# Urteil des EuGH vom 16. Juli 2020, Az. C-311/18 (Schremms II) mit Bezügen zu den Argumenten des Generalstaatsanwalts Henrik Saumandsgaard ØE

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

## Inhalt




| Dienstort | Telefon und Fax | elektronische Post | Internet |
|---|---|---|---|
| Rechenzentrum<br>c/o Universität Würzburg<br>Am Hubland Z 8<br>97074 Würzburg | Telefon<br>+49(0)931/31-84217<br>Telefax<br>+49(0)931/31-84217-0 | rz-stabsstelle-it-recht@uni-wuerzburg.de | https://www.rz.uni-wuerzburg.de/dienste/it-recht/ |

## 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 (Räum-

liche 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.

**Ausführungen des GA zu Rn. 93 EuGH:**

117. Die Art. 45 und 46 DSGVO sollen den Fortbestand des von dieser Verordnung gewährleisteten hohen Niveaus des Schutzes personenbezogener Daten gewährleisten, wenn diese aus der Union übermittelt werden. In Art. 44 („Allgemeine Grundsätze der Datenübermittlung“) DSGVO am Beginn von deren Kapitel V betreffend Übermittlungen personenbezogener Daten an Drittländer heißt es, dass alle Bestimmungen dieses Kapitels so anzuwenden sind, dass sichergestellt wird, dass das durch die DSGVO gewährleistete Schutzniveau im Fall einer Übermittlung in einen Drittstaat nicht untergraben wird(*44*). Durch diesen Grundsatz soll verhindert werden, dass die aus dem Unionsrecht fließenden Schutzstandards umgangen werden, indem personenbezogene Daten aus der Union in Drittländer übermittelt werden, um dort verarbeitet zu werden(*45*). Im Hinblick auf dieses Ziel ist es unerheblich, ob die Übermittlung auf einen Angemessenheitsbeschluss oder auf von dem Verantwortlichen u. a. durch Vertragsklauseln gebotene Garantien gestützt wird. Die Erfordernisse des Schutzes der durch die Charta garantierten Grundrechte sind nicht unterschiedlich je nachdem, auf welcher Rechtsgrundlage eine bestimmte Übermittlung stattfindet(*46*).

118. Dagegen unterscheidet sich die Art und Weise, wie der Fortbestand des hohen Schutzniveaus gewahrt wird, nach Maßgabe der Rechtsgrundlage für die Übermittlung.

119. Auf der einen Seite soll mit einem Angemessenheitsbeschluss festgestellt werden, dass das betreffende Drittland selbst ein dem vom Unionsrecht geforderten Schutzniveau der Sache nach gleichwertiges Schutzniveau sicherstellt. Der Erlass eines Angemessenheitsbeschlusses setzt voraus, dass die Kommission für ein bestimmtes Drittland zuvor das vom Recht und von der Praxis dieses Landes gewährleistete Schutzniveau anhand der in Art. 45 Abs. 3 DSGVO aufgeführten Faktoren beurteilt. Personenbezogene Daten können dann in dieses Drittland übermittelt werden, ohne dass der Verantwortliche dafür eine besondere Genehmigung benötigt.

120. Auf der anderen Seite soll, wie im folgenden Abschnitt näher auszuführen sein wird, mit den vom Verantwortlichen gebotenen Garantien ein hohes Schutzniveau sichergestellt werden, falls die im Bestimmungsdrittland verfügbaren Garantien unzureichend sind. So erlaubt zwar Art. 46 Abs. 1 DSGVO die Übermittlung personenbezogener Daten in Drittländer, die kein angemessenes Schutzniveau sicherstellen, dies allerdings nur dann, wenn geeignete Garantien durch andere Mittel geboten werden. Die von der Kommission erlassenen Standardvertragsklauseln sehen in dieser Hinsicht einen allgemeinen Mechanismus vor, der für sämtliche Übermittlungen unabhängig vom Bestimmungsdrittland und von dem dort gebotenen Schutzniveau gilt.

