cepStudie

„Privacy Shield“: Kein ausreichender Datenschutz im unsicheren Hafen USA

Eine Kritik der „Safe Harbour“- Nachfolgeregelung und der alternativen Transfermethoden

Dr. Anja Hoffmann, LL.M. Eur.

April 2016

Kernpunkte

- Bis zum 6. Oktober 2015 war die „Safe Harbour“-Entscheidung der Europäischen Kommission Rechtsgrundlage für transatlantische Datentransfers. Nachdem der Europäische Gerichtshof (EuGH) diese für ungültig erklärt hat, ist die Rechtslage unsicher. Auch alternative Rechtsgrundlagen wie Standarddatenschutzklauseln oder verbindliche unternehmensinterne Datenschutzregelungen versprechen derzeit keine dauerhafte rechtssichere Abhilfe.
- Als Ersatz für die „Safe Harbour“-Entscheidung plant die Kommission – auf Basis einer erfolgten Verständigung mit den USA – einen „Privacy Shield“-Beschluss. Er enthält als Anlage „Privacy Principles“, denen sich teilnehmende US-Unternehmen durch Selbstzertifizierung unterwerfen müssen, sowie sechs Briefe von US-Behörden und -Ministerien, in denen diese die US-Rechtslage beschreiben und Zusicherungen machen.
- Der „Privacy Shield“-Beschluss trägt laut Kommission dem EU-Datenschutz in allen Punkten Rechnung. Dies trifft nicht zu:
  - Der Schutz vor staatlichen Zugriffen auf personenbezogene Daten ist unzureichend. Massenhafte Datenerhebungen und -nutzungen durch US-Behörden bleiben möglich. Die vorgesehenen Einschränkungen für US-Sicherheitsbehörden dürften nicht der Vorgabe des EuGH entsprechen, dass Eingriffe in das Grundrecht auf Achtung des Privatlebens „absolut notwendig und verhältnismäßig“ sein müssen.
  - Der Rechtsschutz ist ebenfalls unzureichend. Insbesondere erfüllt der „Ombudsperson-Rechtsbehelf“ nicht die Anforderungen des EuGH an einen „gerichtlichen Rechtsschutz“. Die „Ombudsperson“ ist nicht vollkommen unabhängig, hat möglicherweise unzureichende Befugnisse und fällt intransparente Entscheidungen.
  - Um wettbewerbsrechtliche Nachteile für EU-Unternehmen zu vermeiden, muss sichergestellt sein, dass die zertifizierten US-Unternehmen die „Privacy Principles“ auch tatsächlich einhalten. Daher sollten Kontrollen nicht im Wesentlichen auf Rüge hin, sondern anlasslos, regelmäßig, unangekündigt und flächendeckend erfolgen. Auch sollte die Zertifizierung nicht durch kaum kontrollierbare Selbstunterwerfung, sondern durch unabhängige akkreditierte Stellen vorgenommen werden.
- Die „Privacy Principles“ sollten bereits jetzt an der voraussichtlich ab 2018 geltenden Datenschutzgrundverordnung ausgerichtet werden, um Anpassungsbedarf und Nachverhandlungen mit den USA zu vermeiden.
- Die rechtliche Bindungswirkung der in Briefen gemachten Zusicherungen ist fraglich. Geboten wäre ein völkerrechtliches Abkommen sowie eine bindende Umsetzung in den USA mit Gesetzescharakter.
- Die Kommission will auf die US-amerikanischen Zusicherungen vertrauen und den „Privacy Shield“-Beschluss bei Fehlverhalten aussetzen. Dies wird weder dem Interesse der Wirtschaft an einer langfristigen rechtssicheren Grundlage für transatlantische Datentransfers noch demjenigen der EU-Bürger an einem dauerhaften angemessenen Datenschutz gerecht.
- Die EU sollte zunächst konsequent auf weitere spürbare Änderungen im US-Recht hinwirken und erst auf Basis der geänderten Rechtslage einen Angemessenheitsbeschluss erlassen. Dass es hierzu kommt, ist allerdings wenig wahrscheinlich.
- Unternehmen, die Rechtssicherheit suchen, sollten erwägen, ihre Datenverarbeitung in die EU zu verlagern oder zu Dienstleistern zu wechseln, die personenbezogene Daten ausschließlich in der EU speichern.

Inhaltsverzeichnis

1 Einleitung

Die Übermittlung personenbezogener Daten ist notwendiger und integraler Bestandteil der transatlantischen Handelsbeziehungen zwischen der Europäischen Union (EU) und den Vereinigten Staaten von Amerika (USA), für die große Datenmengen von der EU in die USA fließen.[1] Dies gilt vor allem für die sozialen Netzwerke wie Facebook sowie für Anbieter und Nutzer zahlreicher Online-Dienste, darunter Cloud Computing-Services und Online-Shops. Digitale Geschäftsmodelle basieren wesentlich auf einem weltweiten Austausch personenbezogener Daten[2] über das Internet. Daneben verarbeiten Tochtergesellschaften von US-Unternehmen in Europa oder US-Tochtergesellschaften europäischer Unternehmen personenbezogene Daten ihrer Mitarbeiter oder Kunden häufig in den USA. Zahlreiche Unternehmen übermittelten solche Daten bislang auf der Basis des sogenannten „Safe Harbour“-Systems, geschaffen durch eine Kommissionsentscheidung, welches einen legalen Transfer von Daten in die USA ermöglichte.

Im „Schrems-Urteil“ vom 6. Oktober 2015[3] hat der Europäische Gerichtshof (EuGH) die Entscheidung der EU-Kommission (nachfolgend: „Kommission“), auf der das „Safe Harbour“-System basierte, für ungültig erklärt. Damit ist eine in der Praxis vielgenutzte Rechtsgrundlage für die legale Übermittlung personenbezogener Daten von EU-Bürgern in die USA zum Zwecke der dortigen Speicherung oder sonstiger Verarbeitung weggefallen. Für viele Unternehmen ist hierdurch eine missliche Situation entstanden. Unklarheiten bestehen insbesondere darüber, ob und auf welcher alternativen Rechtsgrundlage ein Transfer personenbezogener Daten an Unternehmen mit Sitz in den USA gegenwärtig und zukünftig überhaupt noch legal erfolgen kann. Um die entstandene Lücke zu füllen, hat sich die Kommission nach langen Verhandlungen mit den USA auf einen neuen transatlantischen „Datenschutzschild“ verständigt. Auf dessen Basis strebt sie den Abschluss eines neuen, verbesserten Angemessenheitsbeschlusses an. Parallel hierzu steht innerhalb der EU die neue Datenschutz-Grundverordnung unmittelbar vor der Verabschiedung, die ab dem Jahr 2018 die geltende EU-Datenschutzrichtlinie aus dem Jahr 1995 ersetzen wird.

Die vorliegende cepStudie gibt einen Überblick über die rechtliche Lage und die derzeitige missliche Situation für Unternehmen und Dateninhaber und untersucht, ob die in Betracht kommenden Alternativlösungen Auswege aus dieser Situation bieten können. Dabei wird auch das aktuelle Vorhaben der Kommission zur Legalisierung des transatlantischen Datentransfers und damit zur Schaffung von Rechtssicherheit unter die Lupe genommen.

2 EU-Datenschutzrichtlinie und Datenschutzgrundverordnung

Das in der EU derzeit (noch) gültige Datenschutzrecht wurde – neben weiteren sektorspezifischen Regelungen – maßgeblich durch die Richtlinie 95/46/EG[4] (nachfolgend: „DSRL“) harmonisiert. Diese soll innerhalb der EU bei der Verarbeitung personenbezogener Daten einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechten des Einzelnen, insbesondere des

---

1 Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA vom 27. November 2013, COM(2013) 846 final), S. 2, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52013DC0846&qid=1456303173095&from=DE. Vgl. auch Erwägungsgrund 56 der EU-Datenschutzrichtlinie (Fn. 4).

2 Moos/Schefzig, CR 2015, S. 625.

3 Entscheidung 2000/520/EG (Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates 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 vom 25.08.2000, S. 7-47.

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 2.11.1995, S. 31.

Grundrechts auf Achtung der Privatsphäre, auf einem homogenen, hohen Niveau gewährleisten.[5] Gleichzeitig soll ein angemessener Ausgleich zwischen diesen Schutzrechten einerseits und dem Ziel der Errichtung eines gemeinsamen Marktes mit freiem Waren-, Personen-, Dienstleistungs- und Kapitalverkehr andererseits geschaffen werden, für den ein freier und grenzüberschreitender Datenverkehr unerlässlich ist.[6]

Diese Ziele und Grundsätze sind nach wie vor gültig. Die unterschiedliche Umsetzung der DSRL in den EU-Mitgliedstaaten hat jedoch zu einer Rechtszersplitterung innerhalb der EU geführt. Zunehmende Globalisierung, Internet und technologischer Fortschritt ließen Datenerhebungen und Datenverkehr auf ein Ausmaß ansteigen, auf das die Vorschriften der Richtlinie nicht mehr ohne weiteres passen. Um eine neue Vertrauensbasis für die digitale Wirtschaft zu schaffen, gleichzeitig aber dem Grundrecht der EU-Bürger auf Datenschutz angemessen Rechnung zu tragen, brachte die Kommission im Jahr 2003 ein Datenschutzpaket auf den Weg. Herzstück dieses Pakets ist die neue Datenschutzgrundverordnung (nachfolgend „DSGV“).[7] Nach fast vier Jahre andauernden zähen Verhandlungen wurde das Trilog-Verfahren[8] zwischen Kommission, Rat und Europäischem Parlament kurz vor Weihnachten 2015 abgeschlossen und ein Kompromiss über die inhaltliche Fassung der Verordnung erzielt.[9] Der ursprüngliche Entwurf[10] der DSGV wurde an zahlreichen Stellen abgeändert. Eine formelle Annahme durch Parlament und Rat gilt als sicher und wird voraussichtlich noch im Frühjahr 2016 erfolgen. Die DSGV soll im ersten Halbjahr 2018 in Kraft treten und wird dann die DSRL ersetzen.

Der Transfer personenbezogener Daten in Drittländer wie die USA setzt zunächst voraus, dass die allgemeinen Voraussetzungen für eine Datenübertragung erfüllt sind, die auch für eine Übertragung innerhalb der EU vorliegen müssten. Zusätzlich hierzu müssen die besonderen Voraussetzungen für den Datentransfer in Drittstaaten erfüllt sein.[11] DSRL und DSGV sehen für diese zweite Anforderung verschiedene Rechtsgrundlagen vor, die nachfolgend näher beleuchtet werden sollen.

3 Grundsatz: Transfer nur in Drittländer mit angemessenem Schutzniveau

Für die Entwicklung des Handels auf internationaler Ebene ist eine grenzüberschreitende Übermittlung personenbezogener Daten notwendig.[12] Problematisch hieran ist, dass in Drittländern häufig keine identischen oder vergleichbaren Datenschutzregelungen existieren. Um eine Umgehung des hohen Schutzniveaus innerhalb der EU zu verhindern und die genannten Schutzrechte des Einzel-

5 Siehe insbesondere Art. 1 sowie die Erwägungsgründe 2 und 10 der DSRL.
6 Siehe insbesondere Erwägungsgrund 3 der DSRL.
7 Im Bereich des Sicherheitsrechts soll daneben eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Polizei- und Justizbehörden einen besseren Austausch von Daten zwischen Strafverfolgungsbehörden in den EU-Mitgliedstaaten ermöglichen, gleichzeitig aber die Daten von Opfern, Zeugen und möglichen Tätern umfassend schützen. Auf diese Richtlinie kann in dieser cepStudie nicht eingegangen werden.
8 Kritisch zum Trilogverfahren allgemein vgl. cep**Input** „Gesetzgebung im Trilog“, abrufbar unter http://www.cep.eu/de/eu-themen/details/cep/gesetzgebung-im-trilog.html.
9 Eine konsolidierte Fassung dieses Kompromisstextes einer DSGV als Ergebnis des Trilogverfahrens vom 15.12.2015 ist abrufbar unter http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884 (unter Miscellaneous_3_consolidated_text).
10 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); KOM/2012/011 endgültig. Vgl. zum mittlerweile geänderten Kommissionsvorschlag einer Datenschutz-Grundverordnung auch cep**Analyse** „Datenschutz-Grundverordnung (KOM(2012) 11, abrufbar unter http://www.cep.eu/de/eu-themen/details/cep/datenschutz-verordnung.html.
11 Borges, NJW 2015, S. 3617.
12 Siehe Erwägungsgrund 56 der EU-Datenschutz-Richtlinie.

nen nicht leerlaufen zu lassen, dürfen personenbezogene Daten nach Art. 25 Abs. 1 DSRL grundsätzlich nur dann in ein Drittland übermittelt werden, wenn dieses ein „angemessenes Schutzniveau“ hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen gewährleistet. Entsprechend stellt die DSGV in Art. 40 S. 1 den allgemeinen Grundsatz auf, dass bei jeder Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen die Bestimmungen über die internationale Datenübermittlung sowie die übrigen Bestimmungen der DSGV eingehalten werden müssen. Hierdurch soll sichergestellt werden, dass das Schutzniveau der DSGV auch bei internationalen Datentransfers nicht unterschritten wird.

4 Angemessenheitsbeschlüsse der Kommission

Ob ein Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet, kann die Kommission im Wege eines sogenannten „Angemessenheitsbeschlusses“ gemäß Art. 41 Abs. 3 DSGV (bislang: Art. 25 Abs. 6 DSRL) feststellen. Nach der noch geltenden Richtlinie kann die Kommission eine solche Entscheidung treffen, wenn sie nach umfassender Prüfung aller relevanten Umstände zu dem Ergebnis kommt, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau i.S.v. Art. 25 Abs. 2 der Richtlinie bietet. Gleiches gilt künftig nach Art. 41 DSGV. Dieser regelt nunmehr im Detail eine ganze Reihe nicht abschließender Prüfpunkte, die die Kommission bei der Prüfung der Angemessenheit des Schutzniveaus berücksichtigen muss.[13] Liegt ein positiver Angemessenheitsbeschluss vor[14], ist dieser für die EU-Mitgliedstaaten bindend. Der Transfer personenbezogener Daten in dieses Gebiet ist dann gemäß Art. 41 Abs. 1 DSGV „ohne besondere Genehmigung“ zulässig. Auf Grundlage der DSRL hat die Kommission in zahlreichen Entscheidungen die Angemessenheit des Schutzniveaus in Staaten wie Andorra, Argentinien, Australien, Israel, Kanada, Neuseeland und der Schweiz anerkannt.[15] Diese Entscheidungen bleiben auch nach Inkrafttreten der DSGV in Kraft, bis sie von der Kommission geändert, ersetzt oder aufgehoben werden.[16] Hinsichtlich der USA hatte die Kommission jedoch, gestützt auf Art. 25 Abs. 6 DSRL, eine besondere Entscheidung getroffen, die weithin als „Safe Harbour-Entscheidung“ bekannt ist.

5 Sonderfall USA: „Safe Harbour“

Aufgrund des Fehlens eines einheitlichen Datenschutzrechts in den USA[17] konnte die Kommission nicht ohne weiteres feststellen, dass die USA als Land insgesamt ein angemessenes Schutzniveau aufweisen. Daher hat die Kommission im Jahr 2000 mit der „Safe Harbour-Entscheidung“[18] eine Ersatzlösung gewählt.

---

[13] Näher hierzu unten Ziffer 8.3.4.

[14] Die Kommission veröffentlicht künftig im Amtsblatt der EU und auf ihrer Webseite eine Liste der Drittländer, internationalen Organisationen oder Gebiete/Sektoren, für die ein Angemessenheitsbeschluss gefasst oder aufgehoben wurde, Art. 41 Abs. 7 DSGV.

[15] Eine Übersicht der bislang ergangenen Angemessenheitsentscheidungen der Kommission findet sich unter http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

[16] Vgl. Art. 41 Abs. 8 DSGV.

[17] Das amerikanische Datenschutzrecht besteht aus einer Mischung aus enggefassten sektoralen Rechtsvorschriften und freiwilliger Selbstregulierung; Vgl. Art. 29-Datenschutzgruppe „Stellungnahme 1/99 zum Stand des Datenschutzes in den Vereinigten Staaten und zu den derzeitigen Verhandlungen zwischen der Europäischen Kommission und der amerikanischen Regierung“ vom 26.01.1999, S. 2 unter Ziffer 1. Vgl. auch Borges, NJW 2015, S. 3617 (3618).

[18] Entscheidung 2000/520/EG, vgl. Fn. 3.

5.1 Was ist „Safe Harbour“?

Anstelle eines umfassenden Angemessenheitsbeschlusses für das Drittland USA insgesamt hat die Kommission in der „Safe Harbour“-Entscheidung ein System der Selbstzertifizierung und Selbstbewertung amerikanischer Datenempfänger anerkannt und eine auf das Datenschutzniveau bei derart zertifizierten Unternehmen beschränkte Angemessenheitsentscheidung getroffen. Interessierte US-amerikanische Unternehmen konnten dem sogenannten „Safe Harbour“-System beitreten, indem sie sich – freiwillig aber bindend – zur Einhaltung der sogenannten „Safe Harbour-Grundsätze“[19] und der beigefügten Umsetzungsleitlinien in Form von „Häufig gestellten Fragen“ (FAQ)[20] verpflichteten. Diese wurden vom Handelsministerium der USA vorgelegt und von der Kommission in ihre Entscheidung integriert. Die Übermittlung personenbezogener Daten von EU-Bürgern in die USA war sodann (nur) an derart zertifizierte Unternehmen zulässig. Insoweit war nach Auffassung der Kommission ein angemessenes Datenschutzniveau gegeben.[21] Die Selbstzertifizierung erfolgte durch eine jährlich zu erneuernde Erklärung gegenüber dem amerikanischen Handelsministerium. Alle beigetretenen Unternehmen wurden zu Transparenzzwecken in ein öffentlich zugängliches Register aufgenommen.[22] Die Federal Trade Commission (FTC) überwachte in den USA die Einhaltung der Safe Harbour-Regeln durch die Unternehmen.

Das „Safe Harbour“-System wurde von zahlreichen kleinen und großen Unternehmen als Rechtsgrundlage für den Transfer personenbezogener Daten in die USA genutzt. Zuletzt wurden auf der Liste der Safe Harbour-Unternehmen 4.389 Unternehmen mit dem Zertifizierungsstatus „current“ geführt.[23] Tatsächlich betroffen sind aber viel mehr Unternehmen, beispielsweise auch diejenigen, die Cloud-Dienste nutzen, welche wiederum personenbezogene Daten über „Safe Harbour“ in die USA übermitteln.

5.2 Kritik an „Safe Harbour“

„Safe Harbour“ geriet jedoch in der Vergangenheit immer wieder in Kritik, maßgeblich auch durch die deutschen Datenschutzaufsichtsbehörden.[24] Umfassende Zweifel an der „Sicherheit des Hafens“ erweckten schließlich die Enthüllungen von Edward Snowden im Jahr 2013 hinsichtlich der weltweiten, umfassenden und anlasslosen Überwachung der digitalen Kommunikation durch den amerikanischen Geheimdienst National Security Agency (NSA). Nach diesen Enthüllungen soll die NSA u.a. das Überwachungsprogramm „PRISM“ aufgelegt und in dessen Rahmen freien Zugang zu großen Datenmengen auf Servern in den USA erlangt haben. Da alle an „PRISM“ beteiligten Unternehmen, die den US-Behörden den Zugriff auf die auf ihren Servern gespeicherten Daten gestatteten, auch der „Safe Harbour“-Regelung beigetreten sind[25], dürften auch die über „Safe Harbour“ übermittelten personenbezogenen Daten von EU-Bürgern von diesem Zugriff erfasst gewesen sein. Diese Entwicklungen nahm die Kommission zum Anlass, die Funktionsweise der „Safe Har-

---

[19] Die „Safe Harbour“-Grundsätze regelten die einzuhaltenden Regelungen über den Schutz der personenbezogenen Daten (Datenintegrität, Sicherheit, Wahlmöglichkeit und Weitergabe an Dritte) sowie die Verfahrensrechte der betroffenen Person (Informationspflicht, Auskunftsrecht und Durchsetzung); sie sind abgedruckt in Anhang I der Entscheidung 2000/520/EG.

[20] Die FAQ enthielten Leitlinien, die den Unternehmen die Umsetzung der Grundsätze erleichtern sollten. Sie sind in Anhang II der Entscheidung 2000/520/EG abgedruckt.

[21] Vgl. Art. 1 und Erwägungsgrund 5 der Entscheidung 2000/520/EG.

[22] Siehe die U.S.-E.U. Safe Harbour List unter https://safeharbour.export.gov/list.aspx.

[23] Stand 02.12.2015.

[24] Kritisiert wurde insbesondere die mangelnde Kontrolle der teilnehmenden US-Unternehmen durch die dortigen Behörden, vgl. etwa die Website des Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, https://www.datenschutzzentrum.de/material/tb/tb32/kap11.htm unter 11.4.

[25] Vgl. Mitteilung der Kommission an das Europäische Parlament und den Rat über die Funktionsweise der Safe Harbour-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen vom 27.11.2013, COM (2013) 847 (final), unter 7. (S. 18), abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52013DC0847&qid=1456303265011&from=DE.

bour“-Entscheidung und das durch diese gewährleistete Schutzniveau zu überprüfen. Auch die deutschen Datenschutzbehörden hatten insoweit Bedenken geäußert.[26] Trotz Zweifeln an dem kontinuierlichen Schutz der Daten von EU-Bürgern angesichts des umfassenden Zugriffs der US-Nachrichtendienste verzichtete die Kommission jedoch entgegen entsprechender Forderungen der deutschen Datenschutzkonferenz[27] darauf, die „Safe Harbour-Entscheidung“ auszusetzen.[28] Stattdessen beschränkte sie sich darauf, 13 Empfehlungen für die US-Seite zu veröffentlichen, mittels derer der auf „Safe Harbour“ gestützte Datentransfer hinsichtlich Transparenz, Rechtsschutz, Durchsetzung und dem Zugriff durch US-Behörden optimiert werden könnte.[29]

5.3 EuGH: „Safe Harbour“ ist ungültig

Der EuGH hat im „Schrems“-Urteil“[30] die Gelegenheit beim Schopf ergriffen, die „Safe Harbour“-Entscheidung der Kommission für ungültig zu erklären. Der Entscheidung vom 6. Oktober 2015, die weitreichende Auswirkungen für die transatlantische Wirtschaft hat, lag eine Beschwerde des österreichischen Staatsangehörigen Maximilian Schrems, Nutzer des sozialen Netzwerks „Facebook“, zugrunde.

5.3.1 Sachverhalt und Hintergrund der Entscheidung

Schrems wandte sich gegen die gängige Praxis von Facebook, die personenbezogenen Daten der in der EU wohnhaften Facebook-Nutzer über die in Dublin ansässige europäische Facebook-Zentrale[31] ganz oder teilweise an in den USA befindliche Server der US-Muttergesellschaft Facebook Inc. zu übermitteln und dort zu speichern. Er war der Auffassung, dass seine personenbezogenen Daten in den USA nach den Enthüllungen von Edward Snowden nicht hinreichend vor der Überwachungstätigkeit der US-Geheimdienste und insbesondere der NSA geschützt seien. Aus diesem Grund erhob er Beschwerde beim irischen Datenschutzbeauftragten (nachfolgend: „Commissioner“) und forderte diesen auf, der Facebook Ireland Ltd. die Übermittlung seiner personenbezogenen Daten in die USA zu untersagen. Der Commissioner wies die Beschwerde als unbegründet zurück. Zum einen gebe es keinen Beweis dafür, dass die NSA auf die Daten von Herrn Schrems zugegriffen habe. Zum anderen habe die Kommission in der „Safe Harbour-Entscheidung“ festgestellt, dass die USA im Rahmen dieser Entscheidung ein angemessenes Schutzniveau der übermittelten personenbezogenen Daten gewährleisteten. Er sehe sich daher durch diese Entscheidung gebunden und daran gehindert, eigene Untersuchungen anzustellen, die diese Feststellung in Frage stellten. Dagegen erhob Schrems Klage beim Irischen High Court. Dieser war der Auffassung, der massenhafte und undifferenzierte Zugriff der US-amerikanischen Sicherheitsbehörden auf personenbezogene Daten sei unverhältnismäßig und verstoße gegen die durch die irische Verfassung geschützten Grundwerte. Die Rechtmäßigkeit der Entscheidung des Commissioners sei aber auch anhand des Unionsrechts zu beurteilen. Die „Safe Harbour-Entscheidung“ genüge je-

---

[26] Vgl. die Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juli 2013: “Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten”, abrufbar unter https://www.datenschutz.hessen.de/presse_2013.htm#entry3939.

[27] Vgl. Fn. 26.

[28] Die Kommission begründete dies damit, dass die Aufhebung von „Safe Harbour“ den Interessen der beteiligten Unternehmen in der EU und den USA schaden würde, vgl. Mitteilung der Kommission COM(2013) 846 (final) (Fn. 1), Ziffer 3.2.

[29] So sollten zertifizierte US-Unternehmen in ihren Datenschutzbestimmungen (1) darüber Auskunft geben, in welchem Umfang die Behörden nach Maßgabe des US-Rechts über „Safe Harbour“ übermittelte Daten erheben und verarbeiten dürfen und (2) angeben, in welchen Fällen sie solche Ausnahmen von den „Safe Harbour“-Grundsätzen anwenden, um Anforderungen der nationalen Sicherheit, des öffentlichen Interesses oder der Rechtsdurchsetzung zu genügen. Von der Ausnahme der nationalen Sicherheit dürfe künftig nur so weit Gebrauch gemacht werden, wie dies unbedingt notwendig oder angemessen sei, vgl. Mitteilung COM (201) 847 (final) (Fn. 25), unter 8. (S. 22).

[30] EuGH, Urteil vom 06.10.2015, C-362/14 Maximilian Schrems ./. Data Protection Commissioner, abrufbar unter http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14.

[31] Facebook Ireland Ltd.

doch nach seiner Auffassung weder den Anforderungen der Art. 7 und 8 der EU-Grundrechtecharta (GRC) noch den vom Gerichtshof in seiner bisherigen Rechtsprechung zum Datenschutz aufgestellten Grundsätzen.

Der Irische High Court setzte daher das Verfahren aus und legte dem EuGH zwei Fragen zur Vorabentscheidung vor. Im Kern ging es hierbei darum, wie sich eine nationale Datenschutzbehörde wie der Commissioner verhalten muss, wenn in einer Beschwerde geltend gemacht wird, dass in einem Drittland wie den USA kein angemessenes Datenschutzniveau vorliege. Ist er an die implizite Feststellung eines angemessenen Schutzniveaus durch die Kommission in der Safe Harbour-Entscheidung gebunden? Oder muss er als unabhängige nationale Datenschutzbehörde eigenständig beurteilen, ob die Übermittlung personenbezogener Daten in die USA mit den Art. 7 und 8 der GRC in Einklang steht? Dies sei dann der Fall, wenn die DSRL, ihr Art. 25. Abs. 6 und die auf dieser Basis ergangene Safe Harbour-Entscheidung im Lichte der nachfolgend in Kraft getretenen Art. 7, 8 und 47 GRC entsprechend auszulegen seien. Auf den Punkt gebracht betrafen die Vorlagefragen somit den Umfang der Untersuchungsbefugnisse der nationalen Datenschutzbehörden bei Vorliegen einer Angemessenheitsentscheidung der Kommission.[32]

5.3.2 Begründung des EuGH

Der EuGH folgte weitgehend den Schlussanträgen des Generalanwalts Yves Bot.[33] Zur Beantwortung der Vorlagefrage nahm er zunächst zu den Befugnissen der nationalen Kontrollstellen Stellung (hierzu sogleich 5.3.2.1). Im Anschluss hieran prüfte der Gerichtshof die Gültigkeit der „Safe Harbour“-Entscheidung (hierzu unten 5.3.2.2). Inhaltlich rügte er dabei insbesondere die folgenden wesentlichen Mängel des „Safe Harbour“-Systems:

(1) die unzureichende Prüfung und Feststellung eines angemessenen Schutzniveaus durch die Kommission,
(2) das Fehlen wirksamer Überwachungs- und Kontrollmechanismen,
(3) die fehlende Begrenzung der Grundrechtseingriffe,
(4) das Fehlen eines wirksamen gerichtlichen Rechtsschutzes gegen solche Eingriffe und
(5) die unrechtmäßige Beschneidung der Befugnisse der nationalen Datenschutzbehörden.

Schließlich erklärte der Gerichtshof die gesamte „Safe Harbour“-Entscheidung für ungültig.

5.3.2.1 Völlige Unabhängigkeit der nationalen Kontrollstellen

Der Gerichtshof beantwortete zunächst die Vorlagefragen. Er stellte klar, dass das Vorliegen einer Angemessenheitsentscheidung der Kommission wie der „Safe Harbour“-Entscheidung die Kontrollbefugnisse der nationalen Datenschutzbehörden, die sich aus der DSRL sowie aus Art. 16 Abs. 2 AEUV und Art. 8 Abs. 3 der GRC ergeben, weder beseitigen noch beschränken könne. Aufgabe der nationalen Kontrollstellen sei es hiernach, die Einhaltung des Unionsrechts über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in völliger Unabhängigkeit zu überwachen. Zwar sei eine Angemessenheitsentscheidung der Kommission grundsätzlich für die EU-Mitgliedstaaten bindend und diese dürften keine ihr entgegenstehenden verbindlichen Feststellungen treffen. Allein der Gerichtshof könne die Ungültigkeit einer solchen Entscheidung feststellen. Die nationalen Datenschutzbehörden müssten aber aufgrund der ihnen ausdrücklich verliehenen Befugnisse bei der Befassung mit einer Beschwerde vollkommen unabhängig prüfen können, ob bei der Übermittlung der Daten in ein Drittland die Anforderungen der DSRL gewahrt

[32] Schlussanträge des Generalanwalts Yves Bot vom 23.09.2015, Rn. 57, abrufbar unter http://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14.
[33] Vgl. Fn. 32.

werden – mit anderen Worten, ob im Drittland ein angemessenes Schutzniveau besteht.[34] Sei eine solche Behörde oder eine beschwerdeführende Person der Auffassung, dass eine Angemessenheitsentscheidung der Kommission ungültig sei, müsse sie die nationalen Gerichte anrufen können, damit diese ihrerseits die Sache dem Gerichtshof vorlegen könnten. Der irische Commissioner muss nunmehr die Beschwerde von Herrn Schrems umfassend prüfen und eigenständig und unabhängig entscheiden, ob die Übermittlung seiner Daten in die USA durch Facebook auszusetzen ist.

5.3.2.2 Zur Ungültigkeit der „Safe Harbour-Entscheidung“

Obwohl die Beantwortung der Vorlagefrage eine weitere Prüfung nicht zwingend erfordert hätte, nahm der Gerichtshof sodann zur Gültigkeit der „Safe Harbour-Entscheidung“ Stellung.[35]

(1) Unzureichende Prüfung und Feststellung eines „angemessenen Schutzniveaus“ durch die Kommission

Der EuGH bemängelte, die Kommission habe in der „Safe Harbour“-Entscheidung nicht festgestellt, dass die USA tatsächlich ein angemessenes Schutzniveau gewährleisten.[36] Eine solche Feststellung sehe der Wortlaut des Art. 25 Abs. 6 DSRL bei einer Angemessenheitsentscheidung jedoch vor. Demnach hätte die Kommission die Rechtslage in den Vereinigten Staaten umfassend prüfen und sodann feststellen – und gebührend begründen – müssen, dass die USA entweder aufgrund ihrer innerstaatlichen Rechtsvorschriften oder aufgrund internationaler Verpflichtungen ein angemessenes – weil der Sache nach gleichwertiges – Niveau hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen gewährleisten.[37] Stattdessen beschränkt sich Artikel 1 der „Safe Harbour“-Entscheidung auf die Annahme, dass die „Safe Harbour“-Grundsätze ein angemessenes Schutzniveau im Sinne der Richtlinie gewährleisten.[38] Er verstößt daher nach Auffassung des EuGH gegen die in Art. 25 Abs. 6 DSRL im Licht der GRC festgelegten Anforderungen. Artikel 1 sei daher ungültig, ohne dass es einer inhaltlichen Prüfung der „Safe Harbour“-Grundsätze bedürfe.[39]

(2) Erfordernis wirksamer Mittel zur Gewährleistung des Schutzniveaus

Dies bedeutet jedoch nicht, dass der EuGH einen Angemessenheitsbeschluss auf der Basis eines Selbstzertifizierungssystems für ausgeschlossen hält. Zwar müsse ein Drittland nach dem Wortlaut des Art. 25 Abs. 6 DSRL „aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen“ ein angemessenes Schutzniveau gewährleisten. Wie der Gerichtshof ausdrücklich ausführt, verstößt der Rückgriff eines Drittlands auf ein System der Selbstzertifizierung als solcher jedoch nicht gegen dieses Erfordernis. Die Zuverlässigkeit eines solchen Systems beruhe aber wesentlich auf der Schaffung wirksamer Überwachungs- und Kontrollmechanismen, die es erlauben,

---

[34] Es handelt sich insoweit um eine geteilte Kompetenz zwischen EU-Mitgliedstaaten und Kommission, vgl. Schlussanträge des Generalanwalts Yves Bot vom 23.09.2015, C-362/14, Rn. 86; siehe auch Bretthauer, K&R 2015, S. 717.

