EuGH Urteil vom 6.10.2015, C-362/14 – *Max Schrems ./. Data Protection Commissioner*

Fundstellen: ECLI:EU:C:2015:650 = jusIT 2015/87, 209 = RdW 2015/591, 691 (Retter/Marko) = RdW 2015/612, 721 = Dako 2015/60, 115 (*Schrems*) = jusIT 2015/95, 234 (*Jahnel*) = jusIT 2015/97, 244

1. Die gesamte Entscheidung der Kommission 2000/520/EG vom 26. Juli 2000 über die Angemessenheit der Grundsätze des „Safe Harbor", insbesondere für den Datenaustausch mit den USA wird für ungültig erklärt.
2. Art. 25 Abs 6 der Datenschutz-RL (RL 95/46/EG) ist im Licht der Art 7, 8 und 47 der Charta der Grundrechte der Europäischen Union (GRC) dahin auszulegen, dass Kommissions-Entscheidung 2000/520/EG eine Prüfung der Unzulässigkeit einer Datenübermittlung außerhalb des EWR/EU-Raumes im Einzelfall weder obsolet macht noch (ver-)hindert.

Leitsätze verfasst von Hon.-Prof. Dr. *Clemens Thiele*, LL.M.

In der Rechtssache C-362/14 betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom High Court (Irland) mit Entscheidung vom 17. Juli 2014, beim Gerichtshof eingegangen am 25. Juli 2014, in dem Verfahren Maximillian Schrems gegen Data Protection Commissioner, Beteiligte: Digital Rights Ireland Ltd, erlässt

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten V. Skouris, des Vizepräsidenten K. Lenaerts, des Kammerpräsidenten A. Tizzano, der Kammerpräsidentin R. Silva de Lapuerta, der Kammerpräsidenten T. von Danwitz (Berichterstatter) und S. Rodin, der Kammerpräsidentin K. Jürimäe, der Richter A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský und D. Sváby, der Richterin M. Berger sowie der Richter F. Biltgen und C. Lycourgos, Generalanwalt: Y. Bot, Kanzler: L. Hewlett, Hauptverwaltungsrätin, aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 24. März 2015, unter Berücksichtigung der Erklärungen von Herrn Schrems, vertreten durch N. Travers, SC, P. O'Shea, BL, und G. Rudden, Solicitor, sowie durch Rechtsanwalt H. Hofmann, des Data Protection Commissioner, vertreten durch P. McDermott, BL, sowie S. More O'Ferrall und D. Young, Solicitors, der Digital Rights Ireland Ltd, vertreten durch F. Crehan, BL, sowie S. McGarr und E. McGarr, Solicitors, Irlands, vertreten durch A. Joyce, B. Counihan und E. Creedon als Bevollmächtigte im Beistand von D. Fennelly, BL, der belgischen Regierung, vertreten durch J.-C. Halleux und C. Pochet als Bevollmächtigte, der tschechischen Regierung, vertreten durch M. Smolek und J. Vlácil als Bevollmächtigte, der italienischen Regierung, vertreten durch G. Palmieri als Bevollmächtigte im Beistand von P. Gentili, avvocato dello Stato, der österreichischen Regierung, vertreten durch G. Hesse und G. Kunnert als Bevollmächtigte, der polnischen Regierung, vertreten durch M. Kamejsza, M. Pawlicka und B. Majczyna als Bevollmächtigte, der slowenischen Regierung, vertreten durch A. Grum und V. Klemenc als Bevollmächtigte, der Regierung des Vereinigten Königreichs, vertreten durch L. Christie und J. Beeko als Bevollmächtigte im Beistand von J. Holmes, Barrister, des Europäischen Parlaments, vertreten durch D. Moore, A. Caiola und M. Pencheva als Bevollmächtigte, der Europäischen Kommission, vertreten durch B. Schima, B. Martenczuk, B. Smulders und J. Vondung als Bevollmächtigte, des Europäischen Datenschutzbeauftragten (EDSB), vertreten durch C. Docksey, A. Buchta und V. Pérez Asinari als Bevollmächtigte, nch Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 23. September 2015 folgendes

Urteil

1 Das Vorabentscheidungsersuchen betrifft die Auslegung, anhand der Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta), der Art. 25 Abs 6 und 28 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281, S. 31) in der durch die Verordnung (EG) Nr. 1882/2003 des Europäischen Parlaments und des Rates vom 29. September 2003 (ABl. L 284, S. 1) geänderten Fassung (im Folgenden: Richtlinie 95/46) sowie, der Sache nach, die Gültigkeit der Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46 über die Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglichen "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (ABl. L 215, S. 7).

2 Dieses Ersuchen ergeht im Rahmen eines Rechtsstreits zwischen Herrn Schrems und dem Data Protection Commissioner (Datenschutzbeauftragter, im Folgenden: Commissioner) wegen dessen Weigerung, eine von Herrn Schrems eingelegte Beschwerde zu prüfen, die sich dagegen richtet, dass die Facebook Ireland Ltd (im Folgenden: Facebook Ireland) personenbezogene Daten ihrer Nutzer in die Vereinigten Staaten übermittelt und auf dort befindlichen Servern speichert.

Rechtlicher Rahmen

Richtlinie 95/46

3 Die Erwägungsgründe 2, 10, 56, 57, 60, 62 und 63 der Richtlinie 95/46 lauten:

"(2) Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum ... Wohlergehen der Menschen beizutragen.

...

(10) Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und -freiheiten, insbesondere des auch in Artikel 8 der [am 4. November 1950 in Rom unterzeichneten] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern muss im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.

...

(56) Grenzüberschreitender Verkehr von personenbezogenen Daten ist für die Entwicklung des internationalen Handels notwendig. Der in der Gemeinschaft durch diese Richtlinie gewährte Schutz von Personen steht der Übermittlung personenbezogener Daten in Drittländer, die ein angemessenes Schutzniveau aufweisen, nicht entgegen. Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, ist unter Berücksichtigung aller Umstände im Hinblick auf eine Übermittlung oder eine Kategorie von Übermittlungen zu beurteilen.

(57) Bietet hingegen ein Drittland kein angemessenes Schutzniveau, so ist die Übermittlung personenbezogener Daten in dieses Land zu untersagen.

...

(60) Übermittlungen in Drittstaaten dürfen auf jeden Fall nur unter voller Einhaltung der Rechtsvorschriften erfolgen, die die Mitgliedstaaten gemäß dieser Richtlinie, insbesondere gemäß Artikel 8, erlassen haben.
...
(62) Die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten ist ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten.
(63) Diese Stellen sind mit den notwendigen Mitteln für die Erfüllung dieser Aufgabe auszustatten, d. h. Untersuchungs- und Einwirkungsbefugnissen, insbesondere bei Beschwerden, sowie Klagerecht. ...
4 Die Artikel 1, 2, 25, 26, 28 und 31 der Richtlinie 95/46 bestimmen:
"Artikel 1

Gegenstand der Richtlinie

(1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten....

Artikel 2
Begriffsbestimmungen
Im Sinne dieser Richtlinie bezeichnet der Ausdruck
a) 'personenbezogene Daten': alle Informationen über eine bestimmte oder bestimmbare natürliche Person ('betroffene Person'); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;
b) 'Verarbeitung personenbezogener Daten' ('Verarbeitung') jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;...
d) 'für die Verarbeitung Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden;...

Artikel 25

Grundsätze

(1) Die Mitgliedstaaten sehen vor, dass die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser

Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt.

(3) Die Mitgliedstaaten und die Kommission unterrichten einander über die Fälle, in denen ihres Erachtens ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

(4) Stellt die Kommission nach dem Verfahren des Artikels 31 Absatz 2 fest, dass ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels aufweist, so treffen die Mitgliedstaaten die erforderlichen Maßnahmen, damit keine gleichartige Datenübermittlung in das Drittland erfolgt.

(5) Zum geeigneten Zeitpunkt leitet die Kommission Verhandlungen ein, um Abhilfe für die gemäß Absatz 4 festgestellte Lage zu schaffen.

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

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

Artikel 26

Ausnahmen

(1) Abweichend von Artikel 25 sehen die Mitgliedstaaten vorbehaltlich entgegenstehender Regelungen für bestimmte Fälle im innerstaatlichen Recht vor, dass eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, vorgenommen werden kann, sofern

a) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat oder

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

c) die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll, oder

d) die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist oder

e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist oder

f) die Übermittlung aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen

können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.
(2) Unbeschadet des Absatzes 1 kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland genehmigen, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben.
(3) Der Mitgliedstaat unterrichtet die Kommission und die anderen Mitgliedstaaten über die von ihm nach Absatz 2 erteilten Genehmigungen.
Legt ein anderer Mitgliedstaat oder die Kommission einen in Bezug auf den Schutz der Privatsphäre, der Grundrechte und [der Grundfreiheiten] der Personen hinreichend begründeten Widerspruch ein, so erlässt die Kommission die geeigneten Maßnahmen nach dem Verfahren des Artikels 31 Absatz 2. Die Mitgliedstaaten treffen die aufgrund des Beschlusses der Kommission gebotenen Maßnahmen....

Artikel 28

Kontrollstelle
(1) Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen.
Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.
(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.
(3) Jede Kontrollstelle verfügt insbesondere über:
- Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;
- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;
- das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.
Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.
(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.
Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, dass eine Überprüfung stattgefunden hat....
(6) Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gemäß Absatz 3 übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht,

das auf die jeweilige Verarbeitung anwendbar ist. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden....

Artikel 31
...
(2) Wird auf diesen Artikel Bezug genommen, so gelten die Artikel 4 und 7 des Beschlusses 1999/468/EG [des Rates vom 28. Juni 1999 zur Festlegung der Modalitäten für die Ausübung der der Kommission übertragenen Durchführungsbefugnisse (ABl. L 184, S. 23)] unter Beachtung von dessen Artikel 8. ..."

Entscheidung 2000/520

5 Die Entscheidung 2000/520 wurde von der Kommission auf der Grundlage von Art. 25 Abs 6 der Richtlinie 95/46 erlassen.

6 Die Erwägungsgründe 2, 5 und 8 dieser Entscheidung lauten:

"(2) Die Kommission kann feststellen, dass ein Drittland ein angemessenes Datenschutzniveau gewährleistet. In diesem Fall können personenbezogene Daten aus den Mitgliedstaaten übermittelt werden, ohne dass zusätzliche Garantien erforderlich sind.

...

(5) Das durch diese Entscheidung anerkannte angemessene Schutzniveau für die Übermittlung von Daten aus der Gemeinschaft in die Vereinigten Staaten sollte erreicht sein, wenn die Organisationen die 'Grundsätze des ´sicheren Hafens´ zum Datenschutz' für den Schutz personenbezogener Daten, die aus einem Mitgliedstaat in die Vereinigten Staaten übermittelt werden (im Folgenden 'die Grundsätze' genannt) sowie die 'Häufig gestellten Fragen' ('Frequently Asked Questions', im Folgenden 'FAQ' genannt) beachten, die Leitlinien für die Umsetzung der von der Regierung der Vereinigten Staaten von Amerika am 21. Juli 2000 veröffentlichten Grundsätze darstellen. Die Organisationen müssen ferner ihre Geschäftsbedingungen zum Datenschutz offen legen und der Zuständigkeit der Federal Trade Commission (FTC) gemäß Abschnitt 5 des Federal Trade Commission Act, der unlautere und irreführende Handlungen und Praktiken, die im Handel erfolgen oder die den Handel beeinträchtigen, verbietet, bzw. der Zuständigkeit anderer gesetzlicher Organe unterliegen, die die Einhaltung der entsprechend den FAQ umgesetzten Grundsätze effektiv gewährleisten.

...

(8) Im Interesse der Transparenz und um die Fähigkeit der zuständigen Behörden in den Mitgliedstaaten zu erhalten, den Schutz von Personen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten, ist es ungeachtet der Feststellung des angemessenen Schutzniveaus notwendig, in dieser Entscheidung die besonderen Umstände zu nennen, unter denen die Aussetzung bestimmter Datenübermittlungen gerechtfertigt sein sollte."

7 Die Art. 1 bis 4 der Entscheidung 2000/520 lauten:

"Artikel 1

(1) Es wird davon ausgegangen, dass die dieser Entscheidung als Anhang I beigefügten 'Grundsätze des ´sicheren Hafens´ zum Datenschutz', im Folgenden 'die Grundsätze' genannt, die gemäß den in den vom US-Handelsministerium am 21. Juli 2000 herausgegebenen, dieser Entscheidung als Anhang II beigefügten, 'Häufig gestellten Fragen' (FAQ) enthaltenen Leitlinien umgesetzt werden, für alle unter die Richtlinie 95/46/EG fallenden Tätigkeiten ein im Sinne des Artikels 25 Absatz 2 dieser Richtlinie angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die von der Europäischen Union an in den Vereinigten Staaten niedergelassene Organisationen übermittelt werden, unter Berücksichtigung folgender vom US-Handelsministerium veröffentlichter Dokumente:

a) die 'sicherer Hafen Durchsetzungsmechanismen' (Anhang III),

b) ein Memorandum über Entschädigungen für die Verletzung der Privatsphäre und ausdrückliche Ermächtigungen gemäß dem US-Recht (Anhang IV),

c) ein Schreiben der Federal Trade Commission (Anhang V),

d) ein Schreiben des US-Verkehrsministeriums (Anhang VI).