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.

**Ausführungen des GA zu Rn. 96 EuGH:**

113. In diesem Kontext wird der Gerichtshof mit dem ersten Teil der sechsten Frage gefragt, ob die Anwendung von „Standardvertragsklauseln“, die die Kommission gemäß Art. 26 Abs. 4 der Richtlinie 95/46 erlassen hat – und die den nunmehr in Art. 46 Abs. 2 Buchst. c DSGVO genannten „Standarddatenschutzklauseln“ entsprechen –, das Erreichen eines Schutzniveaus erlauben muss, das demselben Standard der „Gleichwertigkeit der Sache nach“ entspricht.

114. Hierzu sieht Art. 46 Abs. 1 DSGVO vor, dass der für die Verarbeitung Verantwortliche, falls kein Angemessenheitsbeschluss vorliegt, personenbezogene Daten nur in ein Drittland

übermitteln darf, „sofern [er] geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen“ (Hervorhebung nur hier)(*43*). Nach Art. 46 Abs. 2 Buchst. c DSGVO können sich diese Garantien u. a. aus von der Kommission erarbeiteten Standardschutzklauseln ergeben.

115. Wie der DPC, Herr Schrems und Irland bin ich der Ansicht, dass die in Art. 46 Abs. 1 DSGVO angesprochenen vom Verantwortlichen gebotenen „geeigneten Garantien“ sicherstellen müssen, dass die Rechte der Personen, deren Daten übermittelt werden, wie im Rahmen einer auf einen Angemessenheitsbeschluss gestützten Übermittlung auf einem Niveau geschützt werden müssen, das dem sich aus der DSGVO im Licht der Charta ergebenden Schutzniveau der Sache nach gleichwertig ist.

116. Dies folgt aus dem Zweck dieser Bestimmung und der Regelung, zu der sie gehört.

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.

**Ausführungen des GA zu Rn. 113 EuGH:**

147. Die zuständige Aufsichtsbehörde muss auch angemessen auf Verletzungen der Rechte der betroffenen Person reagieren, die sie gegebenenfalls zum Abschluss ihrer Untersuchung feststellt. Hierzu verfügt jede Aufsichtsbehörde nach Art. 58 Abs. 2 DSGVO über eine große Bandbreite von Mitteln – die verschiedenen Befugnisse zum Erlass der in dieser aufgeführten Abhilfemaßnahmen – zur Erfüllung der ihr zugewiesenen Aufgabe(58).

148. Die Wahl des wirksamsten Mittels steht zwar im Ermessen der zuständigen Aufsichtsbehörde unter Berücksichtigung aller Umstände der jeweiligen Übermittlung, doch muss diese Behörde den ihr übertragenen Überwachungsauftrag umfassend erfüllen. Gegebenenfalls muss sie die Übermittlung aussetzen, wenn sie nach dieser Untersuchung zu dem Schluss kommt, dass die Standardvertragsklauseln nicht eingehalten werden und ein geeigneter Schutz der übermittelten Daten nicht durch andere Mittel sichergestellt werden kann, wenn der Datenexporteur die Übermittlung nicht selbst beendet hat.

149. Diese Auslegung wird durch Art. 58 Abs. 4 DSGVO bestätigt, wonach die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit Art. 47 der Charta erfolgt. In Art. 78 Abs. 1 und 2 DSGVO wird zudem jeder Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf zuerkannt, wenn eine Aufsichtsbehörde einen sie betreffenden rechtsverbindlichen Beschluss erlassen oder sich nicht mit ihrer Beschwerde befasst hat(59).