[35] Kritisch insoweit Bretthauer, K&R 2015, S. 717 und Moos/Schefzig, CR 2015, S. 625 (628); zustimmend hingegen Kühling, NVwZ 2016, S. 7 (9).

[36] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 71 ff, 97.

[37] EuGH, Rechtssache „Schrems“, a.a.O. (Fn. 30)., Tz. 96, 71 ff. Zwar schloss der Gerichtshof nicht grundsätzlich aus, dass ein angemessenes Schutzniveau in einem Drittland i.S.v. Art. 25 Abs. 2, 6 der EG-Datenschutzrichtlinie auch über ein System der Selbstzertifizierung sichergestellt werden kann (EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 81). Die „Safe Harbour“-Entscheidung enthalte jedoch keine hinreichenden Feststellungen zu den Maßnahmen, mit denen die USA aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau gewährleisteten (EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 83).

[38] An anderer Stelle kritisierte der EuGH, die „Safe Harbour“-Entscheidung enthalte auch keine hinreichenden Feststellungen zu den Maßnahmen, mit denen die USA ein angemessenes Schutzniveau gewährleisteten, vgl. EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 83.

[39] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 98.

in der Praxis etwaige Verstöße gegen Grund- und Datenschutzrechte zu ermitteln und zu ahnden.[40] Die Mittel, auf die das Drittland zurückgreife, um ein angemessenes Schutzniveau zu gewährleisten, könnten sich von denen unterscheiden, die in der Union herangezogen werden, um die Wahrung der Anforderungen aus der Richtlinie im Licht der Charta zu gewährleisten. Sie müssten sich aber gleichwohl in der Praxis als wirksam erweisen, um einen der Sache nach gleichwertigen Schutz zu gewährleisten.[41] Demnach kann ein zuverlässiges Selbstzertifizierungssystem nach Auffassung des EuGH bei der Beurteilung des angemessenen Schutzniveaus durchaus eine Rolle spielen. Seine Ausführungen lassen jedoch den Schluss zu, dass der Gerichtshof die existierenden Überwachungs- und Kontrollmechanismen des „Safe Harbour“-Systems nicht als ausreichend erachtete. Dabei bemängelte er auch, dass die „Safe Harbour“-Grundsätze nur für selbstzertifizierte US-Organisationen gälten, aber nicht von amerikanischen Behörden einzuhalten seien.[42]

(3) Unverhältnismäßigkeit grenzenloser Grundrechtseingriffe

Weiterhin kritisierte der EuGH, die „Safe Harbour“-Entscheidung ermögliche weitreichende Grundrechtseingriffe[43], insbesondere in das in Art. 7 GRC geregelte Grundrecht auf Achtung der Privatsphäre sowie das durch Art. 8 GRC gewährleistete Grundrecht auf Schutz personenbezogener Daten, ohne als Ausgleich hierfür eine wirksame Begrenzung vorzusehen. Denn die Entscheidung regele Ausnahmetatbestände, mit Hilfe derer der durch die „Safe Harbour-Grundsätze“ gewährleistete Schutz unter Berufung auf Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen eingeschränkt werden könne. Diesen Erfordernissen werde grundsätzlich Vorrang vor den Schutzregeln des „Safe Harbour“ eingeräumt.[44] Dies habe zur Folge, dass die zertifizierten Unternehmen verpflichtet seien, die „Safe Harbour“-Schutzregeln unangewandt zu lassen, wenn sie in Widerstreit zu solchen Erfordernissen stünden. Eine Feststellung dazu, ob in den USA staatliche Regelungen zur Begrenzung solcher Eingriffe existierten, enthalte die Entscheidung nicht.[45] Im Gegenteil habe die Kommission selbst festgestellt, dass die US-Behörden auf die aus der EU in die USA übermittelten personenbezogenen Daten zugreifen und sie in einer Weise verarbeiten konnten, die mit den Zielsetzungen ihrer Übermittlung unvereinbar war und über das hinausging, was zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig war.[46]

Nach ständiger Rechtsprechung des EuGH müsse eine Unionsregelung, die einen Eingriff in die durch Art. 7 und 8 GRC garantierten Grundrechte enthält, klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen. Nur dann gewährleiste sie den Betroffenen ausreichende Garantien, die einen wirksamen Schutz ihrer Daten vor Missbrauch und der Gefahr des unberechtigten Zugangs böten. Diese Gefahr sei aber gerade bei der automatischen Verarbeitung der Daten erheblich.[47] Der Schutz des Grundrechts auf Achtung des Privatlebens verlange, dass etwaige Ausnahmen und Einschränkungen des Schutzes personenbezogener Daten sich auf das absolut Notwendige beschränkten.[48] Eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus

[40] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 81.
[41] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 74.
[42] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 82.
[43] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 87.
[44] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 86.
[45] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 89.
[46] Vgl. die Mitteilung der Kommission COM(2013) 846 (final) (Fn. 1), Ziffern 2 und 3.2 sowie Mitteilung der Kommission COM (2013) 847 (final), (Fn. 25), Ziffern 7.1, 7.2 und 8.
[47] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 91 und EuGH, verbundene Rechtssachen C-293/12 (Digital Rights Ireland Ltd.) und C-594/12 (Kärntner Landesregierung), Urteil vom 08.04.2014, Tz. 55. Das Urteil ist abrufbar unter http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=DE.
[48] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 92 und EuGH, Digital Rights Ireland Ltd. (Fn. 47), Tz. 51.

der EU in die USA übermittelt wurden, gestatte, sei nicht auf das absolut Notwendige beschränkt.[49] Denn sie nehme keine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vor. Sie enthalte auch kein objektives Kriterium, das es ermögliche, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die solche Eingriffe rechtfertigen könnten. Eine Regelung, die es den Behörden gestatte, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, verletze den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens.[50] Es liegt nahe, dass der Gerichtshof bei dieser Aussage die von Herrn Schrems gerügte Zugriffspraxis der US-amerikanischen Geheimdienste im Hinterkopf hatte.[51]

(4) Fehlen eines wirksamen gerichtlichen Rechtsschutzes

Darüber hinaus bemängelte der Gerichtshof, dass die Kommission in der „Safe Harbour“-Entscheidung keine Feststellung zum Bestehen eines wirksamen gerichtlichen Rechtsschutzes gegen Grundrechtseingriffe getroffen habe.[52] Die vorgesehenen Überwachungsinstrumente in Form privater Schiedsgerichte und Verfahren vor der Federal Trade Commission (FTC) dienten nur der Kontrolle der Einhaltung der „Safe Harbour“-Grundsätze durch die US-Unternehmen, böten aber kein Rechtsmittel gegen Grundrechtseingriffe durch staatliche Maßnahmen.[53] Auch gebe es, wie die Kommission selbst festgestellt habe[54], keine administrativen oder gerichtlichen Rechtsbehelfe, die es den Betroffenen erlaubten, Zugang zu den sie betreffenden personenbezogenen Daten zu erhalten oder ihre Berichtigung oder Löschung zu erwirken.[55] Eine Regelung, die solche Möglichkeiten nicht vorsehe, verletze den Wesensgehalt des in Art. 47 GRC verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz.[56]

(5) Unrechtmäßige Beschränkung der Befugnisse der nationalen Datenschutzbehörden

Schließlich erklärte der Gerichtshof auch Art. 3 der „Safe Harbour-Entscheidung“ für ungültig.[57] Dieser erhöhe die Schwelle für Eingriffsmaßnahmen der nationalen Kontrollstellen wie etwa die Aussetzung von Datenübermittlungen. Er entziehe damit den nationalen Kontrollstellen Befugnisse, die ihnen eigentlich nach Art. 28 DSRL im Licht insbesondere des Grundrechts auf Schutz personenbezogener Daten nach Art. 8 GRC zustünden. Wie schon ausgeführt, besitzen die nationalen Datenschutzbehörden bei Eingaben von Personen zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten ein vollkommen unabhängiges Prüfungsrecht. Dies gilt nach Ansicht des EuGH insbesondere dann, wenn es um die Frage der Vereinbarkeit einer Angemessenheitsentscheidung der Kommission mit dem Schutz der Privat-sphäre sowie der Freiheiten und Grundrechte von Personen gehe.[58] Die Durchführungsbefugnis des Art. 25 Abs. 6 DSRL ermächtige die Kommission nicht dazu, die Befugnisse der nationalen Kontrollstellen zu beschränken. Die Kommission habe insoweit ihre Zuständigkeit überschritten.

---

[49] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 93 und EuGH, Digital Rights Ireland Ltd. (Fn. 47), Tz. 57-61.
[50] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 94 und EuGH, Digital Rights Ireland Ltd. (Fn. 47), Tz. 39 – Umkehrschluss.
[51] Siehe auch Kühling/Heberlein, NVwZ 2016, S. 7 (10); Moos/Schefzig, CR 2015, S. 625 (630).
[52] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 89.
[53] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 89.
[54] Mitteilungen der Kommission, COM(2001) 846 (final) (Fn. 1), Ziffer 3.4 und COM (201) 847 (final) (Fn. 25), Ziffer 7.2.
[55] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 90.
[56] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 95.
[57] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 102-104.
[58] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 99.

Weil die ungültigen Art. 1 und 3 der „Safe Harbour-Entscheidung“ aber untrennbar mit deren Art. 2 und 4 sowie den Anhängen verbunden seien, erklärte der Gerichtshof letztlich die gesamte „Safe Harbour“-Entscheidung ohne Übergangsfrist für ungültig.[59]

5.4 Bewertung und Folgen des Urteils

Die Entscheidung des EuGH ist unter dem Gesichtspunkt eines effektiven Schutzes der personenbezogenen Daten von EU-Bürgern zu begrüßen und wurde daher von Verbraucher- und Datenschützern auch weithin bejubelt. Der Gerichtshof hebt in seinem Urteil die Unabhängigkeit der nationalen Datenschutzbehörden und die Bedeutung ihrer Aufgaben hervor und stellt hohe Maßstäbe für die Datenübermittlung in Drittstaaten auf. Dabei macht er klare Vorgaben, wie hinreichende Garantien für einen wirksamen Datenschutz gewährleistet werden können. Der Gerichtshof setzt damit ein deutliches Zeichen, dass der wirksame und gleichwertige Schutz der personenbezogenen Daten von EU-Bürgern außerhalb der EU mehr erfordert als eine Zertifizierungslösung ohne wirksame Kontrolle und Effizienz.

Dennoch hat der Wegfall von „Safe Harbour“ die Wirtschaft weithin unvorbereitet getroffen. Betroffen sind hierdurch alle EU-Unternehmen, die unmittelbar personenbezogene Daten über „Safe Harbour“ in die USA übermittelten. Gleiches kann auch für Unternehmen gelten, die „Facebook“-Seiten verwenden oder ihrerseits Cloud-Dienste wie „Google Cloud“ nutzen. Denn derartige Dienstleister speichern ihrerseits personenbezogene Daten von Mitarbeitern oder Kunden auf US-Servern oder verarbeiten diese sonst in den USA. Auch diese Daten wurden häufig auf der Basis von „Safe Harbour“ transferiert.

Da die Übermittlung von personenbezogenen Daten in die USA nicht mehr auf die ungültige „Safe Harbour“-Entscheidung gestützt werden kann, besteht seit dem „Schrems-Urteil“ des EuGH in der Praxis eine erhebliche Rechtsunsicherheit, die von Vertretern der Wirtschaft zu Recht kritisiert wird. Denn nach dem Grundsatz des Art. 25 Abs. 1 DSRL ist der Transfer personenbezogener Daten aus der EU in die USA in Ermangelung eines angemessenen Schutzniveaus in den Vereinigten Staaten gegenwärtig unzulässig, sofern er nicht auf eine alternative Rechtsgrundlage gestützt werden kann. Dies setzt jedoch voraus, dass die Voraussetzungen eines anderen von der DSRL bzw. künftig der DSGV vorgesehenen rechtlichen Instruments oder Erlaubnistatbestands für eine Übermittlung in die USA vorliegen. Zum anderen dürfen diese alternativen Rechtfertigungsgründe nicht gleichermaßen durch die neueren Entwicklungen „infiziert“ sein und an den gleichen Mängeln wie die „Safe Harbour“-Entscheidung kranken. Denn damit wären sie zwar nicht automatisch unwirksam, faktisch jedoch ihrer Rechtfertigungskraft beraubt.

Mit anderen Worten müssen angesichts der kritisierten Unzulänglichkeiten und bei konsequentem Fortdenken der vom EuGH aufgestellten Maßstäbe sämtliche Übermittlungen personenbezogener Daten in die USA neu bewertet werden, auch wenn sie auf andere Rechtfertigungsgründe gestützt werden. Es ist zu prüfen, ob und inwieweit der transatlantische Transfer personenbezogener Daten gegenwärtig noch mit den verbleibenden Erlaubnistatbeständen gerechtfertigt werden kann. Ein Überblick über die möglichen Alternativen zu „Safe Harbour“ wird nachfolgend unter Ziffer 6., eine Einschätzung zur deren weiterer Verwendbarkeit unten unter Ziffer 7. gegeben.

Zudem gilt es, nach dem Wegfall von „Safe Harbour“ als einheitlich genutzter Rechtsgrundlage für den transatlantischen Datenverkehr eine Rechtszersplitterung in der EU zu verhindern. Als Reaktion auf das Urteil haben Vertreter bedeutender Industriegruppen, Wirtschaftsverbände und Unternehmen aus der EU und den USA die Kommission am 13. Oktober 2015 in einem offenen Brief an

[59] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 106.

Kommissionspräsident Juncker[60] aufgefordert, in enger Kooperation mit den nationalen Datenschutzbehörden eine harmonisierte Umsetzung des Urteils sicherzustellen und eine Rechtszersplitterung durch unterschiedliche Vorgehensweisen auf nationaler Ebene zu verhindern. Ferner forderten sie Leitlinien für die betroffenen Unternehmen sowie eine hinreichende Übergangszeit für die Umstellung ihrer Übermittlungspraktiken. Schließlich appellierten sie an die Kommission und die USA, ihre langwierigen Verhandlungen dringend zu vollenden, ein neues, gestärktes „Safe Harbour“-Framework abzuschließen und wieder Rechtsklarheit zu schaffen. Demgegenüber hat die Art. 29-Datenschutzgruppe[61] in einer Stellungnahme vom 16. Oktober 2015[62] ein Durchgreifen der nationalen Datenschutzbehörden angekündigt, sofern bis zum 31.01.2016 keine neue Rechtsgrundlage für einen legalen Datentransfer in die USA in Kraft gesetzt werde. Ob und inwiefern solche Durchgriffe tatsächlich erfolgen, wird allerdings maßgeblich von der noch ausstehenden Einschätzung der Datenschutzgruppe zur Zulässigkeit alternativer Übermittlungsinstrumente abhängen.

Solange eine sichere Rechtsgrundlage für den transatlantischen Datenverkehr fehlt, sind unterschiedliche Maßnahmen der durch den EuGH in ihrer Rolle gestärkten nationalen Datenschutzbehörden zu befürchten. Die Kommission plant gerade den Erlass eines neuen Angemessenheitsbeschlusses. Auf die aktuellen Entwicklungen wird nachfolgend unter Ziffer 8.3 noch näher eingegangen. Ob ein solcher Beschluss tatsächlich zeitnah erlassen wird und bereits in naher Zukunft als Grundlage für einen Transfer genutzt werden kann, bleibt abzuwarten. In der Zwischenzeit gilt es zu prüfen, auf welcher alternativen Basis eine legale Übertragung personenbezogener Daten in die USA nach der Ungültigkeit von „Safe Harbour“ überhaupt noch möglich ist.

6 Alternative Rechtsgrundlagen für Datenübermittlungen in die USA

Solange kein neuer Angemessenheitsbeschluss der Kommission zum Schutzniveau in den USA in Kraft ist[63], muss der Transfer personenbezogener Daten in die USA nach dem Wegfall von „Safe Harbour“ auf einen anderen Rechtfertigungsgrund gestützt werden – ansonsten wäre er illegal. Sowohl nach der DSRL als auch künftig nach der DSGV dürfen personenbezogene Daten auch in ein Drittland ohne angemessenes Datenschutzniveau übermittelt werden, wenn anderweitig für ausreichende Garantien hinsichtlich des Datenschutzes gesorgt wird, die das unzulängliche Schutzniveau in dem Drittstaat kompensieren. Solche Garantien können sich insbesondere aus vertraglichen Vereinbarungen zwischen Datenexporteur und Datenimporteur (hierzu sogleich Ziffer 6.1) oder verbindlichen unternehmensinternen Datenschutzregelungen („Binding Corporate Rules“, vgl. unten Ziffer 6.2) ergeben. Daneben kann eine transatlantische Datenübermittlung unter bestimmten Voraussetzungen auch durch einen Ausnahmetatbestand gerechtfertigt sein (hierzu unten Ziffer 6.3)

---

[60] Open letter on the implementation of the CJEU Judgement on Case C-362/14 Maximilian Schrems v Data Protection Commissioner, abrufbar unter http://cdn.ccianet.org/wp-content/uploads/2015/10/JointindustryletteronCJEUjudgment1013.pdf.

[61] Die Art. 29-Datenschutzgruppe ist ein durch die EU-Datenschutzrichtlinie geschaffenes unabhängiges Beratungsgremium, eine Art europäische Kooperationsplattform, die sich aus je einem Vertreter der nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten und einem Vertreter der Kommission zusammensetzt und die Kommission insbesondere in Datenschutzfragen berät.

[62] Statement der Artikel-29-Datenschutzgruppe vom 16.10.2015, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/StatementOfTheArticle29WorkingParty_DeutscheFassung.pdf?__blob=publicationFile&v=2.

[63] Zu den neueren Entwicklungen in diesem Bereich vgl. unten Ziffer 8.3.

6.1 Vertragliche Vereinbarungen und Standarddatenschutzklauseln (SDPC)

Vertragliche Vereinbarungen zwischen EU-Datenexporteur und US-Datenimporteur, die das fehlende Datenschutzniveau ausgleichen, können individuell ausgehandelt werden und sind dann auf Einzelfallbasis durch die nationalen Datenschutzbehörden zu genehmigen.[64] Unter der DSGV wird einer solchen Genehmigung ausdrücklich ein Kohärenzverfahren vorgeschaltet[65], um einheitliche Genehmigungsstandards sicherzustellen. Diese Variante ist jedoch recht aufwändig und kommt daher nicht für jedes Unternehmen in Frage.

Um vertragliche Vereinbarungen zwischen Datenexporteur und Datenimporteur zu vereinfachen, kann die Kommission gemäß Art. 26 Abs. 2, 4 DSRL sowie Art. 42 Abs. 1, Abs. 2 lit. (c) DSGV sogenannte Standarddatenschutzklauseln erlassen („Standard Data Protection Clauses, nachfolgend „SDPC“[66]). Hierbei handelt es sich um harmonisierte vertragliche Transferregelungen in Form von Musterverträgen, die nach Auffassung der Kommission ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der hiermit verbundenen Rechte bieten und daher von ihr anerkannt und zur allgemeinen Nutzung freigegeben werden. Nach Art. 42 Abs. 1, 2 Abs. 2 lit. (d) DSGV kann die Kommission künftig auch SDPC, die von einer nationalen Aufsichtsbehörde angenommen wurden, genehmigen und somit europaweit zur Nutzung freigeben.

Die Kommission hat in verschiedenen Entscheidungen[67] insgesamt drei Versionen von SDPC anerkannt, die die datenschutzrechtlichen Verpflichtungen von EU-Datenexporteur und Datenimporteur im Drittland sowie die Rechte der Betroffenen im Detail regeln. Danach können Unternehmen für die Übermittlung vom EU-Verantwortlichen zum Verantwortlichen im Drittland zwischen „Standardvertrag I“[68] und „Standardvertrag II“[69] wählen.[70] Für die Übermittlung vom EU-Verantwortlichen zum Auftragsdatenverarbeiter im Drittland steht ein Standardvertrag „Auftragsverarbeiter“ zur Verfügung.[71] Gemäß Art. 1 der jeweiligen Kommissionsentscheidung gelten die jeweils in deren Anhang abgedruckten SDPC als ausreichende Garantien gemäß Art. 26 Abs. 2 DSRL.[72]

SDPC müssen unverändert übernommen und in einen Vertrag zwischen EU-Datenexporteur und US-Datenimporteur integriert werden. Diese Lösung ist daher relativ leicht umsetzbar. Internationale Datentransfers auf der Basis solcher SDPC bedürfen dann keiner weiteren Genehmigung der Datenschutzbehörden mehr. Der Nachteil von SDPC besteht allerdings darin, dass grundsätzlich

---

64 Vgl. Art. 26 Abs. 2 EU-Datenschutzrichtlinie und Art. 42 Abs. 1, Abs. 2a lit. (a) DSGV.

65 Art. 42 Abs. 5a DSGV.

66 Die hier als „Standarddatenschutzklauseln“ (SDPC) bezeichneten Klauseln waren bislang unter dem Namen „Standardvertragsklauseln bzw. „Standard Contractual Clauses“ (SCC) bekannt. Der hier verwendete Begriff knüpft an die neue Terminologie in der DSGV an.

67 Vgl. etwa *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 04.07.2001, S. 19ff., in der durch die *Entscheidung 2004/915/EG* der Kommission vom 27.12.2004 („Entscheidung (…) zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer“) geänderten Fassung, ABl. L 385 vom 29.12.2004, S. 74ff., sowie *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 des Europäischen Parlaments und des Rates, ABl. L 39 vom 12.02.2010, S. 5 ff.

68 Anhang zu Entscheidung 2001/497/EG (Fn. 68).

69 Anhang zu Entscheidung 2004/915/EG (Fn. 68).

70 Diese Klauseln betreffen typischerweise Unternehmen, die CRM (Customer Relationship Management) und Personaldaten übermitteln.

71 Dies betrifft die meisten Cloud-Diensteanbieter, die Kundendaten übermitteln.

72 Vgl. Art. 1 der Entscheidung 2001/497/EG in der durch die Entscheidung 2004/915/EG geänderten Fassung (Fn. 67), sowie Art. 1 des Beschlusses 2010/7/EU (Fn. 68).

zwischen jedem EU-Datenexporteur und jedem (US-)Datenimporteur ein eigener Vertrag geschlossen werden muss.

Die Entscheidungen der Kommission zu den Standardvertragsklauseln sind nach wie vor gültig. Der EuGH hat im „Schrems-Urteil“ ausschließlich die „Safe Harbour“-Entscheidung für ungültig erklärt. Auch unter der DSGV bleiben diese Kommissionsentscheidungen weiterhin in Kraft, bis sie von der Kommission ersetzt oder aufgehoben werden, vgl. Art. 42 Abs. 5b i.V.m. Abs. 2 DSGV. Entsprechend bleiben auch die von den nationalen Aufsichtsbehörden genehmigten SDPC bis zu einer abändernden Entscheidung durch die zuständige Aufsichtsbehörde gültig.[73]

6.2 Verbindliche unternehmensinterne Datenschutzregelungen (BCR)

Neben den SDPC besteht insbesondere für multinationale Unternehmensgruppen die Möglichkeit, verbindliche unternehmensinterne Datenschutzregelungen, sogenannte „Binding Corporate Rules“ (nachfolgend: „BCR“) einzuführen. BCR sind unternehmensinterne Datenschutzvorschriften für internationale Datentransfers. Genauer gesagt handelt es sich um selbst auferlegte konzerninterne Richtlinien zum Umgang mit personenbezogenen Daten bei internationalen Datentransfers, die für alle Mitglieder einer bestimmten Unternehmensgruppe rechtsverbindlich gelten und von allen Mitarbeitern zu befolgen sind. Die Art. 29-Datenschutzgruppe[74] hat in verschiedenen Arbeitsdokumenten („Working Papers“, nachfolgend: „WP“) einen Rahmen geschaffen, innerhalb dessen sich die Regelungen bewegen müssen. WP 153[75] enthält eine Übersicht über die Bestandteile und Grundsätze, die nach Maßgabe der WP 74[76] und WP 108[77] in den BCR geregelt werden müssen.[78] WP 154[79] beinhaltet einen Vorschlag für die Struktur von BCR, WP 155[80] listet FAQ zu den BCR auf.

Ob die von einem Unternehmen entworfenen BCR den Vorgaben dieses Rahmens gerecht werden, wird in einem recht langwierigen Verfahren geprüft. Das Unternehmen muss zunächst einen Entwurf seiner BCR bei der leitenden nationalen Datenschutzbehörde einreichen. Diese muss den Entwurf prüfen und sich mit den Behörden aller EU-Mitgliedstaaten abstimmen, von deren Territorium aus Konzernunternehmen Daten in Drittländer transferieren wollen.[81] Die meisten EU-Mitgliedstaaten haben ein System gegenseitiger Anerkennung vereinbart und erkennen das Ergebnis der prüfenden Behörde an; die übrigen Behörden müssen den BCR zustimmen. Die BCR gelten dann als geeignete Garantie i.S.v. Art. 26 Abs. 2 DSRL (künftig Art. 42 DSGV), weil sie innerhalb der Unternehmensgruppe ein adäquates Schutzniveau schaffen. Damit erlauben sie konzerninterne Datentransfers auch in Drittländer, in denen kein angemessenes Datenschutzniveau besteht, sofern der entsprechende Transfer innerhalb der EU rechtmäßig wäre. Manche EU-Mitgliedstaaten verlangen trotz BCR für den konkreten Datentransfer ins Drittland zusätzlich eine

---

[73] Siehe ebenfalls Art. 42 Abs. 5 b) DSGV.

[74] Zur Art. 29-Datenschutzgruppe vgl. Fn. 62.

[75] Art. 29-Datenschutzgruppe, Arbeitsdokument vom 24.06.2008, 1271-00/08/DE (WP153), abrufbar unter https://www.dsb.gv.at/DocView.axd?CobId=53527.

[76] Art. 29-Datenschutzgruppe, Arbeitsdokument „Übermittlung personenbezogener Daten in Drittländer: Anwendung von Art. 26 Abs.2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer“ vom 03.06.2003, 11639/02/DE (WP 74).

[77] Art. 29-Datenschutzgruppe, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules vom 14.04.2005, (WP 108, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf).

[78] Zum Inhalt gehören etwa Datenschutzgrundsätze, Geltungsbereich, Transparenzgebot, Selbstverpflichtung zu Audits, Regelungen zu Haftung und Schadensersatz bei Missachtung der BCR sowie Kooperationspflichten.

[79] Art. 29-Datenschutzgruppe, Arbeitsdokument „Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR) vom 24.06.2008, 1271-00-01/08/DE (WP 154).

[80] Art. 29-Datenschutzgruppe, Arbeitsdokument zu „Häufig gestellten Fragen“ über verbindliche unternehmensinterne Datenschutzregelungen (BCR)“ vom 24.06.2008, zuletzt überarbeitet und angenommen am 08.04.2009, 1271-04-02/08/DE (WP 155 Rev. 04).

[81] Näher zum Prüfverfahren: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm.

„Transfer notification“ oder gar Genehmigung der lokalen Datenschutzbehörden, die allerdings auf der Basis der vorliegenden BCR in der Regel erleichtert erteilt wird.[82] Unter der DSGV dürfte dies nicht mehr nötig sein, da Art 42 Abs. 1 DSGV ausdrücklich regelt, dass eine weitere Genehmigung nicht erforderlich ist.[83]

Da die Arbeitsdokumente lediglich einen Rahmen vorgeben, sind BCR flexibler als SDPC und können individuell an die Bedürfnisse und Struktur eines Konzerns angepasst werden. Dies bedeutet aber gleichzeitig, dass die Unternehmen in ihren BCR alle Vorgaben des Rahmens im Detail regeln und umsetzen, konzernintern abstimmen und durch Verträge zwischen Konzernmutter und allen Konzernunternehmen rechtsverbindlich machen müssen. Wie schon dargelegt, ist auch das Anerkennungsverfahren recht kompliziert und langwierig.[84]

Das Instrument der BCR wird in der DSGV nunmehr ausdrücklich und umfassend geregelt (vgl. Art. 42 Abs. 1, Abs. 2 lit. b), Art. 43 DSGV). Künftig sollen BCR nach Durchführung eines gestrafften Kohärenzverfahrens durch die zuständige nationale Aufsichtsbehörde genehmigt werden.[85] Eine Datenübermittlung auf Basis der BCR ist dann ohne weitere Genehmigung zulässig. Die DSGV enthält allerdings einen umfangreichen Katalog von Anforderungen, die die BCR integriert werden müssen, so dass die Umsetzung weiterhin recht aufwändig ist.

6.3 Ausnahmen für bestimmte Fälle von Datenübertragungen

Ferner kann eine internationale Datenübermittlung gemäß Art. 26 DSRL, Art. 44 DSGV gerechtfertigt und damit ohne weitere Genehmigung zulässig sein, wenn die Voraussetzungen eines der dort geregelten – eng auszulegenden – Ausnahmefälle vorliegen. In diesen Fällen kann vom Erfordernis des „angemessenen Schutzniveaus“ ausnahmsweise praktisch abgewichen werden.[86] Hintergrund ist, dass die Risiken für die betroffene Person insoweit relativ gering sind oder dass in diesen Fällen andere Interessen (wichtige öffentliche Interessen oder andere Interessen der betroffenen Person selbst) Vorrang vor dem Recht der betroffenen Person auf den Schutz der Privatsphäre genießen.[87]

Gemäß Art. 26 Abs. 1 lit. a) DSRL, künftig Art. 44 Abs. 1 lit. (a) DSGV, dürfen personenbezogene Daten in ein Drittland übermittelt werden, wenn und soweit die betroffene Person eingewilligt hat. Während die DSRL eine Einwilligung „ohne jeden Zweifel“ fordert, verlangt die DSGV künftig eine „ausdrückliche“ bzw. „eindeutige“ Einwilligung in die Datenübermittlung.[88] Gemäß Art. 2 lit (h) DSRL muss eine Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgen. Voraussetzung für eine wirksame Einwilligung ist daher auch, dass der Betroffene zuvor hinreichend über die Gefährdung seiner personenbezogenen Daten bei Übermittlung in einen Staat ohne angemessenes Datenschutzniveau aufgeklärt wurde. Art. 7 DSGV regelt die Bedingungen für eine wirksame Einwilligung künftig detaillierter.

Daneben ist die Übermittlung gemäß Art. 26 Abs.1 lit. b) und c) DSRL, künftig Art. 44 Abs. 1 lit. (b) und (c) DSGV in bestimmten Fällen zulässig, in denen der Datentransfer für die Anbahnung oder Erfüllung eines Vertrags zwischen der verantwortlichen Stelle und dem Betroffenen oder zwischen

---

[82] https://www.datenschutzbeauftragter-info.de/bcr-die-antwort-bei-internationaler-datenverarbeitung/. Vgl. auch https://www.thomashelbing.com/de/binding-corporate-rules-bcr-datenschutz-eu-drittstaaten-datenschutzgrundverordnung-bdsg.

[83] Vgl. den Wortlaut des Art. 42 Abs.1 „without requiring any specific authorization”.

[84] Näher zu BCR und ihrer Anwendung in der Praxis Helbing unter https://www.thomashelbing.com/de/datenschutz-konzern-internationale-datentransfer-teil-2-safe-harbour-bcr-binding-corporate-rules-eu-standardvertragsklauseln.

[85] Art. 43 Abs. 1 DSGV.

