NETZWERK DATENSCHUTZEXPERTISE

Der EuGH zu Safe Harbor – das Urteil und seine Konsequenzen

Auf dem Weg zu datenschutzkonformen Datenübermittlungen in die USA

Stand: 26.11.2015

Dr. Thilo Weichert
Waisenhofstr. 41, 24103 Kiel
0431 9719742
weichert@netzwerk-datenschutzexpertise

Karin Schuler
Kronprinzenstr. 76, 53173 Bonn
0228/24 20 733
schuler@netzwerk-datenschutzexpertise

www.netzwerk-datenschutzexpertise.de

Inhalt

1 Das Safe-Harbor-Urteil des EuGH

Mit Urteil vom 06.10.2015 entschied der Europäische Gerichtshof (EuGH), dass die Safe-Harbor-Entscheidung der Kommission vom 26.07.2000 ungültig ist, wonach unter bestimmten, festgelegten Voraussetzungen in den Vereinigten Staaten von Amerika (USA) ein angemessenes Datenschutzniveau zur Übermittlung personenbezogener Daten fingiert wird., Sie erklärte damit *Safe Harbor für unwirksam*.[1]

Mit diesem Urteil entschied der EuGH über eine grundlegende, bisher streitige Frage das Datenschutzrechts, nämlich die Zulässigkeit von *Datenübermittlung ins Drittausland*, und legte Maßstäbe fest, die bisher weder Unternehmenspraxis noch Prüfgrundlage der Aufsichtsbehörden waren. Das Urteil führt dazu, dass europäische wie auch nationale Exekutiven und Gesetzgeber tätig werden müssen. Der vorliegende Beitrag stellt das Urteil sowie die aktuellen Reaktionen hierauf dar und zieht rechtliche, praktische Schlüsse für die Zukunft.

2 Rechtliche Grundlagen

Maßstab der rechtlichen Prüfung durch den EuGH waren die europäischen Grundrechte sowie die europäische Datenschutzrichtlinie (EG-DSRl) aus dem Jahr 1995.[2]

In der seit 2009 gültigen *Europäischen Grundrechte-Charta* (EuGRCh) werden in den Art. 7 und 8 die Achtung des Privat- und Familienlebens sowie der Schutz personenbezogener Daten gewährleistet. In Art. 7 heißt es: „Jeder Mensch hat das Recht auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seiner Kommunikation.“ Art. 8 hat folgenden Wortlaut: „(1) Jeder Mensch hat das Recht auf Schutz der ihn betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu bewirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“ Weiterhin garantiert Art. 47 EuGRCh einen Anspruch auf wirksamen Rechtsbehelf und ein unparteiisches Gericht: „(1) Jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, hat das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. (2) Jede Person hat ein Recht darauf, dass ihre Sache von einem unabhängigen, unparteiischen und zuvor durch Gesetz errichteten Gericht in einem fairen Verfahren, öffentlich und innerhalb angemessener Frist verhandelt wird. Jede Person kann sich beraten, verteidigen und vertreten lassen.“

In der *europäischen Datenschutzrichtlinie* (EG-DSRl) wird festgelegt, dass die Übermittlung personenbezogener Daten in ein Drittland, also in ein Land außerhalb der Europäischen Union (EU) oder des europäischen Wirtschaftsraums, grundsätzlich nur dann zulässig ist, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Gemäß Art. 25 Abs. 6 EG-DSRl darf die

[1] EuGH, U. v. 06.10.2015, C-362/14, abzurufen unter http://curia.europa.eu/juris/liste.jsf?td=ALL&language=de&jur=C,T,F&num=C-362/14.
[2] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, S. 31.

Kommission feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau gewährleistet. Weiterhin sieht die EG-DSRl in Art. 28 Abs. 1 vor, dass jeder EU-Mitgliedstaat eine oder mehrere öffentliche Stellen benennt, die in seinem Hoheitsgebiet mit der Überwachung der Anwendung der zur Umsetzung der Richtlinie erlassenen nationalen Vorschriften beauftragt sind („Datenschutzbehörden“).

3 Der Sachverhalt

Der Kläger, der Österreicher Max Schrems, nutzt seit 2008 Facebook. Wie bei allen anderen in der Union wohnhaften Nutzern von Facebook werden seine Daten von der irischen Tochtergesellschaft von Facebook ganz oder teilweise an Server übermittelt, die sich in den USA befinden, und dort verarbeitet. Schrems legte bei der irischen Datenschutzbehörde wegen der Verarbeitung seiner Daten bei Facebook mehrere Beschwerden ein. Nach den Enthüllungen Edward Snowdens über die u. a. vom US-Geheimdienst National Security Agency (NSA) durchgeführten Überwachungs- und Kontrollaktivitäten im Internet, die auch Facebook erfassen, erweiterte Schrems seine Beschwerde und vertrat die Ansicht, dass das Recht und die Praxis in den *USA keinen ausreichenden Schutz* der in dieses Land übermittelten Daten vor Überwachungstätigkeiten der dortigen Behörden bieten. Die irische Behörde wies die Beschwerde insbesondere mit der Begründung zurück, die Kommission habe in ihrer Entscheidung vom 26.07.2000 festgestellt, dass im Rahmen der sogenannten „Safe-Harbor-Regelung“ ein angemessenes Datenschutzniveau für die übermittelten Daten gewährleistet sei.[3] Der auf die Klage von Schrems hiermit befasste Irish High Court hinterfragte die Wirksamkeit der Safe-Harbor-Regelung. Die Safe-Harbor-Regelung enthält eine Reihe von Grundsätzen über den Schutz personenbezogener Daten, denen sich amerikanische Unternehmen im Rahmen einer Selbstzertifizierung freiwillig unterwerfen können. Das irische Gericht machte eine Vorlage beim EuGH und wollte wissen, ob die Safe-Harbor-Entscheidung der EU-Kommission eine nationale Datenschutzbehörde daran hindert, eine Beschwerde zu prüfen, mit der geltend gemacht wird, dass ein Drittland kein angemessenes Schutzniveau gewährleiste. Wenn dies nicht der Fall ist, so sollte der EuGH die Frage beantworten, ob die Datenschutzbehörde befugt ist, die angefochtene Datenübermittlung auszusetzen.

4 Wesentliche Aussagen de Urteils

Zuständiger Berichterstatter beim EuGH war der deutsche Richter Thomas von Danwitz. In seinem Urteil führt die große Kammer des Gerichts aus, dass Entscheidungen der Kommission über die Annahme eines angemessenen Schutzniveaus eines Drittlandes, die Befugnisse der nationalen Datenschutzbehörden aufgrund des Art. 8 EuGRCh weder beseitigen noch beschränken können. Entsprechendes gelte für die den Art. 8 konkretisierende EG-DSRl. Der EuGH stellt fest, dass keine Bestimmung der EG-DSRl die nationalen Datenschutzbehörden an der Kontrolle der Übermittlungen personenbezogener Daten in Drittländer hindert, die Gegenstand einer *Entscheidung der Kommission* sind. Auch bei Vorliegen einer solchen EU-Kommissions-Entscheidung müssen die nationalen

[3] Entscheidung 2000/520/EG der Kommission vom 26.07.2000 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, S. 7.

Datenschutzbehörden, wenn sie mit einer Beschwerde befasst werden, in völliger Unabhängigkeit prüfen können, ob bei der Übermittlung der Daten einer Person in ein Drittland die in der EG-DSRl aufgestellten Anforderungen gewahrt werden.

