschutzklauseln im Anhang des SDK-Beschlusses gestützten Übermittlung personenbezogener Daten in ein Drittland als auch für die Beurteilung der etwaigen Pflichten der Aufsichtsbehörde, eine solche Übermittlung auszusetzen oder zu verbieten.

155 Zur Verbindlichkeit des DSS-Beschlusses wird in dessen Art. 1 Abs. 1 nämlich festgestellt, dass im Sinne von Art. 45 Abs. 1 der DSGVO „die Vereinigten Staaten ein angemessenes Schutzniveau für personenbezogene Daten [gewährleisten], die im Rahmen des EU-US-Datenschutzschilds aus der Europäischen Union an Organisationen in den Vereinigten Staaten übermittelt werden“. Gemäß Art. 1 Abs. 3 des DSS-Beschlusses gelten personenbezogene Daten als im Rahmen dieses Datenschutzschilds übermittelt, wenn sie aus der Union an Organisationen in den Vereinigten Staaten übermittelt werden, die in der „Datenschutzschild-Liste“ aufgeführt sind, die in Übereinstimmung mit den Abschnitten I und III der Grundsätze in Anhang II dieses Beschlusses vom amerikanischen Handelsministerium geführt und der Öffentlichkeit zugänglich gemacht wird.

156 Wie sich aus der in den Rn. 117 und 118 des vorliegenden Urteils wiedergegebenen Rechtsprechung ergibt, ist der DSS-Beschluss für die Aufsichtsbehörden insofern verbindlich, als in diesem Beschluss festgestellt wird, dass die Vereinigten Staaten ein angemessenes Schutzniveau gewährleisten, und als der Beschluss damit die Genehmigung von Übermittlungen personenbezogener Daten bewirkt, die im Rahmen des EU-US-Datenschutzschilds erfolgen. Solange dieser Beschluss vom Gerichtshof nicht für ungültig erklärt wurde, darf die zuständige Aufsichtsbehörde daher eine Übermittlung personenbezogener Daten an eine Organisation, die in der Schutzschild-Liste aufgeführt ist, nicht mit der Begründung aussetzen oder verbieten, dass sie entgegen der Beurteilung durch die Kommission im DSS-Beschluss der Auffassung sei, dass die Rechtsvorschriften der Vereinigten Staaten, die den Zugang zu den im Rahmen dieses Schutzschilds übermittelten personenbezogenen Daten und ihre Verwendung durch die Behörden dieses Drittlands aus Gründen der nationalen Sicherheit, der Strafverfolgung oder des öffentlichen Interesses regelten, kein angemessenes Schutzniveau gewährleisteten.

157 Gleichwohl muss die zuständige Aufsichtsbehörde gemäß der in den Rn. 119 und 120 des vorliegenden Urteils wiedergegebenen Rechtsprechung, wenn sich eine Person mit einer Beschwerde an sie wendet, in völliger Unabhängigkeit prüfen, ob bei der fraglichen Übermittlung personenbezogener Daten die in der DSGVO aufgestellten Anforderungen gewahrt werden, und, falls sie die von dieser Person zur

Infragestellung der Gültigkeit eines Angemessenheitsbeschlusses vorgebrachten Rügen für begründet hält, Klage vor den nationalen Gerichten erheben, damit diese den Gerichtshof um Vorabentscheidung über die Gültigkeit dieses Beschlusses ersuchen.

158 Eine Beschwerde im Sinne von Art. 77 Abs. 1 der DSGVO, mit der eine Person, deren personenbezogene Daten in ein Drittland übermittelt wurden oder werden könnten, geltend macht, dass ungeachtet der Feststellungen der Kommission in einem nach Art. 45 Abs. 3 der DSGVO ergangenen Beschluss das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleisteten, ist nämlich dahin zu verstehen, dass sie der Sache nach die Vereinbarkeit dieses Beschlusses mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte von Personen betrifft (vgl. entsprechend, zu Art. 25 Abs. 6 und Art. 28 Abs. 4 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 59).

159 Im vorliegenden Fall hat Herr Schrems der Sache nach den Commissioner aufgefordert, die Übermittlung seiner personenbezogenen Daten durch Facebook Ireland an die in den Vereinigten Staaten ansässige Facebook Inc. zu verbieten oder auszusetzen, weil dieses Drittland kein angemessenes Schutzniveau gewährleiste. Im Anschluss an eine Untersuchung des Vorbringens von Herrn Schrems hat der Commissioner das vorlegende Gericht angerufen. Für dieses Gericht stellt sich in Anbetracht der vorgelegten Beweise und der vor ihm erfolgten kontradiktorischen Erörterung offenbar die Frage, ob die Zweifel von Herrn Schrems an der Angemessenheit des im genannten Drittland gewährleisteten Schutzniveaus – entgegen den von der Kommission zwischenzeitlich im DSS-Beschluss getroffenen Feststellungen – berechtigt sind. Dies hat das vorlegende Gericht dazu veranlasst, dem Gerichtshof die Vorlagefragen 4, 5 und 10 zu stellen.