[86] Vgl. Art. 29-Datenschutzgruppe, Arbeitsunterlage: Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU vom 24. Juli 1998, GD XV D/5025/98 (WP 12), S. 3, 26, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_de.pdf.

[87] Vgl. Art. 29-Datenschutzgruppe, WP 12 (Fn. 87), S. 26ff.

[88] Vgl. Art. 4 lit. (8), Art. 44 Abs. 1 lit. (a) DSGV.

der verantwortlichen Stelle und einem Dritten im Interesse des Betroffenen erforderlich ist. Hiernach können beispielsweise Datentransfers zur Buchung eines Fluges oder Hotelzimmers in den USA oder zur Ausführung von Überweisungen gerechtfertigt sein.

Zulässig sind neben weiteren Ausnahmen auch Datenübermittlungen, die zur Wahrung wichtiger Interessen oder zur gerichtlichen Geltendmachung von Ansprüchen erforderlich sind, Art. 26 Abs. 1 lit. d) und e) DSRL, künftig Art. 44 Abs. 1 lit. (d), (e) und (f).

Die meisten dieser Ausnahmen betreffen jedoch eher Einzelfälle oder vermögen nur die Übermittlung spezifischer Informationen zu rechtfertigen. Die Masse der in der Praxis erforderlichen Datenübermittlungen (z.B. von Beschäftigtendaten oder Übermittlung von Daten zu Marketingzwecken) lässt sich hierunter jedoch nicht subsumieren.

7 Zur Anwendbarkeit der alternativen Übermittlungsinstrumente nach dem „Schrems-Urteil“ des EuGH

Seit dem Wegfall der „Safe Harbour“-Lösung wird betroffenen Unternehmen in der Praxis als Alternativlösung weithin der Abschluss von Verträgen auf der Basis von SDPC oder die Einführung von BCR empfohlen. Vor dem Hintergrund der gängigen Zugriffspraktiken der amerikanischen Geheimdienste und den Ausführungen des EuGH wird die Schutzwirkung dieser Instrumente jedoch insbesondere von einigen nationalen Datenschutzbehörden zu Recht in Frage gestellt (näher hierzu sogleich unter Ziffer 7.1).

Auch eine Einwilligung kann nach verbreiteter Ansicht nur in engen Fällen zulässige Basis für einen Transfer bleiben (näher hierzu unten Ziffer 7.2).

7.1 SDPC oder BCR als Rechtsgrundlage für Datentransfers

Die Ansichten über die Zulässigkeit der existierenden alternativen Übermittlungsinstrumente gehen weit auseinander. Einigkeit besteht lediglich dahingehend, dass Datenübermittlungen, die nach dem Urteil ausschließlich auf „Safe Harbour“ gestützt werden, rechtswidrig sind und künftig untersagt und sanktioniert werden sollen. [89]

Die strengste Ansicht vertritt das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein. Das ULD Schleswig-Holstein hält bei unveränderter Rechtslage – wohl angesichts des Risikos eines massiven staatlichen Zugriffs auf personenbezogene Daten – einen legalen Datentransfer in die USA derzeit so gut wie überhaupt nicht mehr für möglich. Mit Blick auf die hohen Anforderungen, die der EuGH in seinem Urteil aufgestellt habe, könne eine dauerhafte Lösung nur in einer wesentlichen Änderung des US-amerikanischen Rechts liegen, die in absehbarer Zeit nicht zu erwarten sei.[90] Demgegenüber gehen die meisten anderen deutschen und EU-Datenschutzbehörden[91] ebenso wie die Kommission, die deutsche Bundesregierung[92] und andere

[89] So etwa die Konferenz der deutschen Datenschutzbeauftragten, vgl. das Positionspapier der DSK vom 21.10.2015, https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/EuGH_erkl__rt_Safe_Harbour_f__r_ung__ltig_-_UPDATE/DSK_Positionspapier_151026.pdf.

[90] Positionspapier des ULD Schleswig-Holstein vom 14.10.2015 zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14, abrufbar unter https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf.

[91] So etwa der britische Deputy Commissioner and Director of Data Protection, David Smith, vgl. https://iconewsblog.wordpress.com/2015/10/27/the-us-safe-harbour-breached-but-perhaps-not-destroyed/.

[92] Antwort der Bundesregierung auf die Kleine Anfrage verschiedener Abgeordneten und der Fraktion DIE LINKE, BT-Drucksache 18/7134, Vorabfassung vom 21.12.2015, S. 4..

Stimmen in der Literatur[93] davon aus, dass eine Datenübermittlung jedenfalls vorläufig noch auf SDPC oder bestehende BCR gestützt werden kann.[94] Neue Genehmigungen für BCR oder individuelle Datenexportverträge sollen aber derzeit nicht erteilt werden. Damit haben Unternehmen, die bislang noch nicht über genehmigte BCR verfügen, derzeit allerdings gar keine Möglichkeit, auf diese Alternative umzustellen. Nach Auffassung des cep können SDPC und BCR derzeit keine hinreichenden Garantien i.S.v. Art. 26 Abs. 2 DSRL bieten und stellen daher keine rechtssicheren Alternativen dar.

Nachfolgend wird zunächst der Meinungsstand zur weiteren Verwendbarkeit von SDPC und BCR im Einzelnen dargestellt (vgl. sogleich Ziffer 7.1.1). Im Anschluss hieran wird dann die Einschätzung des cep näher dargelegt (vgl. unten Ziffer 7.1.2).

7.1.1 Zum Meinungsstand im Einzelnen

Nach Auffassung des **ULD Schleswig-Holstein** ist die Übermittlung personenbezogener Daten in die USA auf der Basis von SDPC bei konsequenter Anwendung der Vorgaben des EuGH nicht mehr zulässig. Denn der US-Datenimporteur könne nicht garantieren, wissentlich keinen Gesetzen zu unterliegen, die ihm die Einhaltung der nach den SDPC obliegenden Pflichten unmöglich machten.[95] Hierzu sei er aber nach den Kommissionsentscheidungen zu den Standardverträgen verpflichtet. Der Datenexporteur müsse daher den Standardvertrag kündigen oder die Datenübermittlung aussetzen.[96]

Auch die **Artikel 29-Datenschutzgruppe** hat in ihrer Stellungnahme vom 16. Oktober 2015[97] angemerkt, dass die bestehenden Übermittlungsinstrumente im Fall der massenhaften und willkürlichen Überwachung „keine Lösung darstellen“. Daher werde die Gruppe weiter untersuchen, wie sich das EuGH-Urteil auf andere Übermittlungsinstrumente auswirke. Während der Zeit dieser Untersuchung könnten SDPC und BCR grundsätzlich weiter verwendet werden. Dennoch würden die Datenschutzbehörden weiterhin bestimmte Übermittlungen untersuchen und ggf. ihre Befugnisse zum Schutz von Einzelpersonen ausüben. Unternehmen sollten rechtliche oder technische Lösungen zur Einhaltung des EU-Datenschutzes erwägen. Daneben fordert die Gruppe die EU-Mitgliedstaaten und die EU-Institutionen nachdrücklich dazu auf, in Zusammenarbeit mit den US-amerikanischen Behörden Lösungen zu finden, etwa durch Abschluss eines zwischenstaatlichen Abkommens, das Betroffenen in der EU stärkere Garantien u.a. im Hinblick auf Kontrollen des staatlichen Zugriffs, Transparenz, Verhältnismäßigkeit und Rechtsmittel biete. Falls bis Ende Januar 2016 noch keine angemessene Lösung gefunden worden sei, seien die EU-Datenschutzbehörden verpflichtet, alle notwendigen und angemessenen Maßnahmen und notfalls auch koordinierte Durchsetzungsmaßnahmen zu ergreifen – je nachdem, wie die Gruppe bis dahin die Zulässigkeit der übrigen Übermittlungsinstrumente einschätze.

Die **Konferenz der deutschen Datenschutzbeauftragten** (DSK) stellt in ihrem Positionspapier vom 21.10.2015[98] ebenfalls die Zulässigkeit von Transfers auf Basis von SDPC und BCR in Frage, ohne dies jedoch näher zu begründen. Sie teilt lediglich mit, dass die deutschen Behörden derzeit keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von BCR oder individuellen Datenexportverträgen erteilen werden. Die Behörden würden vielmehr ihre Prüfbe-

---

93 Borges, NJW 2015, S. 3617 (3620).
94 Näher hierzu sogleich unter Ziffer 7.1.1.
95 Siehe hierzu auch unten Ziffer 7.1.2.3.
96 Positionspapier des ULD Schleswig-Holstein (Fn. 90), Ziffer 4.
97 Statement der Artikel-29-Datenschutzgruppe vom 16. Oktober 2015, vgl. Fn. 63.
98 Positionspapier der DSK vom 21.10.2015, abrufbar unter https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/EuGH_erkl__rt_Safe_Harbour_f__r_ung__ltig_-_UPDATE/DSK_Positionspapier_151026.pdf.

fugnisse nach Art. 4 der Kommissionsentscheidungen ausüben und dabei die Grundsätze des EuGH zugrunde legen. Dies spricht für eine eher kritische Sichtweise. Bereits in ihrer Pressemitteilung vom 24. Juli 2013[99] nach Bekanntwerden des routinemäßigen Zugriffs des US-amerikanischen Geheimdienstes hatte die DSK die Auffassung vertreten, dass ein angemessener Schutz auch durch die SDPC nicht (mehr) gewährleistet werden könne.

Ähnlich haben sich der **Hamburgische**[100] und der **Rheinland-Pfälzische Datenschutzbeauftragte**[101] geäußert. Letztgenannter hat angekündigt, ab dem 01.02.2016 überprüfen zu wollen, ob die US-Datenimporteure ihren Mitteilungspflichten bei Bekanntwerden entgegenstehender US-amerikanischen Rechtsvorschriften nachgekommen sind und der EU-Datenexporteur hierauf angemessen reagiert und insbesondere den Datenübermittlungsvertrag gekündigt habe.

Die **Kommission** hat am 06.11.2015 eine Mitteilung an das Europäische Parlament und den Rat betreffend die Übermittlung personenbezogener Daten von der EU in die USA nach dem „Schrems“-Urteil des EuGH veröffentlicht.[102] Darin führt sie aus, dass alternative Übermittlungsinstrumente weiter verwendet werden dürfen. Hierzu verweist sie[103] auf die Aussage der Art. 29-Datenschutzgruppe in ihrer vorstehend zitierten Stellungnahme vom 16.10.2015.[104] Die Gruppe hatte aber zunächst lediglich während der Prüfphase bis Ende Januar 2016 grünes Licht für die weitere Verwendung von SDPC und BCR gegeben. Die Kommission scheint jedoch davon auszugehen, dass SDPC und BCR unabhängig von dieser „Galgenfrist“ [105] grundsätzlich weiterhin taugliche Mittel sind. Denn sie hebt die bindende Wirkung der Kommissionsentscheidungen zu den SDPC hervor, die von den nationalen Behörden grundsätzlich akzeptiert werden müssten. Diese dürften einen Datentransfer in ein Drittland nicht allein mit der Begründung untersagen, dass die SDPC keine hinreichenden Garantien böten. Die Behörden dürften die Klauseln im Lichte der vom EuGH im „Schrems-Urteil“ aufgestellten Anforderungen untersuchen und bei Zweifeln einen Fall vor die nationalen Gerichte bringen, damit diese den Fall dann dem EuGH zur Vorabentscheidung vorlegen könnten.[106] Die Kommission knüpft die Nutzung alternativer Übermittlungsmethoden jedoch an zwei Bedingungen: Zum einen erinnert sie daran, dass die originäre Datenerhebung und Verarbeitung vor dem Transfer ebenso wie dieser im Einklang mit der DSRL und den nationalen Umsetzungsgesetzen erfolgen muss. Zweitens müsse der Datenexporteur gegebenenfalls zusätzliche Maßnahmen zum Schutz der übermittelten personenbezogenen Daten ergreifen, wenn er erfahre, dass sich der Datenimporteur aufgrund der Rechtslage in seinem Land zur Einhaltung seiner vertraglichen Verpflichtungen gehindert sieht. Denn die Verantwortung für das Vorhandensein ausreichender Garantien, bei deren Vorliegen personenbezogene Daten auch in ein Drittland ohne angemessenes Schutzniveau übertragen werden dürfen, liege bei der verantwortlichen Stelle und damit maßgeblich beim EU-Datenexporteur.[107] Die Spanne solcher Schutzmaßnahmen, die der Datenexporteur in Erwägung ziehen müsse, reiche von technischen, organisatorischen, geschäfts-

[99] Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juli 2013, vgl. Fn. 26.

[100] „Information zum Safe-Harbour-Urteil des Europäischen Gerichtshofs“ des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vom 05.11.2015, https://www.datenschutz-hamburg.de/uploads/media/Information_zum_Safe-Harbour-Urteil_des_Europaeischen_Gerichtshofs.pdf.

[101] “Folgerungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz aus dem Urteil des EuGH vom 6. Oktober 2015 (C-62/14) „Safe Harbour“, https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbour.pdf.

[102] EU-Kommission, Communication from the Commission to the European Parliament and the Council on the Transfer of Personal data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-62/14 (Schrems), COM(2015) 566 final.

[103] EU-Kommission, Communication (vgl. Fn. 102), S. 12, 15.

[104] Statement der Artikel-29-Datenschutzgruppe vom 16. Oktober 2015, vgl. Fn. 62.

[105] Kühling/Heberlein, NVwZ 2016, S. 7 (12).

[106] EU-Kommission, Communication (vgl. Fn. 102), S. 6.

[107] EU-Kommission, Communication (vgl. Fn. 102), S. 12f., 14, 15.

modellbezogenen oder rechtlichen Maßnahmen bis hin zu einer Aussetzung der Übermittlung oder Kündigung des Datenexportvertrags.[108]

Die Ausführungen der Kommission und der DSK lassen sich so deuten, dass SDPC jedenfalls in bestimmten Fällen noch verwendet werden können, jedoch Ergänzungen zur Absicherung des Garantieniveaus erforderlich sind.[109] Die insoweit geforderten Zusatzmaßnahmen der Datenexporteure sollen offenkundig die (nunmehr) unzureichenden Garantien, die das Übermittlungsinstrument als solches bietet, ergänzen und so wieder auf das erforderliche Maß aufstocken. Unternehmen sollen sich nach Ansicht der DSK[110] insoweit an zwei Dokumenten[111] orientieren, in denen verschiedene technische Mittel wie etwa die Verwendung sicherer Verschlüsselungsverfahren insbesondere beim Transport und bei der Speicherung von personenbezogenen Daten empfohlen werden. Hierdurch könnte eine nachträgliche Entschlüsselung (etwa durch US-amerikanische Geheimdienste) zumindest erschwert werden.[112] Ferner sollen sich Dienstleister hinsichtlich der Einhaltung der Datenschutz- und IT-Sicherheitsstandards einem Zertifizierungsverfahren bei einer unabhängigen Prüfstelle unterwerfen. US-Datenimporteure sollen vertraglich verpflichtet werden, ihren EU-Auftraggebern zu Prüfzwecken Zugriff auf Protokolldaten zu gewähren. Dies legt den Schluss nahe, dass aus Sicht der DSK eine Ergänzung der Datenexportverträge um eine entsprechende vertragliche Verpflichtung zur wirksamen Verschlüsselung und zur Einsichtnahme in Protokolldaten zu einer Rechtmäßigkeit der Datenübermittlung in die USA führen kann.[113]

Auch nach einer Ansicht in der **Literatur** sind Datentransfers in die USA nunmehr nicht pauschal unzulässig. Eine Speicherung von Daten, die den Zugriff durch US-amerikanische Stellen ermögliche, sei nicht schlechthin mit Art. 7, 8 GRC unvereinbar. Es komme auf die Intensität und Gefahr für die Persönlichkeitsrechte des Betroffenen und damit auf eine Abwägung im Einzelfall an.[114] Die bloße vertragliche Vereinbarung von Datenschutzanforderungen ohne Kontrolle durch einen unabhängigen Dritten genüge jedoch nicht. Dies gelte auch bei SDPC. Vielmehr müsse sich der Datenexporteur selbst von der Einhaltung überzeugen. Zertifizierungen oder sonstige Kontrollmechanismen sollen ausreichen, um eine hinreichende Überprüfung im Sinne des EuGH-Urteils zu gewährleisten.[115]

Dennoch wird überwiegend bezweifelt, dass die Kommissionsentscheidungen zu den SDPC bei Heranziehung des vom EuGH im „Schrems-Urteil“ aufgestellten Prüfmaßstabs Bestand haben können.[116] Die Begründung des EuGH sei in großen Teilen auf die Entscheidungen zu den SDPC übertragbar.[117] Die formalen Defizite seien identisch. Die Kommission habe auch in den Entscheidungen zu den SDPC keine Feststellungen getroffen, ob die zwingenden nationalen Gesetzesvorschriften im Drittland zum Schutz wichtiger Interessen, die nach den Entscheidungen pauschal Geltungsvorrang gegenüber den Grundsätzen in den Standardverträgen genössen, angemessen seien. Auch die Grundrechtsgefährdung sei die gleiche. Bei der gebotenen grundrechtskonformen Auslegung der Art. 26 Abs. 2 und 4 DSRL ergebe sich, dass SDPC nur über solche Datenschutzdefizite hinweghelfen könnten, die sich durch eine bilaterale, privatrechtliche Vereinbarung ausgleichen lassen.

---

[108] EU-Kommission, Communication (vgl. Fn. 102), S. 13.
[109] Vgl. auch Piltz, K&R 2016, S. 1 (6).
[110] Positionspapier der DSK vom 21.10.2015 (Fn. 98), S. 2.
[111] Entschließung zur „Gewährleistung Menschenrechte bei der elektronischen Kommunikation“ vom 27.03.2014, erlassen auf der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, und „Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Ländersowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Version 2.0 vom 09.10.2014.
[112] Piltz, K&R 2016, S. 1 (6).
[113] Ausführlicher zu dieser Thematik Piltz, K&R 2016, S. 1 (6).
[114] Borges, NJW 2015, S. 3617 (3620).
[115] Borges, NJW 2015, S. 3617 (3620).
[116] Moos/Schefzig, CR 2015, S. 625 (631f.).
[117] Piltz, K&R 2016, S. 1 (6).

Dies sei bei Defiziten aufgrund staatlicher Zugriffsbefugnisse aber gerade nicht der Fall. Sei ein grundrechtswidriger staatlicher Datenzugriff möglich, könne daher wohl auch der Abschluss eines Standardvertrags keinen Zustand herstellen, der den Anforderungen der DSRL und der GRC genüge.[118] Es handle sich daher nicht um eine garantiert nachhaltige Lösung. Auch BCR könnten den Zugriff staatlicher Sicherheitsbehörden nicht verhindern und daher wohl ebenfalls das aus diesen Gründen unzureichende Datenschutzniveau nicht kompensieren. Unklar sei, ob der EuGH die Kommissionsentscheidungen zu den SDPC für ungültig erklären könne. Denn diese könnten in bestimmten Situationen weiterhin einsetzbar sein. Ihre Verwendbarkeit sei eher eine Frage des Einzelfalls und liege in der Verantwortung des Datenexporteurs. [119] Andere wie wohl auch die deutsche Bundesregierung gehen davon aus, dass die Kommission ihre Entscheidungen in näherer Zukunft selbst überprüfen und ggf. anpassen wird.[120] Soweit ein grundrechtswidriger Zugriff drohe, müsse die Kommission den Einsatz der SDPC entsprechend einschränken.[121]

7.1.2 cep-Einschätzung

Ob die SDPC und BCR langfristig weiter verwendet werden können, hängt davon ab, ob die Mängel, die der EuGH dem „Safe Harbour“-Regime bescheinigt hat,[122] auch bei diesen Instrumenten bestehen. Die folgende Analyse wird auf Basis der Rechtslage zum Zeitpunkt des „Schrems-Urteils“ vorgenommen.[123]

7.1.2.1 Gleiche Mängel wie „Safe Harbour“?

Die Kommission hat im jeweiligen Art. 1 der Entscheidungen zu den SDPC festgestellt, die Standardvertragsklauseln gälten als ausreichende Garantien im Sinne von Art. 26 Abs. 2 DSRL. Fraglich ist insoweit bereits, ob die Kommission die Schutzwirkung dieser Garantien hinreichend geprüft und begründet hat.[124] Auch diesbezüglich hat die Kommission einen Wertungsspielraum, der wohl entsprechend dahingehend begrenzt sein dürfte, als die Kommission eine strikte Kontrolle der Anforderungen aus Art. 25, 26 DSRL im Lichte der GRC vorzunehmen hat.[125] Jedenfalls bei der gebotenen Überprüfung ihrer Entscheidungen müsste die Kommission zu dem Ergebnis kommen, dass diese Garantien derzeit nicht „ausreichend“ sind, um den Schutz der Privatsphäre, der Grundrechte und Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte zu gewährleisten. Dies ergibt sich aus folgenden Überlegungen:

Geht man davon aus, dass in den USA noch immer eine generelle Zugriffsregelung und -praxis existiert, die sich nicht auf dasjenige beschränkt, was (nach EU-Verständnis) zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig wäre, so verletzt eine Regelung, die einen solchen generellen Zugriff ermöglicht, nach Auffassung des EuGH den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens. Die Gefahr des routinemäßigen Zugriffs der US-Geheimdienste ist aber nicht auf personenbezogene Daten von EU- Bürgern beschränkt, die über „Safe Harbour“ in die USA gelangt sind. Betroffen sind vielmehr alle Daten, die

[118] Moos/Schefzig, CR 2015, S. 625 (632).
[119] Moos/Schefzig, CR 2015, S. 625 (632).
[120] Piltz, K&R 2016, S. 1 (6); Antwort der Bundesregierung auf die Kleine Anfrage verschiedener Abgeordneten und der Fraktion DIE LINKE, BT-Drucksache 18/7134, Vorabfassung vom 21.12.2015, S. 8.
[121] Borges, NJW 2015, S. 3617 (3620).
[122] Hierzu im Einzelnen oben unter Ziffer 5.3.2.
[123] Unten unter Ziffer 8.3.6 wird dann kurz darauf eingegangen, ob der geplante „EU-U.S. Privacy Shield“ und die in der Zwischenzeit erfolgten rechtlichen Reformen in den USA zu einem anderen Ergebnis führen könnte.
[124] In der „Schrems-Entscheidung“ hatte der EuGH der Kommission vorgeworfen, dass sie das Bestehen eines angemessenen Schutzniveaus in den USA nicht festgestellt habe. Erforderlich sei insoweit eine gebührend begründete Feststellung (vgl. EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Rn. 96, 97). Im Rahmen des Art. 26 Abs. 2 muss die Kommission zwar nicht die Angemessenheit des Schutzniveaus prüfen, aber das Vorliegen ausreichender Garantien.
[125] So der EuGH zum Wertungsspielraum der Kommission bei der Prüfung der Angemessenheit nach Art. 25 Abs. 2, 6 DSRL.

auf US-amerikanischen Servern gespeichert sind, unabhängig davon, auf welcher Rechtsgrundlage diese aus der EU dorthin gelangt sind. Damit besteht die Gefahr von Eingriffen in den Wesensgehalt des Grundrechts auf Achtung des Privatlebens auch für personenbezogene Daten, die auf Basis von SDPC oder BCR in die USA übermittelt wurden. Durch den Abschluss von SDPC oder BCR können solche Zugriffe nicht verhindert werden. Die Grundrechtsgefährdungslage ist also insoweit die gleiche wie bei der Übertragung nach „Safe Harbour“.[126]

Ungeachtet dessen dürfte es auch bei den Entscheidungen zu den SDPC ebenso wie bei den BCR an wirksamen Überwachungs- und Kontrollmechanismen fehlen, die es erlauben, etwaige Verstöße zu ermitteln und zu ahnden. Darüber hinaus sehen auch die Entscheidungen zu den SDPC keinen wirksamen gerichtlichen Rechtsschutz gegen staatliche Eingriffe vor. Zwar enthält deren Klausel 3 jeweils eine Drittbegünstigtenklausel, mit denen der Betroffene bestimmte Regelungen, die im Verhältnis Datenexporteur-Datenimporteur gelten, selbst gegenüber einer der beiden Vertragsparteien geltend machen kann. Soweit in Klausel 3 gelistet, entfalten die in diesen Klauseln festgeschriebenen Datenschutzgrundsätze damit eine Schutzwirkung zugunsten des Betroffenen. Dieser kann dann gegen die Verletzung einer drittschützenden Klausel vorgehen und ggf. Schadensersatzansprüche geltend machen. Hierzu kann er gemäß Klausel 7 auch ein Schlichtungsverfahren anstrengen oder die Gerichte des Mitgliedstaats anrufen, in dem der Datenexporteur niedergelassen ist. Vorrangig muss er jedoch gegen den Datenexporteur vorgehen; gegen den Datenimporteur kann er gemäß Klausel 3 Abs. 2 nur vorgehen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht.[127] Ein Rechtsmittel gegen Grundrechtseingriffe durch staatliche Maßnahmen oder wirksame administrative oder gerichtliche Rechtsbehelfe, die es dem Betroffenen erlauben, Zugang zu den sie betreffenden personenbezogenen Daten zu erhalten oder ihre Berichtigung oder Löschung zu erwirken, sehen weder die Kommissionsentscheidungen zu den SDPC noch der BCR-Rahmen vor. Daher liegt der Schluss nahe, dass auch die Entscheidungen zu den SDPC und die BCR gleichermaßen wie die „Safe Harbour“-Grundsätze den Wesensgehalt des in Art. 47 GRC verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz verletzen.

Fraglich ist, ob die Kommissionsentscheidungen zu den SDPC darüber hinaus ebenso wie Art. 3 der „Safe Harbour“-Entscheidung die Befugnisse der unabhängigen nationalen Datenschutzbehörden in unzulässiger Weise beschneiden.

Art. 4 Abs. 1 der Entscheidungen zu den SDPC[128] ermächtigt die mitgliedstaatlichen Kontrollstellen, zum Zwecke des Schutzes von Privatpersonen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung in Drittländer unter bestimmten Voraussetzungen zu verbieten oder auszusetzen. Dies soll beispielsweise dann möglich sein, wenn feststeht, dass der Datenimporteur (oder Unterauftragsdatenverarbeiter) nach seinem innerstaatlichen Recht gezwungen ist, vom vereinbarten Datenschutz in einem Maß abzuweichen, das über die in Art. 13 DSRL geregelten erforderlichen Beschränkungen des Datenschutzes hinausgeht. Zusätzlich müssen sich diese zwingenden nationalen Anforderungen wahrscheinlich sehr nachteilig auf die Garantien auswirken, die die SDPC bieten sollen.[129] Gleiches gilt, wenn eine zuständige Kontrollstelle die Nichteinhaltung der Klauseln durch den Datenimporteur festgestellt hat oder eine hohe Wahrschein-

[126] Ebenso Moos/Schefzig, CR 2015, S. 625 (632) (siehe schon oben unter Ziffer 7.1.1).
[127] Selbst dann kann der Betroffene beispielsweise wegen des fehlenden Verweises auf Klausel 5 lit. f) bzw. d) in Klausel 3 Abs. 2 gegenüber dem Datenimporteur keine Prüfung von dessen Datenverarbeitungseinrichtungen zur Kontrolle der unter die Klauseln fallenden Verarbeitungstätigkeiten durchsetzen.
[128] Entscheidung 2001/497/EG (Standardvertrag I und II) und Beschluss 2010/87/EU (Auftragsdatenverarbeiter), vgl. Fn. 67.
[129] Vgl. Art. 4 Abs. 1 lit. a). der Entscheidung 2001/497/EG.

lichkeit für deren Nichteinhaltung besteht und hierdurch ein nicht wieder gutzumachender Schaden entstünde.[130]

Es liegt nicht ganz fern, dass auch diese Voraussetzungen die Schwelle für Eingriffsmaßnahmen jedenfalls in gewisser Weise erhöhen und damit den nationalen Kontrollstellen Befugnisse entziehen, die ihnen nach Art. 28 DSRL im Lichte der GRC zustehen. Insoweit hätte die Kommission ebenso wie in der „Safe Harbour“-Entscheidung ihre Kompetenzen überschritten, so dass der jeweilige Art. 4 der Entscheidungen zu den SDPC ungültig wäre.

7.1.2.2 Zwischenfazit

Damit kann festgestellt werden, dass die Übermittlungsinstrumente der SDPC und BCR weithin an denselben Unzulänglichkeiten kranken, wie sie der EuGH bezüglich des „Safe Harbour“-Systems festgestellt hat. Auch insoweit fehlt es an einer wirksamen Kontrolle der Einhaltung der SDPC und BCR durch eine unabhängige Stelle. Zudem unterliegen durch SDPC und BCR übermittelte personenbezogene Daten von EU-Bürgern gleichermaßen dem (unverhältnismäßigen) Zugriff durch US-amerikanische Behörden. Auch hinreichende Rechtsschutzmöglichkeiten für EU-Bürger werden weder durch die Kommissionsentscheidungen noch durch die BCR geschaffen. Insoweit handelt es sich um rechtsstaatliche Defizite der USA, die nicht durch vertragliche Regelungen kompensiert werden können.[131] Aus diesen Gründen kann der bereits erfolgte oder künftige Einsatz von SDPC und BCR aus Sicht des cep derzeit keine ausreichenden Garantien i.S.v. Art. 26 Abs. 2 DSRL, Art. 42 Abs. 1 DSGV bieten, welche die fehlende Angemessenheit des Datenschutzniveaus in den USA kompensieren und einen legalen Transfer personenbezogener Daten in die USA rechtfertigen könnten.

7.1.2.3 Konsequenzen für künftige Datenübermittlungen auf Basis von SDPC und BCR

Unklar ist, welche Handlungsmöglichkeiten die nationalen Aufsichtsbehörden angesichts der obigen Erkenntnisse bezüglich solcher Übermittlungen haben, die auf SDPC oder BCR gestützt sind. Da dem EuGH bezüglich der Kommissionsentscheidungen zu den SDPC das Verwerfungsmonopol zusteht und diese daher bis auf Weiteres wirksam und damit bindend bleiben, dürften die nationalen Datenschutzbehörden keine diesen Entscheidungen „zuwiderlaufenden Maßnahmen“ treffen.[132] Aber was wäre eine zuwiderlaufende Maßnahme?

Der EuGH führt insoweit aus, dass die nationalen Kontrollstellen nicht befugt sind, selbst die Ungültigkeit einer solchen Entscheidung festzustellen.[133] Dies präzisiert er dahingehend, dass die nationalen Behörden keinen Rechtsakt erlassen dürfen, mit dem verbindlich festgestellt wird, dass das Drittland kein angemessenes Schutzniveau gewährleistet.[134] Übertragen auf die Entscheidungen zu den SDPC dürften die nationalen Datenschutzbehörden keine verbindliche Feststellung treffen, dass die SDPC keine „angemessenen Garantien“ i.S.d. Art. 26 DSRL bieten. Dies bedeutet aber wohl lediglich, dass die Behörden nicht allgemeingültig feststellen dürfen, dass die Kommissionsentscheidungen zu den SDPC generell keinen angemessenen Schutz bieten. Oder verbietet die Bindungswirkung der Kommissionsentscheidungen der Behörde auch im Einzelfall, eine bestimmte Datenübermittlung auf der Basis von SDPC mit der Begründung zu untersagen oder auszusetzen,

---

[130] Vgl. Art. 4 Abs. 1 lit. b), c), der Entscheidung 2001/497/EG.
[131] Zu diesem Ergebnis tendieren nach Aussage des Hamburgischen Landesdatenschützers Johannes Caspar nunmehr offenbar auch die deutschen Datenschutzbehörden, vgl. http://www.heise.de/newsticker/meldung/EU-US-Datenschutz-Nachfolgeabkommen-fuer-Safe-Harbour-auf-der-Kippe-3089437.html.
[132] So der EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 52 bezüglich der „Safe Harbour“-Entscheidung.
[133] So der EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 62 bezüglich der „Safe Harbour“-Entscheidung.
[134] So der EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 52 bezüglich der „Safe Harbour“-Entscheidung.

dass diese *jedenfalls bezogen auf den konkreten Transfer* keine adäquate Garantie i.S.v. Art. 26 Abs. 2 DSRL bieten können?