Der EuGH weist jedoch darauf hin, dass er allein befugt sei, die *Ungültigkeit eines Unionsrechtsakts,* wie einer Kommissions-Entscheidung, festzustellen. Ist eine nationale Behörde oder die Person, die sie angerufen hat, der Auffassung, dass eine Entscheidung der Kommission ungültig ist, muss diese Behörde oder diese Person folglich die nationalen Gerichte anrufen können, damit diese, falls sie ebenfalls Zweifel an der Gültigkeit der Entscheidung der Kommission haben, die Sache dem Gerichtshof vorlegen können. Der EuGH hat letztlich darüber zu befinden, ob eine Entscheidung der Kommission gültig ist.

Der EuGH prüfte zudem die Gültigkeit der Kommissions-Entscheidung zu Safe Harbor. Er vertritt die Ansicht, dass die Kommission hätte aktiv und ausdrücklich feststellen müssen, dass die USA aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein *Schutzniveau der Grundrechte* gewährleisten, das dem in der Europäischen Union (EU) aufgrund der Richtlinie im Licht der Charta garantierten Niveau gleichwertig ist. Eine solche Feststellung hatte die Kommission nicht getroffen. Sie beschränkte sich damals darauf, die Safe-Harbor-Regelung positiv zu bewerten. Der EuGH prüfte nicht, ob diese Regelung ein Schutzniveau gewährleistet, das dem in der Union garantierten Niveau gleichwertig ist. Er stellte vielmehr fest, dass sie nur für die amerikanischen Unternehmen gilt, die sich ihr unterwerfen, nicht aber für die Behörden der USA. Die US-Gesetze geben den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses Vorrang vor der Safe-Harbor-Regelung. US-Unternehmen sind deshalb ohne jede Einschränkung verpflichtet, die in dieser Regelung vorgesehenen Schutzregeln nicht anzuwenden, wenn sie in Widerstreit zu solchen Erfordernissen stehen.

Die amerikanische Safe-Harbor-Regelung ermöglicht daher *Eingriffe der amerikanischen Behörden* in die Grundrechte der von Datenübermittlungen betroffenen Personen, ohne dass es in den USA Regeln gibt, die dazu dienen, etwaige Eingriffe zu begrenzen und einen wirksamen gerichtlichen Rechtsschutz gegen solche Eingriffe zu gewähren. Der EuGH sah sich bei der Analyse der Regelung durch zwei Mitteilungen der Kommission bestätigt, aus denen u. a. hervorgeht, dass die amerikanischen Behörden auf die in die USA übermittelten personenbezogenen Daten von EU-Bürgern zugreifen und sie in einer Weise verarbeiten konnten, die mit den Zielsetzungen ihrer Übermittlung unvereinbar war und über das hinausging, was nach Ansicht der Kommission zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig gewesen wäre.[4] Desgleichen stellte die Kommission fest, dass es für die Betroffenen keine administrativen oder gerichtlichen Rechtsbehelfe gibt, die es diesen erlaubten, zu den sie betreffenden Daten Zugang zu erhalten und gegebenenfalls deren Berichtigung oder Löschung zu erwirken.

[4] Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA“, COM[2013] 846 final, 27.11.2013, und Mitteilung der Kommission an das Europäische Parlament und den Rat über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen, COM[2013] 847 final, 27.11.2013.

Der EuGH stellte fest, dass nach dem Unionsrecht eine Regelung *nicht auf das absolut Notwendige beschränkt* ist, wenn sie ohne irgendeine Differenzierung, Einschränkung oder Ausnahme generell die Speicherung sämtlicher personenbezogener Daten gestattet, die aus der Union in die USA übermittelt werden. Es fehlt an Regelungen zu legitimen Zwecken und zu objektiven Kriterien, die den Zugang zu den Daten und deren spätere Nutzung beschränken. Eine Regelung, die es den Behörden generell gestattet, auf den Inhalt elektronischer Kommunikation zuzugreifen, verletze den Wesensgehalt des Grundrechts auf Achtung des Privatlebens. Verletzt sei außerdem der Wesensgehalt des Grundrechts auf wirksamen *gerichtlichen Rechtsschutz*, da für die Betroffenen keine Möglichkeit eröffnet ist, mittels Rechtsbehelf Zugang zu den sie betreffenden Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken. Eine solche Möglichkeit sei dem Wesen eines Rechtsstaats jedoch inhärent.

Schließlich stellte der EuGH fest, dass die Kommissions-Entscheidung zu Safe Harbor den nationalen Datenschutzbehörden die Befugnis entzieht, auf Beschwerde eines Betroffenen hin die Vereinbarkeit der Entscheidung mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte in Frage zu stellen. Gemäß dem EuGH hatte die Kommission keine Kompetenz, die *Befugnisse der nationalen Datenschutzbehörden* in dieser Weise zu beschränken.

Aus den vorgenannten Gründen erklärte der EuGH die Safe-Harbor-Entscheidung für ungültig. Dies hat zur Folge, dass die irische Datenschutzbehörde die Beschwerde von Max Schrems mit aller gebotenen Sorgfalt prüfen und am Ende der Untersuchung entscheiden muss, ob nach der EG-DSRl die Übermittlung der Daten europäischer Facebook-Nutzer in die USA auszusetzen ist, weil dort kein angemessenes Schutzniveau für personenbezogene Daten besteht. Es sei nun Sache der Datenschutzbehörden, über weitere Schritte zu entscheiden. Für künftige Datenschutzabkommen behielt sich der EuGH eine strikte Kontrolle vor.

5 Erste Stellungnahmen

Der *Kläger Max Schrems* interpretierte das Urteil umgehend dahingehend, dass nach dem Wegfall von Safe Harbor der Rückgriff auf Einwilligungen, aber angesichts der inhaltlichen Defizite auch materiell auf Standardvertragsklauseln und Binding Corporate Rules nicht mehr möglich ist. Verhandlungen mit den USA müssten ganz von vorne beginnen. Angesichts des Umstandes, dass die USA inhaltlich weitgehend die bisherige EG-DSRl übernehmen müssten, sei das Hoffen auf ein „Safe Harbor 2.0“ unrealistisch.[5]

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Andrea Voßhoff sah in dem Urteil eine erhebliche Stärkung der *Datenschutzbehörden*. Der in Deutschland für Facebook zuständige Hamburgische Datenschutzbeauftragte meinte, die Kritik des EuGH sei so fundamental, dass ein Stopp der Datenflüsse in die USA in Betracht kommt und stellte fest: „Das ist eine späte Genugtuung für Edward Snowden.“ Dem gegenüber meinte David Smith, der stellv. Britische Datenschutzbeauftragte, in einem Blogpost: „Keine Panik, keine Hektik, warten Sie auf weitere Hinweise“.[6] Der Verhandlungsführer des EU-Parlaments für die Europäische Datenschutz-

[5] Vgl. http://www.europe-v-facebook.org/EN/Complaints/PRISM/Response/response.html#alts.
[6] Vgl. https://iconewsblog.wordpress.com/2015/10/27/the-us-safe-harbor-breached-but-perhaps-not-destroyed/.

Grundverordnung (EU-DSGVO), der Abgeordnete Jan-Philipp Albrecht (Grüne), forderte, den Datentransfer auf der Grundlage von Safe Harbor zu unterbinden.