150. Diese Bestimmungen besagen, wie Herr Schrems, die BSA, Irland, die polnische Regierung und die Regierung des Vereinigten Königreichs sowie die Kommission vortragen, dass eine Entscheidung, mit der es eine Aufsichtsbehörde ablehnt, auf Antrag einer Person, die geltend macht, sie betreffende Daten könnten in einem Drittland unter Verletzung ihrer Grundrechte verarbeitet werden, eine Übermittlung dorthin zu untersagen oder auszusetzen, Gegenstand eines gerichtlichen Rechtsbehelfs sein kann. Die Anerkennung eines Rechts auf einen solchen Rechtsbehelf setzt aber das Bestehen einer gebundenen Zuständigkeit und nicht eines bloßen Ermessens auf Seiten der Aufsichtsbehörden voraus. Zudem haben Herr Schrems und die Kommission zu Recht darauf hingewiesen, dass die Ausübung einer wirksamen gerichtlichen Kontrolle verlangt, dass die den angefochtenen Rechtsakt erlassende Behörde diesen angemessen begründet(60). Diese Begründungspflicht erstreckt sich meines Erachtens auf die Entscheidung der Aufsichtsbehörden, von ihren Befugnissen nach Art. 58 Abs. 2 DSGVO Gebrauch zu machen oder nicht.

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.

**Ausführungen des GA zu Rn. 134 EuGH:**

125. Wie der DPC, Herr Schrems, die BSA, Irland, die französische, die österreichische, die polnische und die portugiesische Regierung sowie die Kommission ausgeführt haben, können die in den Standardvertragsklauseln enthaltenen Garantien abgeschwächt oder sogar beseitigt werden, wenn das Recht des Bestimmungsdrittlands dem Datenimporteur Verpflichtungen

auferlegt, die dem zuwiderlaufen, was diese Klauseln vorschreiben. Der rechtliche Kontext im Bestimmungsdrittland kann also je nach den konkreten Umständen der Übermittlung(48) die Erfüllung der in diesen Klauseln vorgesehenen Verpflichtungen unmöglich machen.

126. Unter diesen Umständen beruht, wie Herr Schrems und die Kommission hervorgehoben haben, der in Art. 46 Abs. 2 Buchst. c DSGVO vorgesehene vertragliche Mechanismus darauf, dass das Verantwortungsbewusstsein des Datenexporteurs und in zweiter Linie der Aufsichtsbehörden geweckt wird. In jedem Einzelfall, für jede einzelne Übermittlung, hat der Verantwortliche oder andernfalls die Aufsichtsbehörde zu prüfen, ob das Recht des Bestimmungsdrittlands der Erfüllung der Standardklauseln und damit einem geeigneten Schutz der übermittelten Daten entgegensteht, so dass die Übermittlung untersagt oder ausgesetzt werden muss.

127. Daher führt meiner Ansicht nach der Umstand, dass der Beschluss 2010/87 und die in ihm aufgeführten Standardvertragsklauseln die Behörden des Bestimmungsdrittlands nicht bindet, als solcher nicht zur Ungültigkeit dieses Beschlusses. Die Vereinbarkeit des Beschlusses 2010/87 mit den Art. 7, 8 und 47 der Charta hängt meines Erachtens davon ab, ob hinreichend solide Mechanismen bestehen, die sicherstellen, dass die auf die Standardvertragsklauseln gestützten Übermittlungen im Fall von Verstößen gegen diese Klauseln oder der Unmöglichkeit ihrer Beachtung ausgesetzt oder untersagt werden.

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.

**Ausführungen des GA zu Rn. 141 EuGH:**

130. Demgemäß verpflichtet sich der Datenimporteur nach Klausel 5 Buchst. a, die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den Standardvertragsklauseln zu verarbeiten. Für den Fall, dass der Importeur diese Klauseln nicht einhalten kann, erklärt er sich bereit, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten(*49*).