(2) Im Hinblick auf jede Datenübermittlung müssen folgende Voraussetzungen erfüllt sein:

a) Die Organisation, die die Daten erhält, hat sich eindeutig und öffentlich verpflichtet, die Grundsätze einzuhalten, die entsprechend den FAQ umgesetzt wurden; und

b) die Organisation unterliegt den gesetzlichen Befugnissen einer in Anhang VII dieser Entscheidung aufgeführten staatlichen Einrichtung in den Vereinigten Staaten, die berechtigt ist, im Fall der Nichtbeachtung der Grundsätze, die entsprechend den FAQ umgesetzt wurden, Beschwerden zu prüfen und Abhilfe wegen unlauterer und irreführender Praktiken sowie Schadenersatz für Privatpersonen zu erwirken, und zwar ungeachtet des Landes, in dem sie ihren Wohnsitz haben, oder ihrer Nationalität.

(3) Die Voraussetzungen des Absatzes 2 gelten ab dem Zeitpunkt als erfüllt, zu dem die Organisation, die ihren Beitritt zu den entsprechend den FAQ umgesetzten Grundsätzen bescheinigt, dem Handelsministerium der USA (oder der von ihm benannten Stelle) die öffentliche Bekanntgabe ihrer Verpflichtung nach Absatz 2 Buchstabe a) und die Identität der staatlichen Einrichtung nach Absatz 2 Buchstabe b) mitteilt.

Artikel 2

Die vorliegende Entscheidung betrifft nur die Angemessenheit des Schutzes, der in den Vereinigten Staaten nach den entsprechend den FAQ umgesetzten Grundsätzen gewährt wird, um die Anforderungen des Artikels 25 Absatz 1 der Richtlinie 95/46/EG zu erfüllen. Die Anwendung anderer Bestimmungen der Richtlinie, die sich auf die Verarbeitung personenbezogener Daten in den Mitgliedstaaten beziehen, einschließlich Artikel 4, [bleibt] von dieser Entscheidung unberührt.

Artikel 3

(1) Ungeachtet ihrer Befugnisse, tätig zu werden, um die Einhaltung einzelstaatlicher Vorschriften, die gemäß anderen Bestimmungen als denjenigen des Artikels 25 der Richtlinie 95/46/EG erlassen wurden, zu gewährleisten, können die zuständigen Behörden in den

Mitgliedstaaten ihre bestehenden Befugnisse ausüben, zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung an eine Organisation auszusetzen, die den Grundsätzen, die entsprechend den FAQ umgesetzt wurden, beigetreten ist, wenn

a) die in Anhang VII dieser Entscheidung erwähnte staatliche Einrichtung in den Vereinigten Staaten oder eine unabhängige Instanz im Sinne von Buchstabe a) des in Anhang I dieser Entscheidung erwähnten Durchsetzungsgrundsatzes feststellt, dass die betreffende Organisation die Grundsätze, die entsprechend den FAQ umgesetzt wurden, verletzt oder

b) eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden; wenn Grund zur Annahme besteht, dass die jeweilige Durchsetzungsinstanz nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den Fall zu lösen; wenn die fortgesetzte Datenübermittlung für die betroffenen Personen das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde und wenn die zuständigen Behörden in den Mitgliedstaaten die Organisation unter den gegebenen Umständen in angemessener Weise unterrichtet und ihr Gelegenheit zu Stellungnahme gegeben haben.

Die Aussetzung ist zu beenden, sobald sichergestellt ist, dass die Grundsätze, die entsprechend den FAQ umgesetzt wurden, befolgt werden, und die zuständigen Behörden in der EU davon in Kenntnis gesetzt sind.

(2) Die Mitgliedstaaten informieren die Kommission unverzüglich, wenn Maßnahmen gemäß Absatz 1 ergriffen wurden.

(3) Die Mitgliedstaaten und die Kommission informieren einander auch über Fälle, bei denen die Maßnahmen der für die Einhaltung der entsprechend den FAQ umgesetzten Grundsätze in den Vereinigten Staaten verantwortlichen Einrichtungen nicht ausreichen, um die Einhaltung zu gewährleisten.

(4) Ergeben die Informationen nach den Absätzen 1, 2 und 3, dass eine der für die Einhaltung der entsprechend den FAQ umgesetzten Grundsätze in den Vereinigten Staaten verantwortlichen Einrichtungen ihrer Aufgabe nicht wirkungsvoll nachkommt, so informiert die Kommission das Handelsministerium der USA und schlägt, wenn nötig, gemäß dem Verfahren nach Artikel 31 der Richtlinie im Hinblick auf eine Aufhebung, Aussetzung oder Beschränkung des Geltungsbereichs dieser Entscheidung entsprechende Maßnahmen vor.

Artikel 4

(1) Diese Entscheidung kann jederzeit im Licht der Erfahrungen mit ihrer Anwendung angepasst werden und/oder dann, wenn das durch die Grundsätze und die FAQ gewährte Schutzniveau in die Rechtsvorschriften der USA übernommen wird.

In jedem Fall nimmt die Kommission drei Jahre, nachdem sie die Mitgliedstaaten von dieser Entscheidung in Kenntnis gesetzt hat, anhand der verfügbaren Informationen eine Bewertung ihrer Umsetzung vor und unterrichtet den nach Artikel 31 der Richtlinie 95/46/EG eingesetzten Ausschuss über sämtliche relevanten Feststellungen, einschließlich aller Erkenntnisse, die die Beurteilung der Vereinbarung in Artikel 1 als zur Gewährleistung des Datenschutzes angemessen im Sinne von Artikel 25 der Richtlinie 95/46/EG berühren könnten, sowie etwaiger Belege dafür, dass die vorliegende Entscheidung in diskriminierender Weise angewandt wird.

(2) Die Kommission legt erforderlichenfalls gemäß dem Verfahren nach Artikel 31 der Richtlinie Vorschläge für Maßnahmen vor."

8 In Anhang I der Entscheidung 2000/520 heißt es:

"Grundsätze des 'sicheren Hafens' zum Datenschutz

vorgelegt vom amerikanischen Handelsministerium am 21. Juli 2000

...

... [D]as Handelsministerium [legt] unter seiner gesetzlichen Autorität, internationalen Handel zu pflegen, zu fördern und zu entwickeln, dieses Papier und so genannte 'Häufig gestellte Fragen' - FAQs ('die Grundsätze') vor. Die Grundsätze wurden in Absprache mit der Industrie und der breiten Öffentlichkeit entwickelt, um den Handel zwischen der Europäischen Union und den Vereinigten Staaten zu erleichtern. Sie sind ausschließlich für den Gebrauch durch US-Organisationen bestimmt, die personenbezogene Daten aus der Europäischen Union erhalten, um sich für den 'sicheren Hafen' und die daraus erwachsende Vermutung der 'Angemessenheit' des Datenschutzes zu qualifizieren. Da die Grundsätze ausschließlich für diesen spezifischen Zweck erarbeitet wurden, können sie für andere Zwecke ungeeignet sein. ...

Die Entscheidung der einzelnen Organisationen, sich für den 'sicheren Hafen' zu qualifizieren, ist vollkommen freiwillig, und die Organisationen können sich für das Konzept des 'sicheren Hafens' auf verschiedene Arten qualifizieren. ...

Die Geltung dieser Grundsätze kann begrenzt werden a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte, oder c) wenn die Richtlinie oder das nationale Recht Ausnahmeregelungen vorsieht, sofern diese Ausnahmeregelungen unter vergleichbaren Voraussetzungen getroffen werden. Im Hinblick auf das Ziel eines wirksameren Schutzes der Privatsphäre sollen die Organisationen die Grundsätze in vollem Umfang und in transparenter Weise anwenden, unter anderem indem sie angeben, in welchen Fällen Abweichungen von den Grundsätzen, die nach b) zulässig sind, bei ihren Datenschutzmaßnahmen regelmäßig Anwendung finden werden. Aus demselben Grund wird, wenn die Wahlmöglichkeit nach den Grundsätzen und/oder nach dem US-Recht besteht, von den Organisationen erwartet, dass sie sich, sofern möglich, für das höhere Schutzniveau entscheiden.

..."

9 In Anhang II der Entscheidung 2000/520 heißt es:

"Häufig gestellte Fragen (FAQ)

...

FAQ 6 - Selbstzertifizierung

F: Wie zertifiziert eine Organisation, dass sie die Grundsätze des 'sicheren Hafens' als verbindlich anerkennt?

A: In den Genuss der Vorteile des 'sicheren Hafens' kommt eine Organisation ab dem Tag, an dem sie dem US-Handelsministerium (oder einer von diesem benannten Stelle) gegenüber erklärt, dass sie entsprechend den nachstehenden Leitlinien den Grundsätzen des 'sicheren Hafens' beitritt (Selbstzertifizierung).

Um sich selbst zu zertifizieren, muss die Organisation dem US-Handelsministerium (oder einer von diesem benannten Stelle) ein von einem leitenden Mitarbeiter im Namen der Organisation unterzeichnetes Schreiben vorlegen, das mindestens folgende Angaben enthält:

1. Name der Organisation, Postanschrift, E-Mail-Adresse, Telefon- und Faxnummer;

2. Beschreibung der Tätigkeit der Organisation im Zusammenhang mit personenbezogenen Daten aus der EU und

3. Beschreibung der Geschäftsbedingungen für den Datenschutz der Organisation, die folgende Angaben umfassen muss: a) Ort, an dem diese Beschreibung von der Öffentlichkeit eingesehen werden kann; b) Tag, an dem diese Vorkehrungen in Kraft gesetzt wurden; c) Kontaktstelle, die für die Bearbeitung von Beschwerden, Auskunftsersuchen und anderen Angelegenheiten des sicheren Hafens zuständig ist; d) die gesetzliche Aufsichtsbehörde, die über Beschwerden gegen die Organisation wegen unlauteren oder irreführenden Geschäftsgebarens und wegen Verletzung von datenschutzrechtlichen Vorschriften entscheidungsbefugt ist (und im Anhang zu den Grundsätzen aufgeführt ist); e) die Bezeichnungen aller Datenschutzprogramme, an denen die Organisation teilnimmt; f) die Art der anlassunabhängigen Kontrolle (z. B. intern oder extern) ... und g) das unabhängige Schiedsverfahren zur Behandlung ungelöster Beschwerdefälle.

Wenn die Organisation wünscht, dass ihr die Vorteile des sicheren Hafens auch bei Personaldaten zuteil werden, die zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, muss es eine gesetzliche Aufsichtsbehörde geben, die über Beschwerden gegen die Organisation hinsichtlich Arbeitnehmerdaten beschwerdebefugt ist; diese Stelle muss im Anhang zu den Grundsätzen genannt sein. ...

Das Ministerium (oder die von ihm benannte Stelle) führt eine Liste aller Organisationen, die sich selbst zertifizieren und denen damit die Vorteile des 'sicheren Hafens' zustehen. Die Liste wird nach den jährlich eingehenden Selbstzertifizierungsschreiben und den nach FAQ 11 eingegangenen Mitteilungen aktualisiert. ...

...

FAQ 11 - Schiedsverfahren und Durchsetzungsprinzip

F: Wie sind die im Durchsetzungsprinzip enthaltenen Anforderungen an die Behandlung von Beschwerden in die Praxis umzusetzen und was geschieht, wenn eine Organisation fortgesetzt gegen die Grundsätze des 'sicheren Hafens' verstößt?

A: Im Durchsetzungsprinzip ist festgelegt, wie den Grundsätzen des sicheren Hafens Geltung zu verschaffen ist. Wie Punkt b) des Durchsetzungsgrundsatzes zu entsprechen ist, wird in FAQ 7 (Kontrolle) ausgeführt. Diese FAQ 11 befasst sich mit den Punkten a) und c), die beide die Forderung nach unabhängigen Schiedsstellen enthalten. Das Beschwerdeverfahren kann auf verschiedene Weise ausgestaltet werden, es muss aber die im Durchsetzungsgrundsatz genannten Anforderungen erfüllen. Organisationen können diese Forderungen des Durchsetzungsgrundsatzes wie folgt erfüllen: 1. indem sie von der Privatwirtschaft entwickelte Datenschutzprogramme befolgen, in deren Regeln die Grundsätze des 'sicheren Hafens' integriert sind und die wirksame Durchsetzungsmechanismen vorsehen, wie sie im Durchsetzungsgrundsatz beschrieben sind; 2. indem sie sich gesetzlich oder durch Rechtsverordnung vorgesehenen Kontrollorganen unterwerfen, die Beschwerden von Einzelpersonen nachgehen und Streitigkeiten schlichten; 3. indem sie sich verpflichten, mit den Datenschutzbehörden in der Europäischen Union oder mit deren bevollmächtigten Vertretern zusammenzuarbeiten. Die hier angeführten Möglichkeiten sind Beispiele, es handelt sich nicht um eine abschließende Aufzählung. Die Privatwirtschaft kann auch andere Durchsetzungsmechanismen einführen, sie müssen nur die Forderungen erfüllen, die im Durchsetzungsgrundsatz und in den FAQ niedergelegt sind. Zu beachten ist, dass die Forderungen des Durchsetzungsgrundsatzes die Forderung ergänzen, die im dritten Absatz der Einführung zu den Grundsätzen des sicheren Hafens formuliert ist. Danach müssen auch bei Selbstregulierung Verstöße gegen die Grundsätze gemäß Abschnitt 5 des Federal Trade Commission Act oder einem ähnlichen Gesetz verfolgbar sein.