Vertreter der deutschen Wirtschaft verwiesen dagegen auf die laufenden Verhandlungen zwischen dem US-Handelsministerium und der EU-Kommission über eine Reform von Safe Harbor. So warnte Markus Kerber, Geschäftsführer des Bundesverbands der Deutschen Industrie (BDI): „Die USA sind Europas wichtigster Handelspartner. Ein Abbruch des Datenaustauschs wäre ein Paukenschlag“.[7] In einem offenen Brandbrief an EU-Kommissionspräsident Jean-Claude Juncker forderten mehrere Wirtschaftsverbände gemeinsam eine „harmonisierte Umsetzung“ des Urteils und eine „ausreichende Übergangsperiode“ für Unternehmen, sich den neuen Anforderungen anzupassen.[8] Mit Datum vom 10.11.2015 veröffentlichte der deutsche IT-Branchenverband „bitkom“ einen ausführlichen Leitfaden „Das Safe-Harbor-Urteil des EuGH und die Folgen – Fragen und Antworten“, in dem Unternehmen Empfehlungen gegeben werden, wie sie mit der neuen Rechtssituation umgehen können.[9]

Facebook, das den Anlass für das Urteil gegeben hatte, erklärte umgehend, von diesem nicht betroffen zu sein, da man sich „wie tausende europäischer Unternehmen“ auf weitere Möglichkeiten nach dem europäischen Recht verlasse, um „unabhängig von Safe Harbor“ legal Daten aus Europa in die USA zu übermitteln. Man könne zudem beim Registrierungsprozess vom Nutzer dessen Einverständnis einholen, womit die Übermittlung in die USA legitimiert werde.

Erstaunlich waren die Reaktionen aus der *EU-Kommission*. Der erste Vizepräsident der Kommission, Frans Timmermans, erklärte, er sehe im Urteil eine „Bestätigung für das Bestreben, den ´sicheren Hafen` neu zu verhandeln“. Die Justizkommissarin Vera Jourová ergänzte, man habe seit 2013 „unnachgiebig“ mit den USA an der Reform gearbeitet. Es seien „wichtige Fortschritte“ erzielt worden, „auf denen wir im Lichte des Urteils aufbauen können“. Bis ein neuer „sicherer Hafen“ entstehe, könnten die transatlantischen Datenflüsse anhand der anderen verfügbaren rechtlichen Mechanismen, so Timmermans und Jourová, ungehindert weitergehen. Davon ging auch die luxemburgische Präsidentschaft in ihrem Statement aus. Der für das Digitale zuständige EU-Kommissar Günther Oettinger erklärte, dass das Urteil auch Anlass zur Selbstkritik sei: „Wir haben die Praxis in den USA jahrelang nicht konsequent genug beobachtet. … Wir müssen sehen, inwieweit sich unsere amerikanischen Partner auf unser Datenschutzniveau einlassen. Da treffen unterschiedliche Sichtweisen aufeinander. Ich warne davor, dass wir mit übertriebenen Erwartungen in die Verhandlungen gehen – und dann gar nichts erreichen. … Mich wundert immer wieder, dass wir Deutschen sehr sensibel sind, was den Datenschutz im Allgemeinen angeht“.

Das *EU-Parlament* (EP) hatte schon Anfang 2014 gefordert, Safe Harbor zu überprüfen. Nach dem Urteil forderte der Vorsitzende des EP-Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres (LIBE), der britische Labour-Abgeordnete Claude Moraes, nun „einen starken Rahmen für die Weitergabe personenbezogener Informationen“ mit „soliden durchsetzbaren Datenschutzrechten und einer effektiven unabhängigen Aufsicht“.[10] Am 13.10. begrüßte der LIBE-Ausschuss die EuGH-

[7] Abrufbar unter https://www.bitkom.org/Bitkom/Publikationen/Safe-Harbor-Entscheidung-des-EuGH.html.
[8] EU-Datenschützer setzen Ultimatum für Safe Harbor 2.0, www.heise.de 17.10.2015.
[9] Janisch, Historisches Urteil zum Datenschutz, SZ 07.10.2015, 1.
[10] Krempl, Safe Harbor: EU-Kommission sieht nach EuGH-Urteil keinen Grund, Datenflüsse zu stoppen, www.heise.de 07.10.2015; Interview von Müller mit Oettinger, „Anlass zur Selbstkritik“, Der Spiegel 42/2015, 45.

Entscheidung und forderte die EU-Kommission auf, den in einem Entschließungsantrag vom 12.03.2014 gestellten Forderungen im Hinblick auf den Datentransfer mit den USA bis Ende 2015 nachzukommen. Sollte dies nicht geschehen, würde sich das EP das Recht vorbehalten, gegen die Kommission mit einer Untätigkeitsklage und Budgeteinschränkungen vorzugehen. Am 23.10.2015 wurde der Entschließungsantrag aus dem Jahr 2014 entsprechend aktualisiert.[11]

In den *USA* wurde das EuGH-Urteil heruntergespielt. Juristen und Unternehmensvertreter meinten, die meisten großen Unternehmen könnten ihre Datenspeicherung von Daten über Europäer in den USA auf der Basis anderer Regelungen fortsetzen, die vom EuGH nicht aufgehoben wurden. Verwiesen wurde unter anderem auf die von der EU-Kommission anerkannten Standardvertragsklauseln. Außerdem wurde angemerkt, dass auch innerhalb Europas nationale Sicherheitsgesetze ermöglichen, zum Zweck der Terrorismusbekämpfung den vollständigen Internetverkehr zu scannen, wodurch ebenso massiv wie in den USA in den Datenschutz eingegriffen werde.[12]

Eine erste gerichtliche Reaktion bestand darin, dass der *Irish High Court*, der dem EuGH das Safe-Harbor-Thema vorgelegt hatte, am 20.10.2015 gegenüber dem Irischen Datenschutzbeauftragten anordnete, Ermittlungen wegen der Geschäftspraktiken von Facebook aufzunehmen. Der Rechtsanwalt Facebooks kündigte eine „konstruktive Mitarbeit“ bei den Untersuchungen an. Der irische Datenschutzbeauftragte kündigte an, die Schrems-Beschwerde nun „mit aller angemessenen Sorgfalt“zu prüfen.[13] Bei den deutschen Datenschutzbehörden gingen nach dem EuGH-Urteil täglich Beschwerden wegen Safe Harbor ein.

6 Datenschutzaufsicht und EU-Kommissions-Entscheidung

Die vom EuGH in die Pflicht gestellten Aufsichtsbehörden reagierten schnell:

6.1 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Als erste Aufsichtsbehörde äußerte sich ausführlich das *Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein* (ULD) mit einem Positionspapier, in dem die Handlungsmöglichkeiten, genauer die Handlungspflichten von EU-Kommission und USA-Gesetzgeber festgehalten werden: Die EU-Kommission müsse ein effektives angemessenes Datenschutzniveau von den USA fordern, wenn weiterhin ein umfassender Datenaustausch praktiziert werden soll. Letztlich sei eine umfassende Änderung des US-amerikanischen Rechts nötig. Auf der Grundlage einer Einwilligung könne eine Übermittlung in die USA nicht mehr erfolgen; denkbar sei nur die Übermittlung im Rahmen von Vertragsbeziehungen. Standardverträge seien zu kündigen; die darauf basierenden Datenübermittlungen seien auszusetzen. Das ULD wies auf seine Befugnisse hin, per verwaltungsgerichtlicher Anordnung Datenübermittlungen in die USA zu verbieten oder auszusetzen bzw. Bußgelder zu verhängen.[14] Die IT-Rechtsanwältin Nina Diercks kommentierte spontan: „Es ist

[11] Mass surveillance: EU citizens' rights still in danger, MEPs say, http://www.europarl.europa.eu/pdfs/news/expert/infopress/20151012IPR97210/20151012IPR97210_en.pdf, EP, B8-1092/2015, 23.10.2015 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2015-1092+0+DOC+PDF+V0//EN.
[12] Mass Surveillance, The New York Times International Weekly, SZ 16.10.2015, 2.
[13] Humphries, Irish court orders investigation of Facebook data transfer to U.S., www.reuters.com 20.10.2015.
[14] Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14 v. 14.10.2015, https://www.datenschutzzentrum.de/artikel/967-.html.