Hierzu ist zu beachten, dass der EuGH das Prüfungsrecht der nationalen Kontrollstellen im „Schrems-Urteil“ betont und gestärkt hat. Auch bei Existenz einer grundsätzlich bindenden Angemessenheitsentscheidung der Kommission dürfen und müssen diese in völliger Unabhängigkeit prüfen, ob bei der Übermittlung der betreffenden Daten die Anforderungen der DSRL gewahrt werden. Sind aber Angemessenheitsentscheidungen einer solchen Kontrolle nicht entzogen, muss dies gleichermaßen für die Entscheidungen zu den SDPC gelten. Dies würde bedeuten, dass die nationalen Datenschutzbehörden bei der Beurteilung von Datenübermittlungen im Einzelfall prüfen dürfen, ob die SDPC im konkreten Fall angemessene Garantien i.S.d. Art. 26 Abs. 2 DSRL bieten. Was aber kann und soll eine Behörde tun, die bei der Prüfung eines bestimmten Datentransfers in die USA zu dem Ergebnis kommt, dass dies nicht der Fall ist? Darf sie dann lediglich ihr (angesichts der Forderung des EuGH im Schrems-Urteil[135] von den EU-Mitgliedstaaten noch zu schaffendes) Klagerecht ausüben, um die fragliche Entscheidung im Vorabentscheidungswege vor den EuGH zu bringen? Der Betroffene wäre dann bis zu einer solchen Entscheidung des EuGH über die Gültigkeit der Kommissionsentscheidungen zu den SDPC schutzlos, wenn die Behörde den Datentransfer nicht wenigstens bis dahin aussetzen dürfte. Im Ergebnis wären die nach Ansicht des EuGH so wichtigen Kontrollstellen jedenfalls vorübergehend eher „zahnlose Tiger“. Daher spricht viel dafür, dass die nationalen Datenschutzbehörden grundsätzlich alle Befugnisse im Rahmen von Art. 28 DSRL ausüben und insbesondere auch Datentransfers im Einzelfall untersagen dürfen. Dagegen spricht allerdings, dass eine einheitliche Anwendung des Unionsrechts und Rechtssicherheit, die das Verwerfungsmonopol des EuGH sicherstellen soll, jedenfalls vorübergehend nicht gewährleistet wäre, wenn die nationalen Kontrollstellen hier zu unterschiedlichen Bewertungen kommen.

Möglich ist aber in jedem Fall eine Untersagung des Datentransfers, die die Entscheidungen zu den SDPC selbst erlauben und die damit keine „zuwiderlaufende Maßnahme“ wäre.

Wie oben ausgeführt, dürfen die nationalen Kontrollstellen nach Art. 4 Abs. 1 lit. a) der Entscheidungen zu den SDPC die Datenübermittlung in Drittländer u.a. dann verbieten oder aussetzen, wenn feststeht, dass der Datenimporteur nach seinem innerstaatlichen Recht gezwungen ist, vom vereinbarten Datenschutz in einem Maß abzuweichen, das über die in Art. 13 DSRL geregelten für eine demokratische Gesellschaft erforderlichen Beschränkungen des Datenschutzes hinausgeht, und dass sich diese zwingenden nationalen Anforderungen wahrscheinlich sehr nachteilig auf die Garantien auswirken, die die SDPC bieten sollen.[136] Fraglich ist in diesem Zusammenhang bereits, ob die Kommission vor Erlass der Entscheidung hinreichend geprüft hat, in welchem Umfang in den USA zwingende nationale Vorschriften existieren, die über dieses Maß hinausgehen.

Geht man davon aus, dass es feststeht, dass US-Datenimporteure rechtlich verpflichtet sind, US-amerikanischen Geheimdiensten in zu weitem Umfang Zugriff auf personenbezogene Daten von EU-Bürgern zu gewähren, so dürften diese Voraussetzungen erfüllt sein.

Zwar regelt die Entscheidung 2001/497/EG in Anlage 2 zum Standardvertrag I ausdrücklich, dass zwingende nationale Vorschriften, an die der Datenimporteur nach nationalem Recht gebunden ist, Vorrang vor den SDPC haben und die durch diese bezweckte Schutzgarantie somit einschränken können. Dieser Geltungsvorrang gilt jedoch nur für solche zwingende Anforderungen, die nicht weitergehen, als es in einer demokratischen Gesellschaft unter Zugrundelegung der in Art. 13 Abs. 1 DSRL aufgeführten Interessen erforderlich ist. Damit ließen sich staatliche Zugriffe der US-amerikanischen Behörden „rechtfertigen“, die notwendig zum Schutz eines der dort genannten

[135] So der EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 65.
[136] Vgl. Art. 4 Abs. 1 lit. a).

Interessen sind, beispielsweise für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit oder die Strafverfolgung. Der US-Datenimporteur würde seine Vertragspflichten unter den Klauseln dann insoweit nicht verletzen. Eine pauschale und uneingeschränkte Zugriffsmöglichkeit der US-amerikanischen Behörden ist jedoch nicht „notwendig“ und geht damit über die Grenzen dieser Einschränkungsmöglichkeiten hinaus. Durch die Herausgabe der Daten auf eine solche Anfrage hin würde der Datenimporteur dann seine vertraglichen Pflichten verletzen. Auch von einer sehr nachteiligen Wirkung ist bei zu weiter Zugriffsbefugnis der US-amerikanischen Geheimdienste auszugehen, da diese die mit den SDPC anvisierten Garantien vollkommen untergraben. Damit wären die nationalen Kontrollbehörden bei unverhältnismäßigen Zugriffsrechten der US-Behörden bereits aufgrund der SDPC befugt, die Datenübermittlung auf deren Basis zu verbieten oder auszusetzen.

Ferner wäre nach den SDPC unter Umständen schon der Datenexporteur selbst verpflichtet, die Übermittlung auszusetzen oder vom Standardvertrag zurückzutreten. Bei Abschluss der Datenexportverträge unterwerfen sich Datenexporteur und insbesondere der Datenimporteur den in den SDPC näher geregelten Datenschutzverpflichtungen und geben bestimmte Zusicherungen und Garantien. So garantiert der US-Datenimporteur unter anderem, dass er seines Wissens keinen nationalen Gesetzen unterliegt, die ihm die Erfüllung seiner Vertragspflichten unmöglich machen.[137] Zugleich verpflichtet er sich, bei Gesetzesänderungen, die sich voraussichtlich sehr nachteilig auf die mit den Klauseln verbundenen Garantien auswirken, den Datenexporteur zu informieren.[138] Der Datenexporteur ist in diesem Fall gemäß Klausel 5 lit. a) Standardvertrag I und Klausel 5 lit. b) des Standardvertrags „Auftragsdatenverarbeiter“ berechtigt, die Datenübermittlung auszusetzen oder vom Standardvertrag zurückzutreten. Dies erscheint jedenfalls möglich, soweit die Zugriffspraktiken seit Geltung der SDPC durch Gesetzesverschärfungen ausgeweitet wurden, diese Ausweitung sich sehr nachteilig auf die mit den Klauseln bezweckte Garantien auswirkt und der Datenimporteur den Datenexporteur hierüber nicht informiert hat.[139]

Nationale Behörden können Transfers auf der Basis von Standardvertrag I auch untersagen, sobald eine zuständige Kontrollstelle festgestellt hat, dass der Datenimporteur die Vertragsklauseln nicht einhält.[140] Solange die Zugriffsbefugnis der US-Amerikaner sich nicht im Rahmen des Art. 13 DSRL hält, hat sie keinen Geltungsvorrang vor den Vertragsklauseln, die daher auch von EU-Datenexporteur und US-Datenimporteur vollumfänglich einzuhalten sind. Es ist wohl zutreffend, dass US-Datenimporteure die oben angegebene vertragliche Zusicherung bei der derzeitigen Rechtslage und weiterhin drohendem generellen Zugriff durch die NSA nicht mehr guten Gewissens geben kann. Daher dürfte eine Verletzung der Klauseln vorliegen, wenn der Datenimporteur staatlichen Behörden Zugriff auf die Daten gewährt, ohne dass dies durch übergeordnete Interessen, die sich im Rahmen des Art. 13 DSRL halten, gerechtfertigt ist.[141] Sollten die Kommissionsentscheidungen zu den SDPC so auszulegen sein, dass sie eine weitergehende Offenlegung von Daten erlauben, als es die DSRL erlaubt, ist zweifelhaft, ob die SDPC eine „hinreichende Garantie“ i.S.v. Art. 26 Abs. 2 DSRL bieten können.

---

[137] Passend hierzu sichert gemäß Ziffer I b) Standardvertrag II auch der Datenexporteur zu, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur seine Rechtspflichten aus den Klauseln erfüllen kann.

[138] Vgl. die Verpflichtungen des Datenimporteurs in Klausel 5 lit. a) Standardvertrag I, abgedruckt im Anhang der Entscheidung 2001/497/EG; Ziffer II lit. c) Standardvertrag II, abgedruckt im Anhang der Entscheidung 2004/915/EG sowie Klausel 5 lit. b) Standardvertrag „Auftragsverarbeiter“, abgedruckt im Anhang des Beschlusses 2010/87/EU.

[139] Ansonsten müsste man argumentieren, dass dieses Aussetzungsrecht auch bei einer sonstigen verbindlichen Änderung der Zugriffsrechte bestehen muss.

[140] Vgl. Art. 4 Abs. 1 lit. b) der Entscheidung 2001/497/EG (vgl. Fn. 67).

[141] A.A. wohl Borges, NJW 2015, S. 3617 (3620). Danach sei dem US-Datenempfänger die Erfüllung seiner Verpflichtungen möglich. Aus der Unterrichtungspflicht ergebe sich, dass die Herausgabe von Daten bei staatlichen Zugriffsbefugnissen stelle grundsätzlich keinen Pflichtverstoß darstelle.

Ähnliche Fragen stellen sich bei den BCR. So sollen zwingende Erfordernisse nationaler Gesetzgebung, auf deren Grundlage die Mitglieder der jeweiligen Unternehmensgruppe ggf. verpflichtet sind, ihre Verpflichtungen im Rahmen der BCR außer Acht zu lassen, den BCR allenfalls dann nicht widersprechen, wenn sie sich im Rahmen dessen halten, was in einer demokratischen Gesellschaft auf der Basis eines der in Art. 13 Abs. 1 DSRL genannten Interessen notwendig ist.[142] Dies ist jedoch bei anlasslosen und unbegrenzten Zugriffsbefugnissen der US-amerikanischen Geheimdienste zu Zwecken der öffentlichen Sicherheit nicht der Fall, da diese Zugriffe weit über dieses Maß hinausgehen. Auch eine Transparenz ist insoweit nicht vollständig gewährleistet. Denn ein Unternehmen ist bei Zweifeln an der Erfüllbarkeit seiner Verpflichtungen aus den BCR lediglich dann gehalten, die Hauptniederlassung der Unternehmensgruppe in der EU oder das EU-Unternehmen, welches die Haftung für den Datenschutz übernommen hat, über diesen Konflikt zu informieren, wenn dies von der zugreifenden Vollzugsbehörde nicht verboten wurde. Dies ist etwa aus Gründen der Vertraulichkeit der Maßnahme möglich. Relevant wird dies etwa in Fällen, in denen ein Unternehmen nach US-Recht verpflichtet ist, personenbezogene Daten von EU-Bürgern offenzulegen, die BCR eine solche Offenlegung aber gerade nicht vorsehen. Heimliche Zugriffe sind damit gerade nicht ausgeschlossen. [143]

Zusätzlich zu möglichen Durchgriffen von Seiten der Datenschutzbehörden müssen Unternehmen, die personenbezogene Daten ohne hinreichende rechtliche Grundlage in die USA übermitteln und hierdurch Datenschutzverstöße begehen, als weitere Konsequenz Abmahnungen und einstweilige Verfügungen von Wettbewerbern fürchten. Schließlich ist zu erwarten, dass der EuGH früher oder später mit den Kommissionsentscheidungen zu den SDPC befasst wird. Es ist nicht auszuschließen, dass der Gerichtshof dabei ähnliche Erwägungen wie bei „Safe Harbour“ anstellen wird.

7.2 Einwilligung als Rechtsgrundlage für Datentransfers

Wie oben dargelegt,[144] kann eine Einwilligung unter den Voraussetzungen des Art. 26 Abs. 1 lit. a) DSRL, Art. 44 Abs. 1 lit. a) DSGV eine transatlantische Übermittlung personenbezogener Daten rechtfertigen.

7.2.1 Meinungsstand

Nach Ansicht des **ULD Schleswig-Holstein**[145] ist eine Einwilligung jedoch keine taugliche Rechtsgrundlage für eine Übermittlung personenbezogener Daten in die USA. Diese müsse für eine konkrete Datenverarbeitung gegeben werden; Generaleinwilligungen für eine Vielzahl nicht übersehbarer Datenverarbeitungen seien regelmäßig unzulässig. Insbesondere Einwilligungen gegenüber Arbeitgebern seien aufgrund des Über-Unterordnungsverhältnisses mangels freier Entscheidung häufig unwirksam. Selbst bei hinreichender Information über die Risiken und unterstellter Freiwilligkeit geht das ULD Schleswig-Holstein davon aus, dass die Einwilligung in die Datenübermittlung in einen Staat, in dem der Wesensgehalt des Grundrechts auf Achtung der Privatsphäre nicht gewahrt werde, der Disposition des Einzelnen entzogen sei. Eine Einwilligung kommt nach Ansicht

[142] Working Dokument der Art. 29 Data Protection Working Party on Binding Corporate Rules for International Data Transfers (11639/02/EN WP 74) vom 03.06.2003, 3.3.3.

[143] Art. 4 Abs. 2 der Entscheidung 2001/497/EG (vgl. Fn. 67) enthält bei Verwendung des Standardvertrags II weitere Aussetzungsbefugnisse u.a. für den Fall, dass der Datenimporteur sich weigert, eindeutige Vertragspflichten zu erfüllen. So könnte der Importeur sich etwa weigern, Daten nur vertragsgemäß weiterzugeben. Eine Weigerung liegt aber nicht vor, wenn die Erfüllung zu einer Kollision mit für den US-Datenimporteur verbindlichen Rechtsvorschriften führen würde und diese Vorschriften nicht über das hinausgehen, was in einer demokratischen Gesellschaft unter Zugrundelegung der in Art. 13 Abs. 1 DSRL aufgeführten Interessen erforderlich ist. Bei uneingeschränkter Zugriffsmöglichkeit der US-amerikanischen Behörden ist diese Grenze überschritten und die Befugnis der Behörden bei Weigerung eröffnet.

[144] Vgl. oben Ziffer 6.3.

[145] Positionspapier des ULD Schleswig-Holstein (Fn. 90), Ziffer 3.

der **Kommission** sowie der **Art. 29-Datenschutzgruppe** nur in Fällen in Betracht, in denen der Datenexporteur direkten Kontakt mit dem Betroffenen hat, die erforderliche Information einfach bereitgestellt und eine unzweifelhafte Einwilligung eingeholt werden kann.[146] Jedweder Zwang, wie er regelmäßig in durch Über-Unterordnung und Abhängigkeit geprägten Arbeitsverhältnissen drohe, könne die Einwilligung unwirksam machen; gleiches gelte, wo der Betroffene keine Gelegenheit hatte, eine echte Wahlentscheidung zu treffen oder vor vollendete Tatsachen gestellt werde. [147] Vor dem Transfer müsse der Betroffene darüber informiert werden, dass sowie zu welchen Zwecken und unter welchen Konditionen seine Daten in ein Drittland übermittelt werden, in welchem kein angemessenes Datenschutzniveau besteht. Zudem könne eine Einwilligung jederzeit widerrufen werden; in diesem Fall werde jede weitere Verarbeitung unzulässig. Aufgrund dieser beschränkten Einsatzmöglichkeiten könne die Einwilligung aus Sicht der Art. 29-Datenschutzgruppe wahrscheinlich langfristig keinen angemessenen Rechtsrahmen für strukturelle (gemeint sind wohl wiederholte oder gar routinemäßige) Datentransfers bieten.[148]

Andere ziehen eine Einwilligung auch nach dem „Schrems-Urteil“ grundsätzlich noch als Rechtsgrundlage in Betracht. Ausreichend sei, wenn allgemein, jedoch klar und deutlich, auf die Risiken eines Zugriffs durch staatliche Behörden hingewiesen werde.[149] Weithin wird die Einwilligung jedoch in der Praxis weder als praktikable noch – insbesondere wegen der jederzeitigen Widerruflichkeit – als verlässliche Alternative gesehen.[150] Bei Beschäftigtendaten sei diese regelmäßig nicht und bei Kundendaten nur unter engen Bedingungen zulässig.[151] Eine Übermittlung könne nicht auf eine pauschale Einwilligung für eine Vielzahl von Fällen gestützt werden.[152]

7.2.2 cep-Einschätzung

Eine Einwilligung kann aus Sicht des cep grundsätzlich weiterhin Rechtsgrundlage für eine Übermittlung personenbezogener Daten in die USA sein, wenn derselbe Transfer auch innerhalb der EU zulässig wäre. Voraussetzung ist in jedem Fall u.a. eine deutliche und vorherige Information, dass die Daten in die USA übermittelt werden und dort ggf. staatlichen Zugriffen ausgesetzt sind. Eine Einwilligung kommt in der Praxis jedoch nicht für alle Fälle in Betracht und ist insbesondere bei der Übertragung von Beschäftigtendaten oder dort kritisch zu sehen, wo Nutzer pauschal in eine Vielzahl nicht übersehbarer Datenverarbeitungen einwilligen sollen. Grundsätzlich ist davon auszugehen, dass der hinreichend informierte Nutzer seine Dispositionsbefugnis auch dann behalten kann, wenn ein Eingriff in den Wesensgehalt der Art. 7, 8 GRC droht. Denn insoweit sind auch die berechtigten Interessen der Wirtschaft und derjenigen Nutzer zu beachten, für die der Schutz ihrer Daten keinen hohen Stellenwert hat und die sich bewusst dafür entscheiden, einfach zugängliche, „kostenlose“ Dienste im Internet zu nutzen und mit der Preisgabe ihrer Daten zu „bezahlen“.[153] Fraglich ist aber beispielsweise, ob ein Nutzer seine Einwilligung ohne Zwang geben kann, wenn er keine Auswahlmöglichkeiten hat, diese Einwilligung auf bestimmte personenbezogene Daten oder bestimmte Zwecke zu beschränken und auf diese Weise nur begrenzte Transfers seiner Daten in die USA zu erlauben. Denn wenn er ein bestimmtes Angebot unbedingt nutzen will, ist er faktisch gezwungen, der Datennutzung insgesamt zuzustimmen. Im Einzelnen kommt es daher stets auf die

[146] EU-Kommission, Communication (vgl. Fn. 102), S. 11; Art. 29-Datenschutzgruppe, WP 12, (Fn. 87), S. 24.
[147] EU-Kommission, Communication (vgl. Fn. 102), S. 12; Art. 29-Datenschutzgruppe, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, S. 12f., abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_de.pdf. Richtlinie 95/46/EG vom 24. Oktober 1995, 2093-01/05/DE (WP 114), S. 13.
[148] EU-Kommission, Communication (vgl. Fn. 102), S. 12; Art. 29-Datenschutzgruppe, WP 114 (Fn. 147), S. 13.
[149] Piltz, K&R 2016, S. 1 (6); Borges, NJW 2015, S. 3617 (3619f.).
[150] Ebenso Moos/Schefzig, CR 2015, S. 625 (632).
[151] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (Fn. 101), Ziffer II. 5.
[152] Vgl. etwa Kühling/Heberlein, NVwZ 2016, S. 7 (10).
[153] Kühling/Heberlein, NVwZ 2016, S. 7 (12).

Grundrechtssituation im konkreten Fall an[154] und daher – wie so oft – auf eine Abwägung der widerstreitenden Interessen. Zu beachten ist ferner, dass die Einwilligung vom Nutzer jederzeit für die Zukunft widerrufen werden kann. Datentransfers in die USA standardmäßig allein auf eine erteilte Einwilligung zu stützen, stellt daher in der Praxis keine rechtssichere Lösung dar.

7.3 Fazit und weitere Entwicklung

Aus dem oben Gesagten folgt, dass nach dem Wegfall von „Safe Harbour“ außer in den dargestellten, eng auszulegenden Ausnahmefällen des Art. 26 DSRL (Art. 44 DSGV) derzeit kein legaler Transfer personenbezogener Daten in die USA mehr möglich ist.[155] Zu diesen Ausnahmen gehört eine wirksame Einwilligung, deren rechtfertigender Charakter angesichts der tiefgehenden Grundrechtseingriffe allerdings ebenfalls bezweifelt wird.

Ende Januar 2016 ist die von der Art. 29-Datenschutzgruppe gesetzte „Schonfrist“ für Unternehmen abgelaufen. Die Art. 29-Datenschutzgruppe hat sich dennoch bislang nicht weiter zur Zulässigkeit der alternativen Übermittlungsinstrumente geäußert und noch keine der angekündigten „Maßnahmen“ unternommen. Denn zwei Tage nach Ablauf des Ultimatums, just am Tage der Zusammenkunft der Gruppe in Brüssel, hat die Kommission in einer Pressemitteilung mitgeteilt, sie habe sich mit den USA auf einen neuen Rahmen für die transatlantische Datenübermittlung geeinigt: den sogenannten EU-US Datenschutzschild („EU-U.S. Privacy Shield“, nachfolgend: „Privacy Shield“).[156] Die Art. 29-Datenschutzgruppe hat diese Entwicklung in ihrer Stellungnahme vom 03.02.2016 begrüßt.[157] Sie zog es aber vor, ihre Erkenntnisse betreffend der weiteren Verwendbarkeit der alternativen Übermittlungsinstrumente vorläufig noch für sich zu behalten. Dies legt den Schluss nahe, dass die weitere Nutzung dieser Rechtsgrundlagen in der aktuellen Situation auch von der Art. 29-Datenschutzgruppe als problematisch erachtet wird. Man habe die momentane rechtliche Situation in den USA, die Praktiken der US-Geheimdienste und die Bedingungen, unter denen ungerechtfertigte Eingriffe in die EU-Grundrechte auf Privatsphäre und Datenschutz möglich seien, analysiert und zahlreiche Gespräche mit verschiedenen Personen in der EU und den USA geführt. Obwohl die Gruppe die Anstrengungen der USA in den vergangenen Jahren zur Verbesserung des Datenschutzes von Nicht-US-Amerikanern anerkenne, habe man Bedenken, ob die USA auf der Basis des derzeitigen rechtlichen Niveaus die vier notwendigen Garantien gewährleisten könne, welche bei Geheimdienstaktivitäten unabdingbar seien. Garantiert werden müssten: (1) Transparenz, (2) Notwendigkeit und Verhältnismäßigkeit bzw. die Schaffung einer Balance zwischen dem mit der Datenerhebung und dem Zugriff verfolgten Zweck und den Rechten des Betroffenen, (3) die Existenz eines unabhängigen und wirksamen Überwachungs- und Kontrollmechanismus und (4) wirksame Rechtsmittel. Die Kommission solle alle relevanten Dokumente bis Ende Februar übermitteln. Die Gruppe werde die Regelungen des „Privacy Shields“ dann im Lichte der notwendigen Garantien genau analysieren und prüfen, ob diese neue Vereinbarung ihre genannten Bedenken ausräume. Ferner werde man untersuchen, inwieweit der „Privacy Shield“ Rechtssicherheit für die Nutzung der alternativen Übermittlungsinstrumente schaffe und ob die Befugnisse der EU-Datenschutzbehörden gemäß Art. 28 DSRL gewahrt würden. Nach Abschluss dieser Prüfung werde die Gruppe sich zur Zulässigkeit alternativer Mechanismen wie SDPC und BCR äußern.

---

[154] Kühling/Heberlein, NVwZ 2016, S. 7 (12).
[155] Zur möglicherweise geänderten Situation unter dem „EU-U.S. Privacy Shield“ vgl. unten Ziffer 8.3 (zu BCR und SDPC Ziffer 8.3.6).
[156] Europäische Kommission – Pressemitteilung vom 02.02.2016, http://europa.eu/rapid/press-release_IP-16-216_de.htm.
[157] Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment vom 03.02.2016, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf.

In der Zwischenzeit dürften bereits existierende alternative Übermittlungsmechanismen weiter genutzt werden.[158]

Die Art. 29-Datenschutzgruppe erinnerte hingegen daran, dass Unternehmen ihre Datentransfers in die USA seit dem 01.02.16 nicht mehr auf „Safe Harbour“ stützen dürfen. Offenkundig berufen sich aber auch nach dem Ablauf der „Schonfrist“ noch immer zahlreiche Unternehmen auf „Safe Harbour“, darunter große, international tätige Unternehmen.[159] Die Gruppe teilte mit, dass die EU-Datenschutzbehörden Fälle und Beschwerden, mit denen sie befasst werden, bis auf weiteres einer Einzelfallprüfung unterziehen werden.[160] Einige Behörden erhöhen nun den Druck auf solche „Safe Harbour-Sünder“. So hat der Hamburgische Datenschutzbeauftrage Johannes Caspar angekündigt, dass seine Behörde Bußgelder gegen diese Firmen verhängen wird. Zunächst soll es aber Anhörungsverfahren geben.[161] Auch die französische Datenschutzbehörde CNIL geht derzeit gegen Datentransfers ohne Rechtsgrundlage vor und hat Facebook mit Sanktionen gedroht.[162]

Unternehmen, die ihre Datentransfers auf bestehende Verträge mit SDPC oder auf BCR stützen können, dürfen hingegen grundsätzlich davon ausgehen, dass die nationalen Aufsichtsbehörden diese Übermittlungsinstrumente zumindest bis zu einer anderslautenden Stellungnahme der Art. 29-Datenschutzgruppe weiterhin als Interimslösungen akzeptieren werden.[163] Insoweit hat die Gruppe die „Schonfrist“ für die Weiterverwendung existierender SDPC und BCR bis auf Weiteres verlängert. Mit einer Stellungnahme und Bekanntgabe der Untersuchungsergebnisse dürfte frühestens Ende März, eher wohl erst im April 2016 zu rechnen sein. Da SDPC und BCR die dargestellten Schwächen aufweisen, sollten sich Unternehmen, die sich hierauf stützen, engagiert zeigen und in ihre Verträge mit den amerikanischen Empfängern zusätzliche Regelungen[164] aufnehmen, um weitestmögliche Garantien für den Datenschutz zu schaffen. Darin könnten sie die US-Datenimporteure zu weiteren Maßnahmen zum Schutz personenbezogener Daten (z. B. Verschlüsselung, Gewährleistung von Einsicht in Protokolldaten) verpflichten, die allerdings den SDPC nicht widersprechen dürfen. All dies kann derzeit jedoch weder einen unverhältnismäßigen, grundrechtswidrigen Zugriff durch US-amerikanische Behörden vollends verhindern, noch können auf diesem Wege wirksame Rechtsschutzmöglichkeiten gegen staatliche Datenzugriffe geschaffen werden. Ein mögliches Durchgreifen der EU-Datenschutzbehörden trotz Nutzung von SDPC oder BCR ist daher jedenfalls in Zukunft nicht ausgeschlossen. Insgesamt ist die Situation noch immer sehr unbefriedigend. Daher sollen nachfolgend mögliche Auswege aus diesem Dilemma vorgestellt und dabei auch auf die aktuellen Pläne der Kommission zur Schaffung einer neuen Rechtsgrundlage eingegangen werden.

---

[158] Vgl. zu alldem Statement of the Art. 29 Working Party vom 03.02.1016 (Fn. 157).

[159] http://www.spiegel.de/netzwelt/netzpolitik/safe-harbour-hamburgs-datenschuetzer-droht-firmen-mit-bussgeld-a-1079019.html.

[160] Statement of the Art. 29 Working Party vom 03.02.1016 (Fn. 157).

[161] http://www.spiegel.de/netzwelt/netzpolitik/safe-harbour-hamburgs-datenschuetzer-droht-firmen-mit-bussgeld-a-1079019.html.

[162] http://www.sueddeutsche.de/digital/nach-safe-harbour-datenschuetzer-wollen-facebook-zwingen-daten-in-europa-zu-lassen-1.2855563.

[163] Denn wie bereits ausgeführt, sind die Entscheidungen zu den Standardverträgen jedenfalls formal nach wie vor in Kraft, bis sie durch den EuGH aufgehoben oder durch die Kommission geändert werden.

[164] Näher hierzu oben Ziffer 7.1.1.

8 Mögliche Auswege aus dem Dilemma

8.1 Ausweichlösung – Server in Europa

Unternehmen könnten rechtlich unsichere Transfers personenbezogener Daten in die USA dadurch verhindern, indem sie Daten von EU-Bürgern ausschließlich auf Servern innerhalb der EU verarbeiten. Soweit sie die Daten nicht allein selbst verarbeiten, könnten sie zu Dienstleistern wechseln, die die Daten ihrerseits ausschließlich in der EU oder in Ländern mit angemessenem Datenschutzniveau verarbeiten und nicht in die USA übermitteln. Entsprechend haben immer mehr amerikanische Unternehmen wie Amazon[165], Facebook[166] oder Oracle[167] nach dem „Schrems-Urteil“ damit begonnen, ihre Server nach Europa zu verlagern bzw. Rechenzentren in Europa zu eröffnen. Auch deutsche Unternehmen wie Henkel setzen vermehrt auf ein Hosting in Europa.[168] Die Deutsche Telekom hat sich für ein „Internet der kurzen Wege“ ausgesprochen, bei dem die Daten auf direktem Wege vom Absender zum Empfänger transportiert werden. Sie will dies in ihren Netzen bereits umgesetzt haben.[169] Der Software-Riese Microsoft will künftig die Daten seiner europäischen Kunden in Irland speichern und bietet in Deutschland sogar ein vollkommen neues Modell an, bei dem die Deutsche Telekom die Treuhänderschaft über die Daten übernimmt.[170] Teile der „Microsoft Cloud“ sollen dann in den Telekom-Rechenzentren in Frankfurt und Magdeburg liegen.

Bei einer Verlagerung der Datenverarbeitung auf Server innerhalb der EU handelt es sich sowohl derzeit als auch langfristig wohl um die sicherste und damit um eine empfehlenswerte Lösung.[171] Problematisch hieran ist, dass der Umzug der Daten auf Server innerhalb der EU oder gar der Bau eines solchen Servers Zeit braucht und schon aus Kostengründen nicht für alle Unternehmen in Betracht kommt.

Auch Daten auf Servern innerhalb der EU sind allerdings nicht vollumfänglich vor Zugriffen durch den US-amerikanischen Staat geschützt. So können US-amerikanische Unternehmen nach der US-amerikanischen Rechtsprechung verpflichtet sein, personenbezogene Daten herauszugeben, auch wenn diese bei Tochtergesellschaften und auf Servern innerhalb der EU gespeichert sind. Die Frage ist in den USA noch nicht höchstrichterlich geklärt. Derzeit ist bei einem US-amerikanischen Berufungsgericht das Verfahren *Microsoft v. United States* anhängig.[172] In diesem Verfahren wehrt sich Microsoft gegen die Verpflichtung zur Herausgabe von Daten, die auf Servern in Irland gespeichert sind. Mit einer Entscheidung wird noch im Frühjahr 2016 gerechnet. Verliert Microsoft diesen Rechtsstreit, müsste es die Daten ungeachtet entgegenstehender Bestimmungen im EU-Recht herausgeben. Dies steht im klaren Widerspruch zum künftigen Art. 43a DSGV, wonach Gerichtsurteile aus Drittstaaten nur vollstreckbar sind, wenn dies durch ein internationales Abkommen – etwa ein gegenseitiges Rechtshilfeabkommen – gedeckt ist.[173] Eine Lösung könnten Treuhandmodelle

---

[165] Vgl. FAZ vom 01.01.2016, S. 22 „Damit die Daten weiter fließen“; Handelsblatt Wochenende vom 29.01.2016, S. 16 „Wenn Datenverkehr plötzlich illegal ist“.

[166] So baut etwa Facebook derzeit in Irland sein zweites Rechenzentrum in Europa, vgl. http://www.faz.net/aktuell/wirtschaft/facebook-baut-ein-zweites-rechenzentrum-in-europa-14033002.html.

[167] The Irish Times, Oracle keeps European Data within its EU-based data centres, http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505.

[168] So etwa der Henkel-Konzern, vgl. FAZ vom 01.01.2016, S. 22 „Damit die Daten weiter fließen“.

[169] Thomas Kremer, die Abschaffung von Safe Harbour und ihre Folgen, https://www.telekom.com/medien/managementzursache/290370.

