EUROPÄISCHE
KOMMISSION

Brüssel, den 6.11.2015
COM(2015) 566 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

zu der Übermittlung personenbezogener Daten aus der EU in die Vereinigten Staaten von Amerika auf der Grundlage der Richtlinie 95/46/EG nach dem Urteil des Gerichtshofs in der Rechtssache C-362/14 (Schrems)

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

zu der Übermittlung personenbezogener Daten aus der EU in die Vereinigten Staaten von Amerika auf der Grundlage der Richtlinie 95/46/EG nach dem Urteil des Gerichtshofs in der Rechtssache C-362/14 (Schrems)

1. EINFÜHRUNG: DIE AUFHEBUNG DER SAFE-HARBOR-ENTSCHEIDUNG

In seinem Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14 (Schrems)[1] bestätigt der Gerichtshof der Europäischen Union (im Folgenden „Gerichtshof") erneut den Stellenwert des in der EU-Grundrechtecharta verankerten Grundrechts auf den Schutz personenbezogener Daten, und zwar auch bei Übermittlung dieser Daten außerhalb der EU.

Die Übermittlung personenbezogener Daten ist ein wesentliches Element der transatlantischen Beziehungen. Die EU und die USA sind füreinander die wichtigsten Handelspartner, und Datenübermittlungen sind zunehmend Bestandteil ihrer Handelsbeziehungen.

Mit ihrer Entscheidung 2000/520/EG vom 20. Juli 2000 (im Folgenden „Safe-Harbor-Entscheidung") erkannte die Kommission das durch die Safe-Harbor-Regelung gebotene Datenschutzniveau als angemessen an, um den Datenverkehr zu erleichtern und gleichzeitig ein hohes Datenschutzniveau zu gewährleisten. In dieser auf Artikel 25 Absatz 6 der Richtlinie 95/46/EG[2] gestützten Entscheidung hatte die Kommission die vom US-Handelsministerium herausgegebenen Grundsätze des „sicheren Hafens" und die diesbezüglichen „Häufig gestellten Fragen" (FAQ) für die Zwecke der Übermittlung personenbezogener Daten aus der EU als Garantie für einen angemessenen Schutz anerkannt[3]. Infolgedessen konnten personenbezogene Daten aus EU-Mitgliedstaaten ungehindert an Unternehmen in den Vereinigten Staaten, die diesen Grundsätzen beigetreten waren, übermittelt werden, obwohl es in den Vereinigten Staaten kein allgemeines Datenschutzgesetz gibt. Die Funktionsweise der Safe-Harbor-Regelung basiert auf den Verpflichtungserklärungen und Selbstzertifizierungen der beteiligten Unternehmen. Der Beitritt zu den Safe-Harbor-Grundsätzen und den FAQ ist zwar freiwillig, doch ist diese Regelung nach US-Recht für die Unternehmen, die sich ihr anschließen, verbindlich. Für ihre Durchsetzung ist die Federal Trade Commission zuständig.[4]

In seinem Urteil vom 6. Oktober 2015 erklärte der Gerichtshof die Safe-Harbor-Entscheidung für ungültig. Vor diesem Hintergrund soll die vorliegende Mitteilung einen Überblick über alternative Instrumente der Richtlinie 95/46/EG geben, auf die der transatlantische Datentransfer gestützt werden kann, wenn es keinen Kommissionsbeschluss gibt, in dem die Angemessenheit des Datenschutzniveaus festgestellt wird. Gleichzeitig wird kurz auf die

---

1 Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner, ECLI:EU:C:2015:650 (im Folgenden das „Schrems-Urteil" oder das „Urteil").

2 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 – im Folgenden „Richtlinie 95/46/EG" oder „Richtlinie" (ABl. L 281 vom 23.11.1995, S. 31).

3 In dieser Mitteilung schließt der Ausdruck „EU" den EWR ein. Wird demnach auf die Mitgliedstaaten Bezug genommen, sind darunter alle EWR-Staaten zu verstehen.

4 Einen ausführlichen Überblick über die Safe-Harbor-Regelung bietet die Mitteilung der Kommission 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).

Folgen des Urteils für andere Angemessenheitsentscheidungen bzw. -beschlüsse der Kommission eingegangen. In seinem Urteil stellte der Gerichtshof klar, dass eine Angemessenheitsentscheidung gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG auf der Feststellung der Kommission beruht, dass personenbezogene Daten in dem betreffenden Drittland in einem Maße geschützt sind, das mit dem in der Union aufgrund der Richtlinie im Licht der Grundrechtscharta garantierten Schutzniveau zwar nicht unbedingt identisch, aber „der Sache nach gleichwertig" ist. Zu der Safe-Harbor-Entscheidung stellte der Gerichtshof fest, dass sie weder zu den Beschränkungen des Zugangs der US-Behörden zu auf der Grundlage dieser Entscheidung übermittelten Daten noch zum Bestehen eines wirksamen gerichtlichen Rechtsschutzes gegen derartige Eingriffe hinreichende Feststellungen der Kommission enthalte. Insbesondere, so der Gerichtshof weiter, verletze eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens. Der Gerichtshof bestätigte darüber hinaus, dass die Datenschutzbehörden der Mitgliedstaaten auch dann, wenn eine Angemessenheitsentscheidung nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG vorliegt, berechtigt und verpflichtet sind, in völliger Unabhängigkeit zu prüfen, ob die Anforderungen der Richtlinie 95/46/EG in Verbindung mit den Artikeln 7, 8 und 47 der Grundrechtscharta bei der Übermittlung der Daten in ein Drittland gewahrt werden. Gleichzeitig wies der Gerichtshof aber auch darauf hin, dass nur der Gerichtshof der Europäischen Union befugt ist, die Ungültigkeit eines Unionsrechtsakts wie eines Angemessenheitsbeschlusses der Kommission festzustellen.

Das Urteil des Gerichtshofs stützt sich auf die Mitteilung der Kommission von 2013 über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen[5], in der die Kommission auf gewisse Unzulänglichkeiten verwiesen und 13 Empfehlungen formuliert hatte. Auf der Grundlage dieser Empfehlungen führt die Kommission seit Januar 2014 Gespräche mit den US-Behörden im Hinblick auf eine neue, robustere Regelung des transatlantischen Datenaustauschs.

Die Kommission bleibt nach diesem Urteil dem Ziel eines neuen, soliden Rahmens für den transatlantischen Transfer personenbezogener Daten verpflichtet. Dementsprechend hat sie die Gespräche mit der US-Regierung umgehend wiederaufgenommen und vertieft, um sicherzustellen, dass jede neue Regelung des transatlantischen Datentransfers mit den Anforderungen des Gerichtshofs in vollem Umfang vereinbar ist. Eine solche Regelung muss hinreichende Beschränkungen, Garantien und gerichtliche Kontrollmechanismen enthalten, um den kontinuierlichen Schutz der personenbezogenen Daten von EU-Bürgern auch im Hinblick auf einen möglichen behördlichen Zugriff zu Strafverfolgungszwecken und Zwecken der nationalen Sicherheit zu gewährleisten. Die Wirtschaft äußerte sich besorgt, was die Möglichkeit angeht, Datenübermittlungen bis zu einer neuen Regelung fortzusetzen.[6] Es

---

[5] Mitteilung der Kommission 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 vom 27.11.2013). Siehe auch Mitteilung der Kommission an das Europäische Parlament und den Rat „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA" (COM(2013) 846 final vom 27.11.2013) und die diesbezügliche Pressemitteilung „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA – Häufig gestellte Fragen" (MEMO/13/1059 vom 27.11.2013).