Wahnsinn, einfach nur Wahnsinn. Da wird ewige Zeiten verschlafen, sich grundlegend um Datenschutz bzw. internationale Datenschutzniveaus zu kümmern und wundert sich dann über ein Urteil, dessen zu Grunde liegende Tatsachen nicht erst seit gestern bekannt sind".[15]

6.2 Artikel-29-Arbeitsgruppe

Am 15.10.2015 gab die *Artikel-29-Arbeitsgruppe* ihr erstes Statement ab. Sie wies darauf hin, dass sie wiederholt auf die Rechtswidrigkeit der massenhaften und willkürlichen Überwachung hingewiesen habe und forderte die EU-Mitgliedstaaten und die europäischen Institutionen auf, „offene Gespräche mit den US-amerikanischen Behörden zu führen, um politische, rechtliche und technische Lösungen zu finden", damit die Grundrechte bei Übermittlungen in die USA gewahrt würden. Die aktuellen Verhandlungen für ein neues „Safe Harbor" könnten allenfalls „Teil der Lösung sein", nötig seien umfassende „politische, rechtliche und technische Lösungen". Es bedürfe verbindlicher Mechanismen „in Bezug auf die nötige Kontrolle des staatlichen Zugriffs, Transparenz, Verhältnismäßigkeit, Rechtsmittel und Datenschutzrechte." Die Überprüfung von Standardvertragsklauseln und Binding Corporate Rules (BCRs) wurde angekündigt. Sollte bis Ende Januar 2016 keine Lösung „in Zusammenarbeit mit den US-Behörden" gefunden sein, seien die EU-Datenschutzbehörden verpflichtet, „alle notwendigen und angemessenen Maßnahmen zu ergreifen, einschließlich koordinierter Durchsetzungsmaßnahmen".[16]

6.3 Konferenz der Deutschen Datenschutzbeauftragten

Am 26.10.2015 folgte ein Positionspapier der deutschen *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*. Dieses schließt sich in vieler Hinsicht der Artikel-29-Arbeitsgruppe an. „Soweit Datenschutzbehörden Kenntnis über ausschließlich auf Safe Harbor gestützte Datenübermittlungen in die USA erhalten, werden sie diese untersagen." Die Unternehmen werden aufgefordert, „unverzüglich ihre Verfahren zum Datentransfer datenschutzgerecht zu gestalten". Anders als das ULD meint die Konferenz, kämen Einwilligungen „unter engen Bedingungen" als tragfähige Grundlage in Betracht. Schließlich werden Kommission, Rat und Parlament der EU aufgefordert, in den laufenden Trilog-Verhandlungen dem EuGH-Urteil zu genügen.[17] In Reaktion hierauf beklagte der Industrieverband DigitalEurope, an dem Google, Apple, IBM und Nokia beteiligt sind, dass allein diese Stellungnahme schon zu einer unnötigen Wettbewerbsverunsicherung führen werde.[18]

6.4 EU-Kommission

Mit Datum vom 06.11.2015 äußerte sich die EU-Kommission erstmals mit einem offiziellen Dokument. Sie weist darauf hin, dass sie seit Januar 2014 daran arbeitet, auf der Grundlage von 13 Empfehlungen[19] Datenübertragungen für EU-Bürger sicherer zu machen. Nach dem EuGH-Urteil habe

---

[15] Diercks, Safe Harbor, www.socialmediarecht.de 14.10.2015.

[16] http://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/StatementOfTheArticle29WorkingParty_DeutscheFassung.html;jsessionid=AB482F0EC78D440833FEDDCF54B7822F.1_cid329?nn=5217154.

[17] http://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/Safe-Harbor_Update%2026_10_2015_Positionspapier%20DSK.html;jsessionid=AB482F0EC78D440833FEDDCF54B7822F.1_cid329?nn=5217154.

[18] Stupp, Tech Industry association bashes German privacy watchdogs, www.euractiv.com, 28.10.2015.

[19] Communication from the Commission to th European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, 27.11.2013, COM(2013) 847 final.

sie die *Verhandlungen mit den USA* intensiviert. Ziel der Kommission sei es, die Gespräche innerhalb von drei Monaten abzuschließen. In der Zwischenzeit müssten Unternehmen das Urteil befolgen und nach Möglichkeit auf alternative Datenübermittlungsinstrumente zurückgreifen. In den Leitlinien für die „Übergangszeit bis zur Annahme eines neuen Rechtsrahmens" hebt die Kommission hervor, dass das Safe-Harbor-Abkommen nicht mehr als Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA dienen kann. Bei ihren Verhandlungen mit den USA müsse die Kommission insbesondere erreichen, dass „in Bezug auf die Beschränkungen und Garantien bezüglich des Zugriffs auf personenbezogene Daten durch die US-amerikanischen Behörden" den EuGH-Anforderungen genügt wird. Darüber hinaus müssten weitere Angemessenheitsbeschlüsse geändert werden.

In der Mitteilung werden *alternative Grundlagen für die Übermittlung* personenbezogener Daten in die USA dargelegt, ohne der Unabhängigkeit und den Befugnissen der Datenschutzbehörden der Mitgliedstaaten bei der Rechtmäßigkeitskontrolle vorgreifen zu wollen. Datenübertragungen von Unternehmen könnten derzeit auf folgenden Grundlagen erfolgen: vertragliche Regeln, Binding Corporate Rules sowie die Ausnahmeregelungen nach Art. 26 Abs. 1 EG-DSRl. Am 15.10.2015 hatten sich EU-Vizepräsident Ansip sowie die Kommissionsmitglieder Oettinger und Jourová mit Vertretern der Unternehmen und der Industrie getroffen, wobei letztere eine einheitliche Auslegung des Urteils und mehr Klarheit über die ihnen für Datenübermittlungen zur Verfügung stehenden Instrumente gefordert hatten.[20]

7 Generelle Einordnung des Urteils

7.1 Der EuGH als Grundrechtsgarant

Nachdem sich der EuGH lange Zeit in Fragen des Datenschutzes eher zurückgehalten hatte, schärfte das oberste europäische Gericht in den letzten 18 Monaten sein Profil massiv. Ähnliche Paukenschlag-Entscheidungen waren das Urteil zum „Recht auf Vergessen" bei der Google-Suche[21] sowie die Ungültigkeitserklärung der EU-Richtlinie über die Vorratsspeicherung von Telekommunikationsverkehrsdaten.[22] Damit profilierte sich der EuGH als Konkurrenz und zugleich als Partner des deutschen Bundesverfassungsgerichts (BVerfG), das hinsichtlich der *Präzisierung des Grundrechts auf Datenschutz* bisher meinungsführend war. Die Rechtsprechung des EuGH gleicht teilweise bis in die Wortwahl hinein der des BVerfG, allerdings mit der Besonderheit, dass die Aussagen nun europaweit gelten.

7.2 Die Geschichte von Safe Harbor

Safe Harbor war von Anfang an ein *politischer Kuhhandel* ohne grundrechtliche Basis. Es ging darum, trotz des europäischen digitalen Grundrechtsschutzes, der keine Entsprechung in den USA findet, den transatlantischen Datenaustausch aufrecht zu erhalten. Angesichts der großen Bedeutung der

[20] Communication from the Commission to th 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-362/14 (Schrems), 6.11.2015, COM(2015) 566 final; PM Europäische Kommission v. 06.11.2015, Kommission veröffentlicht Leitlinien für transatlantische Datenübermittlungen und fordert rasche Einigung auf neuen Rechtsrahmen als Konsequenz aus dem Schrems-Urteil.
[21] EuGH, U. v. 13.05.2014, C-131/12, AfP2014, 245.
[22] EuGH, U. v. 08.04.214, C-293/12, C-594/12, NVwZ 2014, 709.

informationellen Verflechtung zwischen den Informationswirtschaften von USA und EU sollten dem ungehinderten Profitstreben beim personenbezogenen Datenverkehr keine grundrechtlichen Hindernisse in den Weg gelegt werden.