160 Wie der Generalanwalt in Nr. 175 seiner Schlussanträge ausgeführt hat, sind diese Vorlagefragen daher so zu verstehen, dass mit ihnen im Kern die von der Kommission im DSS-Beschluss getroffene Feststellung, die Vereinigten Staaten gewährleisteten ein angemessenes Schutzniveau für die aus der Union dorthin übermittelten Daten, und folglich die Gültigkeit dieses Beschlusses in Frage gestellt werden.

161 In Anbetracht der Erwägungen in den Rn. 121 und 157 bis 160 des vorliegenden Urteils und um dem vorlegenden Gericht eine vollständige Antwort zu geben, ist daher zu prüfen, ob der DSS-Beschluss den Anforderungen entspricht, die sich aus der im Licht der Charta ausgelegten DSGVO ergeben (vgl. entsprechend Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 67).

162 Der Erlass eines Angemessenheitsbeschlusses der Kommission nach Art. 45 Abs. 3 der DSGVO erfordert die gebührend begründete Feststellung dieses Organs, dass das betreffende Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen tatsächlich ein Schutzniveau der Grundrechte gewährleistet, das dem in der Rechtsordnung der Union garantierten Niveau der Sache nach gleichwertig ist (vgl. entsprechend, zu Art. 25 Abs. 6 der Richtlinie 95/46, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 96).

Zum Inhalt des DSS-Beschlusses

163 Nach den Feststellungen der Kommission in Art. 1 Abs. 1 des DSS-Beschlusses gewährleisten die Vereinigten Staaten für personenbezogene Daten, die im Rahmen des EU-US-Datenschutzschilds aus der Union an Organisationen in den Vereinigten Staaten übermittelt werden, ein angemessenes Schutzniveau. Gemäß Art. 1 Abs. 2 dieses Beschlusses besteht dieser Schutzschild namentlich aus den Grundsätzen, die am 7. Juli 2016 vom amerikanischen Handelsministerium herausgegeben wurden und in Anhang II des Beschlusses aufgeführt sind, sowie aus den offiziellen Erklärungen und Zusagen, die in den Schriftstücken der Anhänge I und III bis VII des Beschlusses enthalten sind.

164 Allerdings wird in Abschnitt I.5 des Anhangs II („Grundsätze des EU-US-Datenschutzschilds[,] vorgelegt vom amerikanischen Handelsministerium“) des DSS-Beschlusses auch ausgeführt, dass die Einhaltung dieser Grundsätze u. a. insoweit begrenzt sein könne, „als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss“. Somit wird in diesem Beschluss, ebenso wie in der Entscheidung 2000/520, diesen Erfordernissen Vorrang vor den genannten Grundsätzen eingeräumt. Aufgrund dieses Vorrangs sind die selbstzertifizierten US-Organisationen, die aus der Union personenbezogene Daten erhalten, ohne jede Einschränkung verpflichtet, diese Grundsätze unangewendet zu lassen, wenn sie in Widerstreit zu den genannten Erfordernissen stehen und sich deshalb als mit ihnen unvereinbar erweisen (vgl. entsprechend, zur Entscheidung 2000/520, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 86).

165 Angesichts ihres generellen Charakters ermöglicht die Ausnahme in Abschnitt I.5 des Anhangs II des DSS-Beschlusses es also, gestützt auf Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder auf Rechtsvorschriften der Vereinigten Staaten in die Grundrechte der Personen einzugreifen, deren personenbezogene Daten aus der Union in die Vereinigten Staaten übermittelt werden oder werden könnten (vgl. entsprechend, zur Entscheidung 2000/520, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 87). Solche Eingriffe können, wie auch im DSS-Beschluss festgestellt wird, insbesondere daraus resultieren, dass die amerikanischen Behörden auf die aus der Union in die Vereinigten Staaten übermittelten personenbezogenen Daten zugreifen und sie verwenden, was sowohl im Rahmen der auf Section 702 des FISA gestützten Überwachungsprogramme PRISM und UPSTREAM als auch auf der Grundlage der E.O. 12333 geschehen kann.