Anrufung unabhängiger Beschwerdestellen:

Die Verbraucher sollen dazu angehalten werden, Beschwerden zunächst an die Organisation zu richten, die ihre Daten verarbeitet, ehe sie eine unabhängige Beschwerdestelle anrufen. ...

...

Befassung der FTC:

Die FTC will Beschwerden wegen Verletzung der Grundsätze des sicheren Hafens, die Selbstregulierungsorgane für den Datenschutz wie BBBOnline und TRUSTe und EU-Mitgliedstaaten an sie verweisen, vorrangig behandeln, und feststellen, ob gegen Abschnitt 5 des FTC Act verstoßen wurde, der unlautere und irreführende Geschäftspraktiken verbietet. ...

..."

10 Anhang IV der Entscheidung 2000/520 sieht vor:

"Datenschutz und Schadenersatz, rechtliche Ermächtigungen, Fusionen und Übernahmen im Rahmen des US-amerikanischen Rechts

Diese Stellung[nahme] nimmt Bezug auf das Ersuchen der Europäischen Kommission um Klärung des US-amerikanischen Rechts in Bezug auf a) Schadenersatzansprüche wegen Verletzung der Privatsphäre, b) 'ausdrückliche Ermächtigungen' im Rahmen des US-amerikanischen Rechts für die Verwendung personenbezogener Informationen auf eine Art und Weise, die nicht in Einklang mit den US-Grundsätzen des sicheren Hafens steht, sowie c) die Auswirkungen von Fusionen und Übernahmen auf nach Maßgabe der Grundsätze des sicheren Hafens übernommene Verpflichtungen.

...

B. Ausdrückliche rechtliche Ermächtigungen

Die Grundsätze des sicheren Hafens sehen eine Ausnahme vor, wenn aufgrund der Gesetze, Rechtsvorschriften oder des Fallrechts 'widersprüchliche Verpflichtungen oder ausdrückliche Ermächtigungen entstehen, stets vorausgesetzt, dass ein Unternehmen bei der Ausübung einer solchen Ermächtigung demonstrieren kann, dass seine Nichtbefolgung der Grundsätze auf den Umfang beschränkt ist, der erforderlich ist, um den durch eine solche Ermächtigung geförderten ausschlaggebenden legitimen Interessen nachzukommen'. Es steht jedoch eindeutig fest, dass, wenn aufgrund des US-amerikanischen Rechts eine den Grundsätzen des sicheren Hafens entgegenstehende Verpflichtung auferlegt wird, die US-Unternehmen die Gesetze einhalten müssen, und zwar ungeachtet dessen, ob sie auf die Grundsätze des sicheren Hafens verpflichtet sind oder nicht. Während die Grundsätze des sicheren Hafens darauf abzielen, die Unterschiede zwischen dem US-amerikanischen und den europäischen Rechtssystemen für den Schutz der Privatsphäre zu überbrücken, haben wir uns, was ausdrückliche Ermächtigungen betrifft, den Vorrechten unserer gewählten Gesetzgeber zu fügen. Durch die in beschränktem Umfang mögliche Abweichung von einer strikten Befolgung der Grundsätze des sicheren Hafens soll ein Gleichgewicht geschaffen werden, um somit den berechtigten Interessen beider Seiten nachzukommen.

Ausnahmen sind beschränkt auf Fälle, bei denen eine ausdrückliche Ermächtigung vorliegt. Daher müssen in dieser Grenzsituation die entsprechenden Gesetze, Rechtsverordnungen oder Gerichtsentscheidungen das spezifische Verhalten der auf die Grundsätze des sicheren Hafens verpflichteten Unternehmen ausdrücklich genehmigen. Anders ausgedrückt, würde die Ausnahme nicht in Fällen gelten, hinsichtlich deren keine entsprechende rechtliche Äußerung vorliegt. Darüber hinaus würde die Ausnahme nur gelten, wenn die ausdrückliche Ermächtigung der Befolgung der Grundsätze des sicheren Hafens entgegensteht. Auch in einem solchen Fall 'beschränkt sich die Ausnahme auf das Maß, das erforderlich ist, um den durch eine solche Ermächtigung geförderten ausschlaggebenden rechtmäßigen Interessen nachzukommen'. So würde beispielsweise in Fällen, bei denen das Recht eine Gesellschaft lediglich ermächtigt, staatlichen Stellen personenbezogene Informationen zu liefern, die Ausnahme nicht gelten. Umgekehrt wäre jedoch in Fällen, bei denen das Recht eine Gesellschaft explizit ermächtigt, staatlichen Stellen ohne die jeweilige Zustimmung des Einzelnen personenbezogene Informationen zu liefern, eine 'ausdrückliche Ermächtigung' gegeben, auf eine Art und Weise zu handeln, die den Grundsätzen des sicheren Hafens entgegensteht. Oder aber spezifische Ausnahmen von den ausdrücklichen Erfordernissen, eine entsprechende Mitteilung zu machen und die Zustimmung einzuholen, würden in den Ausnahmebereich fallen (da dies einer spezifischen Ermächtigung gleichkommen würde, Informationen ohne entsprechende Mitteilung und Zustimmung offen zu legen). So könnte beispielsweise ein Gesetz, das Ärzten gestattet, die medizinischen Daten ihrer Patienten ohne die vorherige Zustimmung der Patienten an Beamte des Gesundheitsamts weiterzugeben, eine Ausnahme vom Mitteilungs- und Wahlmöglichkeitsgrundsatz gewähren. Diese Ermächtigung würde es einem Arzt nicht gestatten, dieselben medizinischen Daten an Gesundheitsvorsorgeeinrichtungen oder kommerzielle pharmazeutische Forschungslabors weiterzugeben, was das Maß der von Rechts wegen erteilten Ermächtigung übersteigen und daher die Reichweite des Ausnahmefalls überschreiten würde. Bei der in Frage stehenden rechtlichen Ermächtigung kann es sich um eine 'einzelne' Ermächtigung handeln, bestimmte Dinge mit personenbezogenen Daten zu tun; wie die nachstehenden Beispiele jedoch zeigen,

handelt es sich eher um eine Ausnahme im Hinblick auf ein weitreichenderes Gesetz, das die Erhebung, Verwendung und Offenlegung personenbezogener Informationen verbietet.

..."

Mitteilung COM(2013) 846 final

11 Am 27. November 2013 erließ die Kommission eine Mitteilung an das Europäische Parlament und den Rat mit dem Titel "Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA" (COM[2013] 846 final) (im Folgenden: Mitteilung COM[2013] 846 final). Begleitet wurde diese Mitteilung von einem ebenfalls vom 27. November 2013 datierenden Bericht über die Ergebnisse der EU-Ko-Vorsitzenden der Ad-hoc-Arbeitsgruppe EU-USA zum Datenschutz ("Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection"). Dieser Bericht war, wie aus seinem Abschnitt 1 hervorgeht, in Zusammenarbeit mit den Vereinigten Staaten von Amerika erstellt worden, nachdem bekannt geworden war, dass es dort mehrere Überwachungsprogramme gibt, die auch die Sammlung und Verarbeitung personenbezogener Daten in großem Umfang einschließen. Der Bericht enthält u. a. eine eingehende Analyse der Rechtsordnung der Vereinigten Staaten, insbesondere in Bezug auf die Rechtsgrundlagen der Überwachungsprogramme sowie der Sammlung und Verarbeitung personenbezogener Daten durch die amerikanischen Behörden.

12 In Abschnitt 1 der Mitteilung COM(2013) 846 final führt die Kommission aus: "Das Thema Handelsbeziehungen ist Gegenstand der Entscheidung [2000/520]. Die Entscheidung bietet die Rechtsgrundlage für die Übermittlung personenbezogener Daten aus der EU an in den USA niedergelassene Unternehmen, die die Datenschutz-Grundsätze ('Safe Harbor') beachten." Ferner hebt die Kommission in Abschnitt 1 den immer größeren Stellenwert des Austauschs personenbezogener Daten hervor, der u. a. mit der Entwicklung der digitalen Wirtschaft zusammenhänge; diese habe nämlich "zu einem exponentiellen Anstieg der Quantität, Qualität, Vielfalt und Art der Tätigkeiten im Bereich der Datenverarbeitung geführt".

13 In Abschnitt 2 dieser Mitteilung führt die Kommission aus, dass "die Bedenken mit Blick auf das Schutzniveau für in die USA übertragene personenbezogene Daten von EU-Bürgern immer weiter zu[nehmen]" und dass "[a]ufgrund des freiwilligen und deklaratorischen Charakters des [Safe-Harbor-]Systems ... das Augenmerk verstärkt auf dessen Transparenz und Durchsetzung gelegt [wird]".

14 Weiter heißt es in Abschnitt 2: "Die im Rahmen des 'sicheren Hafens' an die USA übermittelten personenbezogenen Daten von EU-Bürgern können durch die US-Behörden in einer Weise eingesehen und weiterverarbeitet werden, die mit dem eigentlichen Zweck ihrer Erfassung in der EU und mit den Gründen für ihre Übermittlung in die USA unvereinbar ist. Die Mehrzahl der US-Internetfirmen, bei denen sich ein unmittelbarer Zusammenhang zu den [Überwachungsprogrammen] herstellen lässt, ist den Safe-Harbor-Grundsätzen beigetreten."

15 In Abschnitt 3.2 der Mitteilung COM(2013) 846 final stellt die Kommission fest, dass es bei der Umsetzung der Entscheidung 2000/520 eine Reihe von Schwachstellen gebe. Zum einen hielten sich amerikanische zertifizierte Unternehmen nicht an die in Art. 1 Abs 1 der Entscheidung 2000/520 aufgestellten Grundsätze (im Folgenden: Grundsätze des "sicheren Hafens"), so dass Verbesserungen der Entscheidung erforderlich seien, die "sowohl auf die strukturellen Mängel bei der Transparenz und der Durchsetzung als auch auf die wichtigsten

Grundsätze des 'sicheren Hafens' und die Ausnahmeregelungen aus Gründen der nationalen Sicherheit" ausgerichtet sein sollten. Zum anderen diene das System des sicheren Hafens "als Kanal für die Übertragung personenbezogener Daten von EU-Bürgern von der EU in die USA durch Unternehmen, die zur Freigabe von Daten an US-Geheimdienste im Rahmen der Datenerhebungsprogramme dieser Dienste aufgefordert werden".

16 Die Kommission zieht daraus in Abschnitt 3.2 folgenden Schluss: "Angesichts der festgestellten Schwachstellen kann das Safe-Harbor-System nicht wie bisher fortgeführt werden. Seine Aufhebung würde allerdings den Interessen der beteiligten Unternehmen in der EU und in den USA schaden." Schließlich fügt sie in Abschnitt 3.2 hinzu, sie werde "mit den US-Behörden unverzüglich Gespräche über die festgestellten Mängel aufnehmen".

Mitteilung COM(2013) 847 final

17 Am 27. November 2013 erließ die Kommission ferner eine Mitteilung an das Europäische Parlament und den Rat über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen (COM[2013] 847 final) (im Folgenden: Mitteilung COM[2013] 847 final). Wie sich aus Abschnitt 1 dieser Mitteilung ergibt, beruht sie u. a. auf Informationen der Ad-hoc-Arbeitsgruppe EU-USA und stützt sich auf zwei in den Jahren 2002 und 2004 veröffentlichte Bewertungsberichte der Kommission.

18 Nach Abschnitt 1 der Mitteilung basiert die Funktionsweise der Entscheidung 2000/520 "auf den Verpflichtungserklärungen und Selbstzertifizierungen der beteiligten Unternehmen". Weiter heißt es dort: "Die Beteiligung ist zwar freiwillig, jedoch sind die Unternehmen danach an die geltenden Vorschriften gebunden."

19 Außerdem geht aus Abschnitt 2.2 der Mitteilung COM(2013) 847 final hervor, dass am 26. September 2013 insgesamt 3 246 Unternehmen zahlreicher Wirtschafts- und Dienstleistungsbranchen zertifiziert waren. Dabei handelte es sich hauptsächlich um Unternehmen, die auf dem Binnenmarkt der Union Dienstleistungen anboten, insbesondere um Internetfirmen; teilweise waren es Niederlassungen von Unternehmen aus der Union mit Tochtergesellschaften in den Vereinigten Staaten. Einige dieser Unternehmen verarbeiteten Daten von Mitarbeitern in Europa, die zu personaltechnischen Zwecken in die Vereinigten Staaten übermittelt wurden.

20 In Abschnitt 2.2 hebt die Kommission überdies Folgendes hervor: "Ist seitens der USA keine ausreichende Transparenz oder Durchsetzung gewährleistet, liegt die Verantwortung bei den europäischen Datenschutzbehörden sowie bei den an der Safe-Harbor-Regelung beteiligten Unternehmen."

21 Wie insbesondere den Abschnitten 3 bis 5 und 8 der Mitteilung COM(2013) 847 final zu entnehmen ist, hielt eine erhebliche Zahl zertifizierter Unternehmen die Grundsätze des "sicheren Hafens" nicht oder nicht vollständig ein.