[6] Diesbezügliche Bedenken wurden beispielsweise von Wirtschaftsverbänden auf einer Sitzung geäußert, die kurz nach dem Schrems-Urteil am 14. Oktober von Vizepräsident Ansip und den Kommissionsmitgliedern Jourová und Oettinger einberufen worden war. Vgl. Daily News vom 14.10.2015 (MEX/15/5840). In diesem Sinne auch der offene Brief vom 13. Oktober 2015 an Kommissionspräsident Jean-Claude Juncker, der von mehreren Wirtschaftsverbänden und Unternehmen aus der EU und den USA unterzeichnet worden ist: „Open letter on the implementation of the CJEU Judgement on Case C-362/14 Maximillian Schrems v

muss daher geklärt werden, unter welchen Bedingungen Daten weiter übermittelt werden können. Die Artikel-29-Datenschutzgruppe – das unabhängige Beratungsgremium, in dem alle Datenschutzbehörden der Mitgliedstaaten sowie der Europäische Datenschutzbeauftragte vertreten sind – hat daraufhin am 16. Oktober in einer Stellungnahme[7] erste Schlussfolgerungen aus dem Urteil gezogen. Die Gruppe gab unter anderem folgende Empfehlungen für Datenübermittlungen ab:

– Datenübermittlungen können nicht länger auf die für ungültig erklärte Safe-Harbor-Entscheidung der Kommission gestützt werden.

– In der Zwischenzeit können als Grundlage für Datenübermittlungen Standardvertragsklauseln und verbindliche unternehmensinterne Datenschutzvorschriften (BCR) verwendet werden. Die Artikel-29-Datenschutzgruppe wird aber die Auswirkungen des Urteils auf diese Optionen weiter prüfen.

Die Gruppe ruft die Mitgliedstaaten und EU-Organe auf, Gespräche mit den US-Behörden aufzunehmen, um eine rechtliche und technische Lösung für den Datentransfer zu finden. Die Verhandlungen über eine neue Safe-Harbor-Regelung könnten nach Auffassung der Gruppe Teil dieser Lösung sein.

Die Gruppe kündigte ferner an, dass die Datenschutzbehörden nach Prüfung alternativer Möglichkeiten für den Datentransfer alle notwendigen und geeigneten Maßnahmen einschließlich abgestimmter Durchsetzungsmaßnahmen ergreifen werden, wenn bis Ende Januar 2016 keine geeignete Lösung mit den US-Behörden gefunden wird.

Abschließend unterstrich die Datenschutzgruppe die gemeinsame Verantwortung der Datenschutzbehörden, EU-Organe, Mitgliedstaaten und Unternehmen, zu einer tragfähigen Lösung zu gelangen, um dem Urteil des Gerichtshofs nachzukommen. Insbesondere forderte die Gruppe die Unternehmen dringend auf, rechtliche und technische Lösungen zu erwägen, um etwaige Risiken, mit denen sie bei der Datenübermittlung konfrontiert sein können, zu begrenzen.

Die vorliegende Mitteilung lässt die Befugnis und die Pflicht der Datenschutzbehörden, die Rechtmäßigkeit solcher Datenübermittlungen in voller Unabhängigkeit zu prüfen, unberührt.[8] Sie enthält keinerlei verbindliche Regeln und achtet vollumfänglich die Befugnisse der nationalen Gerichte zur Auslegung des anzuwendenden Rechts und zur Vorlage eines Vorabentscheidungsersuchens an den Gerichtshof, sollte sich dies als notwendig erweisen. Auch kann auf diese Mitteilung kein individueller oder kollektiver Rechtsanspruch oder sonstiger Anspruch gestützt werden.

Data Protection Commissioner – http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353.

[7] Stellungnahme der Artikel-29-Datenschutzgruppe: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

[8] Vgl. Artikel 8 Absatz 3 der Grundrechtscharta und Artikel 16 Absatz 2 AEUV. Auch der Gerichtshof hat in seinem Schrems-Urteil auf diese Unabhängigkeit verwiesen.

2. ALTERNATIVE RECHTSGRUNDLAGEN FÜR DIE ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DIE USA

Die Vorschriften für internationale Datenübermittlungen in der Richtlinie 95/46/EG unterscheiden klar zwischen Übermittlungen in Drittstaaten, die ein angemessenes Schutzniveau gewährleisten (Artikel 25 der Richtlinie), und Übermittlungen in Drittstaaten, die kein angemessenes Schutzniveau gewährleisten (Artikel 26 der Richtlinie).

Der Gerichtshof befasst sich im Schrems-Urteil mit den Voraussetzungen, unter denen die Kommission gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG

‚feststellen kann, dass ein Drittstaat ein angemessenes Schutzniveau gewährleistet.

Für den Fall, dass der Drittstaat, in den personenbezogene Daten aus der EU übermittelt werden sollen, kein angemessenes Schutzniveau gewährleistet, ist in Artikel 26 der Richtlinie 95/46/EG geregelt, unter welchen Voraussetzungen Daten dennoch übermittelt werden können. Danach können Daten unter anderem übermittelt werden, wenn die Einrichtung, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (d. h. der „für die Verarbeitung Verantwortliche“),

- ausreichende Garantien im Sinne des Artikels 26 Absatz 2 der Richtlinie 95/46/EG 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 für den Datenexporteur und den Datenimporteur verbindlichen Vertragsklauseln ergeben (siehe Abschnitte 2.1 und 2.2). Hierzu zählen von der Kommission herausgegebene Standardvertragsklauseln und bei Datenübermittlungen innerhalb einer multinationalen Unternehmensgruppe von den Datenschutzbehörden genehmigte BCR;

- oder sich auf eine der explizit in Artikel 26 Absatz 1 Buchstaben a bis f der Richtlinie 95/46/EG aufgeführten Ausnahmen beruft (siehe Abschnitt 2.3).

Verglichen mit Angemessenheitsbeschlüssen, bei denen das System eines bestimmten Drittstaats insgesamt geprüft wird und die sich im Prinzip auf sämtliche Datenübermittlungen in dieses Land erstrecken können, sind die alternativen Rechtsgrundlagen für Datenübermittlungen von ihrem Anwendungsbereich her begrenzt (da sie nur für einen bestimmten Teil des Datenverkehrs gelten), nicht aber in Bezug auf den geografischen Geltungsbereich (da sie nicht unbedingt auf ein bestimmtes Land beschränkt sind). Sie gelten für Datenübermittlungen, die von bestimmten Stellen vorgenommen werden, die beschlossen haben, von einer der in Artikel 26 der Richtlinie 95/46/EG gebotenen Möglichkeiten Gebrauch zu machen. Die Verantwortung für die Rechtmäßigkeit der Datenübermittlung im Sinne der Richtlinie liegt bei den Datenexporteuren und -importeuren, wenn sie ihre Datenübermittlung auf diese alternativen Grundlagen stützen, da sie sich nicht auf die von der Kommission im Wege eines Beschlusses festgestellte Angemessenheit des Datenschutzes in dem betreffenden Drittstaat berufen können.

