Aus Safe Harbor wird Privacy Shield: Folgen des Urteils des EuGH i.S. Schrems

Zum Urteil des EuGH in der Rechtssache C-362/14 vom 6. Oktober 2015, Maximilian Schrems vs. Data Protection Commissioner

IRIS SIDLER* / **DAVID VASELLA****

Der EuGH erklärte die Entscheidung der Europäischen Kommission für ungültig, welche das US-amerikanische Recht aufgrund des Safe-Harbor-Abkommens als angemessen anerkannt und dadurch eine Grundlage für die Datenübermittlung an zertifizierte US-amerikanische Unternehmen geschaffen hatte. Die Safe-Harbor-Zertifizierung eines US-Unternehmens kann daher keine Datentransfers aus Europa zu diesem Unternehmen mehr legitimieren. Nicht abschliessend klar ist aber, ob andere Grundlagen, die in der europäischen Datenschutz-Richtlinie vorgesehen sind, weiterhin Datentransfers in die USA rechtfertigen können. Ob der Nachfolger des Safe-Harbor-Abkommens, der «EU-US Privacy Shield», die vom EuGH aufgezeigten Mängel des Safe-Harbor-Abkommens beseitigen kann, ist heute ebenfalls noch offen. Dieser Bericht fasst das Urteil des EuGH zusammen und nimmt zu dessen Folgen, die auch die Schweiz betreffen, Stellung.

La décision de la Commission européenne qui considérait que le droit américain était adapté au vu de l'accord relatif au Safe Harbor et qu'il constituait ainsi une base pour la transmission de données à des entreprises américaines certifiées a été invalidée par la CJUE. La certification Safe Harbor d'une entreprise américaine ne peut donc plus légitimer le transfert de données à une telle entreprise depuis l'Europe. Il n'est toutefois pas établi de façon définitive si d'autres bases légales prévues dans la directive européenne sur la protection des données peuvent encore justifier le transfert de données aux États-Unis: La question de savoir si le successeur de l'Accord Safe Harbor, le «EU-US Privacy Shield», pourra remédier aux manquements relevés par la CJUE demeure également ouverte à ce jour. La présente contribution résume la décision de la CJUE et prend position sur les conséquences qu'elle pourra avoir, également en Suisse.

I. Ausgangslage
1. Europäisches Datenschutzrecht
2. Safe Harbor
II. Das Urteil des EuGH i.S. Schrems vom 6. Oktober 2015
1. Ausgangslage und Prozessverlauf
2. Kernaussagen
III. Reaktionen auf das Urteil in Europa
1. Restriktiv: Datentransfers in die USA sind zurzeit kaum mehr erlaubt
2. Abwartend: Andere Grundlagen für Datentransfers in die USA müssen überprüft werden
3. Pragmatisch: Andere Grundlagen für Datentransfers in die USA sind nicht infrage gestellt
4. Phoenix aus der Asche: Aus Safe Harbor wird Privacy Shield
5. Wirtschaftliche Folgen des Urteils
IV. Rechtslage in der Schweiz
1. Grundsätze des schweizerischen Datenschutzrechts
2. Reaktion des EDÖB auf das Urteil des EuGH
3. Zwischenfazit zur Rechtslage in der Schweiz
Zusammenfassung / Résumé

* Rechtsanwältin, Aarau.
** Dr. iur., Rechtsanwalt, Zürich.

I. Ausgangslage

1. Europäisches Datenschutzrecht

Das europäische Datenschutzrecht will ein hohes Datenschutzniveau gewährleisten. Bei der Bearbeitung personenbezogener Daten müssen die Grundrechte und -freiheiten gewährleistet sein, insbesondere das Recht auf Privatsphäre[1]. Dies verlangt bei einer grenzüberschreitenden Bekanntgabe von Personendaten an einen Empfänger ausserhalb der EU, dass das Recht des Empfängerstaats ein angemessenes Datenschutzniveau gewährleistet[2]. Fehlt ein solcher Schutz, ist die Bekanntgabe deshalb verboten, sofern nicht mindestens eine der in der Richtlinie vorgesehenen Ausnahmen erfüllt ist[3].