22 Überdies weist die Kommission in Abschnitt 7 der Mitteilung darauf hin, dass "alle Unternehmen, die am Programm PRISM [Programm zur umfassenden Sammlung von Informationen] beteiligt sind und den US-Behörden den Zugriff auf in den USA gespeicherte und verarbeitete Daten gestatten, der Safe-Harbor-Regelung beigetreten [sind]", die damit "zu einem Informationskanal geworden [ist], über den die US-Nachrichtendienste auf personenbezogene Daten zugreifen können, die ursprünglich in der EU verarbeitet worden

sind". Hierzu stellt die Kommission in Abschnitt 7.1 der Mitteilung fest, dass "das US-amerikanische Recht die umfassende Erhebung und Verarbeitung personenbezogener Daten zu[lässt], die von Unternehmen mit Sitz in den USA gespeichert oder in anderer Weise verarbeitet werden. ... Diese groß angelegten Programme können dazu führen, dass auf der Grundlage der Safe-Harbor-Regelung transferierte Daten von US-Behörden über das Maß hinaus, das für den Schutz der nationalen Sicherheit (im Sinne der Ausnahmeklausel in der [Entscheidung 2000/520]) unbedingt nötig und angemessen wäre, abgerufen und weiterverarbeitet werden."

23 In Abschnitt 7.2 ("Beschränkungen und Rechtsschutzmöglichkeiten") der Mitteilung COM(2013) 847 final hebt die Kommission hervor, dass "die nach US-amerikanischem Recht verfügbaren Garantien größtenteils nur US-Bürgern oder Personen mit rechtmäßigem Wohnsitz in den USA zu[stehen]. Auch gibt es weder für EU- noch für US-Bürger die Möglichkeit, Auskunft über ihre Daten, deren Berichtigung oder Löschung zu erwirken, die im Rahmen der US-Überwachungsprogramme erhoben und weiterverarbeitet werden. Administrative oder gerichtliche Rechtsbehelfe stehen gleichfalls nicht zur Verfügung."

24 Nach Abschnitt 8 der Mitteilung COM(2013) 847 final gehörten zu den zertifizierten Unternehmen "Web-Unternehmen wie Google, Facebook, Microsoft, Apple und Yahoo" mit "mehreren Hundert Millionen Kunden in Europa", die personenbezogene Daten zur Verarbeitung in die Vereinigten Staaten übermittelten.

25 Die Kommission kam in Abschnitt 8 zu folgendem Schluss: "Ernsthaft in Frage zu stellen ist ..., ob die Datenschutzrechte europäischer Bürger, deren Daten in die USA übermittelt werden, angesichts des umfassenden Zugriffs der Nachrichtendienste auf Daten, die von Safe-Harbor-Unternehmen in die USA übermittelt werden, kontinuierlich geschützt sind."

Ausgangsverfahren und Vorlagefragen

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

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

28 Am 25. Juni 2013 legte Herr Schrems beim Commissioner eine Beschwerde ein, mit der er ihn im Wesentlichen aufforderte, in Ausübung der ihm übertragenen Befugnisse Facebook Ireland die Übermittlung seiner personenbezogenen Daten in die Vereinigten Staaten zu untersagen. Er machte geltend, das Recht und die Praxis der Vereinigten Staaten gewährleisteten keinen ausreichenden Schutz der in diesem Land gespeicherten personenbezogenen Daten vor den Überwachungstätigkeiten der dortigen Behörden. Dabei verwies er auf die von Herrn Edward Snowden enthüllten Tätigkeiten der Nachrichtendienste der Vereinigten Staaten, insbesondere der National Security Agency (im Folgenden: NSA).

29 Da sich der Commissioner nicht für verpflichtet hielt, die von Herrn Schrems in seiner Beschwerde gerügten Tatsachen zu untersuchen, wies er die Beschwerde als unbegründet zurück. Er war nämlich der Ansicht, dass es keine Beweise für einen Zugriff der NSA auf die

personenbezogenen Daten von Herrn Schrems gebe. Er fügte hinzu, die von Herrn Schrems in seiner Beschwerde erhobenen Rügen könnten nicht mit Erfolg geltend gemacht werden, da alle die Angemessenheit des Schutzes personenbezogener Daten in den Vereinigten Staaten betreffenden Fragen im Einklang mit der Entscheidung 2000/520 zu klären seien und da die Kommission in dieser Entscheidung festgestellt habe, dass die Vereinigten Staaten von Amerika ein angemessenes Schutzniveau gewährleisteten.

30 Herr Schrems erhob gegen die im Ausgangsverfahren in Rede stehende Entscheidung Klage beim High Court. Dieser stellte nach Prüfung der von den Parteien des Ausgangsverfahrens vorgelegten Beweise fest, dass die elektronische Überwachung und Erfassung der aus der Union in die Vereinigten Staaten übermittelten personenbezogenen Daten notwendigen und unerlässlichen Zielen von öffentlichem Interesse diene. Die Enthüllungen von Herrn Snowden hätten jedoch gezeigt, dass die NSA und andere Bundesbehörden "erhebliche Exzesse" begangen hätten.

31 Der High Court fügte hinzu, die Unionsbürger hätten keinen wirksamen Anspruch auf rechtliches Gehör. Die Überwachung der Handlungen der Nachrichtendienste finde ex parte und unter Geheimhaltung statt. Sobald die personenbezogenen Daten in die Vereinigten Staaten übermittelt worden seien, könnten die NSA und andere Bundesbehörden wie das Federal Bureau of Investigation (FBI) darauf im Rahmen der von ihnen praktizierten massenhaften und wahllosen Überwachung und Erfassung zugreifen.

32 Das irische Recht verbiete die Übermittlung personenbezogener Daten ins Ausland, es sei denn, das betreffende Drittland gewährleiste ein angemessenes Schutzniveau der Privatsphäre sowie der Grundrechte und Grundfreiheiten. Der Stellenwert der durch die irische Verfassung garantierten Rechte auf Privatsphäre und auf Unverletzlichkeit der Wohnung gebiete es, dass jeder Eingriff in diese Rechte verhältnismäßig sei und den gesetzlichen Anforderungen entspreche.

33 Der massenhafte und undifferenzierte Zugriff auf personenbezogene Daten verstoße offenkundig gegen den Grundsatz der Verhältnismäßigkeit und die durch die irische Verfassung geschützten Grundwerte. Die Erfassung elektronischer Kommunikation könne nur dann als verfassungsgemäß angesehen werden, wenn nachgewiesen werde, dass sie zielgerichtet sei, dass die Überwachung bestimmter Personen oder Personengruppen im Interesse der nationalen Sicherheit oder der Verbrechensbekämpfung objektiv gerechtfertigt sei und dass es angemessene und nachprüfbare Schutzmechanismen gebe. Wäre die Rechtssache des Ausgangsverfahrens allein anhand des irischen Rechts zu prüfen, wäre daher festzustellen, dass der Commissioner in Anbetracht ernster Zweifel daran, ob die Vereinigten Staaten von Amerika ein angemessenes Schutzniveau der personenbezogenen Daten gewährleisteten, eine Untersuchung der von Herrn Schrems in seiner Beschwerde gerügten Tatsachen hätte vornehmen müssen und die Beschwerde zu Unrecht zurückgewiesen hätte.

34 Da diese Rechtssache jedoch die Durchführung des Rechts der Union im Sinne von Art. 51 der Charta betreffe, sei die Rechtmäßigkeit der im Ausgangsverfahren in Rede stehenden Entscheidung anhand des Unionsrechts zu beurteilen. Die Entscheidung 2000/520 genüge aber weder den Anforderungen der Art. 7 und 8 der Charta noch den vom Gerichtshof im Urteil Digital Rights Ireland u. a. (C-293/12 und C-594/12, EU:C:2014:238) aufgestellten Grundsätzen. Das durch Art. 7 der Charta und durch die Grundwerte, die sich aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten ergäben, gewährleistete Recht auf Achtung der Privatsphäre würde seiner Tragweite völlig beraubt, wenn den Behörden gestattet würde, auf die elektronische Kommunikation in beliebiger und pauschaler Weise,

ohne jede auf Erwägungen der nationalen Sicherheit oder der Verbrechensverhütung, die speziell mit den Betroffenen in Zusammenhang stünden, basierende objektive Rechtfertigung und ohne begleitende angemessene und nachprüfbare Schutzmechanismen zuzugreifen.

35 Im Übrigen stelle Herr Schrems mit seiner Klage de facto die Rechtmäßigkeit der durch die Entscheidung 2000/520 geschaffenen Safe-Harbor-Regelung in Frage, auf der die im Ausgangsverfahren in Rede stehende Entscheidung beruhe. Auch wenn er die Gültigkeit weder der Richtlinie 95/46 noch der Entscheidung 2000/520 förmlich angefochten habe, stelle sich daher die Frage, ob der Commissioner im Hinblick auf Art. 25 Abs 6 der Richtlinie an die von der Kommission in ihrer Entscheidung getroffene Feststellung, dass die Vereinigten Staaten von Amerika ein angemessenes Schutzniveau gewährleisteten, gebunden gewesen sei oder ob Art. 8 der Charta ihn ermächtigt hätte, sich gegebenenfalls über eine solche Feststellung hinwegzusetzen.

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

1. Ist ein unabhängiger Amtsträger, der von Rechts wegen mit der Handhabung und der Durchsetzung von Rechtsvorschriften über den Datenschutz betraut ist, bei der Prüfung einer bei ihm eingelegten Beschwerde, dass personenbezogene Daten in ein Drittland (im vorliegenden Fall in die Vereinigten Staaten von Amerika) übermittelt würden, dessen Recht und Praxis keinen angemessenen Schutz der Betroffenen gewährleisteten, im Hinblick auf die Art. 7, 8 und 47 der Charta, unbeschadet der Bestimmungen von Art. 25 Abs 6 der Richtlinie 95/46, absolut an die in der Entscheidung 2000/520 enthaltene gegenteilige Feststellung der Union gebunden?

2. Oder kann und/oder muss der Amtsträger stattdessen im Licht tatsächlicher Entwicklungen, die seit der erstmaligen Veröffentlichung der Entscheidung der Kommission eingetreten sind, eigene Ermittlungen in dieser Sache anstellen?

Zu den Vorlagefragen

37 Mit seinen Vorlagefragen, die gemeinsam zu prüfen sind, möchte das vorlegende Gericht wissen, ob und inwieweit Art. 25 Abs 6 der Richtlinie 95/46 im Licht der Art. 7, 8 und 47 der Charta dahin auszulegen ist, dass eine aufgrund dieser Bestimmung ergangene Entscheidung wie die Entscheidung 2000/520, in der die Kommission feststellt, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, eine Kontrollstelle eines Mitgliedstaats im Sinne von Art. 28 der Richtlinie daran hindert, die Eingabe einer Person zu prüfen, die sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten, die aus einem Mitgliedstaat in dieses Drittland übermittelt wurden, bezieht, wenn diese Person geltend macht, dass das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleisteten.

Zu den Befugnissen der nationalen Kontrollstellen im Sinne von Art. 28 der Richtlinie 95/46 bei Vorliegen einer nach Art. 25 Abs 6 dieser Richtlinie ergangenen Entscheidung der Kommission

38 Zunächst ist darauf hinzuweisen, dass die Bestimmungen der Richtlinie 95/46, soweit sie die Verarbeitung personenbezogener Daten regeln, die zu Beeinträchtigungen der Grundfreiheiten und insbesondere des Rechts auf Achtung der Privatsphäre führen kann, notwendigerweise im Licht der durch die Charta garantierten Grundrechte auszulegen sind

(vgl. Urteile Österreichischer Rundfunk u. a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 68, Google Spain und Google, C-131/12, EU:C:2014:317, Rn. 68, sowie Rynes, C-212/13, EU:C:2014:2428, Rn. 29).

39 Wie sich aus Art. 1 und aus den Erwägungsgründen 2 und 10 der Richtlinie 95/46 ergibt, soll diese nicht nur einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechte natürlicher Personen, insbesondere des Grundrechts auf Achtung der Privatsphäre, bei der Verarbeitung personenbezogener Daten gewährleisten, sondern auch ein hohes Niveau des Schutzes dieser Grundrechte und Grundfreiheiten. Die Bedeutung sowohl des durch Art. 7 der Charta gewährleisteten Grundrechts auf Achtung des Privatlebens als auch des durch ihren Art. 8 gewährleisteten Grundrechts auf Schutz personenbezogener Daten wird im Übrigen in der Rechtsprechung des Gerichtshofs hervorgehoben (vgl. Urteile Rijkeboer, C-553/07, EU:C:2009:293, Rn. 47, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 53, sowie Google Spain und Google, C-131/12, EU:C:2014:317, Rn. 53, 66 und 74 sowie die dort angeführte Rechtsprechung).

40 Zu den Befugnissen, über die die nationalen Kontrollstellen hinsichtlich der Übermittlung personenbezogener Daten in Drittländer verfügen, ist festzustellen, dass Art. 28 Abs 1 der Richtlinie 95/46 den Mitgliedstaaten vorschreibt, eine oder mehrere öffentliche Stellen damit zu beauftragen, in völliger Unabhängigkeit die Einhaltung der Unionsvorschriften über den Schutz natürlicher Personen bei der Verarbeitung solcher Daten zu überwachen. Dieses Erfordernis ergibt sich auch aus dem Primärrecht der Union, namentlich aus Art. 8 Abs 3 der Charta und aus Art. 16 Abs 2 AEUV (vgl. in diesem Sinne Urteile Kommission/Österreich, C-614/10, EU:C:2012:631, Rn. 36, und Kommission/Ungarn, C-288/12, EU:C:2014:237, Rn. 47).