131. Nach Fn. 1 zu Klausel 5 widerspricht es nicht den Standardklauseln, wenn der Datenimporteur den zwingenden Erfordernissen des für ihn geltenden nationalen Rechts nachkommt, sofern diese nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Art. 13 Abs. 1 der Richtlinie 95/46 (dessen Inhalt im Wesentlichen in Art. 23 Abs. 1 DSGVO übernommen worden ist) aufgelisteten Interessen erforderlich ist, zu denen die öffentliche Sicherheit und die Sicherheit des Staates gehören. Umgekehrt wird es als ein Verstoß gegen diese Klauseln behandelt, wenn diese nicht beachtet werden, um einer aus

dem Recht des Bestimmungsdrittlands folgenden entgegenstehenden Verpflichtung nachzukommen, die über das hinausgeht, was zum Schutz eines von der Union anerkannten legitimen Interesses verhältnismäßig ist.

132. Meines Erachtens kann, wie Herr Schrems und die Kommission geltend gemacht haben, Klausel 5 Buchst. a nicht dahin ausgelegt werden, dass die Aussetzung der Übermittlung oder der Rücktritt vom Vertrag im Fall des Verstoßes gegen die Standardvertragsklauseln nur eine Option ist. In dieser Klausel ist zwar nur von einem dahin gehenden Recht des Datenexporteurs die Rede, doch ist dieser Wortlaut in dem vertraglichen Rahmen zu verstehen, in den er sich einfügt. Das dem Datenexporteur in seinen zweiseitigen Beziehungen zum Datenimporteur das Recht zusteht, die Übermittlung auszusetzen oder vom Vertrag zurückzutreten, wenn Letzterer nicht in der Lage ist, die Standardklauseln einzuhalten, tut der Verpflichtung des Exporteurs, angesichts der aus der DSGVO folgenden Erfordernisse des Schutzes der Rechte der betroffenen Personen so vorzugehen, keinen Abbruch. Jede andere Auslegung zöge die Ungültigkeit des Beschlusses 2010/87 nach sich, da sich die Übermittlung mit den in ihm vorgesehenen Vertragsklauseln nicht mit den „geeigneten Garantien“ versehen ließe, wie es in Art. 46 Abs. 1 DSGVO im Licht der Bestimmungen der Charta verlangt wird(*50*).

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 Aufsichts-

behörde 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.

**Ausführungen des GA zu Rn. 160 EuGH:**

175. Das Vorbringen von Herrn Schrems stellt die von der Kommission im „Datenschutzschild"-Beschluss getroffene Feststellung in Frage, dass die Vereinigten Staaten in Anbetracht der Beschränkungen, die für den Zugriff auf diese Daten für und ihre Verwendung durch die amerikanischen Nachrichtendienste bestünden, ein angemessenes Schutzniveau für die gemäß diesem Beschluss übermittelten Daten sicherstellten(*71*). Auch mit den vom DPC vorläufig(*72*) wie auch den vom vorlegenden Gericht im Rahmen seiner Fragen 4, 5 und 10 zum Ausdruck gebrachten Bedenken wird indirekt die Begründetheit dieser Feststellung in Zweifel gezogen.

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.

**Ausführungen des GA zu Rn. 180 EuGH:**

290. Der Gerichtshof hat wiederholt hervorgehoben, dass die in den Art. 7 und 8 der Charta verankerten Rechte keine uneingeschränkte Geltung beanspruchen können, sondern im Hinblick auf ihre gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden müssen(174). Wie Facebook Ireland ausgeführt hat, gehört zu diesen anderen Rechten das in Art. 6 der Charta garantierte Recht auf Sicherheit.

291. Nach ebenfalls ständiger Rechtsprechung muss jeder Eingriff in die Ausübung der in den Art. 7 und 8 der Charta garantierten Rechte einer strikten Verhältnismäßigkeitskontrolle unterliegen(175).

292. Nach dem Urteil Schrems ist insbesondere „[n]icht auf das absolut Notwendige beschränkt … eine Regelung, die generell die Speicherung aller personenbezogenen Daten … gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen“(176).