[170] http://www.welt.de/print/die_welt/wirtschaft/article148748329/Microsoft-fluechtet-nach-Deutschland.html. Vgl. auch Handelsblatt Wochenende vom 29.01.2016, S. 36 „Wenn Datenverkehr plötzlich illegal ist“.

[171] Vgl. auch die „Folgerungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz“ (Fn. 101).

[172] U.S. Court of Appeals for the Second Circuit, Fall-Nr. 14-2985-cv – Microsoft v. U.S.

[173] Kühling/Heberlein, NVwZ 2016, S. 7 (11).

sein, wie sie beispielsweise die Deutsche Telekom ab der zweiten Jahreshälfte 2016 anbieten will. Unternehmen wie Microsoft, Cisco, VMware, Salesforce oder Huawei[174], die mit der Deutschen Telekom kooperieren, können in deren Datenzentren ihre eigenen Server aufbauen. Die Deutsche Telekom übernimmt dann als Treuhänder deren Betrieb und Administration und hat das alleinige Zugriffsrecht auf die Daten.[175] Hierdurch sollen etwaige Verpflichtungen zur Datenherausgabe nach US-amerikanischem Recht umgangen werden, ohne dass dies über geordnete Wege wie Rechtshilfeabkommen läuft.

8.2 Technische Lösungen – Verschlüsselung und Anonymisierung

In Betracht kommen ferner technische Lösungen wie die Verschlüsselung (insbesondere eine wirksame Ende-zu-Ende-Verschlüsselung) oder Anonymisierung von Daten. Diese können unangemessene Zugriffe von Sicherheitsbehörden jedenfalls erschweren und sind daher als zusätzliche Maßnahmen für mehr Sicherheit zu empfehlen.

Eine Anonymisierung kommt allerdings nicht in Betracht, wo Unternehmen die personenbezogenen Daten benötigen oder gerade mit deren Nutzung Geld verdienen.[176] Zweifelsfreien Schutz vor ungerechtfertigten Zugriffen durch US-amerikanische Behörden vermag jedoch auch eine Verschlüsselung nicht zu gewährleisten. Denn eine Rückentschlüsselung ist nicht überall ausgeschlossen; zudem kann eine Herausgabe von Passwörtern ggf. gerichtlich erzwungen werden.[177]

8.3 „EU-U.S. Privacy Shield“ und neuer Angemessenheitsbeschluss der Kommission

8.3.1 Was ist der „Privacy Shield“?

Wie bereits ausgeführt, hat sich die Kommission laut Pressemitteilung[178] vom 02.02.2016 mit den USA unter dem Namen „EU-U.S. Privacy Shield“ (nachfolgend: „Privacy Shield“) politisch auf einen neuen Rahmen für die transatlantische Datenübermittlung geeinigt. Auf Basis dieses Rahmens beauftragte das Plenum der Kommission Kommissarin Jourová und Vizepräsident Ansip am selben Tag mit dem Entwurf eines neuen „Angemessenheitsbeschlusses“ gemäß Art. 25 Abs. 6 DSRL. Am 29.02.2016 hat die Kommission den Entwurf des Beschlusses (nachfolgend: „Privacy Shield-Beschluss“) vorgelegt. Danach soll der neue Rechtsrahmen ähnlich wie bei „Safe Harbour“ auf einem einseitigen Kommissionsbeschluss beruhen. Diesem werden neben neuen „EU-U.S. Privacy Shield Framework Principles“ (nachfolgend: „Privacy Principles“) mehrere in Briefform übermittelte Zusicherungen hoher Vertreter US-amerikanischer Behörden als Anhänge beigefügt. Geplant ist erneut ein Selbstverpflichtungssystem, allerdings mit verschärften Regeln. Ähnlich wie bei „Safe Harbour“ sollen sich US-amerikanische Unternehmen, die personenbezogene Daten aus der EU importieren wollen, noch strengeren Auflagen[179] bezüglich der Art der Verarbeitung personenbezogener Daten und des Schutzes der Rechte Einzelner als unter „Safe Harbour“ unterwerfen.

Das Paket aus Prinzipien und Briefen soll im US-Bundesregister veröffentlicht werden, dem Amtsblatt der US-Bundesregierung. Hierdurch soll die Absicht der USA, die Verpflichtungen auch nach

[174] Handelsblatt Wochenende vom 29.01.16, S. 36 „Wenn Datenverkehr plötzlich illegal ist“.
[175] http://www.welt.de/print/die_welt/wirtschaft/article148748329/Microsoft-fluechtet-nach-Deutschland.html.
[176] Kühling/Heberlein, NVwZ 2016, S. 7 (11).
[177] Kühling/Heberlein, NVwZ 2016, S. 7 (11).
[178] Europäische Kommission – Pressemitteilung vom 02.02.2016, http://europa.eu/rapid/press-release_IP-16-216_de.htm.
[179] Diese Auflagen sind in den „Privacy Principles“, bestehend aus den EU-U.S. „Framework Principles“ und den „Supplemental Principles“ geregelt, die – wie bei „Safe Harbour“ - jeweils vom US-Handelsministerium herausgegeben wurden und dem „Privacy Shield“-Beschluss als Anhang II beigefügt werden sollen.

einem politischen Wechsel aufrechtzuerhalten, öffentlich bekundet werden.[180] Mit anderen Worten soll es künftigen Präsidenten erschwert werden, die Versprechungen zurückzunehmen.[181] Auf der Basis dieser Zusicherungen und der in den Anhängen näher erläuterten US-amerikanischen Rechtslage meint die Kommission den USA nun ein angemessenes Schutzniveau attestieren zu können.[182] Ähnlich wie bei „Safe Harbour“ ist auch diese Beurteilung beschränkt auf Übermittlungen personenbezogener Daten aus der EU an selbstzertifizierte Unternehmen in den USA unter dem „Privacy Shield“.

Im Einzelnen besteht das von der Kommission vorgelegte, mehr als 130 Seiten umfassende „ Paket“ aus

- einer **Mitteilung**[183],
- einem „Fact Sheet“ mit **Fragen und Antworten**[184],
- einem weiteren **Fact Sheet** mit einem Übersichtsschema über die wesentlichen Elemente des „Privacy Shields“[185] sowie
- dem **Entwurf der Angemessenheitsentscheidung** der Kommission[186]
- nebst **sieben Anhängen**.

Der „Privacy Shield“-Beschluss selbst besteht nur aus sechs Artikeln, denen jedoch 129 Erwägungsgründe vorangestellt und sieben Anhänge beigefügt sind. Diese Anhänge umfassen folgende Dokumente:

- einen Entwurf der „Privacy Principles“, erarbeitet vom US-Handelsministerium (**Anhang II**)[187];
- einen Brief des US-Handelsministeriums, welches die Befugnisse und Pflichten dieses Ministeriums zur Überwachung und Kontrolle des „Privacy Shields“ beschreibt, um dessen effektive Umsetzung sicherzustellen (**Anhang I**)[188];
- einen Brief des Secretary of State, John F. Kerry, in dem der neu etablierte „Ombudsmann-Mechanismus“ betreffend „Signals Intelligence“[189] erklärt und beschrieben wird (**Anhang III**)[190];
- einen Brief der US-Handelskammer (FTC), in dem näher dargelegt wird, wie die FTC die Einhaltung des „Privacy Shields“ durch die zertifizierten Unternehmen umsetzen bzw. sicherstellen will (**Anhang IV**)[191];

---

[180] Communication from the Commission to the European Parliament and the Council, “Transatlantic Data Flows: Restoring Trust through Strong Safeguards” vom 29.02.2016, COM(2016) 117 final, Ziffer 3.3; abrufbar unter http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

[181] So das Magazin „Politico“, welches davon spricht, die Kommission habe den „Privacy Shield“ „Trump-Proof“ machen wollen, http://www.politico.eu/article/privacy-shield-agreement-takeaways-text-released/.

[182] Vgl. Recitals 112-116 and Art. 1 des Entwurfs der Angemessenheitsentscheidung der Kommission, „Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, abrufbar unter http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

[183] Communication from the Commission to the European Parliament and the Council, “Transatlantic Data Flows: Restoring Trust through Strong Safeguards”, (Fn. 180).

[184] http://europa.eu/rapid/press-release_MEMO-16-434_en.htm.

[185] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf.

[186] Siehe Fn. 182.

[187] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf.

[188] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-1_en.pdf.

[189] Unter „Signals Intelligence“ versteht man die Gewinnung von Informationen, üblicherweise bestehend aus den beiden Hauptkategorien Fernmeldeaufklärung zum Abhören von Funksignalen und Elektronische Aufklärung, vgl. https://de.wikipedia.org/wiki/Signals_Intelligence.

[190] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-3_en.pdf.

- einen Brief des Secretary of Transportation, in welchem das US-Transportministerium (DOT) seine Befugnisse näher darlegt, die Einhaltung des „Privacy Shields“ betreffend den Schutz von Daten im Luftverkehrsbereich sicherzustellen (**Anhang V**[192]);

- einen Brief des Offices of the Director of National Intelligence (ODNI), unterzeichnet von Robert S. Litt, Justiziar von US-Geheimdienstdirektor James Clapper. Dieser fasst im Wesentlichen die Befugnisse der US-Geheimdienstbehörden bezüglich der Erhebung und Nutzung von Informationen sowie die Begrenzungen zusammen, denen diese Behörden unterliegen (**Anhang VI**[193]);

- einen Brief des U.S.-Justizministeriums, Strafrechtliche Abteilung, der einen Überblick über die Untersuchungsinstrumente geben soll, mit denen die USA von Unternehmen Daten zum Zwecke der Strafverfolgung oder im öffentlichen Interesse erhebt (**Anhang VII**[194]).

Um zu gewährleisten, dass die neue Regelung auch funktioniert, wollen Kommission und US-Handelsministerium jährlich eine gemeinsame Überprüfung durchführen, bei der u.a. Sachverständige der US-Nachrichtendienste und der EU-Datenschutzbehörden hinzugezogen werden sollen.[195] Dabei soll insbesondere geprüft werden, ob das Schutzniveau in den USA noch immer angemessen ist.

Hat die Kommission klare Anhaltspunkte dafür, dass die wirksame Einhaltung der „Privacy Principles“ in den USA nicht mehr sichergestellt oder das erforderliche Schutzniveau angesichts der Handlungen der US-Behörden nicht mehr gewährleistet ist, kann sie ein Verfahren zur vollständigen oder teilweisen Suspendierung oder Aufhebung der Entscheidung einleiten oder den Umfang der Angemessenheitsentscheidung weiter begrenzen, etwa auf Datenübermittlungen, die zusätzlichen Bedingungen unterliegen.[196] Zuvor muss die Kommission jedoch das US-Handelsministerium informieren und auffordern, die Verletzung der „Privacy Principles“ innerhalb angemessener Frist abzustellen. Ein solches Verfahren soll insbesondere in Betracht kommen, wenn

- die US-Behörden die in den Anhängen geregelten Bedingungen nicht einhalten;

- Beschwerden von Betroffenen aus der EU systematisch nicht effektiv bearbeitet werden;

- die Ombudsperson es systematisch versäumt, zeitnahe und angemessene Antworten auf Anfragen von Betroffenen aus der EU zu geben oder

- die beteiligten US-Behörden die notwendige Zusammenarbeit vermissen lassen und die Kommission deshalb nicht feststellen kann, ob ihre Angemessenheitsbewertung noch zutreffend ist.[197]

8.3.2 Anforderungen an den „Privacy Shield“-Beschluss

Die (materielle) Rechtmäßigkeit des geplanten „Privacy Shield“-Beschlusses setzt voraus, dass die Bewertung des Schutzniveaus in den USA durch die Kommission als „adäquat“ bei einer Gesamtbetrachtung der relevanten Umstände gerechtfertigt erscheint.

---

[191] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-4_en.pdf.
[192] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-5_en.pdf.
[193] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.
[194] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-7_en.pdf.
[195] Näher hierzu Erwägungsgründe 120 ff. des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182 sowie die Pressemitteilung der Europäischen Kommission vom 02.02.2016, http://europa.eu/rapid/press-release_IP-16-216_de.htm.
[196] Vgl. Art. 4 Abs. 6 sowie Erwägungsgründe 125 ff. des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[197] Vgl. Art. 4 Abs. 6 und 7 sowie Erwägungsgründe 126 ff. des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).

Erforderlich hierfür ist zum einen, dass die Entscheidung die Vorgaben des EuGH im „Schrems-Urteil“[198] umsetzt, um nicht denselben Mängeln wie „Safe Harbour“ zu unterliegen (hierzu sogleich Ziffer 8.3.3). Hierzu gehören

(1) eine ordnungsgemäße Prüfung und Feststellung des angemessenen Schutzniveaus in den USA durch die Kommission;

(2) die Sicherstellung einer wirksamen Überwachung und Kontrolle der Selbstverpflichtungen zur Ermittlung und Ahndung von Verstößen;

(3) eine klare Beschränkung von staatlichen Zugriffen und Grundrechtseingriffen auf das erforderliche und vom Gerichtshof näher präzisierte Maß;

(4) die Schaffung eines wirksamen (gerichtlichen) Rechtsschutzes, insbesondere

- administrativer oder gerichtlicher Rechtsbehelfe, um Zugang zu den Daten zu erhalten oder deren Berichtigung oder Löschung zu erwirken, sowie

- eines wirksamen gerichtlichen Rechtsschutzes gegen Grundrechtseingriffe durch staatliche Maßnahmen;

(5) die uneingeschränkte Wahrung der Befugnisse der EU-Datenschutzbehörden.

Über diese Vorgaben hinaus muss die Kommission bei ihrer Beurteilung der Angemessenheit des Datenschutzniveaus weitere Umstände berücksichtigen. Bei der erforderlichen Gesamtbetrachtung unter Berücksichtigung aller relevanten Umstände dürfte sie den ihr zustehenden Ermessensspielraum nicht überschritten haben (hierzu unten Ziffer 8.3.4).

Der „Privacy Shield“ kann in dieser cep**Studie** aufgrund des Umfangs und der Detailliertheit der von der Kommission veröffentlichten Dokumentation und der Tatsache, dass seine Umsetzung noch nicht in allen Einzelheiten klar ist, in der Kürze der Zeit nicht vollumfänglich analysiert werden. Einige Punkte, die nach oberflächlicher Durchsicht im Hinblick auf die Vereinbarkeit des geplanten „Privacy Shield“ mit den oben genannten Vorgaben des Gerichtshofs oder hinsichtlich der Adäquanz des Schutzniveaus problematisch erscheinen, sollen jedoch nachfolgend herausgegriffen und näher dargestellt werden.

8.3.3 Umsetzung der Vorgaben des EuGH im „Schrems-Urteil“?

8.3.3.1 Angemessenes Schutzniveau „aufgrund innerstaatlicher Rechtsvorschriften oder internationaler Verpflichtungen“

Gemäß Art. 25 Abs. 6 DSRL muss die Kommission bei einem Angemessenheitsbeschluss feststellen, dass die USA aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen gewährleisten. Nach der Auslegung des EuGH muss sich das Schutzniveau aus der Rechtsordnung der USA ergeben.[199]

Problematisch erscheint insoweit zunächst, dass die Kommission auch im Entwurf des „Privacy Shield“-Beschlusses nicht feststellt, dass die USA generell ein angemessenes Datenschutzniveau gewährleisten. Vielmehr statuiert die Kommission in Art. 1 und in Erwägungsgrund 112 f. dieses Entwurfes, dass die USA für die Zwecke des Art. 25 Abs. 2 DSRL *bezüglich personenbezogener Da-*

[198] Hierzu im Einzelnen oben 5.3.2.2.
[199] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 29), Tz. 74.

ten, die aus der EU an Unternehmen in den USA unter dem „Privacy Shield“ übermittelt werden, ein angemessenes Schutzniveau gewährleisten. Die Angemessenheitsfeststellung der Kommission bleibt daher ähnlich wie bei „Safe Harbour“ auf Daten beschränkt, die aus der EU an unter dem „Privacy Shield“ selbstzertifizierte US-Unternehmen übermittelt werden. Fragwürdig ist dies unter zwei Aspekten: Zum einen sieht der Wortlaut des Art. 25 Abs. 6 DSRL ausdrücklich keine in dieser Weise begrenzte Angemessenheitsfeststellung vor. Darüber hinaus leitet die Kommission die Angemessenheit des Datenschutzniveaus maßgeblich auch aus den der Entscheidung beigefügten „Privacy Principles“ ab. Diese böten in ihrer Gesamtheit einen Schutz, der dem durch die grundlegenden Prinzipien der DSRL garantierten Schutz personenbezogener Daten der Sache nach gleichwertig sei.[200] Diese Prinzipien wurden zwar vom US-Handelsministerium erarbeitet. Sie werden jedoch voraussichtlich nicht in der Rechtsordnung der USA verankert oder in einem völkerrechtlichen Vertrag allgemeingültig vereinbart, was jedoch nach dem Wortlaut wohl erforderlich wäre. Im Ergebnis gelten sie dann offenbar nach wie vor lediglich für die zertifizierten Unternehmen und nicht auch für die US-Behörden, was der EuGH im „Schrems-Urteil“ kritisiert hat.[201]

Andererseits schließt das „Schrems-Urteil“ einen neuen, verbesserten Angemessenheitsbeschluss der Kommission gemäß Art. 25 Abs. 6 DSRL auf der Grundlage eines Selbstverpflichtungssystems nicht kategorisch aus. Der Gerichtshof hat den Rückgriff eines Drittlandes auf ein System der Selbstzertifizierung als solches nicht grundsätzlich abgelehnt. Er hat sogar ausdrücklich ausgeführt, dass der Rückgriff eines Drittlands auf ein System der Selbstzertifizierung als solcher nicht gegen das Erfordernis in Art. 25 Abs. 6 DSRL verstoße, dass in dem betreffenden Drittland „aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen“ ein angemessenes Schutzniveau gewährleistet sein muss.[202] Voraussetzung sei jedoch, dass ein solches System zuverlässig ist und sich in der Praxis als wirksam erweist, um einen gleichwertigen Schutz zu gewährleisten. Der Schutz darf also nicht nur auf dem Papier bestehen.[203] Ist aber ein Selbstzertifizierungssystem damit aus Sicht des EuGH eine grundsätzlich zulässige Möglichkeit, mit Hilfe derer ggf. die Angemessenheit des Schutzniveaus in einem Drittstaat gewährleistet werden kann, erscheint es möglich, dass eine Angemessenheitsfeststellung auf Datentransfers unter einem solchen System beschränkt werden darf. In diesem Fall kommt es entscheidend auf die praktische Wirksamkeit des Systems an.[204] Allerdings ähnelt ein solches System eher einer „Garantie“ i.S.d. 26 Abs. 2 DSRL, die das Fehlen eines allgemeinen angemessenen Schutzniveaus kompensieren soll.

Weiterhin stützt sich die Kommission bei ihrer Angemessenheitsbeurteilung auch auf die schriftlichen Erklärungen und Zusicherungen in den Briefen, die dem Entwurf des „Privacy Shield-Beschlusses“ als Anhänge beigefügt sind. Fraglich ist, inwieweit diese berücksichtigungsfähig sind. Denn es ist unklar, welche Natur und welchen genauen Zweck die Briefe haben. Insoweit wird man davon ausgehen dürfen, dass die Briefe nicht ausschließlich deklaratorischer Natur sind, d.h. nicht

---

[200] Vgl. Erwägungsgrund 49, 113 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[201] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 29), Tz. 82.
[202] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 29), Tz. 81.
[203] Vgl. hierzu oben Ziffer 5.3.2.2 (2) und unten Ziffer 8.3.3.2.
[204] Im Falle einer Angemessenheitsfeststellung, die auf Datentransfers an die zertifizierten Unternehmen beschränkt ist, stellt sich allerdings die Frage nach der Zulässigkeit des Rückgriffs auf alternative Rechtsgrundlagen für den Datentransfer. Nach dem Wortlaut von Art. 26 Abs. 1 und 2 DSRL, Art. 42 Abs. 1. Art. 44 Abs. 1 DSGV kommt ein Rückgriff auf solche alternativen Rechtsgrundlagen nur in Betracht, wenn das Drittland „kein angemessenes Schutzniveau gewährleistet“ bzw. für dieses Land keine Angemessenheitsentscheidung nach Art. 41 Abs. 3 DSGV vorliegt. Hierin wird man aber wohl keinen Zwang zur Selbstzertifizierung unter dem „Privacy Shield“ sehen müssen. Vielmehr ist davon auszugehen, dass der Rückgriff auf SDPC, BCR oder einen der Ausnahmetatbestände weiterhin in Betracht kommt, soweit eben kein angemessenes Schutzniveau besteht, was bei Transfers an solche US-Unternehmen der Fall wäre, die nicht unter „Privacy Shield“ zertifiziert sind. Insoweit bliebe auch nach Inkrafttreten des „Privacy Shield“-Beschlusses die Frage relevant, ob die alternativen Rechtsinstrumente unter den geänderten Rahmenbedingungen hinreichende Garantien bieten können. Vgl. insoweit noch die Kurzeinschätzung unten unter Ziffer 8.3.6.

lediglich das ohnehin geltende US-Recht beschreiben, sondern zumindest teilweise zusätzliche Garantien und Mechanismen etablieren sollen.[205] Was Beschreibung und was zusätzliche Garantie ist, lässt sich auf den ersten Blick jedoch nicht herauslesen. Darüber hinaus stellt sich die Frage, welchen rechtlichen Charakter und welche Bindungswirkung – insbesondere auch nach den anstehenden US-Präsidentschaftswahlen – diese Zusicherungen haben oder dadurch erhalten, dass sie im US-Bundesregister veröffentlicht werden. Denn eine darüber hinausgehende verbindliche Umsetzung dieser Verpflichtungen etwa in Form von Gesetzesänderungen soll es offenkundig nicht geben. Kritiker bemängeln deshalb zu Recht, dass die Briefe keinen Gesetzescharakter haben.[206] Ebenso wenig handelt es sich bei dem „Privacy Shield“ um ein internationales Abkommen.[207] Insbesondere wegen des unklaren Charakters und der unklaren Bindungswirkung der in den Briefen enthaltenen Zusicherungen sind auch insoweit bereits nach dem Wortlaut des Art. 25 Abs. 6 DSRL gewisse Zweifel angebracht, ob diese Zusicherungen als „innerstaatliche Rechtsvorschriften“ oder als „internationale Verpflichtungen“ der USA charakterisiert und so für die Beurteilung des Schutzniveaus herangezogen werden können.

8.3.3.2 Wirksame Überwachung und Kontrolle der Selbstverpflichtungen

Wie dargelegt hat der EuGH im „Schrems“-Urteil die Geeignetheit eines Selbstzertifizierungssystems an die Existenz wirksamer Überwachungs- und Kontrollmechanismen geknüpft, die es erlauben, in der Praxis etwaige Verstöße gegen Regeln zur Gewährleistung des Schutzes der Grundrechte zu ermitteln und zu ahnden.[208] Eine effektive Überwachung und Kontrolle der Einhaltung der „Privacy Principles“ durch die beteiligten US-Unternehmen ist auch unter wettbewerbsrechtlichen Gesichtspunkten wichtig. Denn durch mangelnde Transparenz, Einhaltung und Durchsetzung der Prinzipien in den USA können für EU-Unternehmen gegenüber ihren US-amerikanischen Mittbewerbern Wettbewerbsnachteile entstehen, was zu Wettbewerbsverzerrungen führt.[209] Diese Gefahr bestünde auch, wenn US-Unternehmen mit den „Privacy Principles“ inhaltlich weniger strengen datenschutzrechtlichen Regeln unterlägen als EU-Unternehmen.

In puncto Überwachung und Kontrolle scheint der „Privacy Shield“ bei einer oberflächlichen Durchsicht in der Tat zumindest auf dem Papier zu deutlichen Verbesserungen gegenüber „Safe Harbour“ zu führen. Fraglich ist, ob diese Verbesserungen ausreichen und auch in der Praxis tatsächlich umgesetzt werden, damit das System zuverlässig ist und die vom EuGH geforderte Wirksamkeit verspricht.

Künftig sollen die Selbstverpflichtungen der teilnehmenden Unternehmen veröffentlicht und nach US-Recht von der FTC durchgesetzt werden können.[210] Innerhalb der FTC sollen neue Ressourcen geschaffen und ein besonderes Team zur Überwachung der Einhaltung des „Privacy Shields“ abgestellt werden.[211] Um den Schutz von Daten im Luftverkehrsbereich zu sichern, soll ferner das US-Transportministerium (Department of Transportation, nachfolgend: „DOT“) gewisse Durchsetzungsbefugnisse haben.[212] Das US-Handelsministerium hat verwaltende Funktion und ist dafür

---

[205] Dies dürfte beispielsweise hinsichtlich der Einrichtung des Ombudsmannverfahrens und der Versprechen der FTC gelten, die Durchsetzung des „Privacy Shield“ hohe Priorität einzuräumen. Näher hierzu unten Ziffern 8.3.3.3 (FTC) und 8.3.3.4 (Ombudsmann-Mechanismus).

[206] https://www.datenschutzbeauftragter-info.de/privacy-shield-veroeffentlichter-text-verheisst-nichts-gutes/.

[207] Vgl. auch die Aussage von Justizkommissarin Jourová in ihrer Rede vom 01.02.2016, http://europa.eu/rapid/press-release_SPEECH-16-208_de.htm.

[208] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 29), Tz. 81.

[209] So die Kommission in ihren Mitteilungen zu „Safe Harbour“, Mitteilung COM (2013) 847 (final), (Fn. 25), Ziffer 2.2, und Mitteilung (2013) 846 (final) (Fn. 1), Ziffer 3.2. Dazu auch cep**Study**, Competition Challenges in the Consumer Internet Industry - How to Ensure Fair Competition in the EU, Februar 2016, S. 42 f.

[210] Europäische Kommission – Pressemitteilung vom 02.02.2016, http://europa.eu/rapid/press-release_IP-16-216_de.htm.

[211] https://www.commerce.gov/print/1781.

[212] Vgl. Anhang V zum Entwurf des „Privacy Shield“-Beschlusses (Fn. 192) sowie Erwägungsgrund 15 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).

zuständig, eine Liste der zertifizierten Unternehmen zu führen und zu aktualisieren. Ferner wird es in einer weiteren Liste Unternehmen aufführen, die aus der Liste entfernt wurden, also nicht mehr zertifiziert sind. Das Ministerium soll ferner missbräuchliche Behauptungen tatsächlich nicht (mehr) bestehender Zertifizierungen unter dem „Privacy Shield“ unterbinden und Unternehmen dahingehend überwachen.[213] Es kann auch von Amts wegen Untersuchungen tätigen, etwa durch Zusendung detaillierter Fragebögen. Bei Beschwerden, mangelnder Reaktion eines teilnehmenden Unternehmens oder bei glaubhaften Hinweisen auf eine Verletzung der Prinzipien sollen Untersuchungen standardmäßig erfolgen.[214] Unternehmen, die die Prinzipien dauerhaft verletzen, sollen von der Liste gestrichen werden.[215] Dies galt allerdings auch bereits unter „Safe Harbour“.[216]

Die Kontrolle der inhaltlichen Einhaltung der Prinzipien obliegt hingegen den Unternehmen selbst sowie der FTC. Allerdings hatte die FTC ebenso wie das US-Handelsministerium bereits unter „Safe Harbour“ gewisse Kontroll- und Durchsetzungsbefugnisse.[217] Auch das neue System baut zunächst weiter auf die Selbstkontrolle der Unternehmen, ob die Prinzipien des „Privacy Shields“ eingehalten werden. Unternehmen können hier zwischen internen Prozeduren und Auditing oder „random checks“ durch externe Dienstleister wählen.[218] Darüber hinaus kann die FTC von einer unabhängigen Streitbeilegungsstelle, vom US-Handelsministerium oder von den EU-Datenschutzbehörden und teilweise von Individuen mit weitergeleiteten Beschwerden wegen der Nichteinhaltung der Prinzipien befasst werden. Diese werden daraufhin geprüft, ob unfaire oder irreführende Praktiken i.S.v. Section 5 des FTC Act vorliegen. Die FTC will der Bearbeitung von Beschwerden, die durch die EU-Mitgliedstaaten an sie weitergeleitet werden, „Priorität“ einräumen.[219] Zum einen bleibt unklar, was dies genau bedeutet. Zum anderen ist nicht zu erkennen, worin insoweit ein Fortschritt gegenüber „Safe Harbour“ oder gar eine erweiterte Garantie liegen soll, denn entsprechende Versprechungen gab es bereits dort.[220] Mit Hilfe sogenannter „consent orders“ kann die FTC die Einhaltung der Prinzipien – notfalls auch gerichtlich – durchsetzen.[221] Allerdings scheint die FTC offenbar überwiegend nur auf eine Rüge der EU-Mitgliedstaaten oder der zertifizierten Unternehmen hin verpflichtet zu sein, tätig zu werden und konkrete Durchsetzungsmaßnahmen zu ergreifen. Unabhängige Kontrollen sollten jedoch nicht im Wesentlichen auf Rüge hin, sondern anlasslos, regelmäßig, unangekündigt und flächendeckend erfolgen. Zwar will die FTC auch proaktiv eigene Recherchen mit verschiedenen Mitteln vornehmen, um Verletzungen aufzudecken. Wie umfassend und regelmäßig solche Untersuchungen sind, bleibt jedoch unklar, da diese nichtöffentlich und geheim durchgeführt werden.[222] Genaue Vorgaben für eine anlasslose, regelmäßige, unangekündigte und flächendeckende Kontrolle aller Unternehmen auf Einhaltung der „Privacy Principles“ durch eine vom Unternehmen getrennte Aufsichtsstelle scheint es aber nicht zu geben. Auch lässt die Tatsache, dass die FTC unter „Safe Harbour“ in 16 Jahren bei 4.000 teilnehmenden Unternehmen lediglich 9 Durchsetzungsmaßnahmen unternommen hat, von denen lediglich drei Verfahren inhaltliche Verletzungen der Prinzipien betrafen,[223] Zweifel an der Effektivität dieser Kontrollen aufkommen. Unklar ist, ob die (in welchem Umfang?) gesteigerten Mittel, Ressourcen und Befugnisse der FTC hieran etwas ändern werden. Einige Details müssen auch erst noch umgesetzt werden. Insgesamt erscheint es nach vorläufiger Bewertung trotz erkennbarer Verbesserungen fraglich, ob die geplanten Ressourcen und Befugnisse von US-Handelsministerium, FTC und DOT aus-

[213] Vgl. Erwägungsgründe 24-28 des Entwurfs des „Privacy Shield“-Beschlusses (vgl. Fn. 182).
[214] Vgl. Erwägungsgrund 35 des Entwurfs des „Privacy Shield“-Beschlusses (vgl. Fn. 182).
[215] Vgl. Erwägungsgrund 38 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[216] Vgl. Anhang II zur „Safe Harbour“-Entscheidung (Fn. 3), FAQ 11 B.
[217] Hierzu näher Mitteilung COM (201) 847 (final) (Fn. 25), Ziffern 2.1, 4 und 5.1.
[218] Vgl. Erwägungsgrund 23 des Entwurfs des „Privacy Shield“-Beschlusses (vgl. Fn. 182).
[219] Vgl. Anhang IV (Fn. 191), Ziffer II.
[220] Vgl. Anhang II zur „Safe Harbour“-Entscheidung (Fn. 3), FAQ 11 B.
[221] Vgl. Erwägungsgrund 41 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[222] Vgl. Anhang IV (Fn. 191), Ziffer II (S. 7).
[223] Vgl. Anhang IV (Fn. 191), Ziffer I C (S. 4).

reichen, um eine effektive Kontrolle und Durchsetzung der Einhaltung der „Privacy Principles“ zu gewährleisten. Wie dargelegt, sollten regelmäßig anlasslose, unangekündigte und flächendeckende Kontrollen durchgeführt werden. Hilfreich könnte es sein, neben den geplanten Sanktionen abschreckende Geldstrafen für US-Unternehmen vorzusehen, die die „Privacy Principles“ verletzen. Zu erwägen wäre auch, ob anstelle der möglicherweise unzureichend kontrollierbaren Selbstunterwerfungen Zertifizierungen besser durch unabhängige akkreditierte Stellen vorgenommen werden sollten.