166 In diesem Zusammenhang hat die Kommission in den Erwägungsgründen 67 bis 135 des DSS-Beschlusses die Einschränkungen und Garantien bewertet, die im amerikanischen Recht, insbesondere nach Section 702 des FISA, der E.O. 12333 und der PPD-28, für den Zugang zu den im Rahmen des EU-US-Datenschutzschilds übermittelten Daten gelten, die durch staatliche Einrichtungen der Vereinigten Staaten aus Gründen der nationalen Sicherheit, der Strafverfolgung oder anderer im öffentlichen Interesse liegender Ziele gesammelt und genutzt werden.

167 Am Ende dieser Bewertung hat die Kommission im 136. Erwägungsgrund des DSS-Beschlusses festgestellt, dass „die Vereinigten Staaten einen angemessenen Rechtsschutz für personenbezogene Daten gewährleisten, die im Rahmen des EU-US-Datenschutzschilds aus der … Union an selbstzertifizierte Organisationen in den Vereinigten Staaten übermittelt werden“, und im 140. Erwägungsgrund „aufgrund der verfügbaren Informationen über die Rechtsordnung der [Vereinigten Staaten]“ die Auffassung vertreten, dass „jegliche Eingriffe in die Grundrechte von Personen, deren Daten im Rahmen des EU-US-Datenschutzschilds aus Gründen der nationalen Sicherheit, der Strafverfolgung oder für andere im öffentlichen Interesse liegende Zwecke aus der Europäischen Union in die Vereinigten Staaten übermittelt werden, sowie die deshalb den selbstzertifizierten Organisationen bei der Einhaltung der Grundsätze auferlegten Beschränkungen auf das für die Erreichung solcher legitimen Ziele absolut notwendige Maß beschränkt werden und dass damit ein wirksamer Rechtsschutz vor derartigen Eingriffen gewährleistet ist“.

Zur Feststellung eines angemessenen Schutzniveaus

168 Das vorlegende Gericht hegt in Anbetracht der von der Kommission im DSS-Beschluss angeführten und der von ihm selbst im Rahmen des Ausgangsverfahrens festgestellten Umstände Zweifel daran, ob das Recht der Vereinigten Staaten tatsächlich das nach Art. 45 der DSGVO im Licht der durch die Art. 7, 8 und 47 der Charta verbürgten Grundrechte erforderliche Schutzniveau gewährleistet. Insbesondere ist es der Auffassung, dass das Recht dieses Drittlands hinsichtlich der nach seinem nationalen Recht zulässigen Eingriffe nicht die erforderlichen Einschränkungen und Garantien vorsehe und auch keinen effektiven gerichtlichen Rechtsschutz vor solchen Eingriffen gewährleiste. Zum

letztgenannten Punkt fügt es hinzu, die Einsetzung der Ombudsperson des Datenschutzschilds könne seines Erachtens keinem dieser Mängel abhelfen, da sie einem Gericht im Sinne von Art. 47 der Charta nicht gleichgestellt werden könne.

169 Was erstens die Art. 7 und 8 der Charta anbelangt, die für das in der Union erforderliche Schutzniveau maßgebend sind und deren Einhaltung von der Kommission festgestellt werden muss, bevor sie einen Angemessenheitsbeschluss im Sinne von Art. 45 Abs. 1 der DSGVO erlässt, ist festzustellen, dass Art. 7 der Charta jeder Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Kommunikation garantiert. Art. 8 Abs. 1 der Charta räumt jeder Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten ein.

170 Der Zugriff auf personenbezogene Daten einer natürlichen Person zum Zweck ihrer Speicherung oder Verwendung berührt das durch Art. 7 der Charta garantierte Grundrecht dieser Person auf Achtung des Privatlebens, das sich auf jede Information erstreckt, die eine bestimmte oder bestimmbare natürliche Person betrifft. Außerdem fallen solche Datenverarbeitungen unter Art. 8 der Charta, weil sie Verarbeitungen personenbezogener Daten im Sinne dieses Artikels darstellen und deshalb zwangsläufig die dort vorgesehenen Erfordernisse des Datenschutzes erfüllen müssen (vgl. in diesem Sinne Urteile vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 49 und 52, und vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 29, sowie Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 122 und 123).