Ob das Schutzniveau des Empfängerstaats angemessen ist, ist dabei unter Berücksichtigung aller relevanten Umstände festzustellen[4]. Die Kommission kann mit Drittländern ohne angemessenem Schutzniveau sodann Verhandlungen aufnehmen, um diese dazu zu bewegen, durch internationale Verpflichtungen ein angemessenes Schutzniveau zu erreichen[5]. Sodann kann die Kommission feststellen, dass ein Drittland aufgrund von innerstaatlichen Rechtsvorschriften oder von internationalen Verpflichtungen über ein angemessenes Schutzniveau verfügt[6].

2. Safe Harbor

Das US-Handelsministerium hat am 21. Juli 2000 – nach entsprechenden Verhandlungen mit der Kommission – «Grundsätze des sicheren Hafens» und zugehörige «häufig gestellte Fragen (FAQ)» vorgelegt. Diese Grundsätze und FAQ enthalten Datenschutzbestimmungen, denen sich US-Unternehmen freiwillig unterstellen konnten. Mit Entscheidung 2000/520[7] hat die Kommission anerkannt, dass diese Regeln im Verbund mit der entsprechenden Selbstverpflichtung der Unternehmen ein angemessenes Datenschutzniveau gewährleisten (Angemessenheit aufgrund der internationalen Verpflichtungen des sogenannten Safe-Harbor-Abkommens). Infolgedessen durften personenbezogene Daten aus der EU an US-amerikanische Unternehmen weitergeleitet werden, welche sich den Safe-Harbor-Grundsätzen unterstellt hatten, ohne dadurch europäisches Datenschutzrecht zu verletzen (deshalb «Safe Harbor»).

II. Das Urteil des EuGH i.S. Schrems vom 6. Oktober 2015

1. Ausgangslage und Prozessverlauf

Maximilian Schrems, ein österreichischer Staatsbürger und bekannter Datenschutzaktivist[8], ist seit 2008 Nutzer von Facebook. Durch die Eröffnung des Facebook-Nutzerkontos ging er – wie alle europäischen Nutzer – einen Vertrag mit Facebook Ireland ein, einer europäischen Tochtergesellschaft von Facebook, Inc., mit Sitz in Kalifornien. Ein Teil der Infrastruktur von Facebook befindet sich jedoch in den USA. Facebook Ireland übermittelt deshalb Personendaten an Facebook, Inc. Diese Übermittlung stützte sich auf die Safe-Harbor-Zertifizierung von Facebook, Inc.[9].

---

[1] E. 3 des hier besprochenen Urteils des EuGH vom 6. Oktober 2015, Rechtssache C-362/14, nachfolgend «Urteil», sowie Erwägungsgründe 3 und 7 der Richtlinie 95/46 vom 24. Oktober 1995, nachfolgend «Richtlinie».

[2] Art. 25 Abs. 1 der Richtlinie; E. 3 des Urteils; Erwägungsgrund 56 der Richtlinie; so auch Art. 41 Abs. 1 des Entwurfs der Datenschutz-Grundverordnung vom 25. Januar 2012, 2012/0011 (COD); vgl. dazu auch E. SCHWEIGHOFER, Die neue EU-Datenschutz-Grundverordnung: Entstehung und Überblick, Jusletter IT Flash vom 21. Januar 2016.

[3] Die Ausnahmen sind in Art. 26 der Richtlinie festgehalten und betreffen insbesondere die Einwilligung (Art. 26 Abs. 1 lit. a der Richtlinie), den Abschluss oder die Abwicklung eines Vertrags, die Abwehr oder Durchsetzung von Rechtsansprüchen im Ausland, die Konzerndatenschutzregeln (Art. 26 Abs. 2 f. der Richtlinie) sowie die Datenübermittlungsvereinbarung, z.B. gemäss den EU-Standardvertragsklauseln (Art. 26 Abs. 4 der Richtlinie und Beschluss der Kommission vom 5. Februar 2010, [2010/87/EU], Amtsblatt der Europäischen Union L 39 vom 12. Februar 2010, 5 ff.). Die Schweiz kennt eine vergleichbare Regelung in Art. 6 DSG.