293. Der Gerichtshof hat auch entschieden, dass der Zugang außer in hinreichend begründeten Eilfällen einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen sein muss, deren Entscheidung den Zugriff auf die Daten und ihre

Verwendung auf das beschränken soll, was zur Erreichung des angestrebten Ziels absolut erforderlich ist(177).

294. In Art. 23 Abs. 2 DSGVO ist eine Reihe von Garantien festgelegt, die ein Mitgliedstaat vorsehen muss, wenn er von den Bestimmungen dieser Verordnung abweicht. Die eine solche Abweichung gestattende Regelung muss Bestimmungen u. a. zu den Zwecken der Verarbeitung, zum Umfang der Abweichung, zu den Garantien, mit denen Missbräuchen vorgebeugt werden soll, und zum Recht der betroffenen Personen auf Unterrichtung über die Abweichung enthalten, sofern dies nicht dem Zweck der Abweichung abträglich ist.

295. Herr Schrems meint, Section 702 FISA sei nicht mit hinreichenden Garantien gegen die Gefahren von Missbrauch und unrechtmäßigem Zugriff auf die Daten versehen. Insbesondere sei die Wahl der Kriterien nicht ausreichend geregelt, so dass diese Bestimmung keine Sicherheit vor einem generellen Zugriff auf den Inhalt der Kommunikation biete.

296. Die Regierung der Vereinigten Staaten und die Kommission machen demgegenüber geltend, Section 702 FISA begrenze die Wahl der Selektoren durch objektive Kriterien, da diese Bestimmung nur die Sammlung von Daten der elektronischen Kommunikation von Nicht-US-Personen, die sich außerhalb der Vereinigten Staaten befänden, zur Erlangung von Informationen im Bereich der Auslandsaufklärung erlaube.

297. Meines Erachtens darf bezweifelt werden, ob diese Kriterien für die Wahl der Selektoren hinreichend klar und genau sind und ob ausreichende Garantien zur Vorbeugung gegen Missbrauchsgefahren bestehen.

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.

**Ausführungen des GA zu Rn. 195 und Rn. 196 EuGH:**

*333. Dem 116. Erwägungsgrund des „Datenschutzschild"-Beschlusses zufolge soll der in Anhang III A dieses Beschlusses beschriebene Ombudsmechanismus den Lücken im gerichtlichen Rechtsschutz der Personen abhelfen, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden.*

*334. Wie die Regierung der Vereinigten Staaten ausgeführt hat, hängt die Zulässigkeit einer Beschwerde bei der Ombudsperson nicht von der Einhaltung von Regeln betreffend die Klagebefugnis ab, die den für den Zugang zu den amerikanischen Gerichten geltenden ähneln. Nach dem 119. Erwägungsgrund dieses Beschlusses setzt die Befassung der Ombudsperson nicht den Nachweis durch den Betroffenen voraus, dass die Regierung der Vereinigten Staaten auf die ihn betreffenden personenbezogenen Daten zugegriffen hat.*

*335. Wie der DPC, Herr Schrems, die polnische und die portugiesische Regierung sowie das EPIC bezweifle auch ich, dass dieser Mechanismus die Unzulänglichkeiten des Rechtsschutzes ausgleichen kann, der den Personen geboten wird, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden.*

*336. Zunächst kann zwar ein außergerichtlicher Rechtsbehelfsmechanismus einen wirksamen Rechtsbehelf im Sinne von Art. 47 EMRK darstellen, doch ist dies insbesondere nur dann der Fall, wenn das fragliche Organ eine gesetzliche Grundlage hat und die Voraussetzung der Unabhängigkeit erfüllt(213).*

*337. Aus dem „Datenschutzschild"-Beschluss geht indes hervor, dass der auf der PPD 28(214) beruhende Ombudsmechanismus keine gesetzliche Grundlage hat. Die Ombudsperson wird vom Außenminister benannt und gehört dem Außenministerium der Vereinigten Staaten*