171 Der Gerichtshof hat bereits entschieden, dass die Weitergabe personenbezogener Daten an einen Dritten, etwa eine Behörde, unabhängig von der späteren Verwendung der übermittelten Informationen einen Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte darstellt. Dasselbe gilt für die Speicherung personenbezogener Daten und den Zugang zu ihnen für ihre Nutzung durch die Behörden, wobei es nicht darauf ankommt, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten (vgl. in diesem Sinne Urteile vom 20. Mai 2003, Österreichischer Rundfunk u. a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 74 und 75, und vom 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 33 bis 36, sowie Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 124 und 126).

172 Die in den Art. 7 und 8 der Charta niedergelegten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden (vgl. in diesem Sinne Urteile vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 48 und die dort angeführte Rechtsprechung, und vom 17. Oktober 2013, Schwarz, C-291/12, EU:C:2013:670, Rn. 33 und die dort angeführte Rechtsprechung, sowie Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 136).

173 Insoweit ist ferner darauf hinzuweisen, dass nach Art. 8 Abs. 2 der Charta personenbezogene Daten nur „für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage“ verarbeitet werden dürfen.

174 Zudem muss gemäß Art. 52 Abs. 1 Satz 1 der Charta jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Nach Art. 52 Abs. 1 Satz 2 der Charta dürfen Einschränkungen dieser Rechte und Freiheiten unter Wahrung des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

175 Zum letztgenannten Punkt ist hinzuzufügen, dass das Erfordernis einer gesetzlichen Grundlage für jede Einschränkung der Ausübung der Grundrechte bedeutet, dass die gesetzliche Grundlage für den Eingriff in die Grundrechte den Umfang der Einschränkung der Ausübung des betreffenden Rechts selbst festlegen muss (Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 139 und die dort angeführte Rechtsprechung).

176 Schließlich muss die fragliche, den Eingriff enthaltende Regelung, um dem Erfordernis der Verhältnismäßigkeit zu genügen, wonach sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das absolut Notwendige beschränken müssen, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut Notwendige beschränkt wird. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden (vgl. in diesem Sinne Gutachten 1/15 [PNR-Abkommen EU-Kanada] vom 26. Juli 2017, EU:C:2017:592, Rn. 140 und 141 sowie die dort angeführte Rechtsprechung).

177 Hierzu bestimmt Art. 45 Abs. 2 Buchst. a der DSGVO, dass die Kommission bei der Prüfung der Angemessenheit des von einem Drittland gebotenen Schutzniveaus u. a. „wirksame und durchsetzbare Rechte der betroffenen Person“, deren personenbezogene Daten übermittelt werden, berücksichtigt.

178 Im vorliegenden Fall ist die von der Kommission im DSS-Beschluss getroffene Feststellung, dass die Vereinigten Staaten ein Schutzniveau gewährleisteten, das dem in der Union durch die DSGVO im Licht der Art. 7 und 8 der Charta garantierten Niveau der Sache nach gleichwertig sei, u. a. mit der Begründung in Frage gestellt worden, dass die Eingriffe, die sich aus den auf Section 702 des FISA und die E.O. 12333 gestützten Überwachungsprogrammen ergäben, keinen Anforderungen unterlägen, mit denen unter Wahrung des Grundsatzes der Verhältnismäßigkeit ein Schutzniveau gewährleistet werde, das dem durch Art. 52 Abs. 1 Satz 2 der Charta garantierten Niveau der Sache nach gleichwertig sei. Daher ist zu prüfen, ob diese Überwachungsprogramme unter Einhaltung solcher Anforderungen durchgeführt werden, ohne dass vorab untersucht werden müsste, ob im genannten Drittland Bedingungen eingehalten werden, die den in Art. 52 Abs. 1 Satz 1 der Charta vorgesehenen Bedingungen der Sache nach gleichwertig sind.

179 Insoweit hat die Kommission im 109. Erwägungsgrund des DSS-Beschlusses zu den auf Section 702 des FISA gestützten Überwachungsprogrammen festgestellt, dass „d[er] FISC nach [dieser Vorschrift] keine individuellen Überwachungsmaßnahmen [autorisiert]; vielmehr genehmigt e[r] Überwachungsprogramme (wie PRISM oder UPSTREAM) auf der Grundlage jährlicher Zertifizierungen, die vom Justizminister und [vom] Director of National Intelligence vorgenommen werden“. Wie aus diesem Erwägungsgrund hervorgeht, zielt die vom FISC ausgeübte Kontrolle darauf ab, zu prüfen, ob diese Überwachungsprogramme dem Ziel entsprechen, Auslandsaufklärungsdaten zu erlangen, betrifft aber nicht die Frage, „ob die Personen vorschriftsgemäß als Zielpersonen für die Beschaffung von Auslandsaufklärungsdaten ausgewählt wurden“.