[4] Insbesondere der Art und der Zweckbestimmung der Daten, der Dauer der Aufbewahrung und Verarbeitung der Daten sowie des rechtlichen Rahmens, der sich aus nationalem Recht oder internationalen Abkommen ergibt, und der Standesregeln und Sicherheitsmassnahmen im Bestimmungsland, vgl. Art. 25 Abs. 2 und 6 der Richtlinie.

[5] Art. 25 Abs. 5 und Abs. 6 der Richtlinie.

[6] Art. 25 Abs. 6 der Richtlinie.

[7] Entscheidung der Kommission vom 26. Juli 2000 (2000/520/EG).

[8] Siehe dessen Kampagne auf www.europe-v-facebook.org (Februar 2016) sowie <en.wikipedia.org/wiki/Max_Schrems>; im Unterschied zu diesen zwei Verweisen wird im Urteil «Maximillian mit zwei «l» geschrieben, hier zitieren wir Maximilian Schrems so, wie er sich selber nennt.

[9] Siehe E. 26 ff. des Urteils.

Am 25. Juni 2013, kurz nach den Enthüllungen von Edward Snowden[10], reichte Maximilian Schrems Beschwerde ein bei der irischen Datenschutzbehörde (dem Data Protection Commissioner, nachfolgend «Commissioner»). Er brachte vor, das US-amerikanische Recht schütze seine personenbezogenen Daten kaum vor behördlicher Überwachung. Die USA verfügten deshalb, so Schrems, nicht über ein angemessenes Datenschutzniveau, sodass die Weitergabe seiner personenbezogenen Daten an Facebook, Inc. gegen europäisches Recht verstosse[11].

Der Commissioner wies die Beschwerde zurück. Zum einen sah er keine Beweise für Zugriffe der NSA («National Security Agency», der grösste US-amerikanische Auslandsgeheimdienst) auf personenbezogene Daten von Schrems; und zum anderen hielt er sich aufgrund der Safe-Harbor-Entscheidung der Kommission nicht für verpflichtet, die behaupteten Tatsachen zu untersuchen[12]. Die Beschwerde von Schrems sei vielmehr unseriös und schikanös[13].

Schrems zog diese Entscheidung des Commissioner an den irischen High Court weiter. Der High Court befand am 18. Juni 2014, dass die personenbezogenen Daten der Facebook-Nutzer durchaus einer massenhaften und ungezielten Überwachung der NSA ausgesetzt sein konnten[14]. Das geheime Spezialgericht zur Überwachung des Auslandgeheimdienstes mache zudem eine unabhängige Überprüfung seiner Tätigkeit unmöglich[15]. Die Enthüllungen von Snowden hätten vielmehr gezeigt, dass die US-Geheimdienste routinemässig auf personenbezogene Daten von europäischen Bürgern zugreifen können. Zudem sei es in der Tat fraglich, ob die USA über angemessene Kontrollmöglichkeiten verfügten[16]. Somit sei Schrems befugt, auch wenn er den Zugriff der US-Behörden auf seine personenbezogenen Daten nicht belegen könne, sich gegen den Datentransfer zur Wehr zu setzen[17].

Vor diesem Hintergrund unterbreitete der High Court dem EuGH zusammengefasst die Frage zur Vorabentscheidung, ob eine europäische Datenschutzaufsichtsbehörde bei der Prüfung einer Bschwerde an die Entscheidung der Kommission gebunden ist, welche ein angemessenes Datenschutzniveau eines Drittlandes feststellt, oder ob sie vielmehr eigene Ermittlungen zur Sache anstellen muss[18].

2. Kernaussagen

a) Kommission und Mitgliedstaaten müssen die Angemessenheit des Schutzniveaus jeweils unabhängig prüfen

Der EuGH stellt zunächst fest, dass die nationalen Behörden befugt sein müssen, auf Antrag unabhängig von den Entscheidungen der Kommission zu prüfen, ob bei der Übermittlung von personenbezogenen Daten die Anforderungen des Europäischen Datenschutzrechts eingehalten wurden[19]. Somit können und müssen sowohl die Kommission als auch die Mitgliedstaaten prüfen, ob ein Drittland über ein angemessenes Schutzniveau verfügt. Andernfalls würde die Charta der Grundrechte der Europäischen Union[20] (nachfolgend «Charta») unterlaufen[21].