8.3.3.3 Klare Beschränkung von Zugriffen und sonstigen Grundrechtseingriffen

Ferner ist es nach den Ausführungen des EuGH unabdingbar, dass die USA den anlasslosen und unverhältnismäßigen Zugriff auf Daten von EU-Bürgern auf das „absolut Notwendige“[224] beschränken. Zugriff und Verarbeitung durch US-Behörden dürfen nur in einer Weise erfolgen, die mit den Zielsetzungen ihrer Übermittlung vereinbar ist und nicht über das hinausgeht, was zum Schutz der nationalen Sicherheit „absolut notwendig und verhältnismäßig“[225] ist. Um dies zu gewährleisten, muss es bei Einschränkungen oder Ausnahmen eine Differenzierung anhand des verfolgten Ziels geben. Mit Hilfe objektiver Kriterien muss der Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke beschränkt werden, die solche Eingriffe rechtfertigen können.[226] Eine generelle Speicherung oder generelle Zugriffsrechte darf es nicht geben. Der EuGH fordert vielmehr „klare und präzise Regeln für die Tragweite und die Anwendung“ (staatlicher) Maßnahmen und „Mindestanforderungen“ für Eingriffe, um ausreichende Garantien für die Betroffenen zu schaffen.[227]

Laut der Pressemitteilung der Kommission soll der Zugriff von US-Behörden aus Gründen der Rechtsdurchsetzung oder der nationalen Sicherheit unter dem „Privacy Shield“ künftig nur noch in begrenztem Umfang, nämlich unter rechtlich ganz klar festgelegten Bedingungen, Schutzvorkehrungen und strengen Aufsichtsmechanismen gestattet sein.[228] Eine unterschiedslose Massenüberwachung von personenbezogenen Daten von EU-Bürgern in den USA soll es nicht (mehr) geben; vielmehr müsse ein solcher Zugriff die Ausnahme bleiben und dürfe nur erfolgen, soweit er „notwendig und verhältnismäßig“ sei. Anhang VI zum Entwurf des „Privacy Shield“- Beschlusses enthält wie oben ausgeführt einen Brief, in welchem Zusicherungen gemacht und die Begrenzungen und Sicherheiten detailliert beschrieben werden, denen die US-Geheimdienstbehörden bezüglich der Erhebung und Nutzung von Informationen unterliegen. Der Brief stammt aus der Feder des Justiziars von US-Geheimdienstdirektor James Clapper, derzeitiger Direktor der nationalen Nachrichtendienste, welcher seinerzeit die später durch Edward Snowden enthüllten Überwachungsmaßnahmen durch die CIA öffentlich geleugnet hatte.

Eine kursorische Durchsicht des Anhangs VI[229] ergibt, dass die Erhebung und Nutzung personenbezogener Daten durch die US-amerikanischen Geheimdienste in der Tat verschiedenen Begrenzungen unterliegen, insbesondere dank des Erlasses der „Presidential Policy Directive 28“ (PPD-28). Dennoch bleibt in bestimmten Fällen auch unter dem „Privacy Shield“ eine massenhafte Erhebung und Nutzung solcher Daten zulässig. Dies gilt etwa dann, wenn ein gültiger auslandsgeheimdienstlicher Zweck vorliegt oder die Erhebung der Spionageabwehr dient. Die Datenerhebung scheint nur insoweit beschränkt zu sein, dass bestimmte Zwecke ausgeschlossen sind. So darf die Erhebung etwa nicht erfolgen, um die Meinungsfreiheit zu unterdrücken oder zu erschweren, Personen

[224] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 92; EuGH, Digital Rights Ireland Ltd. (Fn. 48), Tz. 51. Näher hierzu bereits oben Ziffer 5.3.2.2 (3).
[225] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 90.
[226] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 94.
[227] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 91.
[228] Europäische Kommission – Pressemitteilung vom 02.02.2016, http://europa.eu/rapid/press-release_IP-16-216_de.htm.
[229] Vgl. hierzu näher Anhang VI (Fn. 193).

zu diskriminieren oder um den USA wirtschaftliche Wettbewerbsvorteile zu verschaffen. Grundsätzlich müssen Daten „so zugeschnitten wie machbar“ („as tailored as feasible“) erhoben werden. Wo immer praktikabel, soll die Erhebung bestimmter Daten der massenhaften Erhebung vorgezogen werden.[230] Wenn möglich, sollen andere verfügbare Informationsquellen vorrangig genutzt werden.[231] Dabei sind die Begriffe „machbar“ und „praktikabel“ zwar nicht frei, sondern im Sinne bestimmter behördlicher Richtlinien auszulegen. Wo die Erhebung begrenzter Daten oder die Nutzung anderer Quellen aber nicht „machbar“ bzw. „praktikabel“ ist, dürfen Daten dann offenkundig auch massenhaft erhoben werden. Auch unter Geltung der PPD-28 wird sogar ausdrücklich zugestanden, dass die Geheimdienste in bestimmten Fällen massenhaft Daten erheben dürfen, um „neue oder wachsende Bedrohungen“ zu identifizieren und andere für die nationale Sicherheit wichtige Informationen zu erhalten, die oft „innerhalb des großen und komplexen Systems moderner globaler Kommunikation versteckt“ sind.[232]

Dennoch sollen die Geheimdienste nicht jede theoretisch mögliche Maßnahme ergreifen dürfen, sondern an eine Art Verhältnismäßigkeitsgrundsatz gebunden sein. Insoweit sollen sie Abwägungen zwischen der praktischen Notwendigkeit ihrer Aktivitäten und ihren Bemühungen zum Schutz von Daten und bürgerlichen Freiheiten vornehmen.

Daten, die massenhaft erhoben wurden, dürfen dann „nur“ für sechs spezifische Zwecke verwendet werden[233], nämlich

- um bestimmte Aktivitäten fremder Mächte zu entdecken und ihnen zu begegnen;
- zur Terrorismusbekämpfung;
- zur Bekämpfung der Verbreitung von Massenvernichtungswaffen;
- zu Zwecken der Cybersicherheit;
- um Bedrohungen der US-Streitkräfte oder verbündeter Streitkräfte zu entdecken oder ihnen zu begegnen und
- zur Bekämpfung transnationaler krimineller Bedrohungen, einschließlich der Umgehung von Sanktionen.

Die US-Amerikaner sehen hierin eine „bedeutende und transparente Einschränkung“ der Nutzung von Massendaten. Massenhafte Datenerhebungen würden ohnehin nur „in einem kleinen Teil des Internets“ durchgeführt.[234] Schließlich erwähnt Anhang VI ausdrücklich, dass die USA die Anwendung bestimmter geheimdienstlicher Methoden oder Operationen bezüglich Daten, die unter dem „Privacy Shield“ in die USA übermittelt werden, weder bestätigen noch ausschließen wollen.[235]

Die Anpreisung dieser vermeintlichen „Einschränkungen“ hat bislang überwiegend Kritik nach sich gezogen. Teilweise wird von einer „Farce“ gesprochen.[236] Bürgerrechtsorganisationen wie EDRi[237]

---

[230] Vgl. Anhang IV (Fn. 193) S. 3 und Erwägungsgrund 59 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[231] Vgl. Anhang IV (Fn. 193) S. 3 und Erwägungsgrund 58 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[232] Vgl. Anhang VI (Fn. 193), S. 3. Kritisch hierzu auch http://www.spiegel.de/netzwelt/netzpolitik/privacy-shield-eu-und-usa-versprechen-ein-bisschen-datenschutz-a-1079875.html.
[233] Vgl. Anhang VI (Fn. 193), S. 4 sowie die FAQ-Liste der Kommission (Fn. 184); vgl. auch http://www.spiegel.de/netzwelt/netzpolitik/privacy-shield-eu-und-usa-versprechen-ein-bisschen-datenschutz-a-1079875.html.
[234] Vgl. Anhang VI (Fn. 193), S. 4.
[235] Vgl. Anhang VI (Fn. 193), S. 6.
[236] http://www.spiegel.de/netzwelt/netzpolitik/privacy-shield-eu-und-usa-versprechen-ein-bisschen-datenschutz-a-1079875.html.

sowie der Verein digitalcourage[238] kritisieren, dass die USA keine nennenswerten Reformen durchgeführt haben und solche auch nicht geplant seien. Gegenüber der Rechtslage bei „Safe Harbour“ habe sich kaum etwas verändert.[239] Die US-Amerikaner seien nicht willens, irgendetwas an ihrem Verhalten zu ändern. Kritisiert wird auch, dass die Aufsichtssysteme, die die Arbeit der US-Geheimdienste überwachen sollen, sich in der Vergangenheit als „zahnlos“ erwiesen haben.[240]

In der Tat sind die Zwecke sehr weit gefasst, so dass massenhafte Datenerhebungen weiter in nicht unerheblichem Umfang möglich zu sein scheinen. Die vielschichtigen Befugnisse und Begrenzungen sind komplex und auf den ersten Blick wenig „klar und präzise“. Darüber hinaus ist zweifelhaft, ob das amerikanische Verständnis der Begriffe „machbar“, „praktikabel“ und „verhältnismäßig“ bzw. „notwendig“ sich mit dem demjenigen innerhalb der EU deckt. Dabei ist zu berücksichtigen, dass der EuGH eine Beschränkung auf das „*absolut Notwendige und Verhältnismäßige*“ für einen bestimmten legitimen Zweck gefordert hat.[241] Unklar ist, wie die Notwendigkeitsprüfung in den USA erfolgt und ob darüber hinaus eine weitere Prüfung vorgenommen werden muss. Soweit tatsächlich Abwägungen vorgenommen werden, stellt sich die Frage, wieviel Gewicht der Privatsphäre gegenüber den nationalen Sicherheitsinteressen der USA hierbei in der Praxis tatsächlich beigemessen wird. Hinzu kommt, dass der EuGH die unbegrenzten Zugriffe durch Sicherheitsbehörden nicht lediglich als „einfache“ Eingriffe in das Grundrecht auf Achtung der Privatsphäre, sondern als derart schwerwiegende Maßnahmen gewertet hat, die den *Wesensgehalt* von Art. 7 GRC verletzen. Die Begrenzung von Eingriffen in den USA müsste demnach so umfassend sein, dass der Wesensgehalt der Art. 7, 8 GRC geachtet wird. Eine „absolute“ Notwendigkeit im Sinne der EuGH-Rechtsprechung scheint in den USA aber nicht erforderlich zu sein. Aufgrund unterschiedlicher Begrifflichkeiten und des wohl noch immer abweichenden Stellenwerts der Privatsphäre in den USA ist nicht gewährleistet, dass etwa vorzunehmende Abwägungen dort in der Praxis zu vergleichbaren Ergebnissen wie in der EU führen. Damit erscheinen die vom EuGH geforderten Grenzen aus Sicht des cep insoweit enger als die in Anhang VI geregelten Beschränkungen und Garantien. Sie würden bei einer derart fortgesetzten geheimdienstlichen Praxis daher wohl weiterhin überschritten.

Schließlich ist auch insoweit unklar, welche Rechtswirkung die schriftlichen Zusagen in Anhang VI haben. Soweit der Brief zusätzliche Garantien enthalten soll, ist wiederum fraglich, ob die Veröffentlichung im US-Bundesregister dazu führt, dass insoweit von einer „staatlichen Regelung“ zur Begrenzung von Eingriffen gesprochen werden kann, die der EuGH wohl für erforderlich hält. Dafür spricht, dass der Gerichtshof im „Schrems-Urteil“ gerügt hatte, die Kommission habe die Existenz entsprechender staatlicher Regelungen in den USA nicht geprüft. Ferner sind die US-Geheimdienste und -behörden nur an die im Brief aufgelisteten Beschränkungen gebunden, nicht aber zur Einhaltung der „Privacy Principles“ verpflichtet. Dies hatte der Gerichtshof ebenfalls bemängelt.

---

[237] European Digital Rights, eine internationale Vereinigung von Bürgerrechtsorganisationen zum Schutze der Privatsphäre und der Freiheit der Bürger in der Informationsgesellschaft. Vgl. ihr gemeinsames Positionspapier mit accessnow unter https://edri.org/files/WP29Submission%28Final%29-1.pdf.

[238] https://digitalcourage.de/blog/2016/safe-harbour-ungueltig-privacy-shield-ist-nicht-die-loesung.

[239] https://edri.org/privacy-shield-is-the-same-unsafe-harbour/.

[240] http://www.spiegel.de/netzwelt/netzpolitik/privacy-shield-eu-und-usa-versprechen-ein-bisschen-datenschutz-a-1079875.html.

[241] Vgl. oben Ziffer 5.3.2.2 (3).

All dies spricht dafür, dass die in Anhang VI geregelten Beschränkungen und Garantien noch immer nicht ausreichen, um die über den „Privacy Shield“ übermittelten personenbezogenen Daten aus der EU hinreichend vor Zugriffen durch US-amerikanische Geheimdienste zu schützen.[242]

Klarheit darüber, in welchem Umfang US-Geheimdienste tatsächlich auf über den „Privacy Shield“ übermittelte Daten zurückgreifen werden, kann auch künftig nicht erwartet werden. Denn die Erstellung von „Reports“ durch zertifizierte Unternehmen über den Umfang der Zugriffsanfragen durch US-Behörden zu Zwecken der nationalen Sicherheit oder Strafverfolgung ist freiwillig und nur zulässig, soweit das anwendbare US-Recht die Offenlegung erlaubt.[243]

Eine unzureichende Begrenzung von Zugriffen kann sich nicht zuletzt auch negativ auf das Wirtschaftswachstum auswirken. Denn wenn Bürger wegen der massenhaften Verarbeitung ihrer personenbezogenen Daten durch Privatunternehmen besorgt sind oder weiterhin befürchten müssen, dass ihre Daten bei der Nutzung von Internetdiensten durch Geheimdienste überwacht werden, könnte dies ihrem Vertrauen in die digitale Wirtschaft schaden.[244]

8.3.3.4 Schaffung eines wirksamen (gerichtlichen) Rechtsschutzes

Der EuGH hat die „Safe Harbour“-Entscheidung auch deshalb für ungültig erklärt, weil es in den USA an administrativen oder gerichtlichen Rechtsbehelfen fehlte, mit deren Hilfe die Betroffenen Zugang zu ihren personenbezogenen Daten oder deren Berichtigung oder Löschung erwirken konnten. Auch hierin sah der EuGH eine Verletzung des Wesensgehalts eines Grundrechts, nämlich des in Art. 47 GRC verankerten Rechts des Einzelnen auf gerichtlichen Rechtsschutz.[245] Ferner bemängelte der Gerichtshof, dass die Kommission keine Feststellungen zum Bestehen eines gerichtlichen Rechtsschutzes insbesondere gegen Grundrechtseingriffe durch staatliche Maßnahmen getroffen habe.[246] Um diesen Anforderungen Rechnung zu tragen, müssten die genannten Rechtsbehelfe nunmehr für Betroffene aus der EU, deren personenbezogene Daten über den „Privacy Shield“ übermittelt werden, zur Verfügung stehen. Unter dem „Privacy Shield“ sollen laut der Mitteilung der Kommission[247] „verschiedene Rechtsbehelfe“ für EU-Bürger in den USA bestehen oder noch etabliert werden:

(1) EU-Bürger können datenschutzrechtliche Beschwerden direkt an die US-Unternehmen richten, die von diesen Unternehmen innerhalb von 45 Tagen beantwortet werden müssen.[248]

(2) Es soll ein kostenloses Verfahren zur alternativen Streitbeilegung geben. US-Unternehmen müssen zu diesem Zweck eine unabhängige Streitbeilegungsstelle in der EU oder den USA benennen, die sich mit Individualbeschwerden befasst und eine Entscheidung hierzu trifft.[249]

(3) Die EU-Datenschutzbehörden können Beschwerden an das US-Handelsministerium[250] und an die FTC weiterleiten, die sodann eine Lösung suchen und innerhalb von maximal 90 Tagen eine Rückmeldung über den Status der Bearbeitung geben sollen. Die FTC verspricht in Anhang IV,

---

[242] Ähnlich der Bericht in Spiegel Online, wonach der Zugriff der US-Geheimdienste nicht substanziell beschnitten wird, vgl. http://www.spiegel.de/netzwelt/netzpolitik/privacy-shield-eu-und-usa-versprechen-ein-bisschen-datenschutz-a-1079875.htm.
[243] Vgl. Ziffer 16 der Privacy Principles, Anhang II (Fn 187).
[244] So bereits im Jahr 2013 die Kommission, Mitteilung (2013) 846 (final) (Fn. 1), Ziffer 1.
[245] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 90, 95. Vgl. bereits oben Ziffer 5.3.2.2 (4).
[246] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 89. Vgl. bereits oben Ziffer 5.3.2.2 (4).
[247] Europäische Kommission – Pressemitteilung vom 02.02.2016, http://europa.eu/rapid/press-release_IP-16-216_de.htm
[248] Vgl. Erwägungsgrund 30 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[249] Vgl. Erwägungsgrund 31 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[250] Vgl. Erwägungsgrund 36 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).

der Durchsetzung des „Privacy Shields“ bzw. der Bearbeitung der an sie weitergeleiteten Beschwerden „hohe Priorität“ einzuräumen.[251]

(4) Ein „mechanism of last resort“ in Form eines bindenden Schiedsverfahrens in den USA soll sicherstellen, dass jeder Fall geprüft wird und Entscheidungen bindend und durchsetzbar sind. Er soll nur zum Tragen kommen, wenn einer Individualbeschwerde nicht auf einem der anderen Wege zufriedenstellend abgeholfen werden kann.[252] Hierzu soll ein sogenanntes „Privacy Shield Panel“ aus mindestens 20 Schiedsrichtern errichtet werden, die vom US-Handelsministerium und der Kommission ernannt werden. Die Regeln des Schiedsverfahrens müssen noch im Einzelnen erarbeitet werden. Bestimmte Kosten für die anwaltliche Vertretung vor diesem Panel sollen durch einen Fonds des US-Handelsministeriums weitgehend gedeckt werden. Entscheidungen des Panels können unter dem US Federal Arbitration Act ggf. vor US-Gerichten durchgesetzt werden.[253] Für bestimmte Verstöße gegen US-Recht stehen ggf. weitere Rechtsbehelfe zur Verfügung.

(5) Für Beschwerden, die den möglichen Zugriff durch nationale Nachrichtendienste betreffen, soll auf Ebene des US-Außenministeriums eine „Ombudsperson“ geschaffen werden, die Anfragen und Beschwerden von EU-Bürgern beantworten soll.[254] Diese Ombudsperson soll unabhängig von den US-Geheimdiensten sein und wirksame Befugnisse haben. So soll sie von den Geheimdiensten auch geheime Informationen über konkrete Fälle anfordern können, um zu klären, ob deren Vorgehen rechtens war.[255] Allerdings können die Betroffenen die Ombudsperson nicht direkt anrufen, sondern müssen sich an die zuständige Behörde in ihrem Mitgliedstaat oder an eine zentrale, noch zu schaffende EU-Behörde wenden, die solche Beschwerden entgegennimmt und über die dann die Kommunikation läuft. Der neue „Ombudsperson-Mechanismus“ soll sowohl für Daten zur Verfügung stehen, die über den „Privacy Shield“ in die USA gelangen als auch für solche, die über SCC, BCR oder einen der Ausnahmetatbestände des Art. 26 Abs. 1 DSRL an US-amerikanische Empfänger transferiert werden.[256] Die Ombudsperson soll von einem im Einzelnen noch unklaren Mitarbeiterstab von Bediensteten des Auswärtigen Amtes unterstützt werden.

Zweifelhaft ist, ob die unter dem „Privacy Shield“ möglichen Rechtsbehelfe in ihrer Gesamtschau ausreichen und Effektivität versprechen. Soweit in den USA noch eine „gerichtliche Übung“ in Datenschutzfragen fehlt, wird sich die Effizienz auch erst in der Praxis zeigen können. Ein Verfahren zur Alternativen Streitbeilegung (Alternative Dispute Resolution, „ADR“) war bereits unter „Safe Harbour“ vorgesehen.[257]

Aus Platzgründen kann eine Analyse der möglichen Verbesserungen des ADR-Verfahrens sowie des Schiedsverfahrens unter dem „Privacy Shield“ in dieser cepStudie nicht vorgenommen werden. Angemerkt werden soll lediglich kurz, dass die Streitbeilegungsstellen nach den „Privacy Principles“ auch bestimmte Sanktionen unterschiedlicher Härtegrade verhängen können. Genannt werden beispielsweise bestimmte Verpflichtungen zur Herstellung von Transparenz betreffend der Verstöße, Datenlöschungspflichten, Verlust von Siegeln oder Schadensersatz für infolge der Verlet-

[251] Vgl. Anhang IV (Fn. 191), Seite 1 und Seite 5 (Ziffer II).
[252] So Kommissarin Jourova am 02.02.2016, http://europa.eu/rapid/press-release_SPEECH-16-221_fr.htm.
[253] Vgl. Erwägungsgrund 46 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[254] Vgl. hierzu näher Anhang III (Fn. 190). Rechtsgrundlage hierfür ist Sect. 4 d) der Presidential Policy Directive 28 (PPD-28). Als Ombudsfrau soll die als Senior Coordinator tätige „Under Secretary of State “ Catherine Novelli eingesetzt werden.
[255] FAZ vom 04.02.2016, S. 19 „EU verteidigt Datenschutz-Kompromiss“.
[256] Vgl. S. 1 des Anhangs III zum Entwurf des „Privacy Shield“-Beschlusses (Fn. 190).
[257] Mitteilung COM (201) 847 (final) (Fn. 25), Ziffer 6.1.

zung erlittene Verluste. Wirksame Geldstrafen nach dem Muster der neuen DSGV[258] scheinen hingegen nicht vorgesehen zu sein. Vergleichbare Strafen, die vorrangig durch die FTC als Aufsichtsbehörde verhängt werden sollten, wären jedoch aus Sicht des cep zu befürworten.

Unklar ist, ob die vorgesehenen Rechtsbehelfe den Betroffenen hinreichenden „gerichtlichen Rechtsschutz“ im Hinblick auf ihre Rechte auf Zugang, Berichtigung und Löschung ihrer personenbezogenen Daten gewährleisten, welcher nach der Rechtsprechung des EuGH unabdingbar ist. Insoweit sehen die „Privacy Principles“ in den Ziffern II. 1. A vii), II. 6. und III. 8 ein Auskunftsrecht vor, das auf den ersten Blick demjenigen in Art. 12 DSRL ähnelt. Kommt das US-Unternehmen seiner Auskunftspflicht nicht nach, und führt auch der ADR-Mechanismus nicht weiter, kann als „letztes Resort“ das „Privacy Shield Panel“ angerufen werden. Dessen Entscheidungen sollen nach US-Recht unter dem Federal Arbitration Act vor einem Federal District Court überprüft oder durchgesetzt werden können.[259] Gewisse Zugangsrechte und rechtliche Durchsetzungsmöglichkeiten gegenüber den zertifizierten Unternehmen sind also vorhanden. Auch gegenüber Behörden sollen Betroffene unter dem „Privacy Shield“ sogenannte Anfragen unter dem Freedom of Information Act (FOIA) stellen und hierdurch offenbar Zugang zu den über sie gespeicherten Informationen verlangen können. Von dieser Regel gibt es allerdings zahlreiche Ausnahmen. Wird die Einsicht in solche Datensätze verweigert, sollen weitere administrative Rechtsbehelfe und solche vor den Bundesgerichten möglich sein.[260] Offen bleibt, ob all diese Rechtsbehelfe nicht nur theoretisch möglich, sondern in der Praxis für EU-Bürger tatsächlich ein gangbarer Weg sind. Hierzu wären weitere Informationen und eine detailliertere Analyse notwendig, die vorliegend nicht vorgenommen werden kann. Erst dann kann beurteilt werden, ob die Anforderungen des Art. 47 GRC erfüllt sind.

Weiter stellt sich die Frage, ob darüber hinaus unter dem „Privacy Shield“ ein effektiver *gerichtlicher* Rechtsschutz auch und gerade gegen staatliche Eingriffe möglich ist, welchen der Gerichtshof im „Schrems-Urteil“ ebenfalls gefordert hat.[261]

Der „Ombudsperson-Mechanismus“, der zur Überprüfung geheimdienstlicher Datenzugriffe dienen soll, stellt jedoch keinen „gerichtlichen“ Rechtsbehelf dar und schafft daher bereits aus diesem Grund kein Recht i.S.v. Art. 47 GRC. Weder scheint die Ombudsperson vollkommen unabhängig zu sein, noch ist das Verfahren öffentlich. Zwar soll die Ombudsperson unabhängig von den US-Geheimdiensten sein. Zweifelhaft ist jedoch, ob sie auch politisch unabhängig ist, da sie auf der Ebene des US-Außenministeriums angesiedelt ist.[262] Aufgabe der Ombudsperson ist es, an sie gerichtete Anfragen und Beschwerden zu prüfen und der sie anrufenden EU-Beschwerdestelle „innerhalb angemessener Zeit“ eine „adäquate Antwort“ zukommen zu lassen. Dabei ist sie jedoch lediglich befugt zu bestätigen, dass die Beschwerde ordnungsgemäß untersucht und dabei entweder festgestellt wurde, dass das US-Recht eingehalten oder aber dessen etwaige Verletzung behoben wurde. Weder wird angegeben, welcher Verstoß wie behoben wurde, noch äußert sich die Ombudsperson dazu, ob die Person des „Beschwerdeführers“ tatsächlich Gegenstand der

[258] Art. 79 Abs. 3 DSGV sieht bei bestimmten Verstößen gegen die DSGV Sanktionen in Höhe von bis zu 20 Milliarden Euro oder sogar bis zu 4% des weltweiten Umsatzes der Unternehmensgruppe vor. Diese saftigen Strafen können von Unternehmen nicht mehr ohne weiteres „einkalkuliert“ und in Kauf genommen werden.

[259] Vgl. Anhang II zum Entwurf des „Privacy Shield“-Beschlusses (vgl. Fn. 147), dort Annex E, sowie Erwägungsgrund 46 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 190).

[260] Vgl. Ziffer 5 des Anhangs VI zum Entwurf des „Privacy-Shield“-Beschlusses (Fn. 193) sowie Ziffer 5. des Anhangs III zum Entwurf des „Privacy Shield“-Beschlusses (Fn. 190).

[261] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 89.

[262] Aus diesem Grund zweifelt die derzeitige Europäische Ombudsfrau Emily O’Reilly an, dass der Ombudsmann seinen Namen verdient hat. Nach den Kriterien des Internationalen Ombudsmann-Instituts müsse ein Ombudsmann unabhängig sein und dürfe keiner Weisungsabhängigkeit gegenüber Behörden unterliegen, die seine Unabhängigkeit in Frage stelle, vgl. http://www.ombudsman.europa.eu/en/resources/otherdocument.faces/en/64157/html.bookmark.

Überwachung war.[263] Diesem Rechtsbehelf fehlt es somit an Transparenz und Nachvollziehbarkeit.[264] Weiterhin wird zu Recht bemängelt, dass die Ombudsperson zwar behauptete Rechtsverstöße an die zuständigen US-Regierungsstellen melden kann. Ob und inwieweit diese dann tätig werden, scheint sie jedoch nicht beeinflussen zu können.[265] Darüber hinaus ist noch unklar, welche Kapazitäten und Ressourcen die Ombudsstelle tatsächlich erhalten wird und ob diese ausreichen werden, um für Millionen von EU-Bürgern effektiven Rechtsschutz gegen behördliche Datenzugriffe zu gewährleisten.[266] Nicht zu Unrecht wird daher auch die fragwürdige Handlungsmacht der Ombudsperson kritisiert.[267] Schließlich ist nicht erkennbar, ob einem Beschwerdeführer aus der EU ein weiteres (gerichtliches?) Rechtsmittel zusteht, wann immer die Ombudsperson keine wirksame Abhilfe leisten kann oder deren Antwort den Beschwerdeführer nicht zufriedenstellt.

Auch der vieldiskutierte „Judicial Redress Act of 2015“[268] (JRA), der am 24.02.2016 von Präsident Obama unterzeichnet wurde und EU-Bürgern begrenzte Klagerechte unter dem US Privacy Act verschaffen soll,[269] hilft hier nicht weiter. Denn der JRA gilt nur für Daten, die zu Zwecken der Strafverfolgung oder der Gefahrenabwehr an US-Bundesbehörden übermittelt werden. Daten, die auf der Grundlage des „Privacy Shields“ zu kommerziellen Zwecken an Unternehmen in den USA übermittelt werden, werden dagegen vom JRA überhaupt nicht erfasst. Vermutlich aus diesem Grund wird der JRA im Entwurf des „Privacy Shield“-Beschusses auch überhaupt nicht erwähnt. Zudem gewährt der JRA die begrenzten Klagerechte nur EU-Bürgern. Alle Nicht-EU-Bürger, die dem EU-Recht unterliegen, bleiben in den USA weiter rechtlos. Hierzu gehören Studenten, Forscher oder Saisonarbeiter aus Drittländern oder Flüchtlinge, die sich in der EU aufhalten.[270] Selbst EU-Bürger erhalten jedoch nicht denselben Umfang an Rechten wie US-amerikanische „individuals“, sondern unterliegen Beschränkungen oder zusätzlichen Hürden in puncto Passivlegitimation oder Verschulden.[271]

---

[263] Vgl. Erwägungsgrund 104 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182) sowie Anhang III Ziffer 4 e) (S. 4) (Fn. 190).

[264] Vgl. auch http://www.spiegel.de/netzwelt/netzpolitik/privacy-shield-eu-und-usa-versprechen-ein-bisschen-datenschutz-a-1079875.html.

[265] https://www.datenschutzbeauftragter-info.de/privacy-shield-veroeffentlichter-text-verheisst-nichts-gutes/.

[266] Etwaige in Zukunft festgestellte Ressourcenengpässe sollen in Absprache mit der Kommission beseitigt werden, vgl. Ziffer 4. g) des Anhangs III zum Entwurf des „Privacy Shield“-Beschlusses (Fn. 190).

[267] Vgl. http://www.spiegel.de/netzwelt/netzpolitik/privacy-shield-eu-und-usa-versprechen-ein-bisschen-datenschutz-a-1079875.html sowie https://www.datenschutzbeauftragter-info.de/privacy-shield-veroeffentlichter-text-verheisst-nichts-gutes/.

[268] Der JRA (Text abrufbar unter https://www.govtrack.us/congress/bills/114/hr1428/text) wurde seit geraumer Zeit anlässlich der Verhandlungen des sogenannten „Umbrella Agreements“ (ein Rahmenabkommen zwischen EU und USA, das den Datenaustausch zu Strafverfolgungszwecken und der Gefahrenabwehr regeln soll), intensiv diskutiert. Das Abkommen, welches in Kürze von beiden Seiten ratifiziert werden soll, betrifft ausschließlich den Austausch personenbezogener Daten zwischen EU- und US-Behörden im Rahmen der Zusammenarbeit zu Strafverfolgungszwecken. Ein Entwurf des Abkommens ist abrufbar unter http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf. Nach einem vertraulichen Gutachten des juristischen Dienstes des Europäischen Parlaments verstößt das „Umbrella Agreement“ gegen EU-Primärrecht und die Achtung der Grundrechte, da es begrenzten gerichtlichen Rechtsschutz lediglich für EU-Bürger vorsieht, Nicht-EU-Bürger, die dem EU-Recht unterliegen, jedoch von sämtlichen gerichtlichen Rechtsschutz vorenthält (näher hierzu Statewatch News Online, http://statewatch.org/news/2016/feb/eu-umbrella-agreement.html sowie Legal Opinion des EP Legal Service vom 14.01.2016, http://statewatch.org/news/2016/feb/ep-legal-opinion-umbrella.pdf).

[269] Der JRA sieht vor, dass auch EU-Bürger unter dem „U.S. Privacy Act“ zivilrechtliche Klagen bei den US-Gerichten gegen bestimmte Behörden erheben können, um gegen die unrechtmäßige Offenlegung ihrer Daten vorzugehen. Bislang war dies nur US-Bürgern und -Einwohnern möglich.

[270] Gleiches dürfte für Bürger der EWR-Staaten Norwegen, Island und Liechtenstein gelten, die die DSRL übernommen haben.