2.1 Vertragliche Lösungen

Vertragsklauseln, die hinreichende Garantien für die Zwecke des Artikels 26 Absatz 2 der Richtlinie 95/46/EG bieten, müssen, wie die Artikel-28-Datenschutzgruppe ausgeführt hat, die wesentlichen Elemente des Schutzes enthalten, die in einer bestimmten Situation nicht

vorhanden sind, und so einen befriedigenden Ausgleich für das Fehlen eines allgemein angemessenen Schutzniveaus bieten.[9] Um den Rückgriff auf solche Klauseln im internationalen Datenverkehr zu erleichtern, hat die Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie vier Regelungen zu Standardvertragsklauseln erlassen, die den Anforderungen des Artikels 26 Absatz 2 der Richtlinie entsprechen. Zwei der vier Regelungen betreffen Datenübermittlungen zwischen für die Verarbeitung Verantwortlichen[10], während die anderen zwei für Datenübermittlungen zwischen für die Verarbeitung Verantwortlichen und nach deren Weisungen handelnden Auftragsverarbeitern gelten[11]. In allen vier Regelungen sind die Pflichten des Datenexporteurs wie des Datenimporteurs festgelegt. Hierzu zählen unter anderem Pflichten in Bezug auf Sicherheitsmaßnahmen, die Information der betroffenen Person im Falle der Übermittlung sensibler Daten, die Information des Datenexporteurs über von einer Strafverfolgungsbehörde des Drittstaats angeforderte Daten und über jeden zufälligen oder unberechtigten Zugang, Pflichten in Bezug auf die Rechte der betroffenen Personen auf Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten sowie in Bezug auf die Haftung für Schäden, die der betroffenen Person infolge eines von einer Partei zu vertretenden Verstoßes gegen die Standardvertragsklauseln entstanden sind. Den Standardklauseln zufolge müssen betroffene Personen in der EU überdies die Möglichkeit haben, vor einer Datenschutzbehörde und/oder einem Gericht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, ihre Rechte als Drittbegünstigte aus den Vertragsklauseln geltend zu machen.[12] Die Vertragsklauseln müssen diese Rechte und Pflichten enthalten, weil im Gegensatz zu einer Angemessenheitsfeststellung der Kommission nicht angenommen werden kann, dass der Datenimporteur in dem Drittstaat einer angemessenen Aufsicht unterliegt und die Einhaltung der Datenschutzregeln ihm gegenüber durchgesetzt werden kann.

Da Entscheidungen und Beschlüsse der Kommission in allen ihren Teilen für die Mitgliedstaaten verbindlich sind, sind die nationalen Behörden grundsätzlich verpflichtet, solche Standardklauseln in einem Vertrag zu akzeptieren. Sie dürfen folglich die Übermittlung von Daten in einen Drittstaat nicht allein deshalb verweigern, weil diese Standardvertragsklauseln keine hinreichenden Garantien bieten. Ihre Befugnis, diese Klauseln im Hinblick auf die Anforderungen zu prüfen, die der Gerichtshof im Schrems-Urteil erläutert hat, bleibt hiervon unberührt. Im Zweifelsfall sollten sie ein nationales Gericht mit der Sache befassen, das sich seinerseits mit einem Vorabentscheidungsersuchen an den Gerichtshof wenden kann. Die meisten Mitgliedstaaten sehen in ihren innerstaatlichen Vorschriften zur Umsetzung der Richtlinie 95/45/EG für die Datenübermittlung in Drittstaaten keine vorherige Genehmigung vor, doch muss die Verwendung der Standardvertragsklauseln in einigen Mitgliedstaaten gemeldet und/oder vorab genehmigt werden. In diesem Fall muss die

---

9 Vgl. Artikel-29-Datenschutzgruppe, Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU (WP 12), 24. Juli 1998, S. 18.

10 Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (ABl. L 181 vom 4.7.2001, S. 19) und Entscheidung 2004/915/EG der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (ABl. L 385 vom 29.12.2004, S. 74).

11 Entscheidung 2002/16/EG der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (ABl. L 6 vom 10.1.2002, S. 52) und Beschluss 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (ABl. L 39 vom 12.2.2010, S. 5). Die Entscheidung, die in der Folge durch den Beschluss aufgehoben wurde, gilt nur für vor dem 15. Mai 2010 geschlossene Verträge.

12 Vgl. u. a. Erwägungsgrund 6 der Entscheidung 2004/915/EG der Kommission und Klausel V im Anhang zu der Entscheidung; Klausel 7 im Anhang zum Kommissionsbeschluss 2010/87/EU.

nationale Datenschutzbehörde die in dem betreffenden Vertrag enthaltenen Klauseln mit den Standardvertragsklauseln vergleichen und sich vergewissern, dass keine Änderungen vorgenommen wurden.[13] Wurden die Klauseln unverändert übernommen,[14] wird die Genehmigung im Prinzip[15] automatisch erteilt[16]. Wie unter Abschnitt 2.4 erläutert, steht dies zusätzlichen Maßnahmen nicht entgegen, die der Datenexporteur unter Umständen ergreifen muss, wenn er beispielsweise vom Datenimporteur erfährt, dass sich die Rechtslage in dem betreffenden Drittstaat geändert hat und der Datenimporteur infolgedessen seine Pflichten aus dem Vertrag nicht mehr erfüllen kann. Bei der Anwendung der Standardvertragsklauseln unterliegen sowohl der Datenexporteur als auch der Datenimporteur – aufgrund seiner Zustimmung zum Vertrag – der Aufsicht der Datenschutzbehörden.

Standardvertragsklauseln hindern Unternehmen nicht daran, auf andere Instrumente wie individuell vereinbarte Vertragsklauseln als Nachweis dafür zurückzugreifen, dass für ihre Datenübermittlungen ausreichende Garantien im Sinne des Artikels 26 Absatz 2 der Richtlinie 95/46/EG bestehen. Die Garantien müssen dieser Bestimmung zufolge von den nationalen Behörden auf der Grundlage einer Einzelfallprüfung genehmigt werden. Einige Datenschutzbehörden haben hierzu Leitlinien in Form von Musterklauseln oder detaillierten Vorschriften für die Formulierung der Datentransfer-Klauseln erstellt. Die meisten Verträge, die derzeit von Unternehmen für internationale Datenübermittlungen verwendet werden, beruhen allerdings auf den von der Kommission genehmigten Standardvertragsklauseln[17].

2.2 Datenübermittlungen innerhalb einer Unternehmensgruppe

Für eine den Anforderungen des Artikels 26 Absatz 2 der Richtlinie 95/46/EG entsprechende Übermittlung personenbezogener Daten aus der EU an verbundene Unternehmen außerhalb der EU kann ein multinationales Unternehmen verbindliche unternehmensinterne Vorschriften festlegen. Auf der Grundlage sogenannter BCR können Daten aber nur innerhalb der Unternehmensgruppe übermittelt werden.