---

[10] Edward Joseph Snowden ist ein «Whistleblower» und ehemaliger US-Geheimdienstmitarbeiter, der Informationen über das Ausmass der globalen Überwachungsprogramme und das entsprechende Vorgehen der Geheimdienste veröffentlichte und dadurch namentlich die US-Geheimdienste internationaler Kritik aussetzte.

[11] E. 2 und E. 26–36 des Urteils.

[12] E. 29 des Urteils.

[13] *«[F]rivolous and vexatious»*, siehe E. 32 des Urteils des irischen High Courts vom 18. Juni 2014, Rechtssache 2013 No. 765JR, <www.dataprotection.ie/docimages/documents/DOC 180614.pdf>, nachfolgend «Urteil des High Court».

[14] *«[P]ersonal data transferred by companies such as Facebook Ireland […] is […] capable of being accessed by the NSA in the course of a mass and indiscriminate surveillance of such data»,* Urteil des High Court, E. 13 ff.

[15] *«[T]he essentially secret and* ex parte *nature of the FISA Court's activities makes an independent assessment of its orders and jurisprudence all but impossible»,* Urteil des High Court, E. 13 ff.

[16] *«The Snowden revelations demonstrate […] that the US security services can routinely access the personal data of European citizens which has been so transferred to the United States and, in these circumstances, one may fairly question whether US law and practice […] provides for meaningful or effective legal control»,* Urteil des High Court, E. 42.

[17] *«Quite obviously, Mr. Schrems cannot say whether his own personal data has ever been accessed or whether it would ever be accessed by the US authorities. But even if this were considered to be unlikely, he is nonetheless certainly entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents and purposes, appears to provide only a limited protection against any interference with that private data by the US authorities»,* Urteil des High Court, E. 45.

[18] Urteil des High Court, E. 70; Urteil E. 36.

[19] E. 40–58, 63, 66 des Urteils.

[20] Charta der Grundrechte der Europäischen Union (2000/C 364/01).

[21] Art. 8 Abs. 3 der Charta und Art. 28 Abs. 3 und 4 der Richtlinie.

b) Bei widersprüchlichen Ergebnissen muss der EuGH entscheiden

Die Mitgliedstaaten dürfen jedoch trotz ihrer Unabhängigkeit bei der Prüfung der Angemessenheit keine Massnahmen treffen, die einer Kommissionsentscheidung zuwiderlaufen[22].

Die Mitgliedstaaten und die nationalen Datenschutzaufsichtsbehörden sind daher nicht befugt, selbst die Ungültigkeit einer Kommissionsentscheidung festzustellen. Beschreitet eine betroffene Person den Rechtsweg und haben nationale Gerichte Zweifel an der Rechtmässigkeit einer Entscheidung der Kommission, müssen sie diese Frage vielmehr dem EuGH unterbreiten, wie es hier geschehen ist[23]. Ferner müssen die Datenschutzaufsichtsbehörden ein eigenes Klagerecht haben, um bei Zweifeln an der Rechtmässigkeit einer Kommissionsentscheidung über die nationalen Gerichte eine Vorabentscheidung des EuGH zu erwirken[24].

c) Ungültigkeit der Safe-Harbor-Entscheidung der Kommission

Der EuGH prüfte sodann die Entscheidung 2000/520 der Kommission auf der Grundlage der Richtlinie im Licht der Charta, und zwar trotz der Tatsache, dass diese Frage gar nicht zur Vorabentscheidung vorgelegt worden war. Zum «angemessenen Datenschutzniveau» i.S.v. Art. 25 Abs. 2 der Richtlinie hielt er dabei fest, dass das ausländische Schutzniveau jenem des EU-Rechts nicht genau entsprechen muss. Verlangt wird aber, dass praktisch wirksame Mittel einen Schutz sicherstellen, der dem des europäischen Rechts der Sache nach gleichwertig ist[25].