180 Demzufolge lässt Section 702 des FISA in keiner Weise erkennen, dass für die darin enthaltene Ermächtigung zur Durchführung von Überwachungsprogrammen zum Zweck der Auslandsaufklärung Einschränkungen bestehen. Genauso wenig ist erkennbar, dass für potenziell von diesen Programmen erfasste Nicht-US-Personen Garantien existieren. Unter diesen Umständen ist diese Vorschrift, wie der Generalanwalt in den Nrn. 291, 292 und 297 seiner Schlussanträge der Sache nach festgestellt hat, nicht geeignet, ein Schutzniveau zu gewährleisten, das dem durch die Charta – in ihrer Auslegung durch die in den Rn. 175 und 176 des vorliegenden Urteils wiedergegebene Rechtsprechung, wonach eine gesetzliche Grundlage für Eingriffe in Grundrechte, um dem Grundsatz der Verhältnismäßigkeit

zu genügen, den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen sowie klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen muss – garantierten Niveau der Sache nach gleichwertig ist.

181 Nach den Feststellungen im DSS-Beschluss müssen die auf Section 702 des FISA gestützten Überwachungsprogramme zwar unter Beachtung der aus der PPD-28 folgenden Anforderungen durchgeführt werden. Während die Kommission in den Erwägungsgründen 69 und 77 des DSS-Beschlusses hervorgehoben hat, dass solche Anforderungen für die amerikanischen Nachrichtendienste verbindlich seien, hat die amerikanische Regierung jedoch auf eine Frage des Gerichtshofs eingeräumt, dass die PPD-28 den betroffenen Personen keine Rechte verleihe, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden könnten. Folglich ist die PPD-28 nicht geeignet, ein Schutzniveau zu gewährleisten, das dem aus der Charta resultierenden Niveau der Sache nach gleichwertig wäre, entgegen den Anforderungen von Art. 45 Abs. 2 Buchst. a der DSGVO, wonach die Feststellung dieses Niveaus u. a. davon abhängt, ob die Personen, deren Daten in das fragliche Drittland übermittelt wurden, über wirksame und durchsetzbare Rechte verfügen.

182 Was die auf die E.O. 12333 gestützten Überwachungsprogramme anbelangt, geht aus den dem Gerichtshof vorliegenden Akten hervor, dass auch dieses Dekret keine Rechte verleiht, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können.

183 Hinzuzufügen ist, dass die PPD-28, die bei der Anwendung der in den beiden vorstehenden Randnummern genannten Programme zu beachten ist, die „‚Sammelerhebung' … einer relativ großen Menge von signalerfassenden Aufklärungsdaten unter Bedingungen, in denen die Intelligence Community keinen mit einer bestimmten Zielperson verbundenen Identifikator … für eine zielgerichtete Erhebung verwenden kann", erlaubt, wie dem in Anhang VI des DSS-Beschlusses enthaltenen Schreiben des Office of the Director of National Intelligence an das amerikanische Handelsministerium sowie an die International Trade Administration vom 21. Juni 2016 zu entnehmen ist. Hinsichtlich dieser im Rahmen der auf die E.O. 12333 gestützten Überwachungsprogramme bestehenden Möglichkeit, auf Daten während ihrer Übermittlung in die Vereinigten Staaten zuzugreifen, ohne dass dieser Zugriff irgendeiner gerichtlichen Kontrolle unterläge, besteht jedenfalls keine hinreichend klare und präzise Eingrenzung des Umfangs einer solchen Sammelerhebung personenbezogener Daten.

184 Folglich ist davon auszugehen, dass weder Section 702 des FISA noch die E.O. 12333 in Verbindung mit der PPD-28 den im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit bestehenden Mindestanforderungen genügen, so dass nicht angenommen werden kann, dass die auf diese Vorschriften gestützten Überwachungsprogramme auf das zwingend erforderliche Maß beschränkt sind.

185 Unter diesen Umständen sind die von der Kommission im DSS-Beschluss bewerteten Einschränkungen des Schutzes personenbezogener Daten, die sich daraus ergeben, dass die amerikanischen Behörden nach dem Recht der Vereinigten Staaten auf solche Daten, die aus der Union in die Vereinigten Staaten übermittelt werden, zugreifen und sie verwenden dürfen, nicht dergestalt geregelt, dass damit Anforderungen erfüllt würden, die den im Unionsrecht nach Art. 52 Abs. 1 Satz 2 der Charta bestehenden Anforderungen der Sache nach gleichwertig wären.