Die Einhaltung von Safe Harbor war zunächst kein für die Öffentlichkeit relevantes Datenschutzthema. Dies änderte sich 2008 zumindest für die Fachöffentlichkeit, als Chris Connolly in seiner Galexia-Studie feststellte, dass selbst die laxen Safe-Harbor-Regeln von vielen US-Unternehmen missachtet wurden.[23] Ein *Vollzug durch die US-Aufsichtsbehörde*, die Federal Trade Commission (FTC) fand de facto, insbesondere bei großen IT-Unternehmen, nicht statt. Trotz massiver Kritik der deutschen Datenschutzbehörden änderte sich hieran nichts grundlegend.[24] So blieb z. B. eine Beschwerde des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) wegen der Missachtung von Safe Harbor durch Facebook einfach unbeantwortet.[25]

Zum Zeitpunkt der EuGH-Entscheidung nahmen rund 4.400 Unternehmen die Erleichterungen von Safe Harbor in Anspruch, darunter sämtliche *großen US-IT-Unternehmen*: Google, Facebook, Microsoft, Amazon, Salesforce… Es scheint, dass es diese Firmen sind bzw. waren, die Safe Harbor als eine mehr oder weniger lästige Pflicht abgearbeitet haben. Diesen gegenüber hatte sich – zumindest in Fragen von Safe Harbor – die US-amerikanische Aufsichtsbehörde auch als äußerst konziliant erwiesen. Demgegenüber sollen, so anwaltliche Unternehmensberater, kleinere US-amerikanische Datenimporteure die Pflichten von Safe Harbor in größerem Maße ernst genommen haben.

Das EuGH-Urteil kam also *nicht überraschend*. Die von Unternehmen vergossenen Krokodilstränen entwichen Reptilien, die sich jahrelang durch Missachtung der datenschutzrechtlichen Regeln den Bauch gefüllt haben. Nachdem sich schon die EU-Kommission kritisch zu Safe Harbor geäußert und das Votum des Generalanwalts im EuGH-Verfahren an Safe Harbor nichts Gutes gelassen hatte, war nur noch fraglich, wie deutlich und mit welcher Begründung der EuGH Safe Harbor verwerfen würde. Der EuGH hat sich in seiner Begründung im Umfang beschränkt, aber die Kernpunkte mit einer kaum zu übertreffenden Klarheit herausgearbeitet.

Zum Zeitpunkt des EuGH-Urteils verhandelte die EU-Kommission mit den USA bereits seit zwei Jahren über eine Neuregelung von Safe Harbor. Die *geheimen Gespräche* sollen kurz vor einem Abschluss gestanden haben, wobei – soweit dies bekannt ist – bisher nur eher kosmetische Korrekturen der vorherigen Regelung konsentiert waren. Diese dürften in vieler Hinsicht den geleakten Vereinbarungen zu einem Umbrella-Abkommen für Datenübermittlungen zum Zweck der Strafverfolgung entsprochen haben (s. u. 9.1). Das US-Außenministerium hatte noch kurz vor dem EuGH-Urteilsspruch beteuert, das NSA-Überwachungsprogramm Prism richte sich gegen „konkrete zulässige Ziele“. Ein Aus von Safe

[23] Zusammenfassend Chris Connolly, EU/US Safe Harbor–Effectiveness of the Framework in relation to National Security Surveillance, http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf.
[24] Vgl. ULD, PE v. 23.07.2010; 10 Jahre Safe Harbor – viele Gründe zum Handeln, kein Grund zum Feiern, https://www.datenschutzzentrum.de/presse/20100723-safe-harbor.htm.
[25] Schreiben des ULD an die FTC vom 21.08.2012, https://www.datenschutzzentrum.de/facebook/kommunikation/20120821-ftc-facebook-de.pdf.

Harbor würde dem Schutz der Bürgerrechte „erheblichen Schaden“ zufügen und den „freien Fluss von Informationen verhindern.[26]

8 Konsequenzen und Lösungsansätze

Den Stellungnahmen der Aufsichtsbehörden zu den Folgewirkungen ist zuzustimmen: Mit dem Urteil ist ab sofort die Rechtfertigung von Datentransfers in die USA per Safe Harbor nicht mehr möglich. Interessanterweise bleibt Safe Harbor als Selbstverpflichtung nach US-amerikanischem Recht dort weiter wirksam.

Die Ausführungen des EuGH gelten nicht nur für Safe Harbor, sondern *umfassend* auch für Standardvertragsklauseln, Binding Corporate Rules (BCRs) sowie für die Datenweitergabe öffentlicher Stellen, etwa bei der Übermittlungen für Zwecke der Terrorismusbekämpfung und für andere Zwecke der öffentlichen Sicherheit und der Strafverfolgung.

8.1 Standardvertragsklauseln

Die Urteilsgründe sind insofern unmissverständlich, als die aktuellen Standardvertragsklauseln zwar weiter formell wirksam sind, aber keine rechtliche Basis mehr haben und deshalb aufgehoben werden müssen. Wie die Datenschutzaufsichtsbehörden richtig feststellten, beschränkt sich die Wirkung des EuGH-Urteils nicht auf Safe Harbor.

Unternehmensanwälte und sogar die EU-Kommission gaben den Ratschlag, auf dieses Instrument nunmehr auszuweichen. Dies wurde von vielen Unternehmen dann auch tatsächlich umgehend umgesetzt. Um diese nicht in falscher Sicherheit zu wiegen, sollte die EU-Kommission ihre Beschlüsse zu den Standardvertragsklauseln umgehend aufheben und durch neue Regelwerke zu ersetzen (s. u. 8.9).

8.2 Europäische Datenverarbeitung

Die wirksamste und für die Unternehmen wie für die Betroffenen sicherste Reaktion auf das Urteil ist es, wenn die verantwortlichen Stellen ihre bisher in den USA erfolgende Datenverarbeitung nach Europa holen. Dann besteht für die Betroffenen ein geringeres Risiko der Massenüberwachung ohne Rechtsschutz. Dies gilt auch für Konzerne und Firmengruppen, die Unternehmensteile in den USA betreiben. US-Behörden können zwar über den Patriot Act, den Foreign Intelligence Surveillance Act (FISA) und über weitere US-rechtliche Instrumente in Europa gespeicherte Daten einfordern[27], aber hiergegen können sich die Unternehmen tatsächlich und rechtlich zur Wehr setzen, so wie dies – bisher ohne Erfolg – Microsoft in einem konkreten Fall versucht.[28] Werden mit den USA verflochtene Unternehmen in eine Datenverarbeitung einbezogen, so sollte in den entsprechenden Verträgen verpflichtend eine Information über entsprechende Herausgabeforderungen vorgesehen werden, die auch an die eigenen Aufsichtsbehörden und die Betroffenen weitergegeben werden kann. Eine solche Information steht zwar regelmäßig im Widerspruch zu US-Recht, aber derartige Konflikte zwischen widersprechenden Pflichten aus verschiedenen Rechtskreisen sind nichts Ungewöhnliches – gerade für

[26] Hurtz, Sicherer Server gesucht, SZ 07.10.2015, S. 2.
[27] ULD, https://www.datenschutzzentrum.de/internationales/20111115-patriot-act.html.
[28] Bernau/Seeling, Grenzüberschreitung, SZ 22.01.2015, 19.

international tätige Unternehmen. Über das mit diesen Konflikten verbundene Risiko sollten sich die beteiligten Stellen bewusst sein.