---

13 Im Vorschlag für die Datenschutz-Grundverordnung (KOM(2012) 11 endgültig) ist vorgesehen, dass Datenübermittlungen auf der Grundlage von Standardvertragsklauseln oder verbindlichen unternehmensinternen Vorschriften keiner weiteren Genehmigung bedürfen, sofern diese Klauseln oder Vorschriften von der Kommission oder nach Maßgabe des geplanten Kohärenzverfahrens angenommen wurden.

14 Die Parteien können zusätzlich zu den Standardvertragsklauseln weitere Klauseln vereinbaren, solange diese nicht direkt oder indirekt im Widerspruch zu den von der Kommission genehmigten Klauseln stehen oder Grundrechte oder Grundfreiheiten der betroffenen Personen verletzen. Vgl. Europäische Kommission, „Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries" (FAQ B.1.9), S. 28: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

15 Hat eine Datenschutzbehörde Zweifel, ob die Standardvertragsklauseln mit der Richtlinie vereinbar sind, sollte sie die Frage einem nationalen Gericht vorlegen, das dann ein Vorabentscheidungsersuchen an den Gerichtshof richten kann (vgl. Randnrn. 51, 52, 64 und 65 des Schrems-Urteils).

16 Die Artikel-29-Datenschutzgruppe hat auf Ebene der Datenschutzbehörden ein besonderes Kooperationsverfahren für die Genehmigung von Vertragsklauseln eingeführt, die ein Unternehmen in mehreren Mitgliedstaaten verwenden möchte. Vgl. Artikel-29-Datenschutzgruppe, „Arbeitsunterlage zu einem Verfahren der Zusammenarbeit für die Abgabe gemeinsamer Stellungnahmen zu „Vertragsklauseln", die als konform mit den Standardvertragsklauseln der Europäischen Kommission gelten" (WP 226), 26. November 2014. Siehe auch Klausel VII im Anhang zu der Entscheidung 2004/915/EG der Kommission und Klausel 10 im Anhang zum Kommissionsbeschluss 2010/87/EU.

17 Vgl. Artikel-29-Datenschutzgruppe, „Arbeitsunterlage zu einem Verfahren der Zusammenarbeit für die Abgabe gemeinsamer Stellungnahmen zu ‚Vertragsklauseln', die als konform mit den Standardvertragsklauseln der Europäischen Kommission gelten" (WP 226), 26. November 2014, S. 2.

Mit den BCR ist somit ein freier Verkehr personenbezogener Daten zwischen den verschiedenen Unternehmen einer Gruppe weltweit möglich. Die Unternehmen brauchen untereinander keine diesbezüglichen Vereinbarungen mehr zu treffen. Innerhalb der Unternehmensgruppe gewährleisten einheitliche verbindliche und durchsetzbare Datenschutzvorschriften ein in allen Unternehmen gleich hohes Datenschutzniveau. Einheitliche Datenschutzvorschriften innerhalb der Unternehmensgruppe ermöglichen ein einfacheres, wirksameres Datenschutzsystem, das vom Personal leichter anzuwenden und von den Betroffenen leichter zu verstehen ist. Um den Unternehmen die Abfassung verbindlicher unternehmensinterner Vorschriften zu erleichtern, hat die Artikel-29-Datenschutzgruppe die materiellrechtlichen Anforderungen (z. B. Zweckbindung, Sicherheit der Verarbeitung, transparente Information der Betroffenen, Beschränkungen der Datenweitergabe außerhalb der Gruppe, Rechte des Einzelnen auf Auskunft, Berichtigung und Widerspruch) und die verfahrensrechtlichen Anforderungen (z. B. Audits, Konformitätskontrolle, Umgang mit Beschwerden, Zusammenarbeit mit Datenschutzbehörden, Haftung und gerichtliche Überprüfung) für BCR auf der Grundlage der EU-Datenschutzstandards erläutert.[18] Diese Vorschriften sind nicht nur für die Mitglieder der Unternehmensgruppe verbindlich, sondern sie sind ähnlich wie die Standardvertragsklauseln in der EU durchsetzbar: Personen, deren Daten von einem Unternehmen der Gruppe verarbeitet werden, haben als Drittbegünstigte das Recht, die Einhaltung der BCR im Wege einer Beschwerde bei der Datenschutzbehörde oder einer Klage vor einem mitgliedstaatlichen Gericht durchzusetzen. In den BCR muss ein Unternehmen der Gruppe innerhalb der EU bestimmt werden, das die Haftung für Regelverstöße übernimmt, die ein anderes an die BCR gebundenes Mitglied der Gruppe außerhalb der EU begangen hat.

Die meisten mitgliedstaatlichen Vorschriften zur Umsetzung der Richtlinie sehen vor, dass Datenübermittlungen auf der Grundlage der BCR in jedem Mitgliedstaat, von dem aus das multinationale Unternehmen Daten übermitteln will, von der Datenschutzbehörde genehmigt werden müssen. Zur Vereinfachung und Beschleunigung des Verfahrens und zur Reduzierung des Verwaltungsaufwands für die Antragsteller hat die Artikel-29-Datenschutzgruppe ein Antragsformular[19] und ein besonderes Kooperationsverfahren der Datenschutzbehörden[20] mit Bestimmung einer „federführenden Behörde“, die das Genehmigungsverfahren leitet, ausgearbeitet.

2.3 Ausnahmen

Personenbezogene Daten können auch dann an Einrichtungen in Drittstaaten übermittelt werden, wenn die Angemessenheit des Datenschutzniveaus nicht gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG festgestellt wurde und keine Standardvertragsklauseln und/oder BCR verwendet werden, sofern eine der Ausnahmen in Artikel 26 Absatz 1 der Richtlinie greift:[21]

---

[18] Vgl. Artikel-29-Datenschutzgruppe, „Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR)“, (WP 153), 24. Juni 2008; „Arbeitsdokument ‚Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)‘“ (WP 154), 24. Juni 2008; „Arbeitsdokument zu ‚Häufig gestellten Fragen‘ über verbindliche unternehmensinterne Datenschutzregelungen (BCR)“ (WP 155), 24. Juni 2008.

[19] Artikel-29-Datenschutzgruppe, „Antragsformular für die Genehmigung von verbindlichen unternehmensinternen Datenschutzregelungen zur Übermittlung personenbezogener Daten“ (WP 133), 10. Januar 2007.

[20] Artikel-29-Datenschutzgruppe, „Arbeitsdokument ‚Festlegung eines Kooperationsverfahrens zwecks Abgabe gemeinsamer Stellungnahmen zur Angemessenheit der verbindlich festgelegten unternehmensinternen Datenschutzgarantien‘“ (WP 107), 14. April 2005.

[21] Soweit andere Bestimmungen der Richtlinie 95/46/EG zusätzliche Vorgaben für die Anwendung dieser Ausnahmeregelungen enthalten (wie etwa die Beschränkungen für die Verarbeitung sensibler Daten in

– Die betroffene Person hat unmissverständlich in die beabsichtigte Datenübermittlung eingewilligt.

– Die Übermittlung ist 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.

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

– Die Übermittlung ist für die Wahrung eines wichtigen öffentlichen Interesses[22] oder zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben.

– Die Übermittlung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist.

– Die Übermittlung erfolgt aus einem Register, 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.