186 Was zweitens Art. 47 der Charta anbelangt, der ebenfalls für das in der Union erforderliche Schutzniveau maßgebend ist und dessen Einhaltung die Kommission feststellen muss, bevor sie einen Angemessenheitsbeschluss im Sinne von Art. 45 Abs. 1 der DSGVO erlässt, ist darauf hinzuweisen, dass nach Art. 47 Abs. 1 der Charta jede Person, deren unionsrechtlich garantierte Rechte oder Freiheiten verletzt worden sind, das Recht hat, nach Maßgabe der in diesem Artikel vorgesehenen

Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Nach Art. 47 Abs. 2 hat jede Person ein Recht darauf, dass ihre Sache vor einem unabhängigen und unparteiischen Gericht verhandelt wird.

187 Nach ständiger Rechtsprechung ist es dem Wesen eines Rechtsstaats inhärent, dass eine wirksame, zur Gewährleistung der Einhaltung des Unionsrechts dienende gerichtliche Kontrolle vorhanden sein muss. Daher verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz (Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 95 und die dort angeführte Rechtsprechung).

188 In diesem Rahmen verlangt Art. 45 Abs. 2 Buchst. a der DSGVO, dass die Kommission bei ihrer Prüfung der Angemessenheit des von einem Drittland gebotenen Schutzniveaus u. a. „wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden“, berücksichtigt. Insoweit wird im 104. Erwägungsgrund der DSGVO hervorgehoben, dass das Drittland „eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten und Mechanismen für eine Zusammenarbeit mit den Datenschutzbehörden der Mitgliedstaaten vorsehen [sollte]“ und dass „den betroffenen Personen … wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe eingeräumt werden [sollten]“.

189 Das Bestehen solcher wirksamer Rechtsbehelfe im betreffenden Drittland ist im Kontext einer Übermittlung personenbezogener Daten in dieses Drittland besonders wichtig. Wie aus dem 116. Erwägungsgrund der DSGVO hervorgeht, können die betroffenen Personen nämlich mit dem Problem konfrontiert sein, dass die Verwaltungsbehörden und die Gerichte der Mitgliedstaaten nicht über hinreichende Befugnisse und Mittel verfügen, um ihre Beschwerden, mit denen sie eine rechtswidrige Verarbeitung ihrer in das Drittland übermittelten Daten geltend machen, zweckdienlich zu bearbeiten, so dass die betroffenen Personen nicht umhin können, sich an die nationalen Behörden und Gerichte des Drittlands zu wenden.

190 Im vorliegenden Fall ist die von der Kommission im DSS-Beschluss getroffene Feststellung, dass die Vereinigten Staaten ein Schutzniveau gewährleisteten, das dem durch Art. 47 der Charta garantierten Niveau der Sache nach gleichwertig sei, u. a. mit der Begründung in Frage gestellt worden, dass die Einsetzung der Ombudsperson des Datenschutzschilds den von der Kommission selbst festgestellten Mängeln hinsichtlich des gerichtlichen Schutzes von Personen, deren personenbezogene Daten in dieses Drittland übermittelt würden, nicht abzuhelfen vermöge.

191 Hierzu hat die Kommission im 115. Erwägungsgrund des DSS-Beschlusses ausgeführt: „Auch wenn Privatpersonen, einschließlich Betroffene[n] in der [Union], eine Reihe von Rechtsschutzinstrumenten zur Verfügung steht, wenn sie aus Gründen der nationalen Sicherheit rechtswidrig (elektronisch) überwacht wurden, steht doch fest, dass zumindest einige Rechtsgrundlagen, die US-Nachrichtendienste nutzen können (z. B. [die] E.O. 12333), [davon nicht erfasst werden].“ Sie hat also in diesem 115. Erwägungsgrund hinsichtlich der E.O. 12333 das Fehlen jeglichen Rechtsbehelfs hervorgehoben. Nach der in Rn. 187 des vorliegenden Urteils wiedergegebenen Rechtsprechung steht eine solche Lücke im gerichtlichen Rechtsschutz gegen Eingriffe, die mit den auf dieses Präsidialdekret gestützten Aufklärungsprogrammen verbunden sind, der von der Kommission im DSS-Beschluss getroffenen Feststellung entgegen, dass das Recht der Vereinigten Staaten ein Schutzniveau gewährleiste, das dem durch Art. 47 der Charta garantierten Niveau der Sache nach gleichwertig sei.