Es ist eine interessante Frage, inwieweit das EuGH-Urteil Übermittlungen nach Großbritannien (UK) ausschließt, wo – wie in den USA – durch den britischen Geheimdienst *GCHQ* anlasslose Massenüberwachungsmaßnahmen praktiziert werden. Inzwischen wissen wir, dass derartige Maßnahmen nicht nur von Diensten in UK durchgeführt werden, sondern auch vom deutschen Bundesnachrichtendienst sowie anderen europäischen Diensten. In Frankreich sollen derartige flächendeckende Überwachungsmaßnahmen gerade per Gesetz legalisiert werden.[29]

Bei einer Verarbeitung innerhalb der EU ist die Rechtslage zumindest insofern klar: Wegen des normativ gewährleisteten Datenschutzniveaus im Empfängerland darf – dem *europäischen Binnenmarkt* und der europäischen Datenschutzrichtlinie (EG-DSRl) sei Dank – kein Datentransfer verweigert werden. Im Konfliktfall kann – u. a. unter Berufung auf Art. 7, 8 und 47 EuGRCh – Rechtsschutz erlangt werden.

8.3 Regulierung des Datenverkehrs über Freihandelsabkommen?

Derzeit werden von der EU-Kommission mehrere Freihandelsabkommen verhandelt, in denen der kommerzielle grenzüberschreitende Austausch von Waren und Dienstleistungen erleichtert oder gar weitgehend dereguliert werden sollen. Bei informationstechnischen Dienstleistungen findet zumeist auch eine Weitergabe von personenbezogenen Daten statt, so dass das Datenschutzrecht zu einem „Handelshemmnis“ werden kann, das mit den Abkommen abgebaut werden soll. Die Hoffnungen, über solche Freihandelsabkommen, etwa über das transatlantische Abkommen zwischen der EU und den USA (*TTIP*) aus der Grundrechtsbindung von grenzüberschreitenden Datentransfers ausbrechen zu können und so quasi nebenbei neue Zulässigkeitsgrundlagen für die Datenübermittlung in die USA zu schaffen, sind unbegründet. Diese Abkommen enthalten regelmäßig unter Hinweis auf Art. 14 Welthandelsabkommen GATT im Hinblick auf den Datenschutz eine Ausnahmeklausel. Dessen ungeachtet ist bei dem Aushandeln der Handelsabkommen darauf zu achten, dass diese Generalausnahme im GATT nicht durch spezifische Regelungen faktisch ausgehebelt werden.[30]

8.4 Binding Corporate Rules (BCRs)

Die Entscheidung der deutschen Datenschutzbehörden, zunächst keine BCRs mehr nach § 4c Abs. 2 Bundesdatenschutzgesetz (BDSG) zu genehmigen, ist konsequent. Die bestehenden BCRs dürften weitgehend nicht den materiell-rechtlichen Anforderungen des EuGH genügen. Nach entsprechender Anerkennung durch die Aufsichtsbehörden in der Vergangenheit entfalten diese aber weiterhin eine *rechtliche Wirkung*. Angesichts der nun vorliegenden klarstellenden EuGH-Rechtsprechung fehlte den bisher erfolgten Genehmigungen nach heutiger Erkenntnis die materiell-rechtliche Grundlage. Die erfolgt jeweils auf der Grundlage eines von Anfang an rechtswidrigen Verwaltungsaktes. Die Aufsichtsbehörden sind aufgefordert, zunächst generell neue Anforderungen an BCRs zu formulieren, diese den Unternehmen mitzuteilen und zu verlangen, ihre BCRs innerhalb einer angemessenen Frist anzupassen. Wird dem nicht entsprochen, so können die Genehmigungen nach dem jeweiligen Verwaltungsverfahrensrecht (vgl. § 48 BVwVfG) zurückgenommen werden. Hinsichtlich der

[29] Ermert, Überwachung: Frankreichs Senat winkt Carte Blanche für Geheimdienst durch, www.heise.de 28.10.2015.
[30] Weichert, Freihandelsabkommen contra Datenschutz? DuD 2014, 850.

Anforderungen kann auf die Ausführungen zu den Standardvertragsklauseln verwiesen werden (s. u. 8.9).

8.5 Übergangsfrist für rechtliche Konsequenzen?

Hinsichtlich der offiziell noch *nicht aufgehobenen Rechtsgrundlagen* für grenzüberschreitende Datenübermittlungen, also Standardvertragsklauseln und BCRs, genießen die Unternehmen Vertrauensschutz. Dieser sollte so schnell wie möglich durch entsprechende Überarbeitungen korrigiert werden.

Unabhängig davon dürfen die offiziellen Stellen – also auch die Aufsichtsbehörden – dürfen die Unternehmen nicht längere Zeit im Ungewissen lassen, aber auch nicht überfordern. Insofern ist die von der Artikel-29-Arbeitsgruppe gesetzte Frist vom 31.01.2016 als *Stillhaltezusage* in Bezug auf konkrete Sanktionen zu begrüßen. Diese entbindet die Aufsichtsbehörden aber nicht, umgehend die Anforderungen an vertragliche Regelungen zum Datentransfer zu überarbeiten, die betroffenen Unternehmen zu kontaktieren und auf der neuen Grundlage konkrete Lösungen einzufordern. Die mit der Fristsetzung explizit verbundene Erwartung im Hinblick auf die US-Position ist aber illusorisch: Auch wenn die EU-Kommission dies von den USA einfordern wird, so werden diese sich nach den bisherigen Erfahrungen weigern, den Anforderungen des EuGH an gerichtlichen Rechtsschutz, materielle Datenschutzrechte und Umsetzung des Verhältnismäßigkeitsgrundsatzes nachzukommen. Erfolgversprechender ist der Ansatz, die Standardvertragsklauseln möglichst schnell an das EuGH-Urteil anzupassen (dazu näher unten 8.9). Dazu sollte die EU-Kommission bis Ende Januar 2016 in der Lage sein.

8.6 Rechtsgrundlage: Einwilligung

Bevor der rechtlich geforderte Mindestinhalt von Standardvertragsklauseln und BCRs erörtert wird, ist auf die kontrovers erörterte Frage einzugehen, inwieweit Einwilligungen Datentransfers in die USA rechtfertigen können. Insofern weist das ULD zu Recht darauf hin, dass eine Einwilligung nur wirksam sein kann, wenn nachweisbar auf das fehlende Datenschutzniveau und auf die US-staatlichen Zugriffsbefugnisse hingewiesen wurde, um zumindest ansatzweise zu gewährleisten, dass die erteilte Einwilligung informiert erfolgte. Der formularmäßige Hinweis in allgemeinen Geschäftsbedingungen (AGB) genügt hierfür nicht. Sind alle weiteren Anforderungen an eine wirksame Einwilligung – insbesondere Freiwilligkeit, Information über die Art der Daten, die Zwecke und die verarbeitenden Stellen – gegeben, so können Einwilligungen wirksam sein. Einwilligungen in Beschäftigungsverhältnissen sind nur freiwillig, wenn der Beschäftigte diese verweigern kann, ohne berufliche Nachteile befürchten zu müssen.

8.7 Rechtsgrundlage: Vertrag mit dem Betroffenen

Übermittlungen zur Vertragserfüllung können zulässig sein. Da trotz der umfassenden Berichterstattung in den Medien der Mangel des Datenschutzniveaus in den USA nicht als allgemein bekannt vorausgesetzt werden kann, ist es – im Interesse der Wirksamkeit der erfolgenden Willenserklärung bei Vertragsabschluss – dringend zu empfehlen und wohl in den meisten Fällen rechtlich gefordert, in dem Vertragstext einen expliziten Hinweis auf das bestehende Risiko zu geben. Um keine Missverständnisse entstehen zu lassen: Vertragsbasierte Datenübermittlungen setzen Verträge zwischen Betroffenen und verarbeitenden Stellen voraus; Daten über Dritte können auf dieser Grundlage nicht weitergegeben werden.