Das Angemessenheitserfordernis des EU-Rechts verlangt vom Recht des Datenimporteurs daher unter anderem, dass Grundrechtseingriffe durch klare Regeln beschränkt werden. Zudem müssen Mindestanforderungen für den Rechtsschutz der betroffenen Personen bestehen. Dies gilt besonders bei automatischen Datenverarbeitungen und wenn die Gefahr unberechtigter Zugriffe besteht[26]. Ferner müssen Ausnahmen vom Schutz von Personendaten auf das Notwendige beschränkt werden[27].

Ein System der Selbstzertifizierung – wie das Safe-Harbor-System – kann den erforderlichen Schutz durchaus gewährleisten, sofern wirksame Überwachungs- und Kontrollmechanismen bestehen, die es erlauben, Verletzungen des Datenschutzes festzustellen und zu ahnden[28]. Vor dem Hintergrund der genannten Anforderungen stellt der EuGH aber mehrere Mängel des Safe-Harbor-Abkommens fest:

– Das Abkommen bindet nur die Unternehmen, die sich den Regeln des Abkommens unterstellt haben, nicht aber die amerikanischen Behörden[29];
– Safe-Harbor-zertifizierte Unternehmen bleiben entgegenstehendem inneramerikanischem Recht verpflichtet, das den Schutz des Safe-Harbor-Abkommens deshalb unterlaufen kann[30];
– die Kommission hat bei ihrer Entscheidung nicht geprüft, ob US-amerikanische Rechtsvorschriften Grundrechtseingriffe angemessen begrenzen[31];
– zudem hat die Kommission nicht festgestellt, ob die US-amerikanischen Rechtsvorschriften einen wirksamen gerichtlichen Rechtsschutz vermitteln[32];

[22] E. 50–52 des Urteils.
[23] E. 59–62, 64–65 des Urteils.
[24] E. 64 des Urteils.
[25] E. 73 des Urteils.
[26] E. 91 des Urteils.
[27] E. 92 des Urteils.
[28] E. 81 des Urteils.
[29] E. 82 des Urteils.
[30] E. 85 ff. des Urteils; dazu Anhang I der Entscheidung der Kommission vom 26. Juli 2000 (2000/520/EG): *«Die Geltung dieser Grundsätze kann begrenzt werden a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte, oder c) wenn die Richtlinie oder das nationale Recht Ausnahmeregelungen vorsieht, sofern diese Ausnahmeregelungen unter vergleichbaren Voraussetzungen getroffen werden.»*
[31] E. 88 des Urteils.
[32] E. 89 des Urteils.

– die Kommission hätte ihre Entscheidungen zum angemessenen Schutzniveau regelmässig überprüfen müssen, um allfälligen Veränderungen Rechnung zu tragen[33].

Eine Regelung, die eine unterschiedslose Speicherung von Personendaten erlaubt und die behördliche Zugriffe und Datenbearbeitungen nicht auf das Notwendige beschränkt, ist mit den Anforderungen eines angemessenen Datenschutzes nicht vereinbar. Dies gilt umso mehr für eine Regelung, die es Behörden erlaubt, generell auf den Inhalt elektronischer Kommunikation zuzugreifen[34]. Das Fehlen einer effektiven Möglichkeit, Zugang zu den eigenen Personendaten zu erhalten oder gegebenenfalls ihre Berichtigung oder Löschung zu erwirken, verletzt überdies den Anspruch auf wirksamen Rechtsschutz[35].

Die genannten grundsätzlichen Mängel des Safe-Harbor-Abkommens führen zum Ergebnis, dass das US-amerikanische Recht kein angemessenes Datenschutzniveau gewährleistet – und zwar unabhängig vom Inhalt der einzelnen Grundsätze des Abkommens. Der EuGH erklärt die Safe-Harbor-Entscheidung der Kommission deshalb für ungültig.

III. Reaktionen auf das Urteil in Europa

Das Urteil wurde kontrovers diskutiert. Angesichts der grundsätzlichen Bedenken gegenüber der US-amerikanischen Rechtsordnung, die im Urteil aufgeworfen werden, stellt sich vor allem die Frage, inwieweit Datenübermittlungen in die USA zurzeit überhaupt zulässig sind; denn uneingeschränkte Behördenzugriffe können auch Daten betreffen, die auf einer anderen rechtlichen Grundlage in die USA übermittelt wurden, beispielsweise gestützt auf eine Einwilligung, auf Konzerndatenschutzregeln oder auf die EU-Standardvertragsklauseln[36].