41 Die Gewährleistung der Unabhängigkeit der nationalen Kontrollstellen soll die wirksame und zuverlässige Kontrolle der Einhaltung der Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherstellen und ist im Licht dieses Zwecks auszulegen. Sie wurde eingeführt, um die von den Entscheidungen der Kontrollstellen betroffenen Personen und Einrichtungen stärker zu schützen. Die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten stellt daher - wie dem 62. Erwägungsgrund der Richtlinie 95/46 zu entnehmen ist - ein wesentliches Element zur Wahrung des Schutzes der Personen bei der Verarbeitung personenbezogener Daten dar (vgl. Urteile Kommission/Deutschland, C-518/07, EU:C:2010:125, Rn. 25, und Kommission/Ungarn, C-288/12, EU:C:2014:237, Rn. 48 und die dort angeführte Rechtsprechung).

42 Um diesen Schutz zu gewährleisten, müssen die nationalen Kontrollstellen u. a. für einen angemessenen Ausgleich zwischen der Achtung des Grundrechts auf Privatsphäre und den Interessen sorgen, die einen freien Verkehr personenbezogener Daten gebieten (vgl. in diesem Sinne Urteile Kommission/Deutschland, C-518/07, EU:C:2010:125, Rn. 24, und Kommission/Ungarn, C-288/12, EU:C:2014:237, Rn. 51).

43 Zu diesem Zweck verfügen die Kontrollstellen über eine große Bandbreite von Befugnissen, die in Art. 28 Abs 3 der Richtlinie 95/46 in nicht abschließender Weise aufgezählt werden und, wie im 63. Erwägungsgrund der Richtlinie hervorgehoben wird, notwendige Mittel für die Erfüllung ihrer Aufgaben darstellen. So verfügen sie u. a. über Untersuchungsbefugnisse wie etwa das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen, über wirksame Einwirkungsbefugnisse wie etwa die Befugnis, das vorläufige oder endgültige Verbot einer Verarbeitung von Daten anzuordnen, oder über das Klagerecht.

44 Zwar geht aus Art. 28 Abs 1 und 6 der Richtlinie 95/46 hervor, dass die Befugnisse der nationalen Kontrollstellen die Verarbeitung personenbezogener Daten im Hoheitsgebiet ihres Mitgliedstaats betreffen, so dass Art. 28 ihnen keine Befugnisse in Bezug auf die Verarbeitung solcher Daten im Hoheitsgebiet eines Drittlands verleiht.

45 Die Übermittlung personenbezogener Daten aus einem Mitgliedstaat in ein Drittland stellt jedoch als solche eine Verarbeitung personenbezogener Daten im Sinne von Art. 2 Buchst. b der Richtlinie 95/46 dar (vgl. in diesem Sinne Urteil Parlament/Rat und Kommission, C-317/04 und C-318/04, EU:C:2006:346, Rn. 56), die im Hoheitsgebiet eines Mitgliedstaats vorgenommen wird. In dieser Bestimmung wird die "Verarbeitung personenbezogener Daten" nämlich als "jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten" definiert und als Beispiel "die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung" genannt.

46 Im 60. Erwägungsgrund der Richtlinie 95/46 heißt es, dass Übermittlungen personenbezogener Daten in Drittländer nur unter voller Einhaltung der Rechtsvorschriften erfolgen dürfen, die die Mitgliedstaaten gemäß dieser Richtlinie erlassen haben. Insoweit wurde in Kapitel IV der Richtlinie, in dem sich ihre Art. 25 und 26 befinden, eine Regelung geschaffen, die eine Kontrolle der Übermittlungen personenbezogener Daten in Drittländer durch die Mitgliedstaaten gewährleisten soll. Diese Regelung ergänzt die allgemeine Regelung in Kapitel II der Richtlinie über die allgemeinen Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten (vgl. in diesem Sinne Urteil Lindqvist, C-101/01, EU:C:2003:596, Rn. 63).

47 Da die nationalen Kontrollstellen gemäß Art. 8 Abs 3 der Charta und Art. 28 der Richtlinie 95/46 die Einhaltung der Unionsvorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu überwachen haben, ist jede von ihnen zu der Prüfung befugt, ob bei einer Übermittlung personenbezogener Daten aus ihrem Mitgliedstaat in ein Drittland die in der Richtlinie 95/46 aufgestellten Anforderungen eingehalten werden.

48 Im 56. Erwägungsgrund der Richtlinie 95/46 wird zwar anerkannt, dass die Übermittlung personenbezogener Daten aus den Mitgliedstaaten in Drittländer für die Entwicklung des internationalen Handels notwendig ist, doch gilt nach ihrem Art. 25 Abs 1 der Grundsatz, dass eine solche Übermittlung nur zulässig ist, wenn die Drittländer ein angemessenes Schutzniveau gewährleisten.

49 Außerdem heißt es im 57. Erwägungsgrund der Richtlinie, dass Übermittlungen personenbezogener Daten in Drittländer, die kein angemessenes Schutzniveau bieten, zu untersagen sind.

50 Zum Zweck der Kontrolle der Übermittlungen personenbezogener Daten in Drittländer anhand des Schutzniveaus dieser Daten im jeweiligen Drittland werden den Mitgliedstaaten und der Kommission in Art. 25 der Richtlinie 95/46 eine Reihe von Verpflichtungen auferlegt. Insbesondere kann nach diesem Artikel, wie der Generalanwalt in Nr. 86 seiner Schlussanträge ausgeführt hat, die Feststellung, ob ein Drittland ein angemessenes Schutzniveau gewährleistet, sowohl von den Mitgliedstaaten als auch von der Kommission getroffen werden.

51 Die Kommission kann auf der Grundlage von Art. 25 Abs 6 der Richtlinie 95/46 eine Entscheidung erlassen, in der sie feststellt, dass ein Drittland ein angemessenes Schutzniveau gewährleistet. Eine solche Entscheidung richtet sich nach Art. 25 Abs 6 Unterabs. 2 an die Mitgliedstaaten, die die aufgrund der Feststellung gebotenen Maßnahmen treffen müssen. Nach Art. 288 Abs 4 AEUV bindet sie alle Mitgliedstaaten und ist damit für alle Organe der Mitgliedstaaten verbindlich (vgl. in diesem Sinne Urteile Albako Margarinefabrik, 249/85, EU:C:1987:245, Rn. 17, und Mediaset, C-69/13, EU:C:2014:71, Rn. 23), soweit sie die Übermittlung personenbezogener Daten aus den Mitgliedstaaten in das betreffende Drittland gestattet.

52 Solange die Entscheidung der Kommission vom Gerichtshof nicht für ungültig erklärt wurde, können die Mitgliedstaaten und ihre Organe, zu denen ihre unabhängigen Kontrollstellen gehören, somit zwar keine dieser Entscheidung zuwiderlaufenden Maßnahmen treffen, wie etwa Rechtsakte, mit denen verbindlich festgestellt wird, dass das Drittland, auf das sich die Entscheidung bezieht, kein angemessenes Schutzniveau gewährleistet. Für die Rechtsakte der Unionsorgane gilt nämlich grundsätzlich eine Vermutung der Rechtmäßigkeit, so dass sie Rechtswirkungen entfalten, solange sie nicht zurückgenommen, im Rahmen einer Nichtigkeitsklage für nichtig erklärt oder infolge eines Vorabentscheidungsersuchens oder einer Einrede der Rechtswidrigkeit für ungültig erklärt wurden (Urteil Kommission/Griechenland, C-475/01, EU:C:2004:585, Rn. 18 und die dort angeführte Rechtsprechung).

53 Eine nach Art. 25 Abs 6 der Richtlinie 95/46 ergangene Entscheidung der Kommission wie die Entscheidung 2000/520 kann Personen, deren personenbezogene Daten in ein Drittland übermittelt wurden oder werden könnten, jedoch nicht daran hindern, die nationalen Kontrollstellen zum Schutz der diese Personen betreffenden Rechte und Freiheiten bei der Verarbeitung solcher Daten mit einer Eingabe im Sinne von Art. 28 Abs 4 der Richtlinie zu befassen. Desgleichen kann eine derartige Entscheidung, wie der Generalanwalt insbesondere in den Nrn. 61, 93 und 116 seiner Schlussanträge ausgeführt hat, die den nationalen Kontrollstellen durch Art. 8 Abs 3 der Charta und durch Art. 28 der Richtlinie ausdrücklich zuerkannten Befugnisse weder beseitigen noch beschränken.

54 Weder Art. 8 Abs 3 der Charta noch Art. 28 der Richtlinie 95/46 schließt die Kontrolle der Übermittlungen personenbezogener Daten in Drittländer, die Gegenstand einer Entscheidung der Kommission nach Art. 25 Abs 6 der Richtlinie waren, vom Zuständigkeitsbereich der nationalen Kontrollstellen aus.

55 Insbesondere sieht Art. 28 Abs 4 Unterabs. 1 der Richtlinie 95/46, der bestimmt, dass sich jede Person "zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten" mit einer Eingabe an die nationalen Kontrollstellen wenden kann, keine Ausnahme für den Fall vor, dass die Kommission eine Entscheidung nach Art. 25 Abs 6 der Richtlinie erlassen hat.

56 Außerdem würde es dem durch die Richtlinie 95/46 geschaffenen System sowie dem Zweck ihrer Art. 25 und 28 zuwiderlaufen, wenn eine Entscheidung der Kommission nach Art. 25 Abs 6 der Richtlinie eine nationale Kontrollstelle daran hindern würde, die Eingabe einer Person zum Schutz der sie betreffenden Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten zu prüfen, die aus einem Mitgliedstaat in ein Drittland, das Gegenstand dieser Entscheidung ist, übermittelt wurden oder werden könnten.

57 Art. 28 der Richtlinie 95/46 kommt vielmehr seinem Wesen nach bei jeder Verarbeitung personenbezogener Daten zur Anwendung. Auch wenn die Kommission eine Entscheidung nach Art. 25 Abs 6 der Richtlinie getroffen hat, müssen die nationalen Kontrollstellen daher, wenn sich eine Person mit einer Eingabe zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten an sie wendet, in völliger Unabhängigkeit prüfen können, ob bei der Übermittlung dieser Daten die in der Richtlinie aufgestellten Anforderungen gewahrt werden.

58 Wäre dem nicht so, würde den Personen, deren personenbezogene Daten in das betreffende Drittland übermittelt wurden oder werden könnten, das durch Art. 8 Abs 1 und 3 der Charta garantierte Recht vorenthalten, sich mit einer Eingabe zum Schutz ihrer Grundrechte an die nationalen Kontrollstellen zu wenden (vgl. entsprechend Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 68).

59 Eine Eingabe im Sinne von Art. 28 Abs 4 der Richtlinie 95/46, mit der eine Person, deren personenbezogene Daten in ein Drittland übermittelt wurden oder werden könnten, wie im Ausgangsverfahren geltend macht, dass ungeachtet der Feststellungen der Kommission in einer nach Art. 25 Abs 6 der Richtlinie ergangenen Entscheidung das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleisteten, ist dahin zu verstehen, dass sie der Sache nach die Vereinbarkeit dieser Entscheidung mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte von Personen betrifft.

60 Insoweit ist auf die ständige Rechtsprechung des Gerichtshofs hinzuweisen, wonach die Union eine Rechtsunion ist, in der alle Handlungen ihrer Organe der Kontrolle daraufhin unterliegen, ob sie insbesondere mit den Verträgen, den allgemeinen Rechtsgrundsätzen und den Grundrechten im Einklang stehen (vgl. in diesem Sinne Urteile Kommission u. a./Kadi, C-584/10 P, C-593/10 P und C-595/10 P, EU:C:2013:518, Rn. 66, Inuit Tapiriit Kanatami u. a./Parlament und Rat, C-583/11 P, EU:C:2013:625, Rn. 91, und Telefónica/Kommission, C-274/12 P, EU:C:2013:852, Rn. 56). Die nach Art. 25 Abs 6 der Richtlinie 95/46 ergangenen Entscheidungen der Kommission können daher einer solchen Kontrolle nicht entzogen sein.

61 Gleichwohl ist allein der Gerichtshof befugt, die Ungültigkeit eines Unionsrechtsakts wie einer nach Art. 25 Abs 6 der Richtlinie 95/46 ergangenen Entscheidung der Kommission festzustellen, wobei die Ausschließlichkeit dieser Zuständigkeit Rechtssicherheit gewährleisten soll, indem sie die einheitliche Anwendung des Unionsrechts sicherstellt (vgl. Urteile Melki und Abdeli, C-188/10 und C-189/10, EU:C:2010:363, Rn. 54, sowie CIVAD, C-533/10, EU:C:2012:347, Rn. 40).

62 Die nationalen Gerichte sind zwar berechtigt, die Gültigkeit eines Unionsrechtsakts wie einer nach Art. 25 Abs 6 der Richtlinie 95/46 ergangenen Entscheidung der Kommission zu prüfen; sie sind jedoch nicht befugt, selbst die Ungültigkeit eines solchen Rechtsakts festzustellen (vgl. in diesem Sinne Urteile Foto-Frost, 314/85, EU:C:1987:452, Rn. 15 bis 20, sowie IATA und ELFAA, C-344/04, EU:C:2006:10, Rn. 27). Erst recht sind die nationalen Kontrollstellen bei der Prüfung einer Eingabe im Sinne von Art. 28 Abs 4 der Richtlinie, die die Vereinbarkeit einer nach Art. 25 Abs 6 der Richtlinie ergangenen Entscheidung der Kommission mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte von Personen zum Gegenstand hat, nicht befugt, selbst die Ungültigkeit einer solchen Entscheidung festzustellen.