192 Im Übrigen ist sowohl hinsichtlich der auf Section 702 des FISA gestützten als auch hinsichtlich der auf die E.O. 12333 gestützten Überwachungsprogramme in den Rn. 181 und 182 des vorliegenden Urteils festgestellt worden, dass weder die PPD-28 noch die E.O. 12333 den betroffenen Personen Rechte verleihen, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können, so dass diese Personen nicht über einen wirksamen Rechtsbehelf verfügen.

193 Die Kommission hat jedoch in den Erwägungsgründen 115 und 116 des DSS-Beschlusses festgestellt, dass aufgrund des von den amerikanischen Behörden geschaffenen Ombudsmechanismus, wie er in dem in Anhang III dieses Beschlusses enthaltenen Schreiben des amerikanischen Außenministers an die europäische Kommissarin für Justiz, Verbraucher und Gleichstellung vom 7. Juli 2016 beschrieben werde, sowie aufgrund der Funktion der Ombudsperson als „Senior Coordinator for International Information Technology Diplomacy“ davon ausgegangen werden könne, dass die Vereinigten Staaten ein Schutzniveau gewährleisteten, das dem durch Art. 47 der Charta garantierten Niveau der Sache nach gleichwertig sei.

194 Die Prüfung der Frage, ob der im DSS-Beschluss angeführte Ombudsmechanismus tatsächlich die von der Kommission festgestellten Einschränkungen des Rechts auf gerichtlichen Rechtsschutz auszugleichen vermag, muss nach den Anforderungen, die sich aus Art. 47 der Charta und der in Rn. 187 des vorliegenden Urteils wiedergegebenen Rechtsprechung ergeben, von dem Grundsatz ausgehen, dass Einzelne über die Möglichkeit verfügen müssen, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder die Berichtigung oder Löschung solcher Daten zu erwirken.

195 In dem in Rn. 193 des vorliegenden Urteils genannten Schreiben wurde die Ombudsperson des Datenschutzschilds zwar als „von den Nachrichtendiensten unabhängig“ beschrieben, aber weiter heißt es dort, dass sie „unmittelbar dem Außenminister [untersteht], der dafür Sorge trägt, dass [sie] ihre Aufgabe objektiv und frei von unzulässiger Einflussnahme erfüllt, die sich auf die zu erteilende Antwort auswirken kann“. Im Übrigen enthält der DSS-Beschluss, wie der Generalanwalt in Nr. 337 seiner Schlussanträge ausgeführt hat, über die Feststellung der Kommission in seinem 116. Erwägungsgrund hinaus, dass die Ombudsperson vom Außenminister ernannt werde und einen Posten im Außenministerium der Vereinigten Staaten bekleide, keinen Hinweis darauf, dass die Abberufung der Ombudsperson oder der Widerruf ihrer Ernennung mit besonderen Garantien versehen wäre, was Zweifel daran weckt, ob sie von der Exekutive unabhängig ist (vgl. in diesem Sinne Urteil vom 21. Januar 2020, Banco de Santander, C-274/14, EU:C:2020:17, Rn. 60 und 63 sowie die dort angeführte Rechtsprechung).

196 Desgleichen wird zwar im 120. Erwägungsgrund des DSS-Beschlusses festgestellt, dass sich die amerikanische Regierung dazu verpflichtet habe, dass der betroffene Teil der Nachrichtendienste jeden von der Ombudsperson des Datenschutzschilds festgestellten Verstoß gegen die geltenden Bestimmungen abstellen müsse, doch enthält er, wie der Generalanwalt in Nr. 338 seiner Schlussanträge hervorgehoben hat, keinen Hinweis darauf, dass die Ombudsperson ermächtigt wäre, gegenüber den Nachrichtendiensten verbindliche Entscheidungen zu treffen. Zudem werden in diesem Beschluss keine gesetzlichen Garantien angeführt, die mit dieser Verpflichtung einhergingen und auf die sich die betroffenen Personen berufen könnten.

197 Demnach eröffnet der im DSS-Beschluss genannte Ombudsmechanismus keinen Rechtsweg zu einem Organ, das den Personen, deren Daten in die Vereinigten Staaten übermittelt werden, Garantien böte, die den nach Art. 47 der Charta erforderlichen Garantien der Sache nach gleichwertig wären.

198 Daher hat die Kommission bei ihrer Feststellung in Art. 1 Abs. 1 des DSS-Beschlusses, dass die Vereinigten Staaten für personenbezogene Daten, die im Rahmen des EU-US-Datenschutzschilds aus der Union an Organisationen in diesem Drittland übermittelt würden, ein angemessenes Schutzniveau gewährleisteten, die Anforderungen verkannt, die sich aus Art. 45 Abs. 1 der DSGVO im Licht der Art. 7, 8 und 47 der Charta ergeben.