8.8 Betriebsvereinbarungen

Aus Sicht von Beschäftigtenvertretungen mag es zunächst so scheinen, als träfe allein den Arbeitgeber als verantwortliche Stelle die Pflicht, Zulässigkeitsgrundlagen zu prüfen und eventuell neu zu begründen. Haben die Betriebsparteien jedoch im Rahmen der Mitbestimmung Vereinbarungen geschlossen, durch welche die Übermittlung von Beschäftigtendaten in die USA auf die Safe-Harbor-Regelung gestützt wird, so muss auch die Beschäftigtenvertretung handeln.

Betriebsräte sind gem. § 80 Abs. 1 Satz 1 BetrVG[31] verpflichtet, darüber zu wachen, dass die zum Schutz Beschäftigter geltenden Gesetze und Vorschriften eingehalten werden. Betriebsvereinbarungen haben sich daher daran messen zu lassen, ob sie diese Vorgabe erfüllen. Besonders wenn sie gem. § 4 Abs. 1 BDSG als andere Rechtsvorschrift die Zulässigkeitsgrundlage für die Verarbeitung von Beschäftigtendaten herstellen sollen, sind sie aus Sicht der Beschäftigtenvertretung nicht zustimmungsfähig, sobald sie offensichtlich geltendes Recht verletzen. Betriebsvereinbarungen, die den Anforderungen des EuGH an die Datenübermittlung in die USA nicht genügen, etwa weil sie auf Safe Harbor basieren, sind materiell rechtswidrig. Dies muss vom Arbeitgeber wie vom Betriebsrat beachtet werden, da deren Fähigkeit, als andere Rechtsvorschrift i. S. d. § 4 Abs. 1 BDSG die Zulässigkeit einer Verarbeitung von Beschäftigtendaten in den USA zu begründen, wegen Verletzung höherrangigen Rechts nicht mehr besteht.

Beide Betriebsparteien müssen daher Vereinbarungen neu verhandeln, die ganz oder teilweise auf Safe Harbor aufsetzen und neue Grundlagen für die Verarbeitung der betroffenen Beschäftigtendaten schaffen. Verweigert der Arbeitgeber auch nach ausdrücklicher Aufforderung durch den Betriebsrat die Verhandlung über eine Neufassung, sollte der Betriebsrat die fragliche Vereinbarung kündigen, um sich nicht selbst dem Vorwurf auszusetzen, eine Regelung zu Ungunsten der Beschäftigten zu stützen.

8.9 Vertragliche Verpflichtungen Exporteur-Importeur

Es ist wohl realistisch anzunehmen, dass zumindest mittelfristig die anlasslose massenhafte Internetüberwachung in den USA nicht eingestellt werden wird und dass es auch nicht zu einer gesetzlichen Anerkennung eines einklagbaren, dem europäischen Grundrecht auf Datenschutz vergleichbaren Anspruchs von Jedermann auf Datenschutzrechte kommen wird. So stellt sich die Frage: Wie können Stellen in Europa den Anforderungen des EuGH genügen, wenn Übermittlungen absolut unvermeidlich sind? Wie kann ein angemessener Ausgleich zwischen der Achtung des Grundrechts auf Privatsphäre und den Interessen an einen freien Verkehr personenbezogener Daten aussehen?[32]

Insofern dürfte – außer bei direkter Betroffenenbeteiligung (s.o. 8.6 u. 8.7), also insbesondere bei Standardvertragsklauseln und BCRs – mittelfristig nur ein Weg gangbar sein: Der Datenexporteur verpflichtet den Datenimporteur, abgesichert durch hinreichende Sanktionen wie Vertragsstrafen und Haftungsübernahmen – vergleichbar der Auftragsdatenverarbeitung – im Einzelfall umfassend Auskunft über die dort erfolgende Datenverarbeitung zu geben. Diese Auskunft ermöglicht es dem Exporteur, Auskunft an den Betroffenen oder an die für ihn zuständige Aufsichtsbehörde zu geben. Über den Datenexporteur müssen alle dort geltenden gesetzlichen Betroffenenrechte geltend

[31] Analog für Personalräte aufgrund § 68 Abs. 1 Satz 2 BPersVG bzw. entsprechender Bestimmungen der Landespersonalvertretungsgesetze.
[32] EuGH, U. v. 06.10.2015, C-362, Rn. 42.

gemacht werden können, die mangels Rechtsschutz in den USA dort nicht administrativ und gerichtlich durchgesetzt werden können. Zu den Betroffenenrechten gehört auch das Recht eine unabhängige Datenschutzaufsichtsbehörde anzurufen, die dann die Rechtmäßigkeit der Datenübermittlung im konkreten Einzelfall überprüfen kann. Im Rahmen dieser Prüfung muss und kann sie auch ermitteln, ob der Datenimporteur seinen vertraglichen Pflichten und Garantien entspricht bzw. entsprochen hat.[33] Ist der Betroffenen der Ansicht, dass seine Datenschutzrechte verletzt werden, so kann er auch unter Berufung auf diesen Vertrag den Rechtsweg gegen den Datenexporteur beschreiten.[34] Um diese Möglichkeit zu eröffnen, muss der Exporteur seinen Transfervertrag zugunsten der Drittbetroffenen entweder veröffentlichen oder in anderer geeigneter Weise die Betroffenen hierüber informieren.

Eine solche vertragliche „Regulierung“ des personenbezogenen Datenverkehrs kann natürlich in keiner Weise die hoheitlichen Befugnisse von US-Behörden in den USA einschränken. Es wäre auch eine Illusion, damit die in den USA erfolgende Massenüberwachung einschränken zu können. Über einen solchen Vertrag würden aber erstmals den Betroffenen einklagbare Befugnisse eingeräumt, über die problematische Formen der Datenverarbeitung rechtsstaatlich hinterfragt werden könnten.

9 Fernwirkungen

Das EuGH-Urteil hat Wirkungen auf die Trilog-Verhandlungen zwischen Kommission, Parlament und Rat der EU zu einer *Europäischen Datenschutz-Grundverordnung* (EU-DSGVO). Es ist zu hoffen und unabdingbar, dass die Normen zu grenzüberschreitenden Datenübermittlungen in der EU-DSGVO mit den grundrechtlich abgeleiteten Anforderungen des EuGH in Einklang stehen. Entsprechendes gilt auch für die ebenso im Trilog verhandelte Datenschutzrichtlinie für die Bereiche Justiz und Polizei. Das Erfordernis eines angemessenenund vergleichbaren – nicht identischen – Datenschutzniveaus in den Empfängerländern gilt aufgrund der EG-DSRl schon heute. Es wäre wünschenswert, dass der europäische Gesetzgeber gemäß den materiellen Anforderungen des EuGH explizite Prüfkriterien für die Angemessenheit des Datenschutzniveaus im Empfängerland normiert.

9.1 Umbrella-Abkommen

Zwischen der EU und den USA wird ein sog. Umbrella-Abkommen ausverhandelt, mit dem Datenübermittlungen von der EU in die USA zum Zweck der Strafverfolgung erleichtert werden sollen. Ebenso wie bei der Datenübermittlung durch private Stellen muss bei der Übermittlungen zwischen Behörden den Anforderungen an aufsichtsbehördlichen und gerichtlichen Betroffenenschutz sowie an eine Verhältnismäßigkeitsprüfung genügt werden.[35] Die bisherigen Verhandlungsergebnisse genügen diesen Anforderungen bisher nicht.