63 In Anbetracht der vorstehenden Erwägungen ist es, wenn sich eine Person, deren personenbezogene Daten in ein Drittland übermittelt wurden oder werden könnten, das

Gegenstand einer nach Art. 25 Abs 6 der Richtlinie 95/46 ergangenen Entscheidung der Kommission ist, mit einer Eingabe zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung dieser Daten an eine nationale Kontrollstelle wendet und im Rahmen dieser Eingabe - wie im Ausgangsverfahren - die Vereinbarkeit der betreffenden Entscheidung mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte von Personen in Frage stellt, Sache der angerufenen Kontrollstelle, die Eingabe mit aller gebotenen Sorgfalt zu prüfen.

64 Falls die Kontrollstelle zu dem Ergebnis kommt, dass das Vorbringen, auf das sich eine solche Eingabe stützt, unbegründet ist, und die Eingabe deshalb zurückweist, muss der Person, von der die Eingabe stammt, nach Art. 28 Abs 3 Unterabs. 2 der Richtlinie 95/46 im Licht von Art. 47 der Charta der Rechtsweg offenstehen, damit sie eine solche sie beschwerende Entscheidung vor den nationalen Gerichten anfechten kann. Angesichts der in den Rn. 61 und 62 des vorliegenden Urteils angeführten Rechtsprechung müssen diese Gerichte das Verfahren aussetzen und dem Gerichtshof ein Ersuchen um Vorabentscheidung über die Gültigkeit vorlegen, wenn sie der Auffassung sind, dass einer oder mehrere der von den Parteien vorgebrachten oder gegebenenfalls von Amts wegen geprüften Ungültigkeitsgründe durchgreifen (vgl. in diesem Sinne Urteil T & L Sugars und Sidul Açúcares/Kommission, C-456/13 P, EU:C:2015:284, Rn. 48 und die dort angeführte Rechtsprechung).

65 Hält die Kontrollstelle die Rügen der Person, die sich mit einer Eingabe zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten an sie gewandt hat, dagegen für begründet, muss sie nach Art. 28 Abs 3 Unterabs. 1 dritter Gedankenstrich der Richtlinie 95/46 im Licht insbesondere von Art. 8 Abs 3 der Charta ein Klagerecht haben. Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen.

66 Nach alledem ist auf die vorgelegten Fragen zu antworten, dass Art. 25 Abs 6 der Richtlinie 95/46 im Licht der Art. 7, 8 und 47 der Charta dahin auszulegen ist, dass eine aufgrund dieser Bestimmung ergangene Entscheidung wie die Entscheidung 2000/520, in der die Kommission feststellt, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, eine Kontrollstelle eines Mitgliedstaats im Sinne von Art. 28 der Richtlinie nicht daran hindert, die Eingabe einer Person zu prüfen, die sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten, die aus einem Mitgliedstaat in dieses Drittland übermittelt wurden, bezieht, wenn diese Person geltend macht, dass das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleisteten.

Zur Gültigkeit der Entscheidung 2000/520

67 Wie aus den Erläuterungen der vorgelegten Fragen durch das vorlegende Gericht hervorgeht, macht Herr Schrems im Ausgangsverfahren geltend, dass das Recht und die Praxis der Vereinigten Staaten kein angemessenes Schutzniveau im Sinne von Art. 25 der Richtlinie 95/46 gewährleisteten. Wie der Generalanwalt in den Nrn. 123 und 124 seiner Schlussanträge ausgeführt hat, äußert Herr Schrems Zweifel an der Gültigkeit der Entscheidung 2000/520, die das vorlegende Gericht im Übrigen der Sache nach zu teilen scheint. Unter diesen Umständen ist angesichts der Feststellungen in den Rn. 60 bis 63 des

vorliegenden Urteils, um dem vorlegenden Gericht eine vollständige Antwort zu geben, zu prüfen, ob diese Entscheidung im Licht der Charta den Anforderungen der Richtlinie entspricht.

Zu den Anforderungen, die sich aus Art. 25 Abs 6 der Richtlinie 95/46 ergeben

68 Wie bereits in den Rn. 48 und 49 des vorliegenden Urteils ausgeführt, verbietet Art. 25 Abs 1 der Richtlinie 95/46 Übermittlungen personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau gewährleistet.

69 In Bezug auf die Kontrolle solcher Übermittlungen bestimmt jedoch Art. 25 Abs 6 Unterabs. 1 der Richtlinie, dass die Kommission "feststellen [kann], dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ... hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 [dieses Artikels] gewährleistet".

70 Zwar enthält weder Art. 25 Abs 2 der Richtlinie 95/46 noch eine andere Bestimmung der Richtlinie eine Definition des Begriffs des angemessenen Schutzniveaus. Insbesondere sieht Art. 25 Abs 2 der Richtlinie lediglich vor, dass die Angemessenheit des Schutzniveaus, das ein Drittland bietet, "unter Berücksichtigung aller Umstände beurteilt [wird], die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen", und enthält eine nicht abschließende Aufzählung der bei einer solchen Beurteilung zu berücksichtigenden Umstände.

71 Wie schon aus dem Wortlaut von Art. 25 Abs 6 der Richtlinie 95/46 hervorgeht, verlangt diese Bestimmung jedoch zum einen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau "gewährleistet". Zum anderen ist nach dieser Bestimmung die Angemessenheit des Schutzniveaus, das ein Drittland gewährleistet, "hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen" zu beurteilen.

72 Somit setzt Art. 25 Abs 6 der Richtlinie 95/46 die in Art. 8 Abs 1 der Charta ausdrücklich vorgesehene Pflicht zum Schutz personenbezogener Daten um und soll, wie der Generalanwalt in Nr. 139 seiner Schlussanträge ausgeführt hat, den Fortbestand des hohen Niveaus dieses Schutzes im Fall der Übermittlung personenbezogener Daten in ein Drittland gewährleisten.

73 Zwar impliziert das Wort "angemessen" in Art. 25 Abs 6 der Richtlinie 95/46, dass nicht verlangt werden kann, dass ein Drittland ein dem in der Unionsrechtsordnung garantiertes identisches Schutzniveau gewährleistet. Wie der Generalanwalt in Nr. 141 seiner Schlussanträge ausgeführt hat, ist der Ausdruck "angemessenes Schutzniveau" jedoch so zu verstehen, dass verlangt wird, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet, das dem in der Union aufgrund der Richtlinie 95/46 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. Außerdem könnte das durch die Richtlinie 95/46 im Licht der Charta garantierte hohe Schutzniveau leicht umgangen werden, indem personenbezogene Daten aus der Union in Drittländer übermittelt würden, um dort verarbeitet zu werden.

74 Aus dem ausdrücklichen Wortlaut von Art. 25 Abs 6 der Richtlinie 95/46 geht hervor, dass es die Rechtsordnung des Drittlands, auf das sich die Entscheidung der Kommission bezieht, ist, die ein angemessenes Schutzniveau gewährleisten muss. Auch wenn sich die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden können, die in der Union herangezogen werden, um die Wahrung der Anforderungen, die sich aus der Richtlinie im Licht der Charta ergeben, zu gewährleisten, müssen sich diese Mittel gleichwohl in der Praxis als wirksam erweisen, um einen Schutz zu gewährleisten, der dem in der Union garantierten der Sache nach gleichwertig ist.

75 Unter diesen Umständen ist die Kommission bei der Prüfung des von einem Drittland gebotenen Schutzniveaus verpflichtet, den Inhalt der in diesem Land geltenden, aus seinen innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen resultierenden Regeln sowie die zur Gewährleistung der Einhaltung dieser Regeln dienende Praxis zu beurteilen, wobei sie nach Art. 25 Abs 2 der Richtlinie 95/46 alle Umstände zu berücksichtigen hat, die bei einer Übermittlung personenbezogener Daten in ein Drittland eine Rolle spielen.

76 Desgleichen obliegt es der Kommission in Anbetracht der Tatsache, dass das durch ein Drittland gewährleistete Schutzniveau Veränderungen unterworfen sein kann, im Anschluss an den Erlass einer Entscheidung nach Art. 25 Abs 6 der Richtlinie 95/46 in regelmäßigen Abständen zu prüfen, ob die Feststellung zur Angemessenheit des vom fraglichen Drittland gewährleisteten Schutzniveaus in sachlicher und rechtlicher Hinsicht nach wie vor gerechtfertigt ist. Eine solche Prüfung ist jedenfalls dann geboten, wenn Anhaltspunkte vorliegen, die Zweifel daran wecken.

77 Zudem sind, wie der Generalanwalt in den Nrn. 134 und 135 seiner Schlussanträge ausgeführt hat, bei der Prüfung der Gültigkeit einer nach Art. 25 Abs 6 der Richtlinie 95/46 ergangenen Entscheidung der Kommission auch nach dem Erlass dieser Entscheidung eingetretene Umstände zu berücksichtigen.

78 Hierzu ist festzustellen, dass angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung der Privatsphäre und der großen Zahl von Personen, deren Grundrechte im Fall der Übermittlung personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, verletzt werden können, der Wertungsspielraum der Kommission hinsichtlich der Angemessenheit des durch ein Drittland gewährleisteten Schutzniveaus eingeschränkt ist, so dass eine strikte Kontrolle der Anforderungen vorzunehmen ist, die sich aus Art. 25 der Richtlinie 95/46 im Licht der Charta ergeben (vgl. entsprechend Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 47 und 48).

Zu Art. 1 der Entscheidung 2000/520

79 Die Kommission ist in Art. 1 Abs 1 der Entscheidung 2000/520 davon ausgegangen, dass die ihr als Anhang I beigefügten Grundsätze, die gemäß den Leitlinien in den dieser Entscheidung als Anhang II beigefügten FAQ umgesetzt würden, ein angemessenes Schutzniveau für personenbezogene Daten gewährleisteten, die von der Union an in den Vereinigten Staaten niedergelassene Organisationen übermittelt würden. Aus dieser Bestimmung geht hervor, dass sowohl die genannten Grundsätze als auch die FAQ vom amerikanischen Handelsministerium herausgegeben wurden.

80 Der Beitritt einer Organisation zu den Grundsätzen des "sicheren Hafens" erfolgt auf der Grundlage eines Systems der Selbstzertifizierung, wie sich aus Art. 1 Abs 2 und 3 der Entscheidung 2000/520 in Verbindung mit den FAQ 6 in ihrem Anhang II ergibt.

81 Auch wenn der Rückgriff eines Drittlands auf ein System der Selbstzertifizierung als solcher nicht gegen das Erfordernis in Art. 25 Abs 6 der Richtlinie 95/46 verstößt, dass in dem betreffenden Drittland "aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen" ein angemessenes Schutzniveau gewährleistet sein muss, beruht die Zuverlässigkeit eines solchen Systems im Hinblick auf dieses Erfordernis wesentlich auf der Schaffung wirksamer Überwachungs- und Kontrollmechanismen, die es erlauben, in der Praxis etwaige Verstöße gegen Regeln zur Gewährleistung des Schutzes der Grundrechte, insbesondere des Rechts auf Achtung der Privatsphäre sowie des Rechts auf den Schutz personenbezogener Daten, zu ermitteln und zu ahnden.

82 Im vorliegenden Fall sind die Grundsätze des "sicheren Hafens" nach Abs 2 von Anhang I der Entscheidung 2000/520 "ausschließlich für den Gebrauch durch US-Organisationen bestimmt, die personenbezogene Daten aus der Europäischen Union erhalten, um sich für den 'sicheren Hafen' und die daraus erwachsende Vermutung der 'Angemessenheit' des Datenschutzes zu qualifizieren". Diese Grundsätze gelten somit nur für selbstzertifizierte US-Organisationen, die aus der Union personenbezogene Daten erhalten, ohne dass von den amerikanischen Behörden die Einhaltung der genannten Grundsätze verlangt wird.

83 Zudem betrifft die Entscheidung 2000/520 nach ihrem Art. 2 "nur die Angemessenheit des Schutzes, der in den Vereinigten Staaten nach den entsprechend den FAQ umgesetzten Grundsätzen [des 'sicheren Hafens'] gewährt wird, um die Anforderungen des Artikels 25 Absatz 1 der Richtlinie [95/46] zu erfüllen"; sie enthält dagegen keine hinreichenden Feststellungen zu den Maßnahmen, mit denen die Vereinigten Staaten von Amerika aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen im Sinne von Art. 25 Abs 6 der Richtlinie ein angemessenes Schutzniveau gewährleisten.

84 Hinzu kommt, dass die Geltung der genannten Grundsätze nach Abs 4 von Anhang I der Entscheidung 2000/520 begrenzt werden kann, und zwar u. a. "insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss", sowie "durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte".

85 Hierzu wird in Abschnitt B von Anhang IV der Entscheidung 2000/520 hinsichtlich der Grenzen für die Geltung der Grundsätze des "sicheren Hafens" Folgendes hervorgehoben: "Es steht jedoch eindeutig fest, dass, wenn aufgrund des US-amerikanischen Rechts eine den Grundsätzen des sicheren Hafens entgegenstehende Verpflichtung auferlegt wird, die US-Unternehmen die Gesetze einhalten müssen, und zwar ungeachtet dessen, ob sie auf die Grundsätze des sicheren Hafens verpflichtet sind oder nicht."