Aus den vorgenannten Gründen kann somit vom allgemeinen Verbot der Übermittlung personenbezogener Daten an Einrichtungen in Drittländern, die kein angemessenes Datenschutzniveau gewährleisten, abgewichen werden. Der Datenexporteur muss weder sicherstellen, dass der Datenimporteur einen angemessenen Schutz bietet, noch muss er in der Regel die vorherige Genehmigung für die Datenübermittlung bei den zuständigen nationalen Behörden einholen. Die Ausnahmeregelungen sind jedoch nach Ansicht der Datenschutzgruppe aufgrund ihres außerordentlichen Charakters eng auszulegen.[23]

Die Artikel-29-Datenschutzgruppe hat zur Anwendung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG mehrere nicht verbindliche Orientierungshilfen herausgegeben.[24] Hierzu

---

Artikel 8), müssen diese Bestimmungen eingehalten werden. Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG“ (WP 114), 25. November 2005, S. 9. Vgl. Europäische Kommission, „Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries“ (FAQ D.2), S. 50.

22 Hierzu zählen beispielsweise Datenübermittlungen zwischen Steuer- oder Zollbehörden oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind (vgl. Erwägungsgrund 58 der Richtlinie 95/46/EG). Auch für Datenübermittlungen zwischen Aufsichtsbehörden im Finanzdienstleistungssektor können diese Ausnahmen in Anspruch genommen werden. Vgl. Artikel-29-Datenschutzgruppe, „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU“ (WP 12), 24. Juli 1998, S. 26.

23 Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG“ (WP 114), 25. November 2005, S. 9 und 17.

24 Vgl. Artikel-29-Datenschutzgruppe, „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU“ (WP 12), 24. Juli 1998 „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG“ (WP 114), 25. November 2005. Vgl. auch Europäische Kommission, „Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries“ (FAQ D.1 bis D.9), S. 48-54.

zählen eine Reihe von Regeln der „bewährten Praxis“, an denen sich die Datenschutzbehörden bei der datenschutzrechtlichen Durchsetzung orientieren können.[25] Insbesondere empfiehlt die Datenschutzgruppe, dass die wiederholte, massenhafte oder routinemäßige Übermittlung personenbezogener Daten auf der Grundlage ausreichender Garantien und – nach Möglichkeit – eines spezifischen Rechtsrahmens in Form von Standardvertragsklauseln oder BCR erfolgen sollte.[26]

In dieser Mitteilung geht die Kommission nur auf jene Ausnahmeregelungen ein, die nach der Ungültigkeitserklärung der Safe-Harbor-Entscheidung für Datenübermittlungen im wirtschaftlichen Kontext besonders relevant erscheinen.

2.3.1 Für die Erfüllung eines Vertrags oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderliche Datenübermittlungen (Artikel 26 Absatz 1 Buchstabe b)

Auf diese Ausnahme könnte beispielsweise im Zusammenhang mit einer Hotelreservierung oder einer Banküberweisung ins Ausland zurückgegriffen werden. In solchen Fällen muss jedoch nach Auffassung der Artikel-29-Datenschutzgruppe ein „enger und erheblicher“ bzw. „direkter und objektiver Zusammenhang“ zwischen der betroffenen Person und den Zwecken des Vertrags bzw. der vorvertraglichen Maßnahme bestehen (Kriterium des Erfordernisses)[27]. Die Ausnahmeregelung gilt demnach nicht für die Übermittlung zusätzlicher Informationen, die für den Zweck der Übermittlung nicht erforderlich sind, und auch nicht für Übermittlungen für einen anderen Zweck als zur Erfüllung des Vertrags (z. B. Follow-up-Marketing)[28]. In Bezug auf vorvertragliche Maßnahmen vertrat die Datenschutzgruppe die Auffassung, dass es sich nur um von der betroffenen Person initiierte Situationen handeln könne (wie die Anforderung von Informationen zu einem speziellen Dienst) und nicht um solche, die sich aus den Marketingkonzepten der für die Verarbeitung Verantwortlichen herleiten.[29]

2.3.2 Erforderliche Datenübermittlungen für den Abschluss oder die Erfüllung eines Vertrags, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde (Artikel 26 Absatz 1 Buchstabe c)

Auf diese Ausnahme könnte beispielsweise zurückgegriffen werden, wenn die betroffene Person Empfänger einer internationalen Banküberweisung ist oder wenn ein Reisebüro einer

---

[25] Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG“ (WP 114), 25. November 2005, S. 10-11.

[26] Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG“ (WP 114), 25. November 2005, S. 11. Der Datenschutzgruppe zufolge dürfen massenhafte oder wiederholte Übermittlungen nur dann auf der Grundlage der Ausnahmeregelungen vorgenommen werden, wenn der Rückgriff auf Standardvertragsklauseln oder BCR in der Praxis nicht möglich ist und die Risiken für den Betroffenen geringfügig sind (z. B. bei internationalen Geldüberweisungen). Vgl. auch Europäische Kommission, „Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries“ (FAQ D.1), S. 49.

[27] Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG“ (WP 114), 25. November 2005, S. 15. Vgl. auch „Stellungnahme 6/2002 zur Übermittlung von Informationen aus Passagierlisten und anderen Daten von Fluggesellschaften an die Vereinigten Staaten“ (WP 66), 24. Oktober 2002.

[28] Vgl. Artikel-29-Datenschutzgruppe, „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU“ (WP 12), 24. Juli 1998, S. 26; „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG“ (WP 114), 25. November 2005, S. 16.

[29] Vgl. Artikel-29-Datenschutzgruppe, „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU“ (WP 12), 24. Juli 1998, S. 26.

Fluggesellschaft Angaben zu einer Flugbuchung übermittelt. Auch in diesem Fall ist die Erforderlichkeit zu prüfen, d. h. das Bestehen eines engen und erheblichen Zusammenhangs zwischen dem Interesse der betroffenen Person und dem Vertragszweck.

2.3.3 Für die Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen erforderliche oder gesetzlich vorgeschriebene Datenübermittlungen (Artikel 26 Absatz 1 Buchstabe d)

Auf diese Ausnahme könnte beispielsweise zurückgegriffen werden, wenn ein Unternehmen sich gegen einen Rechtsanspruch verteidigen oder selbst einen Rechtsanspruch vor einem Gericht oder einer Behörde geltend machen will und zu diesem Zweck Daten übermitteln muss. Wie bei den vorgenannten Ausnahmeregelungen ist auch hier die Erforderlichkeit der Datenübermittlung zu prüfen:[30] Zwischen der Datenübermittlung und der Streitigkeit oder dem Gerichts- bzw. Verwaltungsverfahren muss ein enger Zusammenhang bestehen.

Der Datenschutzgruppe zufolge kann die Ausnahmebestimmung nur angewendet werden, wenn die für diese Art der Übermittlung geltenden internationalen Regeln für die Zusammenarbeit in Straf- oder Zivilverfahren eingehalten wurden, insbesondere die Regeln des Haager Übereinkommens vom 18. März 1970 über die Beweisaufnahme im Ausland[31].