*an(215). Dieser Beschluss enthält keinen Hinweis darauf, dass die Abberufung der Ombudsperson oder der Widerruf ihrer Benennung mit besonderen Garantien versehen wäre(216). Obwohl die Ombudsperson als unabhängig von der „Intelligence Community“ (Gemeinschaft der Nachrichtendienste) dargestellt wird, ist sie dem Außenminister unterstellt und daher nicht unabhängig von der Exekutive(217).*

*338. Sodann hängt die Wirksamkeit eines außergerichtlichen Rechtsbehelfs meines Erachtens ebenfalls davon ab, ob das betreffende Organ verbindliche und mit Gründen versehene Entscheidungen erlassen kann. Der „Datenschutzschild“-Beschluss enthält keinen Hinweis darauf, dass die Ombudsperson derartige Entscheidungen erlässt. In ihm wird nicht festgestellt, dass die Einrichtung der Ombudsperson den Beschwerdeführern erlaubt, Auskunft über die sie betreffenden Daten zu erhalten und sie berichtigen oder löschen zu lassen, und dass die Ombudsperson den durch eine Überwachungsmaßnahme geschädigten Personen eine Entschädigung gewährt. Insbesondere wird nach Anhang III A Buchst. e dieses Beschlusses „[d]urch die Ombudsstelle … weder bestätigt noch bestritten, dass die betreffende Privatperson Ziel einer Überwachungsmaßnahme war, noch bestätigt die Ombudsstelle die spezielle Abhilfe, die geleistet wurde“(218). Die amerikanische Regierung hat sich zwar dazu verpflichtet, dass der betroffene Teil der Nachrichtendienste jeden von der Ombudsperson festgestellten Verstoß gegen die geltenden Bestimmungen abstellen muss(219), doch werden in diesem Beschluss keine gesetzlichen Garantien angeführt, die mit dieser Verpflichtung einhergehen und auf die sich die betroffenen Personen berufen könnten.*

*339. Folglich wird mit der Einrichtung der Ombudsperson meines Erachtens kein Rechtsbehelf vor einem unabhängigen Organ geschaffen, der den Personen, deren Daten übermittelt werden, eine Möglichkeit bietet, ihr Recht auf Auskunft über diese Daten geltend zu machen oder etwaige Verstöße der Nachrichtendienste gegen die geltenden Bestimmungen zu beanstanden.*

*340. Schließlich setzt nach der Rechtsprechung die Wahrung des in Art. 47 der Charta gewährleisteten Rechts voraus, dass die Entscheidung einer Verwaltungsbehörde, die die Voraussetzungen der Unabhängigkeit und Unparteilichkeit selbst nicht erfüllt, einer späteren Kontrolle durch ein Gericht unterliegt, das insbesondere befugt sein muss, sich mit allen relevanten Fragen zu befassen(220). Nach den Angaben im „Datenschutzschild“-Beschluss sind die Entscheidungen der Ombudsperson jedoch nicht Gegenstand einer unabhängigen gerichtlichen Kontrolle.*

*341. Unter diesen Umständen halte ich es, ebenso wie der DPC, Herr Schrems, das EPIC sowie die polnische und die portugiesische Regierung, für fraglich, ob der von der Rechtsordnung der Vereinigten Staaten gebotene gerichtliche Rechtsschutz für Personen, deren Daten*

*aus der Union dorthin übermittelt werden, dem sich aus der DSGVO im Licht von Art. 47 der Charta und Art. 8 EMRK ergebenden Rechtsschutz der Sache nach gleichwertig ist.*

*342. Nach alledem habe ich Zweifel an der Vereinbarkeit des „Datenschutzschild"-Beschlusses mit Art. 45 Abs. 1 DSGVO im Licht der Art. 7, 8 und 47 der Charta sowie des Art. 8 EMRK.*

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.

## Entscheidung

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.**

## Lizenzhinweis



[1] David Weihbrecht unterstützt die Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen, c/o Universität Würzburg, geleitet von Johannes Nehlsen.