86 In der Entscheidung 2000/520 wird somit den "Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen" Vorrang vor den Grundsätzen des "sicheren Hafens" eingeräumt; aufgrund dieses Vorrangs sind die

selbstzertifizierten US-Organisationen, die aus der Union personenbezogene Daten erhalten, ohne jede Einschränkung verpflichtet, die Grundsätze des "sicheren Hafens" unangewandt zu lassen, wenn sie in Widerstreit zu den genannten Erfordernissen stehen und sich deshalb als mit ihnen unvereinbar erweisen.

87 Angesichts ihres generellen Charakters ermöglicht die Ausnahme in Abs 4 von Anhang I der Entscheidung 2000/520 es daher, gestützt auf Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder von 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. Für die Feststellung des Vorliegens eines Eingriffs in das Grundrecht auf Achtung der Privatsphäre kommt es nicht darauf an, ob die betreffenden Informationen über die Privatsphäre sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten (Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 33 und die dort angeführte Rechtsprechung).

88 Überdies enthält die Entscheidung 2000/520 keine Feststellung dazu, ob es in den Vereinigten Staaten staatliche Regeln gibt, die dazu dienen, etwaige Eingriffe - zu denen die staatlichen Stellen dieses Landes in Verfolgung berechtigter Ziele wie der nationalen Sicherheit berechtigt wären - in die Grundrechte der Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden, zu begrenzen.

89 Hinzu kommt, dass die Entscheidung 2000/520 keine Feststellung zum Bestehen eines wirksamen gerichtlichen Rechtsschutzes gegen derartige Eingriffe enthält. Wie der Generalanwalt in den Nrn. 204 bis 206 seiner Schlussanträge ausgeführt hat, beziehen sich die privaten Schiedsmechanismen und die Verfahren vor der Federal Trade Commission, deren insbesondere in den FAQ 11 in Anhang II der Entscheidung beschriebene Befugnisse auf Handelsstreitigkeiten beschränkt sind, auf die Einhaltung der Grundsätze des "sicheren Hafens" durch die amerikanischen Unternehmen und können nicht im Rahmen von Streitigkeiten über die Rechtmäßigkeit von Eingriffen in Grundrechte, die sich aus Maßnahmen staatlichen Ursprungs ergeben, zur Anwendung kommen.

90 Die vorstehende Analyse der Entscheidung 2000/520 wird im Übrigen bestätigt durch die von der Kommission selbst vorgenommene Beurteilung der aus der Umsetzung dieser Entscheidung resultierenden Sachlage. Sie stellt nämlich insbesondere in den Abschnitten 2 und 3.2 der Mitteilung COM(2013) 846 final sowie in den Abschnitten 7.1, 7.2 und 8 der Mitteilung COM(2013) 847 final, die in den Rn. 13 bis 16 bzw. den Rn. 22, 23 und 25 des vorliegenden Urteils wiedergegeben werden, fest, dass die amerikanischen Behörden auf die aus den Mitgliedstaaten in die Vereinigten Staaten übermittelten personenbezogenen Daten zugreifen und sie in einer Weise verarbeiten konnten, die namentlich mit den Zielsetzungen ihrer Übermittlung unvereinbar war und über das hinausging, was zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig war. Desgleichen stellte die Kommission fest, dass es für die Betroffenen keine administrativen oder gerichtlichen Rechtsbehelfe gab, die es ihnen erlaubten, Zugang zu den sie betreffenden Daten zu erhalten und gegebenenfalls deren Berichtigung oder Löschung zu erwirken.

91 Zu dem innerhalb der Union garantierten Schutzniveau der Freiheiten und Grundrechte ist festzustellen, dass eine Unionsregelung, die einen Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte enthält, nach ständiger Rechtsprechung des Gerichtshofs klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen muss, so dass die Personen, deren personenbezogene

Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht (Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 54 und 55 sowie die dort angeführte Rechtsprechung).

92 Darüber hinaus verlangt der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene vor allem, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken (Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 52 und die dort angeführte Rechtsprechung).

93 Nicht auf das absolut Notwendige beschränkt ist eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, 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 (vgl. in diesem Sinne, in Bezug auf die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG [ABl. L 105, S. 54], Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 57 bis 61).

94 Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens (vgl. in diesem Sinne Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 39).

95 Desgleichen 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. Nach Art. 47 Abs 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Insoweit ist schon das Vorhandensein einer wirksamen, zur Gewährleistung der Einhaltung des Unionsrechts dienenden gerichtlichen Kontrolle dem Wesen eines Rechtsstaats inhärent (vgl. in diesem Sinne Urteile Les Verts/Parlament, 294/83, EU:C:1986:166, Rn. 23, Johnston, 222/84, EU:C:1986:206, Rn. 18 und 19, Heylens u. a., 222/86, EU:C:1987:442, Rn. 14, sowie UGT-Rioja u. a., C-428/06 bis C-434/06, EU:C:2008:488, Rn. 80).

96 Nach den namentlich in den Rn. 71, 73 und 74 des vorliegenden Urteils getroffenen Feststellungen erfordert der Erlass einer Entscheidung der Kommission nach Art. 25 Abs 6 der Richtlinie 95/46 die gebührend begründete Feststellung dieses Organs, dass das betreffende Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Grundrechte gewährleistet, das dem in der

Rechtsordnung der Union garantierten Niveau, wie es sich insbesondere aus den vorstehenden Randnummern des vorliegenden Urteils ergibt, der Sache nach gleichwertig ist.

97 Die Kommission hat jedoch in der Entscheidung 2000/520 nicht festgestellt, dass die Vereinigten Staaten von Amerika aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein angemessenes Schutzniveau "gewährleisten".

98 Daher ist, ohne dass es einer Prüfung des Inhalts der Grundsätze des "sicheren Hafens" bedarf, der Schluss zu ziehen, dass Art. 1 der Entscheidung 2000/520 gegen die in Art. 25 Abs 6 der Richtlinie 95/46 im Licht der Charta festgelegten Anforderungen verstößt und aus diesem Grund ungültig ist.

Zu Art. 3 der Entscheidung 2000/520

99 Wie aus den Erwägungen in den Rn. 53, 57 und 63 des vorliegenden Urteils hervorgeht, müssen die nationalen Kontrollstellen nach Art. 28 der Richtlinie 95/46 im Licht insbesondere von Art. 8 der Charta jede Eingabe einer Person zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten in völliger Unabhängigkeit prüfen können. Dies gilt in besonderem Maß, wenn diese Person im Rahmen einer solchen Eingabe Fragen nach der Vereinbarkeit einer nach Art. 25 Abs 6 der Richtlinie ergangenen Entscheidung der Kommission mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte von Personen aufwirft.

100 Art. 3 Abs 1 Unterabs. 1 der Entscheidung 2000/520 sieht aber eine spezifische Regelung hinsichtlich der Befugnisse vor, über die die nationalen Kontrollstellen in Bezug auf eine von der Kommission zum angemessenen Schutzniveau getroffene Feststellung im Sinne von Art. 25 der Richtlinie 95/46 verfügen.

101 Nach dieser Bestimmung können die Kontrollstellen unter restriktiven Voraussetzungen, mit denen eine erhöhte Eingriffsschwelle geschaffen wird, "[u]ngeachtet ihrer Befugnisse, tätig zu werden, um die Einhaltung einzelstaatlicher Vorschriften, die gemäß anderen Bestimmungen als denjenigen des Artikels 25 der Richtlinie [95/46] erlassen wurden, zu gewährleisten, ... die Datenübermittlung an eine Organisation [aussetzen], die den Grundsätzen [der Entscheidung 2000/520] beigetreten ist". Diese Bestimmung beeinträchtigt zwar nicht die Befugnisse der Kontrollstellen, tätig zu werden, um die Einhaltung einzelstaatlicher Vorschriften zu gewährleisten, die gemäß der Richtlinie erlassen wurden, doch nimmt sie ihnen die Möglichkeit, Maßnahmen zu ergreifen, die die Einhaltung von Art. 25 der Richtlinie gewährleisten sollen.

102 Art. 3 Abs 1 Unterabs. 1 der Entscheidung 2000/520 ist somit dahin zu verstehen, dass er den nationalen Kontrollstellen Befugnisse entzieht, die ihnen nach Art. 28 der Richtlinie 95/46 für den Fall zustehen, dass eine Person im Rahmen einer Eingabe aufgrund dieser Bestimmung Gesichtspunkte vorbringt, die geeignet sind, die Vereinbarkeit einer Entscheidung der Kommission, mit der auf der Grundlage von Art. 25 Abs 6 der Richtlinie festgestellt wird, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte von Personen in Frage zu stellen.

103 Die Durchführungsbefugnis, die der Unionsgesetzgeber der Kommission in Art. 25 Abs 6 der Richtlinie 95/46 einräumt, berechtigt dieses Organ jedoch nicht, die in der vorstehenden Randnummer genannten Befugnisse der nationalen Kontrollstellen zu beschränken.

104 Unter diesen Umständen ist festzustellen, dass die Kommission mit dem Erlass von Art. 3 der Entscheidung 2000/520 die ihr durch Art. 25 Abs 6 der Richtlinie 95/46 im Licht der Charta übertragene Zuständigkeit überschritten hat, so dass dieser Artikel ungültig ist.

105 Da die Art. 1 und 3 der Entscheidung 2000/520 untrennbar mit deren Art. 2 und 4 sowie deren Anhängen verbunden sind, berührt ihre Ungültigkeit die Gültigkeit der gesamten Entscheidung.

106 Aus den vorstehenden Erwägungen ist der Schluss zu ziehen, dass die Entscheidung 2000/520 ungültig ist.

Kosten

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

Aus diesen Gründen hat der Gerichtshof (Große Kammer) für Recht erkannt:
1. Art. 25 Abs 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr in der durch die Verordnung (EG) Nr. 1882/2003 des Europäischen Parlaments und des Rates vom 29. September 2003 geänderten Fassung ist im Licht der Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass eine aufgrund dieser Bestimmung ergangene Entscheidung wie die Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46 über die Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglichen "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, in der die Europäische Kommission feststellt, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, eine Kontrollstelle eines Mitgliedstaats im Sinne von Art. 28 der Richtlinie in geänderter Fassung nicht daran hindert, die Eingabe einer Person zu prüfen, die sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten, die aus einem Mitgliedstaat in dieses Drittland übermittelt wurden, bezieht, wenn diese Person geltend macht, dass das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleisteten.
2. Die Entscheidung 2000/520 ist ungültig.

*Anmerkung**

I. Das Problem

Der aus Salzburg stammende Kläger, Mag. *Max Schrems*, war ca. seit dem Jahr 2008 Facebook-Nutzer. Um dieses soziale Netzwerk verwenden zu dürfen, musste er bei seiner Anmeldung einen Vertrag mit Facebook Limited Ireland abschließen, einer Tochtergesellschaft der US-amerikanischen Facebook Inc. Die Facebook-Nutzung brachte und bringt es mit sich, dass die vornehmlich personenbezogenen Daten der im Unionsgebiet

* RA Hon.-Prof. Dr. *Clemens Thiele*, LL.M. Tax (GGU), *Anwalt.Thiele@eurolawyer.at*, Näheres unter http://www.eurolawyer.at.

wohnhaften Anwender ganz oder teilweise an Server der Facebook Inc., die sich in den USA befinden, übermittelt und dort verarbeitet werden. Der spätere Kläger legte beim *Data Protection Commissioner* (der Irischen Datenschutzbehörde) eine Beschwerde ein, mit der er diesen aufforderte, in Ausübung der ihm übertragenen Befugnisse Facebook Ireland die Übermittlung seiner personenbezogenen Daten in die Vereinigten Staaten zu untersagen.[1]
Er machte geltend, das Recht und die Praxis der US-amerikanischen Behörden bzw. Unternehmen der sog. „Safe Harbor Liste“[2] keinen ausreichenden Schutz der in diesem Land gespeicherten personenbezogenen Daten vor den Überwachungstätigkeiten der dortigen Behörden böten. Dabei verwies er u.a. auf die von *Edward Snowden* enthüllten Tätigkeiten der National Security Agency (im Folgenden: NSA).
Die Irsche Datenschutzbehörde wies die Beschwerde als unbegründet zurück und stützte sich auf das wirksame „Safe Harbor Abkommen“ der EU mit den USA. Die EU-Kommission hätte in der eingangs zitierten Entscheidung vom 26.7.2000, Nr. 2000/520/EG, längst rechtsverbindlich festgestellt, dass die Vereinigten Staaten von Amerika ein angemessenes Schutzniveau für EU-Bürger hinsichtlich ihrer personenbezogenen Daten gewährleisteten. Mag. *Schrems* erhob daraufhin Klage beim High Court, welches Gericht für die Überprüfung datenschutzrechtlicher Entscheidungen zunächst zuständig war. Das Irische Gericht unterbrach das Verfahren und legte dem EuGH folgende Fragen zur Vorabentscheidung vor:

> (1) Ist ein unabhängiger Amtsträger, der von Rechts wegen mit der Handhabung und der Durchsetzung von Rechtsvorschriften über den Datenschutz betraut ist, bei der Prüfung einer bei ihm eingelegten Beschwerde, dass personenbezogene Daten in ein Drittland (im vorliegenden Fall in die Vereinigten Staaten von Amerika) übermittelt würden, dessen Recht und Praxis keinen angemessenen Schutz der Betroffenen gewährleisteten, im Hinblick auf die Art 7, 8 und 47 der Charta, unbeschadet der Bestimmungen von Art 25 Abs 6 der Richtlinie 95/46, absolut an die in der Entscheidung 2000/520 enthaltene gegenteilige Feststellung der Union gebunden?
> (2) Oder kann und/oder muss der Amtsträger stattdessen im Licht tatsächlicher Entwicklungen, die seit der erstmaligen Veröffentlichung der Entscheidung der Kommission eingetreten sind, eigene Ermittlungen in dieser Sache anstellen?