[33] EuGH, U. v. 06.10.2015, C-362, Rn. 47, 57.
[34] EuGH, U. v. 06.10.2015, C-362, Rn. 64.
[35] Kritisch schon zuvor Schaar, Leaky Umbrella, 18.09.2015, http://www.eaid-berlin.de/?p=779; Korff, EU-US Umbrella Data Protection Agreement, 14.10.2015, http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/; Boehm, A Comparison between US and EU data protection legislation for law enforcement puposes, 2015, S. 71 ff., http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf.

9.2 Fluggastdaten- und Bankdatenabkommen

Die EU-Justizkommissarin Vera Jourová vertrat die Ansicht, dass das EuGH-Urteil zu Safe Harbor keine Auswirkungen auf den Flug- und Bankdatentransfer habe, also auf die Übermittlungen von Passenger Name Records (PNR) und von Daten des internationalen Bankdienstleisters SWIFT im Rahmen des Terrorist Finance Tracking Programs (TFTP) an US-Behörden. Sie begründet dies damit, dass der Zugriff der US-Behörden in den vorhandenen Regelwerken an enge Vorgaben geknüpft sei und den EU-Bürgern überdies die Möglichkeit eingeräumt sei, sich per Verwaltungs- oder Gerichtsverfahren gegen ungerechtfertigte Zugriffe zu wehren.[36] Diese Äußerung zeugt von einem in einem Rechtsstaat nicht zu tolerierenden Primat der Politik (s. u. 10). Frau Jourová kann nicht entgangen sein, dass die theoretisch zulässigen Rechtsmittel keine Wirksamkeit entfalten. In den Regelwerken wird keine Transparenz für die Betroffenen geschaffen, so dass deren Rechtsschutzbegehren zwangsläufig ins Leere laufen.

9.3 Geheimdienste

Die Diskussion, inwieweit sich das EuGH-Urteil auf die anlasslose Datenerhebung und den Datenaustausch zwischen nationalen Geheimdiensten – auch innerhalb der EU – auswirkt, hat erst begonnen und muss intensiv geführt werden.

9.4 Facebook-Verfahren vor dem BVerwG

Das EuGH-Urteil wird Einfluss auf die ausstehende Entscheidung des Bundesverwaltungsgerichts (BVerwG) im Rechtsstreit zwischen dem ULD und den Betreibern von Facebook-Fanpages in Deutschland haben, worüber am 26.02.2016 verhandelt werden wird. Das zentrale Argument des ULD, dass das Betreiben einer Fanpage ein rechtlich und technisch einheitlicher Vorgang ist, bei dem Fanpage-Betreiber und Facebook sich gegenseitig ergänzen und voneinander abhängig sind, wird durch das EuGH-Urteil gestützt. Der Betrieb von Facebook-Fanpages verstößt, wie der EuGH klargestellt hat, gegen deutsches und europäisches Datenschutzrecht.[37]

9.5 Klagerecht der Datenschutzaufsichtsbehörden

Angesichts der gewaltigen Bedeutung des EuGH-Urteils für den grenzüberschreitenden Datenverkehr ist eine Erwägung des EuGH bisher wenig diskutiert worden, die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Stellungnahme vom 26.10. unter Punkt 11 kurz und knapp thematisiert wurde: „Die Datenschutzbehörden fordern die Gesetzgeber auf, entsprechend dem Urteil des EuGH den Datenschutzbehörden ein Klagerecht einzuräumen.“[38]

10 Abschlussbemerkungen

Das vorliegende EuGH-Urteil wird noch oft besprochen, diskutiert, kommentiert und zitiert werden. Die sich hieraus ergebenden politischen und rechtlichen Konsequenzen sollten darin bestehen, dass das mit der Safe-Harbor-Entscheidung der EU-Kommission im Jahr 2000 zum Ausdruck gebrachte unsägliche *Primat der Politik* beim internationalen Datenschutz dem „Rule of Law“, also der Herrschaft des Rechts, weicht. Safe Harbor beruhte von Anfang an auf der Überlegung, wirtschaftliche

[36] Ermert, EU-Kommissarin: Safe Harbor ohne Auswirkung auf Flug- und Bankdatentransfer, www.heise.de 27.10.2015.
[37] Bündnis 90/Die Grünen Landtagsfraktion Schleswig-Holstein, PE vom 06.10.2015 Nr. 408.15, Das heutige EuGH-Urteil wird auch Auswirkungen auf den Rechtsstreit des ULD gegen Fanpagebetreiber haben!
[38] EuGH, U. v. 06.10.2015, Rn. 65.

Erwägungen, die Macht des Faktischen und die freundschaftlichen Beziehungen zu den USA über die Rechtsstaatlichkeit zu stellen.

Erschreckend sind die ersten Signale von *EU-Rat und EU-Kommission*, wonach die Lektion bisher nicht verstanden wurde und keine klare Umkehr erfolgen soll. Beim Datenschutz gibt es einen vergleichbaren Dauerkonflikt zwischen dem deutschen Gesetzgeber und dem Bundesverfassungsgericht insbesondere in Sicherheitsfragen. Dieser hat schon zu vielen Gerichtsurteilen gegen Bundesgesetze geführt, nicht aber zu einer verfassungskonformen Selbstbeschränkung des Gesetzgebers. Der Bundesgesetzgeber hat soeben mit seinem Gesetz zur Vorratsdatenspeicherung von Telekommunikationsdaten seine Maßlosigkeit erneut unter Beweis gestellt. Ein klügeres, weniger arbeits- und energieaufwändigeres Prozedere auf europäischer Ebene wäre wünschenswert – ist aber wohl nicht realistisch.

Ein Bekenntnis zu einem grundrechtskonformen gelebten Datenschutz läge auch im Interesse der europäischen *IT-Wirtschaft*. Die Umsetzung des EuGH-Urteils eröffnet für diese die Chance, zumindest auf dem europäischen Markt gleichberechtigt zu sein. Derzeit wird sie dadurch benachteiligt, dass sie durch den direkteren Zugriff der Aufsichtsbehörden – anders als viele große US-Unternehmen – sich an Recht und Gesetz orientieren muss.

Ein beliebtes Argument der offiziellen US-Seite in diesem Konflikt lautet, die Grundrechtsorientierung und der damit einhergehende europäische „Daten-Nationalismus“ sei nicht nur in einer globalen Informationsgesellschaft anachronistisch, sondern auch nichts anderes als ethisch verpackter *Protektionismus*. Selbst wenn es das wäre: Die USA verhalten sich ebenso, wenn sie z. B. den chinesischen Technologiekonzern Huawei von öffentlichen Aufträgen ausschließen.[39]

Die gleichbehandelnde Anwendung des Grundrechtsschutzes der Bürger bei europäischen wie bei US-Unternehmen könnte außerdem den Effekt haben, dass die US-Wirtschaft *Druck auf die US-Regierung* ausübt, endlich auch in den USA digitalen Grundrechtsschutz zu etablieren, der nicht nur für US- und evtl. für EU-Bürger gilt, sondern für alle Menschen. So unwahrscheinlich es derzeit erscheinen mag, das Bestreben muss dahin gehen, mit Hilfe des EuGH-Urteils die USA – eingeschlossen die dortige Regierung und den Supreme Court – dazu zu bringen, sich auf ihre verlorengegangenen freiheitlichen und demokratischen Ursprünge zu besinnen und diese den Umständen unserer hochtechnisierten Informationsgesellschaften und unserer modernen Zeit entsprechend anzupassen und fortzuentwickeln.

[39] Zand, Das digitale Chinatown, Der Spiegel 44/2015, 102.