Innerhalb der Stellungnahmen zum Urteil lassen sich drei Hauptrichtungen unterscheiden: eine restriktive Haltung, eine abwartende Haltung und eine pragmatische Haltung. Nachfolgend werden diese Richtungen in groben Zügen dargestellt.

1. Restriktiv: Datentransfers in die USA sind zurzeit kaum mehr erlaubt

a) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Acht Tage nach dem Urteil, am 14. Oktober 2015, hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein auf der Grundlage des deutschen Datenschutzrechts vertreten[37], dass künftig weder Einwilligungen noch Standardvertragsklauseln Datentransfers in die USA begründen können. In den Standardverträgen sichere der Datenimporteur zu, keinen Gesetzen zu unterliegen, die der Einhaltung seiner vertraglichen Pflichten entgegenstehen; und gerade dies könne ein US-Importeur nicht garantieren. Eine Übermittlung von Personendaten an US-Empfänger sei daher im Wesentlichen nur noch im Zusammenhang mit dem Abschluss oder der Abwicklung von Verträgen und auf Antrag oder im Interesse der betroffenen Person zulässig[38].

b) Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Am 20. Oktober 2015 hielt die deutsche Datenschutzkonferenz fest[39], dass vorläufig keine neuen Genehmigungen für Datenübermittlungen in die USA mehr erteilt werden. Eine generelle Unwirksamkeit von Konzerndatenschutzregeln oder den EU-Standardvertragsklauseln wird aber nicht festgestellt. Auch Einwilligungen seien – unter engen Bedingungen – weiterhin eine tragfähige Grundlage.

---

[33] E. 76–78 des Urteils.
[34] E. 94 f. des Urteils, Unvereinbarkeit mit Art. 7 der Charta «Achtung des Privat- und Familienlebens».
[35] Art. 47 der Charta «Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht».
[36] Siehe vorne Fn. 3.
[37] Positionspapier des ULD zum Safe-Harbor-Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14, <www.datenschutzzentrum.de/artikel/967-.html>.
[38] Art. 26 Abs. 1 lit. b und c der Richtlinie; vgl. ähnlich Art. 6 Abs. 2 lit. c DSG.
[39] Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz), <www.datenschutz. hessen.de/ft-europa.htm#entry4521> (aktualisiert am 26. Oktober).

2. Abwartend: Andere Grundlagen für Datentransfers in die USA müssen überprüft werden

a) Artikel-29-Datenschutzgruppe

Am 16. Oktober 2015 veröffentlichte die Artikel-29-Datenschutzgruppe eine Stellungnahme[40]. Die Datenschutzgruppe kündigte darin an, die Auswirkungen des Urteils auf andere Übermittlungsmechanismen zu überprüfen. In der Zwischenzeit sei davon auszugehen, dass diese Mechanismen weiterhin eine ausreichende Grundlage für Datenübermittlungen in die USA darstellen.

Sollte aber bis Ende Januar 2016 mit den US-Behörden keine angemessene Lösung gefunden werden und sollte die Datenschutzgruppe nach vertiefter Prüfung zum Ergebnis kommen, dass die erwähnten Mechanismen angesichts der Feststellungen des EuGH keine ausreichende Sicherheit bieten, so sei es an den nationalen Aufsichtsbehörden, die erforderlichen und angemessenen Massnahmen zu treffen[41].