Der EuGH hatte sich daher zusammengefasst sowohl mit der Gültigkeit der seinerzeitigen Kommissionsentscheidung als auch mit dem Einfluss der wesentlich später ergangenen EU-Grundrechtecharta (GRC), insbesondere den darin enthaltenen Grundrechten auf Achtung der Privat- und Intimsphäre sowie des Datenschutzgrundrechts nach Art 8 GRC zu befassen.

II. Die Entscheidung des Gerichts

Der EuGH verneinte die Frage, ob die EU-Kommission-Entscheidung aus dem Jahr 2000 die nationale Datenschutzbehörde daran hindert, eine Beschwerde zu prüfen, mit der geltend gemacht wird, dass ein Drittland kein ausreichendes Datenschutzniveau gewährleiste, mit aller Deutlichkeit. Dies verneinte der EuGH.
Die Entscheidung der Kommission vom 26.7.2000 hindert die Kontrolle der Übermittlung personenbezogener Daten in ein Drittland im Einzelfall nicht. Die "Safe-Harbor-Entscheidung" ist ungültig.
Die nationalen Datenschutzbehörden müssen in völliger Unabhängigkeit prüfen können, ob die Europäischen Datenschutzanforderungen der GRC und der DS-RL vzw. EDRL eingehalten werden. Die Kommission hatte keine Kompetenz, diese verfassungsrechtlich gewährleisteten Rechte der EU-Bürger zu beschränken. Die von der Kommission in ihrer Entscheidung geprüfte "Safe-Harbor-Regelung" bietet keinen ausreichenden Schutz

[1] Zu den Hintergründen dieses seit Jahren schwelenden Rechtsstreits vgl. *Thiele*, Europe versus Facebook. Wiener Studenten organisieren den datenschutzrechtlichen Widerstand, jusIT 2011, 174 mwN.
[2] Abrufbar unter https://safeharbor.export.gov/list.aspx (08.01.2016).

personenbezogener Daten. Sie gilt allein für die Unternehmen, die sich ihr unterwerfen, nicht aber für die staatlichen Behörden. Außerdem sind die nationale Sicherheit, das öffentliche Interesse und die Durchführung von Gesetzen nach amerikanischem Recht vorrangig. Amerikanische Unternehmen können daher ohne jede Einschränkung verpflichtet werden, die Datenschutzregeln des "Safe-Harbor-Abkommens" unangwendet zu lassen.
Eine Regelung, die es Behörden gestattet, uneingeschränkt auf den Inhalt elektronischer Kommunikation zuzugreifen, verletzt jedoch das europäische Grundrecht auf Achtung des Privatlebens.
Da es Betroffenen nicht möglich ist, mittels eines Rechtsbehelfs Zugang zu den personenbezogenen Daten zu erhalten oder ihre Berichtigung oder Löschung zu erwirken, ist zudem das Grundrecht auf wirksamen gerichtlichen Rechtsschutz verletzt.
Die Frage, ob die USA außerhalb von "Safe-Harbor" aufgrund von innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen tatsächlich ein Schutzniveau gewährleisten, das dem europäischen Niveau gleichwertig ist, hatte die EU-Kommission in ihrer Entscheidung seinerzeit nicht geprüft.

III. Kritische Würdigung und Ausblick

Das vorliegende Urteil ist nicht nur aufgrund seiner über hundert Randzahlen überaus gewichtig. Es stellt einen „*leading case*“ des Europäischen Datenschutzrechts[3] dar – ähnlich der Lindqvist-Entscheidung[4] oder dem Urteil in der Google-Spain-Sache.[5]
Die juristische Diskussion zum Datentransfer in die USA wird nicht nur in den Fachmedien, sondern auch in den Tageszeitungen geführt.[6]
Von den zahlreichen Aspekten möchte ich jene von *Härting*[7] herausgreifen. Dieser ausgezeichnete Kenner des Internetrechts hält das vorliegende Urteil vor allem deshalb für so richtungsweisend, "weil sich der EuGH selbst die Befugnis einräumt, letztverbindlich darüber zu entscheiden, ob ein europäischer Rechtsakt mit der Grundrechtecharta (GRC) vereinbar ist". Als die EU-Kommission ihre Safe-Harbor-Entscheidung getroffen hat, gehörten die Art 7, 8 GRC noch gar nicht zum Rechtsbestand der Union. Die grundlegende Frage, wer als oberstes Verfassungsgericht der EU über die Einhaltung des Grundrechtekatalogs bei (hoheitlichen) Handlungen der Unions-Organe wacht und gegebenenfalls bei Verstößen zu entscheiden hat, beantwortet die GRC so nicht. Der EuGH beansprucht für sich selbst das alleinige und ausschließliche Recht, über die Verfassungskonformität europäischer Rechtsakte zu entscheiden. Diese Gretchenfrage einer funktionierenden Verfassungsordnung stellt sich unabhängig von der jeweiligen materiell-rechtlichen Ausgestaltung und ist systemimmanent. In den USA ist dieses Auslegungsmonopol zugunsten des US Supreme Court von eben diesem selbst schon in dem jeden "One L"[8] geläufigen *Marbury vs. Madison*[9] Entscheidung

---

[3] Statt vieler *Jahnel*, Keine Datenübermittlung in die USA? – Die EuGH-Entscheidung zum Safe Harbor“, jusIT 2015/95, 234 mwN.
[4] EuGH 6.11.2003, C-101/01 (Lindqvist) = EuGRZ 2003, 714 = MR 2004, 83 (*Kronegger*) = ÖJZ 2004/45, 741 (*Hörlsberger*) = ZER 2004/330, 93.
[5] EuGH 13.5.2014, C-131/12 (Google Spain und Google) = jusIT 2014/53, 111 = RdW 2014/345, 313 = ÖJZ 2014/100, 690 (*Lehofer*) = MR-Int 2014, 3 (Leupold) = MR-Int 2014, 7 (*Briem*) = ecolex 2014, 665 = ecolex 2014, 676 (*Zankl*) = jusIT 2014/72, 149 (*Jahnel*) = Dako 2014/11, 21 = SWI 2014, 293 = ZIR-Slg 2014/81, 203 = ZIR 2014, 204 (*König*) = ZfRV-LS 2014/35, 165 = EuGRZ 2014, 320 = wbl 2014/194, 574 = NLMR 2014, 254 = FJ 2014, 191 (*Novacek*) = ZVG 2014, 749 (*Weh*) = ZTR 2014, 146.
[6] Vgl. die Nachweise bei Jahnel, jusIT 2015, 234.
[7] Entscheidungsanmerkung, CR 2015/ H 10, auch online abrufbar unter http://www.cr-online.de/blog/2015/10/06/safe-harbor-geburtsstunde-eines-europaeischen-verfassungsgerichts/ (08.01.2016).
[8] So die Bezeichnung für einen Jusstudenten im ersten Jahr an der Law School.
[9] US Supreme Court 1.2.1803, *Marbury v. Madison*, 5 U.S. 137, 1 Cranch 137, 2 L. Ed. 60 (1803), abrufbar unter http://caselaw.findlaw.com/us-supreme-court/5/137.html (08.01.2016); zu den historischen Hintergründen vgl. http://www.history.com/topics/marbury-v-madison (08.01.2016).

getroffen worden. Das vorliegende Urteil darf auch insofern als "leading case" bezeichnet werden.

Ausblick: Als unmittelbare Konsequenz für den anhängigen Prozess in Irland bedeutet das Urteil, dass die Irische Datenschutzbehörde die Beschwerde von Mag. *Schrems* nun eingehend prüfen und schließlich entscheiden muss, ob die angefochtene Datenübermittlung auszusetzen ist, weil die USA per se kein angemessenes Schutzniveau für personenbezogene Daten gewährleisten. Unternehmen, die Datenübertragungen personenbezogener Daten mit Unternehmen in den USA auf Basis des Safe-Harbor-Abkommens vereinbart haben, müssen ihre Verträge auf neue Grundlagen stellen, gegebenenfalls die Zusammenarbeit mit dem amerikanischen Unternehmen beenden. Betroffen ist eine Vielzahl von Unternehmen, die heute Cloud-Angebote amerikanischer Anbieter nutzen und dabei personenbezogene Daten in die USA transferieren bzw. dort speichern und verarbeiten.

Die EU-Kommission hat die Verhandlungen mit den USA über einen neuen und sicheren Rahmen für die Übermittlung personenbezogener Daten intensiviert.[10] Für die Übergangszeit hat die Kommission am 6.11.2015 Leitlinien[11] vorgelegt, die erläutern, unter welchen Bedingungen Unternehmen auf rechtmäßige Art und Weise vorübergehend Daten übermitteln können.

Die Kommission verfolgt das Ziel, die Gespräche innerhalb von drei Monaten abzuschließen. Bis dahin bleibt Unternehmen nichts anderes übrig, als das EuGH-Urteil zu befolgen und nach Möglichkeit auf alternative Datenübermittlungsinstrumente zurückzugreifen. In den jetzt veröffentlichten Leitlinien werden die Folgen des Urteils analysiert und alternative Verfahren für die Übermittlung von personenbezogenen Daten in die USA erörtert. Die Kommission wird zudem weiterhin eng mit den unabhängigen Datenschutzbehörden zusammenarbeiten, um eine möglichst einheitliche Umsetzung des Urteils sicherzustellen.

In der Mitteilung werden alternative Grundlagen für die Übermittlung personenbezogener Daten in die USA dargelegt, ohne der Unabhängigkeit und den Befugnissen der Datenschutzbehörden der Mitgliedstaaten zur Prüfung der Rechtmäßigkeit einer solchen Datenübermittlung vorzugreifen. Datenübertragungen von Unternehmen können derzeit auf folgenden Grundlagen erfolgen:

- **vertragliche Regeln**: Vertragliche Regeln müssen bestimmte Pflichten (z.B. Sicherheitsmaßnahmen, Benachrichtigung der betroffenen Person, Sicherheitsvorkehrungen bei der Übermittlung sensibler Daten usw.) vorsehen.[12]
- **verbindliche unternehmensinterne Vorschriften für unternehmensgruppeninterne Datenübermittlungen** ("*binding corporate rules*"): Auf der Grundlage derartiger Vorschriften können personenbezogene Daten unbegrenzt zwischen den Unternehmen einer weltweit operierenden Unternehmensgruppe übermittelt werden. Die Übermittlungen bedürfen jeweils der Zustimmung der Datenschutzbehörde des Mitgliedstaats, aus dem das multinationale Unternehmen Daten übermitteln möchte.
- **Ausnahmeregelungen**:
    - Datenübermittlung zum Abschluss oder zur Erfüllung eines Vertrags (einschließlich vorvertraglicher Situationen, zB zur Buchung eines Flugs oder eines Hotelzimmers in den Vereinigten Staaten);
    - Durchsetzung oder Verteidigung von Rechtsansprüchen;

[10] Vgl. dazu auch die Gemeinsame Erklärung der Art 29 Datenschutzgruppe vom 15.10.2015, die eine "Schonfrist" bis Ende Jänner 2016 vorschlägt, abrufbar in der deutschen Übersetzung unter https://www.datenschutz.hessen.de/download.php?download_ID=335 (08.01.2016).

[11] Abrufbar in englischer Sprache unter http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf (08.01.2016).

[12] Die Mustervertragsklauseln sind abrufbar unter http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (08.01.2016); siehe dazu *Jahnel*, jusIT 2015, 234 (238 f).

- (falls kein anderer Grund[13] besteht): Datenübermittlung bei aus freien Stücken und in voller Sachkenntnis erfolgender Zustimmung der betroffenen Person

Ergänzend ist dazu anzumerken, dass die Einwilligung des Betroffenen nach § 4 Z 14 DSG 2000freiwillig sein muss und darüber hinaus jederzeit ohne Angaben von Gründen widerrufen werden kann. Für einen Datentransfer in die USA bedarf es idR der Erfüllung der Melde- bzw. Genehmigungspflicht an die Datenschutzbehörde, ausgenommen es liegt eine Standard- oder Musteranwendung vor. Insoweit kommt insbes die SA033 "Datenübermittlung im Konzern" in Betracht, die allerdings nur einen eingeschränkten Bereich des konzerninternen Datentransfers erfasst.[14]

IV. Zusammenfassung

Der EuGH hat das Safe-Harbor-Abkommen zwischen den USA und der EU für unwirksam erklärt. Die Übertragung personenbezogener Daten aus der EU in Drittstaaten ist nur zulässig, wenn dort ein vergleichbares Datenschutzniveau gewährleistet ist. Die nationalen Datenschutzbehörden bleiben also uneingeschränkt berechtigt, die Voraussetzungen einer Datenübermittlung in die USA zB durch Facebook eigenständig zu prüfen.

[13] Vgl. §§ 45, 48 DSG 2000; dazu *Jahnel*, jusIT 2015, 234 (238).
[14] Vgl. dazu *Thiele*, Neues zur Datenübermittlung im Konzern, Videoüberwachung & Co, jusIT 2012/85, 178.