[271] Ob der mit diesem JRA geschaffene Rechtsschutz effektiv ist und wirksame Rechtsbehelfe für EU-Bürger bietet, die den Anforderungen des Art. 47 GRC Genüge tun, wird nach alldem zu Recht bezweifelt. Zum einen erweitert der JRA die Klagerechte nur auf natürliche Personen, die Bürger eines designierten Staates sind. Hierin liegen gleich mehrere Einschränkungen: Die EU muss sich als „würdig“ erweisen, von den USA eine solche Designation zu erhalten. Dazu muss die EU (1) entweder ein Datenschutzabkommen mit den USA betreffend den Austausch von Daten zum Zwecke der Strafverfolgung unterzeichnen und einhalten oder effektiv Daten zu solchen Zwecken mit den USA ausgetauscht

Auch die Kompetenzen des „FISA Court“, der die unter dem „Foreign Intelligence Surveillance Act“ (FISA) (insbesondere dessen Section 702) durchgeführte Datenerhebung gerichtlich überwachen soll,[272] scheinen sich auf sogenannte „Überwachungsbeschlüsse“ und dabei insbesondere die Eingrenzung von Überwachungsvorhaben zu beschränken. Von betroffenen Personen kann er hingegen offenbar nicht angerufen werden.

Der Rechtsbehelf des Ombudsmanns basiert zwar auf der PPD-28, wonach für ausländische Regierungen, die gegen US-Geheimdienstaktivitäten Bedenken äußern, eine Kontaktperson eingesetzt werden kann.[273] Die Einsetzung der Ombudsperson für die EU sowie deren Kompetenzen werden aber in den USA vermutlich auch nicht weiter gesetzlich geregelt, was aus Sicht des cep jedoch erforderlich wäre. Etabliert wurde der „Ombudsmann-Mechanismus“ offenkundig, weil die bestehenden Rechtsbehelfe in den USA gegen die unrechtmäßige elektronische Überwachung zum Zwecke der nationalen Sicherheit nach ausdrücklicher Feststellung der Kommission[274] nicht für alle Rechtsgrundlagen gelten, die von US-Geheimdiensten genutzt werden können, oder weil der Umfang dieser Rechtsbehelfe beschränkt ist. Nach dem oben Gesagten spricht jedoch einiges dagegen, dass diese von der Kommission erkannten Lücken im Rechtsschutz mit Hilfe des „Ombudsmann-Mechanismus“ geschlossen und insoweit ein effektiver Rechtsschutz gegen staatliche Zugriffe auf personenbezogene Daten geschaffen werden kann.

Zusammengefasst lässt der „Ombudsmann-Mechanismus“ nach vorläufiger Einschätzung des cep folgende Mängel erkennen:

- offenbar fehlende gesetzliche Regelung und daher fragwürdige rechtliche Bindungswirkung;
- mangelnde Transparenz und Nachvollziehbarkeit der Entscheidungen;
- unklarer Umfang der Ressourcen und Kapazitäten der Ombudsstelle;
- fragwürdiges „Schicksal“ von Beschwerden oder Anfragen, die an US-Regierungsstellen weitergeleitet werden;
- kein darüber hinausgehender Rechtsschutz / kein weiteres Rechtsmittel gegen dessen Entscheidung;
- kein „gerichtlicher“ Rechtsschutz i.S.v. Art. 47 GRC.

8.3.3.5 Keine Beschränkung der Befugnisse von EU-Datenschutzbehörden

Ferner darf der „Privacy Shield“-Beschluss die Kontroll- und Durchführungsbefugnisse der nationalen Kontrollstellen in den EU-Mitgliedstaaten nicht beschränken. So darf er etwa keine restriktiveren Regeln für die Aussetzung der Datenübermittlung zu Datenschutzzwecken vorsehen als die

haben, (2) Datentransfers in die USA zu wirtschaftlichen Zwecken durch ein Abkommen oder anderweitig erlauben und (3) durch ihre EU-Datenschutzregelungen zum Schutz personenbezogener Daten die nationalen Sicherheitsinteressen der USA nicht wesentlich behindern. Hält die EU diese Voraussetzung nicht ein, kann die Designation wieder entzogen werden. EU-Bürger verlören dann ihr Klagerecht. Ungeachtet dieser Einschränkungen soll die Durchsetzung von Rechten gegen den behördlichen Datenzugriff angesichts der bestehenden Hürden auch für US-Amerikaner schwierig sein (näher hierzu Kühling/Heberlein, NVwZ 2016, S. 7 (11)). Diese bemängeln auch, dass der JRA weitreichende Ausnahmen vorsehe, die auch auf Geheimdienste anwendbar sein können, und die Bedingungen des EuGH daher gerade nicht erfülle. Kritiker bezeichnen den JRA daher als „Farce“, vgl. http://www.heise.de/ct/artikel/Datenschutz-fuer-Europaeer-US-Repraesentantenhaus-winkt-Farce-durch-2851826.html.

[272] Vgl. Ziffer II des Anhangs VI zum Entwurf des „Privacy Shield“-Beschlusses (Fn. 193).

[273] Vgl. S. 1 des Anhangs III zum Entwurf des „Privacy Shield“-Beschlusses (Fn. 190).

[274] Vgl. Erwägungsgrund 99 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).

DSRL bzw. die DSGV. Denn ansonsten würden den nationalen Kontrollstellen in den EU-Mitgliedstaaten durch die Hintertür wiederum Befugnisse entzogen. Art. 25 Abs. 6 DSRL als reine Durchführungsbefugnis gibt der Kommission hierzu keine Ermächtigung, sodass die Kommission insoweit ihre Zuständigkeit überschreiten würde. Eine solche Regelung wäre daher ungültig.[275] Der Entwurf des „Privacy Shield“-Beschlusses enthält nach kursorischer Durchsicht keine dem Art. 3 der „Safe Harbour“-Entscheidung vergleichbare Regelung restriktiverer Befugnisse der nationalen Kontrollstellen. Zudem sieht Art. 3 dieses Entwurfs vor, dass die EU-Mitgliedstaaten eine etwaige Aussetzung oder Untersagung des Datentransfers an ein zertifiziertes Unternehmen der Kommission melden müssen. US-Unternehmen, die mit aus der EU übermittelten Personaldaten arbeiten, müssen sich verpflichten, Entscheidungen der EU-Datenschutzbehörden nachzukommen.[276] Allgemein soll die Zusammenarbeit mit den EU-Datenschutzbehörden gestärkt werden.[277] All dies spricht dafür, dass der „Privacy Shield“-Beschluss die Befugnisse der Kontrollstellen nicht einschränkt. Allerdings hebt die Kommission in Erwägungsgrund 119 des „Privacy Shield“-Beschlusses die grundsätzliche Bindungswirkung des Angemessenheitsbeschlusses für die EU-Mitgliedstaaten und die nationalen Datenschutzbehörden hervor. Diese müssten bei Beschwerden, die die Vereinbarkeit dieser Kommissionsentscheidung mit dem Schutz der Grundrechte auf Datenschutz und Achtung der Privatsphäre in Frage stellen, die ihnen aufgrund nationalen Rechts zustehenden Möglichkeiten nutzen, nationale Gerichte anzurufen und auf diesem Weg eine Vorabentscheidung durch den EuGH zu erzwingen. In diesem Zusammenhang ist jedoch an die Feststellung des Gerichtshofs im „Schrems-Urteil“ zu erinnern, wonach die nationalen Kontrollstellen auch bei Vorliegen einer grundsätzlich bindenden Angemessenheitsentscheidung in völliger Unabhängigkeit prüfen dürfen, ob bei der Übermittlung dieser Daten die in der DSRL aufgestellten Anforderungen gewahrt werden.[278] Dabei hat der Gerichtshof betont, dass in der EU als Rechtsunion die nationalen Datenschutzbehörden auch eine Kontrollfunktion dahingehend haben, ob die Handlungen der Kommission mit den Verträgen, den allgemeinen Rechtsgrundsätzen und den Grundrechten in Einklang stehen.[279] Sowohl die nationalen Kontrollstellen als auch die nationalen Gerichte dürfen daher die Angemessenheit des Schutzniveaus und damit die Gültigkeit der neuen Angemessenheitsentscheidung inzident prüfen, wenn auch wegen des Verwerfungsmonopols des EuGH die etwaige Ungültigkeit nicht verbindlich feststellen. Der Aufruf des EuGH an die EU-Mitgliedstaaten, eine Art Normenkontrollklagerecht für die Kontrollstellen einzurichten, schränkt jedoch nach Auffassung des cep die übrigen Befugnisse der Kontrollstellen im Einzelfall nicht ein.[280] Ob sich die nationalen Datenschutzbehörden „trauen“ werden, einzelne Datentransfers an unter dem „Privacy Shield“ zertifizierte Unternehmen nach Inkrafttreten der Angemessenheitsentscheidung unter Berufung auf den mangelnden Schutz im konkreten Fall auszusetzen, bleibt abzuwarten.

8.3.3.6 cep-Zwischenfazit

Die vorgenommene kursorische Prüfung ergibt, dass der Schutz unter dem „Privacy Shield“ zwar auf dem Papier erkennbar gegenüber „Safe Harbour“ verbessert wurde, der Entwurf des „Privacy Shield“-Beschlusses jedoch trotzdem nicht allen Vorgaben des EuGH im „Schrems-Urteil“ vollumfänglich Rechnung trägt oder insoweit zumindest Zweifel aufwirft. Insoweit wurden mehrere Kritikpunkte herausgearbeitet.

---

[275] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 102-104.
[276] Vgl. Erwägungsgrund 42 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[277] Europäische Kommission – Pressemitteilung vom 02.02.2016, http://europa.eu/rapid/press-release_IP-16-216_de.htm. Eine solche Zusammenarbeit gab es im begrenzten Umfang allerdings bereits unter „Safe Harbour“, vgl. Mitteilung COM (201) 847 (final) (Fn. 25), Ziffer 5.1.
[278] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 57.
[279] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30), Tz. 60 m.w.N. zur insoweit „ständigen Rechtsprechung“ des Gerichtshofs.
[280] Siehe hierzu auch die ähnliche Diskussion oben unter Ziffer 7.1.2.3.

Der „Privacy Shield“ ist weder ein internationales Abkommen,[281] noch ist damit zu rechnen, dass seine Inhalte in den USA in Gesetzesform gegossen werden. Die Kommissionsentscheidung sollte jedoch aus cep-Sicht durch ein entsprechendes völkerrechtliches Abkommen mit den USA abgesichert werden. Zugleich sollten seine Inhalte in den USA rechtlich bindend umgesetzt, also idealerweise entsprechende Gesetze erlassen und deren Einhaltung und Durchsetzung durch wirksame Sanktionen sichergestellt werden, wie sie nunmehr in der künftigen DSGV zu finden sind.[282] Dies würde auf US-Seite eine gewisse Rechtssicherheit schaffen und das Risiko mangelnder Kontinuität ausschließen. Ohne ein völkerrechtliches Abkommen und ohne Änderungen mit Gesetzescharakter können die schriftlichen Zusicherungen bei einem politischen Wechsel in den USA infolge der Präsidentschaftswahlen leicht zurückgenommen oder eingeschränkt werden. Inwieweit die Veröffentlichung im US-Bundesregister dieses Risiko eingrenzt, ist fraglich.

Die Kommission hingegen scheint munter auf die Zusicherungen der USA zu vertrauen. Wesentliches „Druckmittel“ der Kommission gegenüber der Einhaltung des „Privacy Shields“ durch die USA scheint dessen eventuelle Aussetzung, Aufhebung oder Änderung im Fehlverhaltensfall zu sein. Die Kommission kündigt an, künftig von diesen Möglichkeiten effektiv Gebrauch machen zu wollen.[283] Eine Aussetzung wurde – obwohl von den EU-Datenschutzbehörden gefordert – von der Kommission aber auch schon bei „Safe Harbour“ nicht vorgenommen, weil dies nach ihrer Auffassung den Interessen der beteiligten Unternehmen in der EU und den USA geschadet hätte.[284] Die Interessenlage hat sich jedoch keineswegs geändert.[285] Im Hinblick auf die Tatsache, dass sämtliche auf dem „Privacy Shield“ beruhenden transatlantischen Datenflüsse dann unter Umständen ersatzlos gestoppt werden müssten, wird eine Aussetzung auch künftig politisch heikel sein und in wirtschaftlicher Hinsicht die beteiligten Unternehmen vor immense Probleme stellen. Denn im Falle einer Aussetzung der Entscheidung stünden diese wiederum ohne Rechtsgrundlage da, es sei denn, sie könnten auf eine funktionsfähige alternative Transfergrundlage zurückgreifen. Um dies gewährleisten zu können, müssten Unternehmen unter Umständen „zweigleisig“ fahren. Die Verwendung von SDPC, BCR und Co. ist jedoch angesichts der dargestellten Defizite im US-amerikanischen Recht ebenfalls problematisch.[286] Der Erlass eines fragwürdigen Angemessenheitsbeschlusses nach dem Motto „wenn es nicht funktioniert, setzen wir die Entscheidung eben aus“ wird daher weder dem Interesse der Wirtschaft an einer langfristigen rechtssicheren Lösung für transatlantische Datentransfers noch dem Interesse der Dateninhaber an einem fortgesetzten angemessenen Schutz ihrer personenbezogenen Daten in den USA gerecht.

Grundsätzlich sinnvoll ist es, dass der „Privacy Shield“-Beschluss nicht mehr auf Jahre in Stein gemeißelt bleiben, sondern in jährlichen Abständen unter Einbeziehung der EU- Datenschutzbehörden und anderer Experten überprüft werden soll. Diese dynamische Prüfung geht sogar über die DSGV hinaus, welche für Angemessenheitsentscheidungen eine Überprüfung in mindestens vierjährigem Turnus vorschreibt.[287] Ob aber eine jährliche Prüfung bei einem derart komplexen Konstrukt im Detail möglich ist und festgestellte Mängel zeitnah behoben werden können oder – andernfalls – die Kommission von der Aussetzungsmöglichkeit tatsächlich Gebrauch machen wird, ist fraglich. In jedem Fall müssen Unternehmen, die sich nach den Vorgaben der neuen Angemessenheitsentscheidung auf Basis des „Privacy Shields“ zertifizieren lassen wollen, damit rechnen, dass

[281] Vgl. auch die Aussage von Justizkommissarin Jourová in ihrer Rede vom 01.02.2016, http://europa.eu/rapid/press-release_SPEECH-16-208_de.htm.
[282] Vgl. Fn. 254.
[283] Communication from the Commission to the European Parliament and the Council vom 29.02.2016, COM(2016) 117 final, “Transatlantic Data Flows: Restoring Trust through Strong Safeguards”, Ziffer 3.2 a. E., abrufbar unter http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.
[284] Vgl. Mitteilung der Kommission COM(2013) 846 (final) (Fn. 1), Ziffer 3.2.
[285] Kritisch insoweit auch die Bürgerrechtsorganisation EDRi, https://edri.org/privacy-shield-is-the-same-unsafe-harbour/.
[286] Vgl. hierzu bereits oben Ziffer 7.1 sowie unten Ziffer 8.3.6.
[287] Vgl. Art. 41 Abs. 3 DSGV.

hier künftig Anpassungsbedarf bestehen kann und sodann weitere „Arbeit“ auf sie zukommen wird.

Die Rechtsunsicherheit für Unternehmen wird zusätzlich dadurch gesteigert, dass vermutlich über kurz oder lang der EuGH mit der Gültigkeit des „Privacy Shield“-Beschlusses befasst werden wird. Ob der „Privacy-Shield“-Beschluss vor dem EuGH Bestand haben oder das gleiche Schicksal wie die „Safe Harbour“-Entscheidung erleiden wird, oder nach dessen Vorgaben korrigiert werden muss, ist unklar.

Ein solches Schicksal des „Privacy Shield“-Beschlusses erscheint nach vorläufiger Bewertung nicht ganz unwahrscheinlich. Denn nach dem oben Gesagten bestehen gewisse Zweifel daran, dass die vorgesehenen Kontrollen und Sanktionen effektiv genug sind, um in der Praxis eine Einhaltung der rein durch Selbstverpflichtung auferlegten Prinzipien zu gewährleisten. Auch die angepriesenen Beschränkungen der Zugriffsmöglichkeiten US-amerikanischer Geheimdienste gehen nicht weit genug. Ferner wird ein wirksamer gerichtlicher Rechtsschutz gegen staatliche Eingriffe auch unter dem „Privacy Shield“ noch immer nicht gewährleistet. Der neue „Ombudsperson-Mechanismus“ allein erfüllt die Vorgaben des EuGH nicht.

Auch von Fachleuten und der Presse wird der Entwurf des „Privacy Shield“-Beschlusses weithin kritisiert. Der „Privacy Shield“ enthalte zwar einige Verbesserungen, das grundsätzliche Problem der US-Massenüberwachungen und der Nichtexistenz von Datenschutz seien nicht gelöst.[288] Andere sprechen von einem „löchrigen Datenschutzschild.“[289]

Insgesamt besteht die Gefahr, dass der „Privacy Shield“-Beschluss langfristig nicht die sichere Rechtsgrundlage sein könnte, die sich viele Unternehmen erhoffen.

Das cep fordert daher insbesondere:

- zusätzliche Kontrollen, etwa in Form anlassloser, regelmäßiger, unangekündigter und flächendeckender Überprüfungen;
- evtl. Zertifizierungen durch eine unabhängige Stelle;
- abschreckende Sanktionen für US-Unternehmen nach dem Vorbild der neuen DSGV;
- die Schaffung zusätzlicher und insgesamt lückenloser gerichtlicher Rechtsschutzmöglichkeiten bzw. Anschlussrechtsmittel für Betroffene aus der EU;
- Setzung klarer und umfassend geltender Grenzen für Eingriffe und Definition der Begriffe „Erforderlichkeit und Verhältnismäßigkeit“;
- die Absicherung der Inhalte des „Privacy Shields“ durch ein völkerrechtliches Abkommen sowie
- eine bindende Verankerung der gemachten Zusicherungen in den USA mit Gesetzescharakter.

[288] So Max Schrems laut einem Bericht des „Spiegel“, vgl. http://www.spiegel.de/netzwelt/netzpolitik/privacy-shield-eu-und-usa-versprechen-ein-bisschen-datenschutz-a-1079875.html.

[289] http://www.heise.de/newsticker/meldung/Privacy-Shield-EU-Kommission-veroeffentlicht-Text-fuer-loechrigen-Datenschutzschild-3120502.html?view=print.

8.3.4 Zur Beurteilung der Angemessenheit des Schutzniveaus

Fraglich ist, ob die Bewertung des US-amerikanischen Datenschutzniveaus durch die Kommission als „adäquat“ (d.h. dem aus den EU-Datenschutzgrundsätzen sowie den EU-Grundrechten resultierenden Schutz im Wesentlichen gleichwertig) gerechtfertigt ist. Dabei müsste die Kommission insbesondere alle relevanten Umstände berücksichtigt haben. Ferner dürfte sie den ihr zustehenden Ermessensspielraum nicht überschritten haben.

8.3.4.1 Bei der Beurteilung zu berücksichtigende Umstände

Gemäß Art. 25 Abs. 1 DSRL muss die Kommission bei der Beurteilung der Angemessenheit des Schutzniveaus alle Umstände berücksichtigen, die bei Datenübermittlungen eine Rolle spielen, insbesondere die Art der Daten, Zweckbestimmung und Dauer der geplanten Verarbeitung, Herkunfts- und Endbestimmungsland, die in den USA geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen. Die DSGV listet die heranzuziehenden Aspekte künftig in Art. 41 Abs. 2 lit. a)- c) wesentlich detaillierter auf.[290] Auch wenn die DSGV noch nicht gilt, können und sollten wegen der weiten Formulierung in der DSRL bereits jetzt auch diese in der DSGV aufgelisteten Punkte bei der Beurteilung berücksichtigt werden. Diese umfassen:

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in den USA geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, einschließlich derjenigen über die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit, das Strafrecht und den Zugriff von Behörden auf personenbezogene Daten, sowie die Umsetzung dieser Rechtsvorschriften, Datenschutzbestimmungen, Standesregeln und Sicherheitsmaßnahmen, einschließlich der Vorschriften für die Weitergabe personenbezogener Daten an ein anderes Drittland oder eine internationale Organisation, juristische Präzedenzfälle sowie die Existenz wirksamer und durchsetzbarer Rechte der betroffenen Person und wirksamer administrativer und gerichtlicher Rechtsbehelfe für Personen, deren personenbezogene Daten übermittelt werden;

b) die Existenz und Wirksamkeit einer oder mehrerer unabhängiger Aufsichtsbehörden in den USA, die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Sanktionsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der EU-Mitgliedstaaten zuständig sind; und

c) die von den USA eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus der Teilnahme der USA an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

Anhand dieser Punkte gilt es zu ermitteln, welche datenschutzrechtlichen Risiken der Transfer personenbezogener Daten für die Betroffenen konkret birgt und welche Schutzelemente oder Garantien in den USA gegen diese zur Verfügung stehen. Im Ergebnis geht es um eine Bewertung der Wahrscheinlichkeit, ob die in den USA vorhandenen Garantien ausreichend sind, um den Risiken so

[290] Art. 41 DSGV bildet die künftige Grundlage für Angemessenheitsbeschlüsse der Kommission unter der DSGV. Gemäß Art. 41 Abs. 1 DSGV dürfen personenbezogene Daten ohne weitere Genehmigung in ein Drittland, ein Gebiet oder Verarbeitungssektor dieses Drittlands oder an eine internationale Organisation übermittelt werden, wenn die Kommission nach umfassender Prüfung im Beschlusswege festgestellt hat, dass das betreffende Drittland, dessen Gebiet oder Verarbeitungssektor oder die internationale Organisation einen angemessenen Schutz bietet. Nunmehr ist ausdrücklich geregelt, dass die Kommission eine solche Entscheidung auf ein bestimmtes geographisches Gebiet oder einen oder mehrere spezifische Sektoren eines Drittlands beschränken kann. Ferner sind die Punkte, welche die Kommission unter Geltung der DSGV bei der Prüfung der Angemessenheit des Schutzniveaus berücksichtigen muss, nunmehr detaillierter aufgelistet.

zu begegnen, dass die Rechte und Freiheiten der betroffenen Person als geschützt angesehen werden können.[291]

Als derartige Schutzelemente und Garantien hat die Kommission offenkundig auch die „Privacy Principles“ sowie die übrigen Anhänge des „Privacy Shield“-Beschlusses gewertet und in ihre Beurteilung mit einbezogen, obwohl dies wegen des Wortlauts des Art. 25 Abs. 6 DSRL nicht unproblematisch erscheint.[292]

8.4.3.2 Eingeschränkter Wertungsspielraum der Kommission

Bezüglich der Beurteilung der Angemessenheit des gewährleisteten Schutzniveaus steht der Kommission ein gewisser Wertungsspielraum zu. Wie der EuGH im „Schrems-Urteil“ erneut festgestellt hat, ist dieser Spielraum der Kommission jedoch eingeschränkt. Der Gerichtshof hat dies mit der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung der Privatsphäre und der großen Zahl von Personen begründet, deren Grundrechte im Fall der Übermittlung personenbezogener Daten in ein Drittland ohne angemessenes Schutzniveau verletzt werden können. Danach muss die Kommission muss eine „strikte Kontrolle“ der Anforderungen vornehmen, die sich aus Art. 25 DSRL im Licht der GRC ergeben.[293]

8.3.4.3 Inhaltliche Vergleichbarkeit der „Privacy Principles“ mit den EU-Datenschutzgrundsätzen?

Angesichts des Fehlens allgemeingültiger Datenschutzgesetze in den USA will die Kommission die Gleichwertigkeit des Datenschutzniveaus in den USA vorliegend wie schon bei „Safe Harbour“ maßgeblich mit Hilfe der „Privacy Principles“ konstruieren.

Durch ihre Selbstverpflichtung zur Einhaltung dieser Prinzipien sollen die zertifizierten Unternehmen vergleichbaren Grundsätzen für die Erhebung und Verarbeitung personenbezogener Daten unterworfen werden, wie sie in der EU gelten. Die „Privacy Principles“ sind nach US-Recht auszulegen.[294] Damit die Angemessenheit des Schutzes bejaht werden kann, müssten die in den „Privacy Principles“ geregelten Auflagen inhaltlich im Wesentlichen den Regelungen der DSRL sowie der GRC entsprechen.

Die Kommission geht davon aus, dass die „Privacy Principles“ einen vergleichbaren Schutz bieten wie die grundlegenden Prinzipien der DSRL.[295] Von den Standards der DSGV ist hingegen nicht die Rede. Mit dem Inkrafttreten der DSGV in voraussichtlich zwei Jahren wird jedoch das Datenschutzniveau in der EU weiter steigen. Aus diesem Grund sollten die „Privacy Principles“ aus cep-Sicht bereits jetzt auf das Schutzniveau der DSGV abgestimmt werden. Ansonsten steht zu befürchten, dass die Prinzipien faktisch allenfalls für den Zeitraum bis zum Inkrafttreten der DSGV einen gleichwertigen Schutz bieten können. Denn spätestens beim nächsten jährlichen Review des „Privacy Shields“ nach Inkrafttreten der DSGV müsste die Kommission zu dem Ergebnis kommen, dass das Schutzniveau nicht mehr äquivalent ist, und die Entscheidung anpassen.[296] Spätestens dann wären Nachverhandlungen mit den USA erforderlich. Aus diesem Grund wird daher teilweise auch

[291] Grabitz/Hilf-Brühann, Das Recht der Europäischen Union, Band IV, 40. Auflage 2009, A 30 Rn. 10 ff.
[292] Zu dieser Problematik vgl. bereits oben Ziffer 8.3.3.1.
[293] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30)., Tz. 78 und EuGH, Digital Rights Ireland Ltd. , a.a.O. (Fn. 48), Tz. 48.
[294] Vgl. Ziffer I.8 des Anhangs II des „Privacy Shield“-Beschlusses (Fn. 187).
[295] Vgl. Erwägungsgrund 49, 113 des Entwurfs des „Privacy Shield“-Beschlusses (Fn. 182).
[296] Wie bereits ausgeführt, bliebe der „Privacy Shield“-Beschluss auch nach dem Inkrafttreten der DSGV gemäß Art. 41 Abs. 8 DSGV weiter in Kraft, bis er von der Kommission aufgehoben oder ersetzt wird.

eine Begrenzung des zeitlichen Geltungsbereichs des „Privacy Shield“-Beschlusses auf zwei Jahre gefordert.[297]

Nach der Ansicht von Kritikern wie Max Schrems sind die „Privacy Principles“ jedoch bereits vom Schutzniveau der DSRL weit entfernt.

Ein inhaltlicher Vergleich der „Privacy Principles“ mit den Standards der DSRL würde jedoch den Rahmen dieser cepStudie sprengen. Eine inhaltliche Prüfung der einzelnen Klauseln wird daher vorliegend nicht vorgenommen. Auch der EuGH hatte in der „Schrems“-Entscheidung auf eine inhaltliche Prüfung der „Safe Harbour“-Grundsätze verzichtet[298], da er die Entscheidung schon aus formellen Gründen für unwirksam erachtete.

8.3.4.4 Vergleichbarer Schutz im Übrigen durch die US-amerikanische Rechtsordnung und die Zusicherungen in den Anhängen?

Ergänzend zu den „Privacy Principles“ müsste die US-amerikanische Rechtsordnung (ggf. in Kombination mit den Zusicherungen in den Anhängen des Entwurfs des „Privacy Shield“-Beschlusses) auch im Übrigen einen adäquaten Schutz bieten, der sowohl den in der DSRL verankerten Rechten als auch den aus den EU-Grundrechten resultierenden Garantien der Sache nach gleichwertig ist.

Der EuGH hat sich im „Schrems-Urteil“ zur Angemessenheit des datenschutzrechtlichen Niveaus in den USA nicht dezidiert geäußert. Es spricht jedoch einiges dafür, dass er das Niveau nicht für gleichwertig hielt.[299]

Die Kommission hat nunmehr das Schutzniveau unter Berücksichtigung der Zusicherungen und Änderungen, die sich durch den „Privacy Shield“ bzw. durch die in den letzten Jahren erfolgten Reformen des US-amerikanischen Rechts ergeben, neu geprüft und positiv bewertet. Ob sich die Rechtslage in den USA aber tatsächlich so deutlich verbessert hat, dass nunmehr von einem der Sache nach gleichwertigen Schutzniveau gesprochen werden kann, ist angesichts der vom EuGH angesprochenen Risiken für bedeutendes Rechtsgut in einer Vielzahl von Fällen kritisch zu hinterfragen.

Die Rechtslage in den USA und insbesondere die Schutzelemente, die das US-amerikanische Recht bietet, können an dieser Stelle nicht umfassend geprüft werden. Einige relevante Punkte wie die noch immer unzureichende Begrenzung von Zugriffsbefugnissen der US-Behörden nach US-Recht wurden oben bereits angesprochen.[300] Um besser zu verstehen, wie komplex die Rechtslage in den USA in vielen Bereichen ist, soll nachfolgend exemplarisch für den Bereich des staatlichen Zugriffs auf personenbezogene Daten ein Überblick über die zahlreichen Rechtsgrundlagen für einen solchen Zugriff sowie die bislang unternommenen Schritte zur Begrenzung desselben gegeben werden.

In den USA bestehen in erheblichem Maße Befugnisse staatlicher Stellen zur Beschaffung und Verarbeitung personenbezogener Daten.[301] So regelt nach Angaben des Vereins „digitalcourage“[302] etwa der **US Patriot Act**, dass US-amerikanische Geheimdienste Zugriff auf Daten erhalten müssen, die bei US-Unternehmen gespeichert sind. Die Betroffenen müssten hierüber nicht informiert wer-

[297] https://www.janalbrecht.eu/presse/pressemitteilungen/eu-kommissionsvorschlag-privacy-shield-neue-datentransfer-regelung-darf-keine-dauerloesung-werden.html.
[298] EuGH, Rechtssache „Schrems“, a.a. O. (Fn. 30)., Tz. 98.
[299] Ebenso Borges, NJW 2015, 3617 (3619).
[300] Vgl. oben Ziffern 8.3.3.3 (Zugriffsbefugnisse der US-Behörden) und 8.3.3.4 (Schaffung wirksamen gerichtlichen Rechtsschutzes).
[301] Borges, NJW 2015, S. 3617 (3618).
[302] Siehe auch https://digitalcourage.de/blog/2016/ohne-reformen-in-der-usa-und-der-eu-wird-auch-safe-harbour-20-untergehen.

den. Die Gesetzgebung in den USA sei insoweit nicht mit dem EU-Datenschutzrecht vereinbar. Auch die Kommission hatte seinerzeit erkannt, dass EU-Unternehmen und in der EU niedergelassene US-Unternehmen durch den Patriot Act auch dann zur Datenübermittlung in die USA unter Verletzung von Rechtsvorschriften der EU und der EU-Mitgliedstaaten verpflichtet werden können, wenn die Daten in der EU gespeichert sind, und auf diese Weise in das Spannungsfeld zweier im Widerspruch zueinander stehender rechtlicher Verpflichtungen geraten könnten.[303]

Ferner regelt der **Foreign Intelligence Surveillance Act (FISA)**, dass Nicht-US-Staatsbürger, die sich nicht auf US-Staatsgebiet befinden, zu Zwecken der nationalen Sicherheit überwacht werden dürfen.[304] Auf FISA Section 702 soll etwa das Überwachungsprogramm „PRISM“ gestützt gewesen sein.[305] EU-Datenschutzexperten fordern daher eine umfassende Reformierung dieser Vorschrift[306] oder eine völkerrechtliche Verpflichtung der USA zur Nichtanwendbarkeit auf EU-Bürger.[307]

Darüber hinaus enthält **Executive Order 12333** Regelungen betreffend die Erhebung, Speicherung und Verbreitung von Informationen von Nutzern weltweit und soll die Sammlung unverschlüsselter Daten durch die NSA bei der Übermittlung von Google- und Yahoo-Datenzentren ermöglicht haben.[308] Im Jahr 2015 sollen die US-Spionagemöglichkeiten durch den **Cybersecurity Act** sogar noch ausgeweitet worden sein.[309]

Ungeachtet dessen haben die USA in den vergangenen Jahren aber bereits gewisse Schritte zur Begrenzung der Überwachungen vorgenommen. Hierzu zählt die bereits erwähnte[310] **Presidential Policy Directive 28** (PPD-28) von Präsident Obama vom 17.01.2014 bezüglich der Sammlung von Kommunikationsdaten. Diese soll die Erhebung und Nutzung von Geheimdienstinformationen auf bestimmte Zwecke begrenzt und – unabhängig von Wohnsitz oder Staatsangehörigkeit – Sicherheiten für darin enthaltene persönliche Informationen etabliert haben.[311]Gewisse Teile des US Patriot Acts, insbesondere die Rechtsgrundlage für Massenüberwachungen in dessen Section 215, sollen zum 01.06.2015 ausgelaufen sein. [312]Auch der **USA Freedom Act**, in Kraft getreten zum 02.06.2015, begrenzt die Datenzugriffsbefugnisse der US-Sicherheitsbehörden zumindest in gewisser Weise.[313] Wie aus US-amerikanischen Kreisen zu hören ist, soll es unter dem USA Freedom Act keine massenhafte und wahllose Überwachung personenbezogener Daten von EU-Bürgern durch die NSA mehr geben. In der Literatur wird jedoch bezweifelt, ob die Überwachungsbefugnisse hierdurch effektiv begrenzt werden.[314]

Wie oben gesehen,[315] wird auch unter dem „Privacy Shield“-Beschluss die Erhebung und Nutzung von Massendaten zu Zwecken der nationalen Sicherheit in gewissem Umfang weiterhin möglich sein. Die in den USA vorhandenen Garantien bzw. die in Anhang VI des „Privacy Shield-Beschlusses“ erläuterten Begrenzungen staatlicher Zugriffe auf personenbezogene Daten reichen nach vorläufiger Einschätzung des cep derzeit nicht aus, um den Risiken des Zugriffs durch US-

[303] Vgl. die Mitteilung (2013) 846 (final) der Kommission (Fn. 1), Ziffer 2.
[304] U.S.C. § 1881 a, vgl. hierzu Kühling/Heberlein, NVwZ 2016, S. 7 (11).
[305] https://edri.org/files/WP29Submission%28Final%29-1.pdf, S. 3.
[306] https://edri.org/files/WP29Submission%28Final%29-1.pdf, S. 3.
[307] So Kühling/Heberlein, NVwZ 2016, S. 7 (11), die es für zweifelhaft halten, ob der US-Kongress dem zustimmen würde.
[308] https://edri.org/files/WP29Submission%28Final%29-1.pdf, S. 3.
[309] https://edri.org/files/WP29Submission%28Final%29-1.pdf, S. 3. Danach soll dieser Act das Departement of Homeland Security (DHS) zur Übermittlung von „Cyber thread“-Indikatoren verpflichten, die an Geheimdienst- und Vollstreckungsbehörden (ggf. geheim) weitergegeben werden und personenbezogene Daten von EU-Bürgern enthalten können. Unternehmen, die solche Indikatoren übermitteln, sollen weitgehende rechtliche Immunität genießen.
[310] Vgl. oben Ziffer 8.3.3.3.
[311] Z.B. dürfen Daten nur eingeschränkt weitergegeben werden, vgl. Moos/Schefzig, a.a.O., S. 633 (Fn. 80) mit weiteren Informationen.
[312] Borges, NJW 2015, 3617 (3618) m.w.N.
[313] Moos/Schefzig, CR 2015, S. 625 (633) m.w.N.
[314] Borges, NJW 2015, S. 3617 (3618) m.w.N.
[315] Vgl. oben Ziffer 8.3.3.3.