3. Pragmatisch: Andere Grundlagen für Datentransfers in die USA sind nicht infrage gestellt

a) Europäische Kommission

Am 6. November 2015 hat die Kommission ihre Analyse des Urteils veröffentlicht[42]. Sie vertritt darin die Meinung, dass Datenübermittlungen in die USA auf der Grundlage von Einwilligungen, Konzerndatenschutzregeln oder EU-Standardvertragsklauseln weiterhin erlaubt seien. Dies wird durch den konzeptionellen Unterschied zwischen dem Angemessenheitsgrundsatz von Art. 25 und den Ausnahmeklauseln in Art. 26 der Richtlinie begründet: Die vom EuGH aufgehobene Kommissionsentscheidung 2000/520 hatte auf der Grundlage von Art. 25 *generell* die Angemessenheit des durch das Safe-Harbor-Abkommen vermittelten Schutzes festgestellt. In dieser Allgemeinheit war die Kommissionsentscheidung nicht haltbar. Die Ausnahmeregelungen in Art. 26 der Richtlinie erlaubten Datenübermittlungen dagegen *im Einzelfall* unter Berücksichtigung aller Umstände[43]. Die Verantwortung für die Einhaltung des Datenschutzes liegt dabei freilich, wie die Kommission betont, beim Datenexporteur.

b) Deutscher Bundestag

Der Deutsche Bundestag hat sich Mitte Dezember ebenfalls zu Safe Harbor geäussert. Er bewertet die Standardvertragsklauseln und die Einwilligung weiterhin als ausreichende Grundlagen für Datentransfers in die USA[44].

4. Phoenix aus der Asche: Aus Safe Harbor wird Privacy Shield

a) Der EU-US Privacy Shield

Das Safe-Harbor-Abkommen wurde seit Langem als unzureichend kritisiert. Die Verhandlungen für ein revidiertes Abkommen zwischen der EU und den USA liefen seit geraumer Zeit[45]. Nun haben das Urteil des EuGH und der durch die Artikel-29-Datenschutzgruppe aufgebaute Druck Wirkung gezeigt: Die beiden Seiten haben sich am 2. Februar 2016 auf die Grundzüge eines revidierten Abkommens

---

[40] Die Datenschutzgruppe ist ein durch Art. 29 der Richtlinie eingesetztes, unabhängiges Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes, die Stellungnahme ist abrufbar auf <ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/ 2015/20151016_wp29_statement_on_schre ms_judgement.pdf>.

[41] Die Art und der Umfang dieser Massnahmen wurde aber nicht näher erläutert, und die Artikel-29-Datenschutzgruppe ist selber nicht befugt, Massnahmen zu treffen; siehe auch D. ROSENTHAL/B. KAISER, Datenschutz: Wie weiter mit Datenübermittlungen in die USA?, Jusletter vom 2. November 2015, Rz. 11.

[42] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data for the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-3/14 (Schrems), COM(2015) 566 final, <ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communi cation_final.pdf>.

[43] Vgl. zu diesem Unterschied auch ROSENTHAL/ KAISER (Fn. 41), Rz. 25.

[44] Deutscher Bundestag, Drucksache 18/7134, 18. Wahlperiode, 21. Dezember 2015, <dipbt.bundestag.de/dip21/btd/18/071/1807134.pdf>.

[45] Vgl. dazu das Memo der Kommission vom 27. November 2013 (MEMO/13/1059), <europa.eu/rapid/press-release_MEMO-13-1059_en.pdf>, nachfolgend «Memo der Kommission».

geeinigt[46], das auf «EU-US Privacy Shield» bzw. «EU-US-Datenschutzschild» getauft wurde (nachfolgend «Privacy Shield»). Am 29. Februar 2016 wurde sodann die Dokumentation des Privacy Shield veröffentlicht[47]. Wie bereits das Safe-Harbor-Abkommen ist auch der Privacy Shield kein eigentliches Abkommen, sondern besteht vielmehr aus Massnahmen und Zusagen seitens der USA, die es der Kommission erlauben sollen, diesbezüglich die Angemessenheit des amerikanischen Datenschutzniveaus festzustellen. Die Dokumentation enthält einführende Unterlagen[48], den Entwurf der Angemessenheitserklärung der Kommission mit einer Übersicht über die «Principles», die für unterstellte Unternehmen gelten werden[49], und mehrere Dokumente mit Zusagen der US-Regierung[50].