2.3.4 Unmissverständliche Einwilligung der betroffenen Person in die beabsichtigte Datenübermittlung (Artikel 26 Absatz 1 Buchstabe a)

Die Einwilligung der betroffenen Person kann zwar als Grundlage für eine Datenübermittlung dienen, doch sind dabei einige Aspekte zu berücksichtigen. Da sich die betroffene Person mit der „beabsichtigten" Datenübermittlung einverstanden erklären muss, muss das Einverständnis für eine bestimmte Datenübermittlung oder für eine bestimmte Kategorie von Übermittlungen vor der betreffenden Übermittlung in Form der Einwilligung erteilt werden. Die Datenschutzgruppe empfiehlt bei Online-Formularen die Verwendung leerer Kästchen, die anzukreuzen sind (statt bereits vorab angekreuzter Kästchen).[32] Da die Einwilligung unmissverständlich erteilt werden muss, würde jeder Zweifel, ob die Einwilligung tatsächlich erteilt wurde, die Anwendung der Ausnahmeregelung ausschließen. Damit würde in einer Vielzahl von Fällen, in denen die Einwilligung bestenfalls unterstellt wird (weil die betreffende Person beispielsweise auf die Übermittlung aufmerksam gemacht wurde und keinen Einwand dagegen erhoben hat), die Ausnahmeregelung nicht greifen. Sie könnte jedoch dann herangezogen werden, wenn der Übermittler in direktem Kontakt mit der

---

30 Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG" (WP 114), 25. November 2005, S. 17. Beispielsweise kann diese Ausnahme in einem arbeitsrechtlichen Kontext nicht zur Rechtfertigung der Übermittlung der Datensätze aller Angestellten an die in einem Drittland ansässige Muttergesellschaft für den Fall herangezogen werden, dass eines Tages ein Gerichtsverfahren angestrengt werden könnte.

31 Haager Übereinkommen vom 18. März 1970 über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen, 23 UST 2555, 847 UNTS 241. Dieses Übereinkommen gilt beispielsweise für Rechtshilfeersuchen, die eine gerichtliche Behörde an die zuständige Behörde eines anderen Staates zwecks Erlangung von Beweisen für ein Gerichtsverfahren im ersuchenden Staat richtet (das in Common-Law-Staaten als „pre-trial discovery of documents" bekannte förmliche Beweisverfahren ist ebenfalls darin erfasst).

32 Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG" (WP 114), 25. November 2005, S. 12, mit Verweis auf die „Stellungnahme 5/2004 zu unerbetenen Direktwerbenachrichten gemäß Artikel 13 der Richtlinie 2002/58/EG" (WP 90), 27. Februar 2004, Abschnitt 3.2.

betroffenen Person steht, die erforderlichen Informationen problemlos mitgeteilt werden können und die Einwilligung ohne jeden Zweifel erlangt wird.[33]

Darüber hinaus muss die Einwilligung nach Artikel 2 Buchstabe h der Richtlinie 95/46/EG ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erteilt werden. Der Datenschutzgruppe zufolge bedeutet die erste Voraussetzung, dass jedweder „Druck" die Einwilligung ungültig machen kann. Dies ist in einem Beschäftigungsverhältnis von besonderer Bedeutung, da zwischen dem Arbeitgeber und dem Arbeitnehmer ein hierarchisches Verhältnis besteht und die hieraus resultierende Abhängigkeit des Arbeitnehmers die Berufung auf dessen Einwilligung in der Regel fragwürdig erscheint.[34] Allgemein ist festzustellen, dass die Einwilligung einer Person, die nicht die Möglichkeit hatte, eine echte Wahl zu treffen oder vor vollendete Tatsachen gestellt wurde, nicht als wirksam angesehen werden kann.[35]

Es kommt entscheidend darauf an, dass die betroffenen Personen im Voraus ordnungsgemäß darüber informiert werden, dass ihre Daten aus der EU transferiert werden, in welches Drittland sie transferiert werden und unter welchen Bedingungen (Zweck des Transfers, Identität und nähere Angaben zu dem oder den Empfängern usw.). Dabei sollte auf das konkrete Risiko hingewiesen werden, dass ihre Daten in ein Drittland transferiert werden, das keinen angemessenen Datenschutz gewährleistet.[36] Die Datenschutzgruppe hat ferner darauf hingewiesen, dass der Widerruf der Einwilligung zwar nicht rückwirkend gilt, aber grundsätzlich jede weitere Verarbeitung der Daten der betroffenen Person verhindert.[37] In Anbetracht dieser Beschränkungen steht die Datenschutzgruppe auf dem Standpunkt, dass die Einwilligung bei routinemäßigen Übermittlungen langfristig wohl kaum eine angemessene Rechtsgrundlage für die für die Verarbeitung Verantwortlichen bietet.[38]

2.4 Alternative Rechtsgrundlagen für die Übermittlung personenbezogener Daten – Zusammenfassung

Aus den vorstehenden Ausführungen folgt, dass die Unternehmen eine Reihe alternativer Instrumente als Grundlage für internationale Datenübermittlungen in Drittstaaten heranziehen können, die kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 der Richtlinie 95/46/EG bieten. Nach dem Schrems-Urteil hat die Artikel-29-Datenschutzgruppe insbesondere klargestellt, dass Daten, solange ihre Prüfung nicht abgeschlossen ist, auf der Grundlage von Standardvertragsklauseln und BCR in die USA übermittelt werden können;

---

33 Vgl. Artikel-29-Datenschutzgruppe, „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU" (WP 12), 24. Juli 1998 S. 26.

34 Vgl. Artikel-29-Datenschutzgruppe, „Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten" (WP 48), 13. September 2001, S. 3, 23 und 27. Nach Dafürhalten der Datenschutzgruppe sollte die Einwilligung der betroffenen Person nur in den Fällen in Anspruch genommen werden, in denen der Beschäftigte eine echte Wahl hat und seine Einwilligung zu einem späteren Zeitpunkt widerrufen kann, ohne dass ihm daraus Nachteile erwachsen. Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG" (WP 114), 25. November 2005, S. 13.

35 Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG" (WP 114), 25. November 2005, S. 13. Vgl. auch „Stellungnahme 6/2002 zur Übermittlung von Informationen aus Passagierlisten und anderen Daten von Fluggesellschaften an die Vereinigten Staaten" (WP 66), 24. Oktober 2002.

36 Vgl. Artikel-29-Datenschutzgruppe, „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU" (WP 12), 24. Juli 1998, S. 26.

37 Vgl. Artikel-29-Datenschutzgruppe, „Stellungnahme 15/2011 zur Definition von Einwilligung" (WP 187), 13. Juli 2011, S. 10.