199 Daraus folgt, dass Art. 1 des DSS-Beschlusses mit Art. 45 Abs. 1 der DSGVO, ausgelegt im Licht der Art. 7, 8 und 47 der Charta, unvereinbar und somit ungültig ist.

200 Da Art. 1 des DSS-Beschlusses untrennbar mit dessen Art. 2 bis 6 sowie dessen Anhängen verbunden ist, führt seine Ungültigkeit zur Ungültigkeit des gesamten Beschlusses.

201 Nach alledem ist festzustellen, dass der DSS-Beschluss ungültig ist.

202 Zu der Frage, ob die Wirkungen dieses Beschlusses aufrechtzuerhalten sind, um die Entstehung eines rechtlichen Vakuums zu vermeiden (vgl. in diesem Sinne Urteil vom 28. April 2016, Borealis Polyolefine u. a., C-191/14, C-192/14, C-295/14, C-389/14 und C-391/14 bis C-393/14, EU:C:2016:311, Rn. 106), ist festzustellen, dass in Anbetracht von Art. 49 der DSGVO durch die Nichtigerklärung eines Angemessenheitsbeschlusses wie des DSS-Beschlusses jedenfalls kein solches rechtliches Vakuum entstehen kann. In dieser Vorschrift ist nämlich klar geregelt, unter welchen Voraussetzungen personenbezogene Daten in Drittländer übermittelt werden können, falls weder ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 der DSGVO vorliegt noch geeignete Garantien im Sinne ihres Art. 46 bestehen.

Kosten

203 Für die Parteien des Ausgangsverfahrens ist das Verfahren ein Zwischenstreit in dem beim vorlegenden Gericht anhängigen Rechtsstreit; die Kostenentscheidung ist daher Sache dieses Gerichts. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Aus diesen Gründen hat der Gerichtshof (Große Kammer) für Recht erkannt:

1. **Art. 2 Abs. 1 und 2 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) ist dahin auszulegen, dass eine zu gewerblichen Zwecken erfolgende Übermittlung personenbezogener Daten durch einen in einem Mitgliedstaat ansässigen Wirtschaftsteilnehmer an einen anderen, in einem Drittland ansässigen Wirtschaftsteilnehmer in den Anwendungsbereich dieser Verordnung fällt, ungeachtet dessen, ob die Daten bei ihrer Übermittlung oder im Anschluss daran von den Behörden des betreffenden Drittlands für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates verarbeitet werden können.**

2. **Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der Verordnung 2016/679 sind dahin auszulegen, dass die nach diesen Vorschriften erforderlichen geeigneten Garantien, durchsetzbaren Rechte und wirksamen Rechtsbehelfe gewährleisten müssen, dass die Rechte der Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden, ein Schutzniveau genießen, das dem in der Europäischen Union durch diese Verordnung im Licht der Charta der Grundrechte der Europäischen Union garantierten Niveau der Sache nach gleichwertig ist. Bei der insoweit im Zusammenhang mit einer solchen Übermittlung vorzunehmenden Beurteilung sind insbesondere die vertraglichen Regelungen zu berücksichtigen, die zwischen dem in der Europäischen Union ansässigen Verantwortlichen bzw. seinem dort ansässigen**

Auftragsverarbeiter und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, sowie, was einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten betrifft, die maßgeblichen Elemente der Rechtsordnung dieses Landes, insbesondere die in Art. 45 Abs. 2 der Verordnung 2016/679 genannten Elemente.

3. **Art. 58 Abs. 2 Buchst. f und j der Verordnung 2016/679 ist dahin auszulegen, dass die zuständige Aufsichtsbehörde, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, verpflichtet ist, eine auf Standarddatenschutzklauseln, die von der Kommission erarbeitet wurden, gestützte Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn diese Behörde im Licht aller Umstände dieser Übermittlung der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht, insbesondere nach den Art. 45 und 46 dieser Verordnung sowie nach der Charta der Grundrechte, erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, es sei denn, der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter hat die Übermittlung selbst ausgesetzt oder beendet.**

4. **Die Prüfung des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates in der durch den Durchführungsbeschluss (EU) 2016/2297 der Kommission vom 16. Dezember 2016 geänderten Fassung anhand der Art. 7, 8 und 47 der Charta der Grundrechte hat nichts ergeben, was seine Gültigkeit berühren könnte.**

5. **Der Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes ist ungültig.**

Unterschriften