Geheimdienste so umfassend zu begegnen, dass die Rechte und Freiheiten der betroffenen Person als gleichermaßen geschützt angesehen werden können.

Bürgerrechtsorganisationen wie EDRi[316], Organisationen wie accessnow[317] oder Vereine wie digitalcourage[318] fordern daher insbesondere eine Reform der Überwachung in den USA, eine Änderung des FISA Section 702 und der Executive Order 12333, eine Reform des Cybersecurity Acts, das Bekenntnis der USA zum Internationalen Pakt über Bürgerliche und Politische Rechte (UN-Zivilpakt, ICCPR) sowie den Erlass umfassender Datenschutzgesetze auf US-Bundesebene. Auch innerhalb der EU müsse die ausufernde Gesetzgebung der EU-Mitgliedstaaten zur Überwachung reformiert werden. Das Europäische Parlament solle in die Verhandlungen und den Abschluss künftiger Vereinbarungen mit den USA einbezogen werden. Auch in der Literatur werden (weitere) Reformen gefordert.[319]

Angesichts der bestehenden Datenschutzdefizite in den USA hatte auch das ULD Schleswig-Holstein in seinem Positionspapier vom 14.10.2015 bezweifelt, dass die Kommission einen Angemessenheitsbeschluss wirksam treffen oder anderweitig kurzfristig eine neue Rechtsgrundlage für den Datentransfer schaffen könne. Eine Entscheidung der Kommission, dass die USA ein angemessenes Schutzniveau aufweisen, sei ebenso wie ein völkerrechtliches Datenschutzabkommen mit den USA nur möglich, wenn das US-amerikanische Recht umfassend geändert werde. Dies sei jedoch kurz- oder mittelfristig nicht zu erwarten.[320] Die deutsche Bundesregierung hat hingegen die Auffassung vertreten, dass eine Nachfolgeregelung für „Safe Harbour“ möglich sei, die den Maßstäben des EuGH gerecht werde.[321]

Da den betroffenen Unternehmen momentan kaum eine Möglichkeit offensteht, ihre Daten weiterhin legal in die USA zu transferieren, ist der Druck aus der Wirtschaft bezüglich der Schaffung einer neuen Rechtsgrundlage enorm. Denn ein Abbruch des transatlantischen Datenaustausches wäre für viele Unternehmen und Nutzer eine Katastrophe.[322] Seit dem Wegfall von „Safe Harbour“ fordern Wirtschaftsverbände deshalb eine schnelle Lösung.[323] Entsprechend neigen Vertreter der Technikindustrie dazu, die rechtlichen Unterschiede zwischen USA und EU herunterzuspielen.[324] Andere sehen hingegen wie oben gesehen eine massive Diskrepanz.

Aus Sicht des cep wäre es vorzugswürdig, auf weitere Reformen im US-Recht zu drängen als einen inhaltlich fragwürdigen Angemessenheitsbeschluss mit zweifelhafter Rechtssicherheit zu erlassen. Zwar kann die EU den demokratisch legitimierten Organen der USA nicht vorschreiben, welche Gesetze sie erlassen sollen.[325] Ein ungenügender „Schnellschuss“ auf Kosten von Rechten und Werten der EU ist jedoch abzulehnen. Die EU sollte konsequent versuchen, weiter auf die Beseitigung der wesentlichen Defizite des US-Rechts hinzuwirken. Hierzu gehören der Erlass von Datenschutzgesetzen auf US-Bundesebene, die Beschränkung der Überwachung auf das nötige Maß und die Sicherstellung eines lückenlosen effektiven (gerichtlichen) Rechtsschutzes gegen Eingriffe und

[316] European Digital Rights, eine internationale Vereinigung von Bürgerrechtsorganisationen zum Schutze der Privatsphäre und der Freiheit der Bürger in der Informationsgesellschaft. Vgl. ihr gemeinsames Positionspapier mit accessnow unter https://edri.org/files/WP29Submission%28Final%29-1.pdf.
[317] Vgl. Fn. 311.
[318] https://digitalcourage.de/blog/2016/ohne-reformen-in-der-usa-und-der-eu-wird-auch-safe-harbour-20-untergehen.
[319] Vgl. etwa Moos/Schefzig, CR 2015, S. 625 (633); Kühling/Heberlein, NVwZ 2016, S. 7 (11).
[320] Positionspapier des ULD Schleswig-Holstein (Fn. 90), Ziffer 2.
[321] Antwort der Bundesregierung auf die Kleine Anfrage verschiedener Abgeordneten und der Fraktion DIE LINKE, BT-Drucksache 18/7134, Vorabfassung vom 21.12.2015, S. 4.
[322] So etwa Markus Kerber, Hauptgeschäftsführer des Bundesverbands der deutschen Industrie, siehe FAZ vom 01.02.2016, S. 22„Damit die Daten weiter fließen“.
[323] So bereits während der Verhandlungen für „Safe Harbour 2.0“, vgl. http://www.heise.de/newsticker/meldung/Verhandlungen-fuer-Safe-Harbour-2-0-Wirtschaftsverbaende-fordern-schnelle-Einigung-3074094.html.
[324] http://mobile.nytimes.com/2016/02/01/technology/us-european-data-transfer-deal.html.
[325] Kühling/Heberlein, NVwZ 2016, S. 7 (11).

sonstige Verletzungen der Datenschutzrechte. Wesensgleicher Schutz bedeutet hingegen keinen hundertprozentigen Schutz vor Zugriffen durch Geheimdienste, den es auch innerhalb der EU nicht gibt. Die sauberste Lösung wäre es, wenn die Kommission auf der Basis einer derart verbesserten Rechtslage einen Angemessenheitsbeschluss für die USA erlassen könnte.

All dies erscheint jedoch illusorisch. Bahnbrechende Änderungen des US-Rechts sind derzeit nach Ansicht des Beratungsunternehmens Fleishman Hillard[326] angesichts der anstehenden Präsidentschaftswahlen in den USA unwahrscheinlich. Die aktuelle Regierung habe wenig Interesse daran, durch den Abschluss eines Abkommens, das die EU auf Kosten der nationalen Sicherheit in den USA zufriedenstellt, Wasser auf die Mühlen der Republikaner zu gießen.

8.3.5 Fazit

Auch ohne vollständige Prüfung des „Privacy Shields“ und ohne inhaltliche Prüfung der „Privacy Principles“ verbleiben nach vorläufiger Einschätzung des cep auch nach den durchgeführten Teilreformen in den USA noch immer datenschutzrechtliche Defizite im US-amerikanischen Recht sowie zahlreiche Unklarheiten ob dessen Reichweite. Fragwürdig ist auch die Bindungswirkung der unter dem „Privacy Shield“ gemachten Zusicherungen. Trotz zahlreicher Verbesserungen „auf dem Papier“ spricht einiges dafür, dass das Datenschutzniveau in den USA auch unter Berücksichtigung der Inhalte des „Privacy Shield“ noch immer nicht gleichwertig ist und damit nicht als angemessen angesehen werden sollte. Angesichts der hohen Anforderungen des EuGH im „Schrems-Urteil“ erscheint es ungewiss, ob die neue Angemessenheitsentscheidung der Kommission bei der zu erwartenden erneuten Vorlage vor dem EuGH Bestand haben wird. Im Einzelnen hängt hier jedoch vieles noch von der praktischen Umsetzung und tatsächlichen Effektivität der geplanten Kontroll- und Rechtsbehelfsmöglichkeiten ab. Wie diese genau aussehen werden, ist jedoch noch nicht gänzlich abzusehen. Hier müssen sowohl die USA als auch die EU noch notwendige Maßnahmen zur Umsetzung treffen.

Nunmehr ist es Aufgabe der EU-Datenschutzbehörden, die festgestellten Mängel des „Privacy Shield“-Beschlusses in ihrer Stellungnahme zum Kommissionsentwurf zu rügen und die Kommission zu Nachbesserungen und Nachverhandlungen zu bewegen. Ansonsten wird sich früher oder später vor dem EuGH zeigen müssen, wie dicht – oder wie löchrig – der „Privacy Shield“ tatsächlich ist. Sollte auch das neue Instrument vor dem EuGH nicht standhalten, wäre dies für die Kommission, mehr aber noch für die betroffenen Unternehmen, die dann trotz all des Umsetzungsaufwands erneut ohne Rechtsgrundlage agierten, wohl die größere Katastrophe.

Solange die Unternehmen nicht auf eine „wasserdichte“, d.h. langfristig rechtssichere Lösung für zukünftige Datentransfers in die USA setzen können, ist zu erwarten, dass sich der derzeitige Trend, Daten in der EU zu speichern oder zu EU-Anbietern zu wechseln,[327] fortsetzt. Dies würde die US-amerikanische Wirtschaft weiter unter Druck setzen. EU-Dienstleistern wie der Deutschen Telekom spielt dieser Trend hingegen in die Karten. Auch Anbieter von Buchungssystemen für Reisebüros wie die Firma Amadeus aus Bad Homburg als Konkurrent des amerikanischen Großanbieters Sabre oder der Buchungsmaschinen-Anbieter Bewotec könnten von dem Trend zur Datenspeicherung in der EU profitieren.[328] Der aus der Not heraus geborene Anreiz zur Verlagerung der Daten auf Server in der EU bietet somit neben allen Unannehmlichkeiten auch Chancen für die Wirtschaft in der EU.

---

[326] Vgl. den Bericht unter https://thewonk.eu/reports/safe-harbour-d-day-approaches-what-to-expect__r1146.html?utm_source=Users+by+interests&utm_campaign=a40a6809b3-All+New+Reports+Weekly&utm_medium=email&utm_term=0_d163844b00-a40a6809b3-282298025.

[327] Vgl. oben Ziffer 8.1.

[328] Handelsblatt Wochenende vom 29.01.2016, S. 16 „Wenn Datenverkehr plötzlich illegal ist“.

8.3.6. Konsequenzen für Datentransfers über BCR und SDPC

Aus den vorstehenden Ausführungen ergibt sich zugleich, dass zahlreiche Probleme, die auch die Rückgriffsmöglichkeit auf alternative Rechtsgrundlagen wie BCR oder SDPC beeinflussen, nach der derzeitigen US-Rechtslage noch immer nicht gelöst erscheinen. Die gleichen Bedenken, die auch für Transfers unter dem „Privacy Shield“ verbleiben, bestehen auch hinsichtlich SDPC und BCR fort. Dies gilt insbesondere für die Zweifel an der hinreichenden Begrenzung der staatlichen Zugriffsmöglichkeiten sowie am Bestehen eines lückenlosen gerichtlichen Rechtsschutzes. Hinzu kommt, dass eine Garantie durch SDPC und BCR ebenso wie die Selbstverpflichtung zur Einhaltung von „Privacy Principles“ nur effektiv sein kann, wenn auch insoweit eine hinreichende Überwachung und Kontrolle dahingehend gewährleistet ist, ob diese Regeln tatsächlich eingehalten werden. Dies ist jedoch bislang nicht der Fall. Soweit aus den Anhängen des „Privacy Shield“-Beschlusses evtl. zusätzliche Garantien resultieren, können diese allenfalls bei Transfers an hierunter zertifizierte Unternehmen Wirkung entfalten. Sie gelten hingegen nicht bei Übermittlungen über SDPC, oder BCR oder sonstige Ausnahmen. Zwar lässt sich Anhang III des Entwurfs des „Privacy Shield“-Beschlusses entnehmen, dass der neue „Ombudsmann-Mechanismus“ für Anfragen, die den Zugriff auf personenbezogene Daten zum Zwecke der nationalen Sicherheit betreffen, offenbar auch insoweit zur Verfügung stehen soll.[329] Dieser soll also nicht nur für Anfragen hinsichtlich personenbezogener Daten greifen, die über den „Privacy Shield“ übertragen wurden, sondern auch dann, wenn die Daten auf der Grundlage von SDPC, BCR oder eines Ausnahmetatbestands transferiert wurden. Der vorgeschlagene Mechanismus weist jedoch wie oben ausgeführt[330] gewisse Mängel auf und vermag daher auch bei Datentransfers über SDPC, BCR oder Ausnahmetatbestände keinen ausreichenden gerichtlichen Rechtsschutz zu bieten.

Sollten die USA hingegen behördliche Zugriffe auf das erforderliche Maß beschränken, einen lückenlosen und wirksamen administrativen und gerichtlichen Rechtsschutz zur Verfolgung von Verstößen gegen solche Regelungen gewährleisten und effektive Überwachungs- und Kontrollmechanismen schaffen, mit denen Verstöße aufgedeckt und die Einhaltung von SDPC und BCR sichergestellt werden kann, könnten Transfers auf der Basis von SDPC und BCR wieder hinreichende Garantien für den Datenschutz bieten. Dabei können ergänzende Maßnahmen wie Zertifizierung, Verschlüsselung sowie ein Recht auf Einsicht in Protokolldaten[331] helfen.

8.3.7 Ablauf des Verfahrens zum Erlass eines Angemessenheitsbeschlusses

Angemessenheitsbeschlüsse (vormals: Entscheidungen) werden gemäß Art. 25 Abs. 6, Art. 31 Abs. 2 DSRL mittels des so genannten „Ausschussverfahrens“ getroffen. Im Einzelnen finden die Regelungen des Prüfverfahrens gemäß Art. 5 der EU-Komitologieverordnung[332] Anwendung. Das Verfahren läuft im Wesentlichen wie folgt[333]: Haben die Kommissionsvertreter den Entwurf für einen Angemessenheitsbeschluss erarbeitet, muss die Art. 29-Datenschutzgruppe zu diesem Entwurf Stellung nehmen (vgl. Art. 30 Abs. 1 lit. (b), Abs. 4 DSRL). Diese Stellungnahme ist jedoch für die Kommission nicht bindend. Die Kommission muss der Gruppe lediglich mitteilen, welche Konsequenzen sie aus der Stellungnahme gezogen hat (vgl. Art. 30 Abs. 5 DSRL). Ferner bedarf es der Anhörung des Ausschusses nach Art. 31 DSRL, der sich aus Vertretern der EU-Mitgliedstaaten unter

[329] Vgl. S. 1 des Anhangs III zum Entwurf des „Privacy-Shield“-Beschlusses (Fn. 190).
[330] Vgl. oben Ziffer 8.3.3.4.
[331] Vgl. hierzu oben Ziffern 7.1.1., 7.3 sowie 8.2.
[332] Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die EU-Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren, ABl. L 55 vom 28.02.2011, S. 13 ff; abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32011R0182&from=DE.
[333] Vgl. https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/Dataprotection/Glossary/pid/71.

Vorsitz eines Vertreters der Kommission zusammensetzt.[334] Gibt der Ausschuss mit qualifizierter Mehrheit der EU-Mitgliedstaaten eine positive Stellungnahme ab, erlässt die Kommission den Beschluss. Gibt er keine Stellungnahme ab, kann die Kommission den Beschluss erlassen. Fällt die Stellungnahme negativ aus, darf die Kommission den Beschluss außer in dringlichen Fällen nicht erlassen. Sie kann dann entweder dem Ausschuss eine geänderte Fassung des Entwurfs unterbreiten oder den Berufungsausschuss anrufen.[335] Laut Presseinformationen haben die EU-Mitgliedstaaten jedoch kein Interesse daran, den Beschluss zu blockieren, sondern sind an einer schnellen Lösung interessiert.[336] Ferner soll auch der Europäische Datenschutzbeauftragte[337] vor Erlass des Beschlusses konsultiert werden.[338]

In jedem Fall muss der „Privacy Shield“-Beschluss abschließend durch das Kollegium der Kommissionsmitglieder angenommen werden. Das Europäische Parlament wird in die Beratungen einbezogen, verfügt insoweit aber über keine Mitbestimmungsrechte. Ebenso wie der Rat kann es lediglich ein beschränktes Kontrollrecht nach Art. 11 der Komitologieverordnung ausüben. Damit könnte aber lediglich gerügt werden, dass der Entwurf des Angemessenheitsbeschlusses die in der DSRL vorgesehenen Durchführungsbefugnisse der Kommission überschreite. Die Kommission muss dann den Entwurf des Angemessenheitsbeschlusses unter Berücksichtigung dieses Hinweises prüfen und Parlament und Rat darüber informieren, ob sie beabsichtigt, den Entwurf beizubehalten, abzuändern oder zurückzuziehen. Unmittelbar verhindern kann das Parlament den Erlass des Angemessenheitsbeschlusses der Kommission jedoch nicht. Das Parlament wird jedoch voraussichtlich eine Stellungnahme oder Resolution verfassen, um Druck auf die Kommission auszuüben.

8.4 Ausblick: Neue Instrumente nach der DSGV

Abschließend sollen kurz die neuen Instrumente vorgestellt werden, auf welche die Übertragung personenbezogener Daten in Drittstaaten unter der DSGV künftig gestützt werden kann. Dies gilt jedoch grundsätzlich nur, soweit bezüglich dieses Drittlands kein Angemessenheitsbeschluss vorliegt.[339]

Wie bereits ausgeführt,[340] können BCR, die nun umfassend in Art. 43 DSGV geregelt wurden, sowie SDPC auch unter der DSGV hinreichende Garantien bieten, die über das fehlende angemessene Schutzniveau in einem Drittland wie den USA hinweghelfen können. Ausdrückliche Voraussetzung ist jedoch nunmehr, dass die Betroffenen über durchsetzbare Rechte und effektive Rechtsschutzmöglichkeiten verfügen.[341] SDPC können weiterhin von der Kommission erlassen werden (Art. 42 Abs. 2 lit. (c) DSGV). Die gleiche Wirkung haben künftig auch SDPC, die von einer Aufsichtsbehörde erlassen und von der Kommission genehmigt wurden (Art. 42 Abs. 2 lit. (d) DSGV).

---

[334] Vgl. Art. 3 Komitologieverordnung (EU) Nr. 182/2011 (Fn. 327). Es handelt sich um den Ausschuss für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Code C27000).
[335] Vgl. Art. 5 Abs. 2-4 Komitologieverordnung (EU) Nr. 182/2011 (Fn. 327).
[336] Vgl. http://www.politico.eu/article/privacy-shield-agreement-takeaways-text-released/.
[337] Der Europäische Datenschutzbeauftragte ist eine Beratungs- und Kontrollbehörde, die nach Art. 41 der Verordnung 45/2001 des Europäischen Parlaments und des Rates vom 18.12.2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr eingerichtet wurde und die Achtung der Grundrechte und Grundfreiheiten natürlicher Personen durch Organe und Einrichtungen der Gemeinschaft sicherstellen soll.
[338] Communication from the Commission to the European Parliament and the Council vom 29.02.2016, COM(2016) 117 final, “Transatlantic Data Flows: Restoring Trust through Strong Safeguards”, Ziffer 3.1 a. E., abrufbar unter http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.
[339] Zu der sich möglicherweise hieraus ergebenden Problematik vgl. oben Ziffer 8.3.3.1, Fn. 204.
[340] Vgl. oben Ziffern 6.1 und 6.2.
[341] Vgl. Art. 42 Abs. 1 a. E. DSGV.

Daneben sieht die DSGV noch weitere Instrumente vor, die hinreichende Garantien i.S.v. Art. 42 Abs. 1 bieten und einen Transfer personenbezogener Daten ohne weitere Genehmigung erlauben. Künftig können sich Unternehmen aus Drittländern auf die Standards der DSGV zertifizieren lassen. Hierdurch soll nachgewiesen werden, dass auch diese Unternehmen die DSGV bei der Verarbeitung personenbezogener Daten von EU-Bürgern einhalten und somit die Übermittlung solcher Daten durch eine zusätzliche Garantie i.S.v. Art. 42 DSGV abgesichert ist. Art. 39 DSGV bildet die Grundlage für die Schaffung datenschutzspezifischer Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen auf EU-Ebene, die von akkreditierten Zertifizierungsstellen, der zuständigen Aufsichtsbehörde oder durch den EU-Datenschutzausschuss noch genehmigt werden müssen.[342] So soll etwa der EU-Datenschutzausschuss ein „Europäisches Datenschutzsiegel“ erteilen können. Gemäß Art. 39 Abs. 1a) DSGV können solche Verfahren, Siegel oder Prüfzeichen auch vorgesehen werden, um nachzuweisen, dass verantwortliche Stellen oder Auftragsdatenverarbeiter, für die die DSGV nicht unmittelbar gilt, im Rahmen der Übermittlung personenbezogener Daten an Drittländer geeignete Garantien i.S.v. Art. 42 Abs. 2 lit. e) DSGV bieten. Zusätzlich müssen die Datenimporteure im Drittland sich vertraglich oder anderweitig verbindlich dazu verpflichten, die geeigneten Garantien auch anzuwenden. Diese Verpflichtung gilt insbesondere im Hinblick auf die Rechte der Betroffenen und muss durchsetzbar sein. Voraussetzung ist, dass die Betroffenen über durchsetzbare Rechte und effektive Rechtsschutzmöglichkeiten verfügen. Die Verantwortung des EU-Datenexporteurs wird durch eine Zertifizierung nicht ausgeschlossen. Die EU-weite Einführung einer Rechtsgrundlage für die Vergabe solcher Datenschutzsiegel ist zu begrüßen. Datenschutzrechtliche Gütesiegelverfahren können datenschutzfreundliche Produkte und Dienstleistungen belohnen und die Entwicklung des Marktsegments in den Bereichen der Datensicherheits- und Datenschutztechnologie fördern.[343]

Daneben sollen künftig sogenannte „genehmigte Verhaltensregeln“ gemäß Art. 38 DSGV zur Einhaltung der DSGV beitragen und hinreichende Garantien i.S.v. Art. 42 Abs. 1 DSGV gewährleisten können. Solche Verhaltensregeln sollen von Verbänden und Vereinigungen ausgearbeitet werden, die Kategorien von verantwortlichen Stellen oder Auftragsdatenverarbeitern vertreten. Werden diese Regeln von der zuständigen Aufsichtsbehörde genehmigt und auch von verantwortlichen Stellen oder Auftragsdatenverarbeitern eingehalten, für die die DSGV nicht unmittelbar gilt, kann hierdurch eine geeignete Garantie geschaffen werden (Art. 38 Abs. 1ab i.V.m. Art. 42 Abs. 2 lit. d) DSGV). Auch hier muss sich der Datenimporteur im Drittland bindend zur Anwendung der Garantien verpflichten und die Betroffenen über durchsetzbare Rechte und effektive Rechtsschutzmöglichkeiten verfügen.

Ferner soll es für den Transfer zwischen Behörden oder staatlichen Stellen ein besonderes Instrument geben (Art. 42 Abs. 2 lit a) DSGV). Schließlich können die zuständigen Aufsichtsbehörden wie schon bislang im Einzelfall vertragliche Regelungen oder Zusatzbestimmungen für Verwaltungsvereinbarungen zwischen EU-Datenimporteur und US-Datenimporteur als ausreichende Garantie genehmigen (Art. 42 Abs. 2a lit. (a) und (b) DSGV).

Schließlich soll es eine neue Sonderregelung für Fälle geben, in denen Datenübermittlungen weder aufgrund eines Angemessenheitsbeschlusses noch infolge einer hinreichenden Garantie i.S.v. Art. 42 DSGV zulässig sind und auch kein Ausnahmetatbestand gemäß Art. 44 Abs. 1 lit. (a) – (g) DSGV greift, das Risiko für die betroffenen Dateninhaber jedoch gering ist. Nach Art. 44 Abs. 1 lit (h) DSGV sollen solche Transfers ausnahmsweise zulässig sein, sofern „die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von Personen betrifft und zur Wahrung zwingender berech-

[342] Vgl. Art. 39 Abs. 2a DSGV.

[343] Aus vergleichbaren Erwägungen spricht sich daher der Hamburgische Datenschutzbeauftragte in seinem 25. Tätigkeitsbericht für die gesetzliche Regelung von Gütesiegelverfahren in Hamburg aus, vgl. https://www.datenschutz-hamburg.de/uploads/media/25._Taetigkeitsbericht_Datenschutz_2014-2015_HmbBfDI_01.pdf, S. 22.

tigter Interessen der verantwortlichen Stelle erforderlich ist“. Voraussetzung ist jedoch, dass die Interessen oder die Rechte und Freiheiten der Betroffenen gegenüber diesen berechtigten Interessen nicht überwiegen und dass „die verantwortliche Stelle alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat“. Da diese Regelung bei wiederholten Transfers oder Übermittlungen personenbezogener Daten einer großen Zahl von Personen nicht greift, werden ihre Einsatzmöglichkeiten allerdings wohl eher begrenzt bleiben.

Einige der neuen Instrumente wie die Zertifizierung oder die Verhaltensregeln sind in der DSGV allerdings nur in Grundsätzen festgelegt. Hier müssen im Einzelnen noch die Details geregelt und umgesetzt werden. Frühestens im Laufe des Jahres 2018 dürfte daher mit einer Einsatzfähigkeit dieser Instrumente zu rechnen sein. Auch diese Instrumente werden in den USA nur zum Tragen kommen können, wenn im US-amerikanischen Recht durchsetzbare Rechte und effektive Rechtsschutzmöglichkeiten für die Betroffenen geschaffen werden.

9. Fazit

- Bis zum 6. Oktober 2015 war die „Safe Harbour“-Entscheidung der Europäischen Kommission Rechtsgrundlage für transatlantische Datentransfers. Nachdem der Europäische Gerichtshof (EuGH) diese für ungültig erklärt hat, ist die Rechtslage unsicher. Auch alternative Rechtsgrundlagen wie Standarddatenschutzklauseln oder verbindliche unternehmensinterne Datenschutzregelungen versprechen derzeit keine dauerhafte rechtssichere Abhilfe.
- Als Ersatz für die „Safe Harbour“-Entscheidung plant die Kommission – auf Basis einer erfolgten Verständigung mit den USA – einen „Privacy Shield“-Beschluss. Er enthält als Anlage „Privacy Principles“, denen sich teilnehmende US-Unternehmen durch Selbstzertifizierung unterwerfen müssen, sowie sechs Briefe von US-Behörden und -Ministerien, in denen diese die US-Rechtslage beschreiben und Zusicherungen machen.
- Der „Privacy Shield“-Beschluss trägt laut Kommission dem EU-Datenschutz in allen Punkten Rechnung. Dies trifft nicht zu:
  - Der Schutz vor staatlichen Zugriffen auf personenbezogene Daten ist unzureichend. Massenhafte Datenerhebungen und -nutzungen durch US-Behörden bleiben möglich. Die vorgesehenen Einschränkungen für US-Sicherheitsbehörden dürften nicht der Vorgabe des EuGH entsprechen, dass Eingriffe in das Grundrecht auf Achtung des Privatlebens „absolut notwendig und verhältnismäßig“ sein müssen.
  - Der Rechtsschutz ist ebenfalls unzureichend. Insbesondere erfüllt der „Ombudsperson-Rechtsbehelf“ nicht die Anforderungen des EuGH an einen „gerichtlichen Rechtsschutz“. Die „Ombudsperson“ ist nicht vollkommen unabhängig, hat möglicherweise unzureichende Befugnisse und fällt intransparente Entscheidungen.
  - Um wettbewerbsrechtliche Nachteile für EU-Unternehmen zu vermeiden, muss sichergestellt sein, dass die zertifizierten US-Unternehmen die „Privacy Principles“ auch tatsächlich einhalten. Daher sollten Kontrollen nicht im Wesentlichen auf Rüge hin, sondern anlasslos, regelmäßig, unangekündigt und flächendeckend erfolgen. Auch sollte die Zertifizierung nicht durch kaum kontrollierbare Selbstunterwerfung, sondern durch unabhängige akkreditierte Stellen vorgenommen werden.
- Die „Privacy Principles“ sollten bereits jetzt an der voraussichtlich ab 2018 geltenden Datenschutzgrundverordnung ausgerichtet werden, um Anpassungsbedarf und Nachverhandlungen mit den USA zu vermeiden.
- Die rechtliche Bindungswirkung der in Briefen gemachten Zusicherungen ist fraglich. Geboten wäre ein völkerrechtliches Abkommen sowie eine bindende Umsetzung in den USA mit Gesetzescharakter.
- Die Kommission will auf die US-amerikanischen Zusicherungen vertrauen und den „Privacy Shield“-Beschluss bei Fehlverhalten aussetzen. Dies wird weder dem Interesse der Wirtschaft an einer langfristigen rechtssicheren Grundlage für transatlantische Datentransfers noch demjenigen der EU-Bürger an einem dauerhaften angemessenen Datenschutz gerecht.
- Die EU sollte zunächst konsequent auf weitere spürbare Änderungen im US-Recht hinwirken und erst auf Basis der geänderten Rechtslage einen Angemessenheitsbeschluss erlassen. Dass es hierzu kommt, ist allerdings wenig wahrscheinlich.
- Unternehmen, die Rechtssicherheit suchen, sollten erwägen, ihre Datenverarbeitung in die EU zu verlagern oder zu Dienstleistern zu wechseln, die personenbezogene Daten ausschließlich in der EU speichern.

Die Autorin:

Dr. Anja Hoffmann ist wissenschaftliche Referentin im Fachbereich „Zivil- und Verfahrensrecht“ am Centrum für Europäische Politik.

cep | Centrum für Europäische Politik
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Telefon +49 761 38693-0 | www.cep.eu

Das cep ist der europapolitische Think Tank der gemeinnützigen Stiftung Ordnungspolitik. Es ist ein unabhängiges Kompetenzzentrum zur Recherche, Analyse und Bewertung von EU-Politik.