38 Vgl. Artikel-29-Datenschutzgruppe, „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG" (WP 114), 25. November 2005, S. 13.

die Kontrollbefugnisse der Datenschutzbehörden in konkreten Fällen bleiben hiervon unberührt.[39] Die Wirtschaft hat auf das Urteil unterschiedlich reagiert, zum Teil aber auch auf diese alternativen Rechtsgrundlagen für ihre Datenübermittlungen zurückgegriffen.[40]

Dabei ist jedoch zweierlei zu beachten. Erstens: Datenübermittlungen in ein Drittland sind unabhängig von der konkreten Rechtsgrundlage nur dann rechtmäßig, wenn die Daten ursprünglich von dem für die Verarbeitung Verantwortlichen in der EU nach Maßgabe der einzelstaatlichen Gesetze zur Umsetzung der Richtlinie 95/46/EG erhoben und verarbeitet worden sind. In der Richtlinie wird eigens darauf hingewiesen, dass Verarbeitungen, die vor der Übermittlung erfolgen, sowie die Übermittlung selbst in vollem Umfang den Rechtsvorschriften genügen müssen, die die Mitgliedstaaten gemäß den anderen Richtlinienbestimmungen erlassen haben.[41] Zweitens: In Ermangelung einer Angemessenheitsfeststellung der Kommission hat der für die Verarbeitung Verantwortliche dafür Sorge zu tragen, dass die Datenübermittlung auf der Grundlage hinreichender Garantien gemäß Artikel 26 Absatz 2 der Richtlinie erfolgt. Bei der Einschätzung sind alle Umstände im Zusammenhang mit dem betreffenden Datentransfer zu berücksichtigen. Die Standardvertragsklauseln und die BCR sehen gleichermaßen vor, dass der Datenimporteur unverzüglich den Datenexporteur in der EU informiert, wenn Grund zu der Annahme besteht, dass die im Empfängerland anwendbaren Vorschriften ihn an der Erfüllung seiner Pflichten hindern könnten. In diesem Fall obliegt es dem Exporteur, die zur Gewährleistung des Schutzes der personenbezogenen Daten notwendigen und geeigneten Maßnahmen zu treffen.[42] Diese können von technischen, organisatorischen, auf sein Geschäftsmodell bezogenen oder rechtlichen Maßnahmen[43] bis hin zu der Möglichkeit reichen, die Datenübermittlung auszusetzen oder den Vertrag zu kündigen. Datenexporteure müssen daher gegebenenfalls unter Berücksichtigung aller mit der Datenübermittlung zusammenhängenden Umstände zusätzlich zu den Schutzvorkehrungen nach Maßgabe der für die Datenübermittlung geltenden Rechtsgrundlage weitere Garantien vorsehen, um den Anforderungen des Artikels 26 Absatz 2 der Richtlinie zu genügen.

Die Einhaltung dieser Anforderungen wird letztlich von den Datenschutzbehörden konkret im Rahmen der Wahrnehmung ihrer Aufsichts- und Durchsetzungsbefugnisse, unter anderem im Zusammenhang mit der Genehmigung von Vertragsklauseln und BCR oder auf der Grundlage individueller Beschwerden, geprüft. Zwar haben manche Datenschutzbehörden die Möglichkeit, Standardvertragsklauseln oder BCE für den transatlantischen Datenverkehr zu nutzen, in Zweifel gezogen,[44] doch wird die Artikel-29-Datenschutzgruppe, wie sie in ihrer

---

39 Stellungnahme der Artikel-29-Datenschutzgruppe vom 16. Oktober 2015 (vgl. Fußnote 8).

40 Mehrere multinationale Unternehmen haben erklärt, dass sie ihre Datenübermittlungen in die USA auf alternative Rechtsgrundlagen stützen. Vgl. hierzu u. a. die Erklärung von Microsoft (http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/) oder Salesforce (http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp). Andere US-Unternehmen wie Oracle erklärten, dass sie ihren Cloud-Kunden die Möglichkeit bieten, ihre Daten in Europa zu speichern, so dass diese nicht zu Speicherzwecken weitertransferiert werden: http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot.

41 Vgl. Erwägungsgrund 60 und Artikel 25 Absatz 1 der Richtlinie 95/46/EG.

42 Vgl. u. a. Klausel 5 im Anhang zum Beschluss 2010/87/EU der Kommission und Artikel-29-Datenschutzgruppe, „Arbeitsdokument ‚Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)'" (WP 154), 24. Juni 2008, S. 9.

43 Vgl. hierzu u. a. die Leitlinien der Europäischen Agentur für Netz- und Informationssicherheit (ENISA): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

44 Vgl. hierzu u. a. das Positionspapier der Datenschutzkonferenz der deutschen Datenschutzbehörden des Bundes und der Länder vom 26.10.2015: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521.

Stellungnahme zum Schrems-Urteil erklärt hat, die Auswirkungen des Urteils auf andere Instrumente für den Datentransfer weiter prüfen[45]. Die Befugnisse der Datenschutzbehörden zur Überprüfung konkreter Fälle und zum Schutz betroffener Personen bleiben hiervon unberührt.

3. DIE FOLGEN DES SCHREMS-URTEILS FÜR ANGEMESSENHEITSBESCHLÜSSE

In seinem Urteil stellt der Gerichtshof nicht die Befugnis der Kommission in Frage, nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG die Feststellung zu treffen, dass ein Drittland ein angemessenes Datenschutzniveau gewährleistet, solange die Vorgaben des Gerichtshofs beachtet werden. Diesen Vorgaben entsprechend wird im Vorschlag für eine Datenschutz-Grundverordnung von 2012,[46] die die Richtlinie 95/46/EG ersetzen soll, klarer und detaillierter geregelt, unter welchen Voraussetzungen Angemessenheitsbeschlüsse erlassen werden können. Im Schrems-Urteil stellte der Gerichtshof ferner klar, dass Angemessenheitsbeschlüsse der Kommission alle Mitgliedstaaten binden und damit für alle Organe der Mitgliedstaaten, zu denen auch die Datenschutzbehörden gehören, verbindlich sind, solange sie nicht zurückgenommen oder vom Gerichtshof, der diesbezüglich ausschließlich zuständig ist, für nichtig oder ungültig erklärt wurden. Die Datenschutzbehörden bleiben zuständig für die Prüfung von Eingaben im Sinne des Artikels 28 Absatz 4 der Richtlinie 95/46/EG, um festzustellen, ob eine bestimmte Datenübermittlung den Anforderungen der Richtlinie (in der Auslegung durch den Gerichtshof) entspricht; sie können aber keine endgültige Feststellung treffen. Die Mitgliedstaaten müssen vielmehr die Möglichkeit vorsehen, ein nationales Gericht mit der Sache zu befassen, das sich seinerseits mit einem Vorabentscheidungsersuchen gemäß Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) an den Gerichtshof wenden kann.

Zudem bestätigte der Gerichtshof ausdrücklich, dass der Rückgriff eines Drittlands auf ein System der Selbstzertifizierung (wie im Fall der Datenschutzgrundsätze des „sicheren

---

Unter Hinweis auf die „strengen materiellrechtlichen Anforderungen" im Schrems-Urteil, die von der Kommission wie von den Datenschutzbehörden zu beachten sind, werden die deutschen Datenschutzbehörden dem Positionspapier zufolge die Rechtmäßigkeit der auf eine alternative Rechtsgrundlage (Standardvertragsklauseln, BCR) gestützte Datenübermittlung prüfen und für die Nutzung dieser Rechtsgrundlagen keine neuen Genehmigungen erteilen. Gleichzeitig haben die Datenschutzbehörden einiger Bundesländer klar darauf hingewiesen, dass diese alternativen Rechtsgrundlagen für den Datentransfer einer rechtlichen Prüfung unterzogen werden. Vgl. u. a. die Positionspapiere der Datenschutzbehörden von Schleswig-Holstein – https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html und Rheinland-Pfalz – https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf.

45 Vgl. Stellungnahme der Artikel-29-Datenschutzgruppe vom 16. Oktober 2015 (siehe oben Fußnote 7).

46 Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Vgl. auch Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung), COM(2012) 0011 – C7-0025/2012 – 2012/0011(COD); Ratsdokument 9565/15 zur Vorbereitung einer allgemeinen Ausrichtung betreffend den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Der Vorschlag befindet sich derzeit in der letzten Phase des Gesetzgebungsverfahrens.

Hafens“) die Feststellung eines angemessenen Schutzniveaus gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG nicht ausschließt, solange es wirksame Überwachungs- und Kontrollmechanismen gibt, die es erlauben, in der Praxis etwaige Verstöße gegen Datenschutzvorschriften zu ermitteln und zu ahnden.

Da die Safe-Harbor-Entscheidung in dieser Hinsicht keine hinreichenden Feststellungen enthielt, wurde sie vom Gerichtshof für ungültig erklärt. Es liegt somit auf der Hand, dass auf dieser Basis, d. h. allein unter Berufung auf den Beitritt zu den Safe-Harbor-Grundsätzen, keine Daten mehr zwischen der EU und den USA übermittelt werden können. Datenübermittlungen in ein Drittland, das kein angemessenes Schutzniveau gewährleistet (oder dessen Schutzniveau nicht gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG von der Kommission in einem Beschluss als angemessen festgestellt wurde), sind im Prinzip zu untersagen.[47] Datenübermittlungen sind unter diesen Umständen nur dann rechtmäßig, wenn der Datenexporteur auf eine der in Abschnitt 2 beschriebenen alternativen Rechtsgrundlagen zurückgreifen kann. In Ermangelung eines Angemessenheitsbeschlusses obliegt es dem Datenexporteur – unter der Aufsicht der Datenschutzbehörden – sicherzustellen, dass die Voraussetzungen für die Anwendung (einer) dieser Rechtsgrundlagen in Bezug auf die betreffende Datenübermittlung gegeben sind.

Die Reichweite des Urteils ist auf die Safe-Harbor-Entscheidung der Kommission beschränkt. Alle anderen Angemessenheitsbeschlüsse[48] enthalten jedoch ebenfalls eine Artikel 3 der Safe-Harbor-Entscheidung vergleichbare Einschränkung der Befugnisse der Datenschutzbehörden, die vom Gerichtshof für ungültig erklärt wurde[49]. Die Kommission wird jetzt Konsequenzen aus dem Urteil ziehen und die betreffende Bestimmung in Kürze in allen Angemessenheitsbeschlüssen im Wege eines im Ausschussverfahren zu erlassenden Beschlusses ersetzen. Zudem wird sie – auch im Rahmen der gemeinsam mit den zuständigen Behörden des betreffenden Drittlands vorzunehmenden regelmäßigen Überprüfung der Anwendung bestehender Angemessenheitsbeschlüsse – solche Beschlüsse in Zukunft regelmäßig überprüfen.

4. FAZIT

Wie von der Artikel-29-Datenschutzgruppe bestätigt, können Unternehmen nach wie vor auf alternative Rechtsgrundlagen zurückgreifen, um Daten rechtmäßig in Drittländer wie die USA zu übermitteln. Ein neuer, solider Rahmen für die Übermittlung personenbezogener Daten in die Vereinigten Staaten bleibt jedoch nach Auffassung der Kommission ein prioritäres Anliegen. Ein solcher Rahmen bietet die umfassendste Lösung für einen wirksamen, ununterbrochenen Schutz der in die USA transferierten personenbezogenen Daten europäischer Bürger. Auch für den transatlantischen Handel ist dies die beste Lösung, da auf diese Weise Daten einfacher, unbürokratischer und damit kostengünstiger – insbesondere für KMU – transferiert werden können.

Bereits im Jahr 2013 hatte die Kommission mit der US-Regierung Verhandlungen über eine neue Regelung des transatlantischen Datentransfers auf der Grundlage ihrer 13 Empfehlungen

---

47 Vgl. Erwägungsgrund 57 der Richtlinie 95/46/EG.

48 Derzeit bestehen Angemessenheitsbeschlüsse in Bezug auf folgende Länder und Gebiete: Andorra, Argentinien, Färöer, Guernsey, Isle of Man, Israel, Jersey, Kanada, Neuseeland, Schweiz und Uruguay. Vgl. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

49 Vgl. Schrems-Urteil, Randnrn. 99-104.

aufgenommen.[50] Beide Seiten haben sich bereits deutlich angenähert: z. B. in Bezug auf eine strengere Kontrolle und Durchsetzung der Safe-Harbor-Grundsätze durch das US-Handelsministerium und die Federal Trade Commission, in Bezug auf mehr Transparenz für die Verbraucher im Hinblick auf ihre Datenschutzrechte, einfachere und kostengünstigere Rechtsschutzmöglichkeiten bei Beschwerden und klarere Regeln für die Weiterübermittlung von Safe-Harbor-Unternehmen an Unternehmen, die diesen Grundsätzen nicht beigetreten sind (z. B. zu Zwecken der Verarbeitung als Haupt- oder Unterauftrag). Nachdem die Safe-Harbor-Entscheidung für ungültig erklärt wurde, hat die Kommission die Gespräche mit der US-Regierung intensiviert, um sicherzustellen, dass die rechtlichen Vorgaben des Gerichtshofs beachtet werden. Ziel der Kommission ist es, diese Gespräche innerhalb von drei Monaten erfolgreich abzuschließen.

Bis die neue Regelung für den transatlantischen Datenverkehr in Kraft ist, müssen die Unternehmen auf die verfügbaren alternativen Rechtsgrundlagen zurückgreifen. Dies legt den Datenexporteuren eine zusätzliche Verantwortung auf, der sie unter der Aufsicht der Datenschutzbehörden nachkommen müssen.

Hat die Kommission in einem Drittland ein angemessenes Datenschutzniveau festgestellt, können sich Datenexporteure, die Daten aus der EU in dieses Drittland transferieren, darauf veranlassen. Gibt es eine solche Feststellung nicht, sind sie selbst dafür verantwortlich, sich zu vergewissern, dass die personenbezogenen Daten, die sie auf einer anderen Rechtsgrundlage übermitteln, effektiv geschützt sind. Hierzu müssen sie, falls nötig, geeignete Maßnahmen ergreifen.

Den Datenschutzbehörden kommt hier eine zentrale Aufgabe zu. Die Durchsetzung der Datenschutzgrundrechte ist in erster Linie ihre Aufgabe. Sie überwachen in völliger Unabhängigkeit den Datenverkehr aus der EU in Drittländer. Die Kommission fordert die für die Verarbeitung Verantwortlichen auf, mit den Datenschutzbehörden zusammenzuarbeiten und ihnen auf diese Weise die Wahrnehmung ihrer Aufsichtsfunktion konkret zu erleichtern. Die Kommission wird auch in Zukunft eng mit der Artikel-29-Datenschutzgruppe zusammenarbeiten, um eine einheitliche Anwendung des EU-Datenschutzrechts zu gewährleisten.

[50] Siehe oben Fußnote 4.