Der Privacy Shield sieht folgende Kernpunkte vor, welche zur Verbesserung des Datenschutzes beitragen sollen:

– US-Unternehmen, die nach der Zertifizierung personenbezogene Daten verarbeiten dürfen, müssen strengere Auflagen einhalten[51]. Neu bestehen besondere Informationspflichten («Notice»), ein Opt-Out-Recht der betroffenen Personen («Choice»), Anforderungen betreffend Weitergabe von Personendaten («Onward Transfer»), Auflagen zur Datensicherheit, Regeln über die Verhältnismässigkeit, Zweckbindung und Datenqualität bei der Datenerhebung, Grundsatzbestimmungen über das Auskunftsrecht der betroffenen Personen und zum Rechtsschutz. «Supplemental Principles» enthalten sodann Vorgaben zu besonders schützenswerten Personendaten, zur Haftung von Infrastrukturanbietern, zur Kooperation mit den EU-Datenschutzbehörden, vorzulegende Informationen und Nachweise für die Zertifizierung, die Detailvorgaben zum Auskunftsrecht, zu den Daten von Arbeitnehmern sowie zur Weitergabe von Daten und zum Rechtsschutz inklusive Schiedsverfahren.

– Die Einhaltung der Auflagen der US-Unternehmen soll künftig besser kontrolliert und durchgesetzt werden. Das US-Handelsministerium wird überwachen, dass die US-Datenempfänger ihre Verpflichtungen publizieren. Die Federal Trade Commission (FTC) soll sodann die Einhaltung der Auflagen kontrollieren[52]. Für Verstösse sind Sanktionen vorgesehen, fehlbare Firmen können von der Liste der zertifizierten Unternehmen gestrichen werden. Empfänger von europäischen Arbeitnehmerdaten müssen sich zudem verpflichten, die Entscheidungen der europäischen Datenschutzaufsichtsbehörden zu befolgen[53]. Zudem hat die Federal Trade Commission (FTC) versprochen, Beschwerden von EU-Mitgliedstaaten prioritär zu behandeln[54]. Im Fall einer Beschwerde oder von Amts wegen kann die Federal Trade Commission (FTC) Abklärungen treffen, formelle Untersuchungen eröffnen und Amtshilfe leisten.

– Beim Zugriff auf Daten durch US-Behörden sind neue Schutzvorkehrungen und gewisse Transparenzpflichten vorgesehen. In diesem Zusammenhang weist die amerikanische Seite darauf hin, dass weitere Bestimmungen des US-Rechts die Bürger vor übermässigen Behördenzugriffen schützen wie beispielsweise das Verbot von «unfair or deceptive acts or practices», der «Computer

[46] Kommission, Medienmitteilung, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, Strasbourg, 2. Februar 2016, <europa.eu/rapid/press-release_IP-16-216_ de.htm>, nachfolgend «Medienmitteilung Privacy Shield»; vgl. auch die Informationen des amerikanischen Handelsministeriums vom 2. Februar 2016, <www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy- shield>.

[47] Die Unterlagen und die Medienmitteilung der Kommission «Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield» vom 29. Februar 2016 sind abrufbar auf <europa.eu/rapid/press-release_IP-16-433_en.htm>. Die gesamte Dokumentation ist als PDF abrufbar unter <datenrecht.ch/privacy-shield-dokumenta tion>.

[48] Medienmitteilung sowie Mitteilung der Kommission an das Parlament und den Rat vom 29. Februar 2016, FAQ und Factsheet.

[49] Vgl. dazu Annex II der Dokumentation (siehe sogleich Fn. 50 und 51).

[50] Annex I: Brief des US-Handelsministeriums an die Kommissarin Vˇera Jourová vom 23. Februar 2016; Annex II: Darstellung der Grundsätze des Abkommens (EU-U.S. Privacy Shield Framework Principles) des US-Handelsministeriums; Annex III: Brief des US Secretary of State John Kerry an Kommissarin Vˇera Jourová vom 22. Februar 2016; Annex IV: Brief der US Federal Trade Commission (FTC) an Kommissarin Vˇera Jourová vom 23. Februar 2016; Annex V: Brief des Secretary of Transportation an die Kommissarin Vˇera Jourová vom 19. Februar 2016; Annex VI: Brief des Director of National Intelligence an das US-Handelsministerium und die US International Trade Administration vom 22. Februar 2016; Annex VII: Brief des US Department of Justice an das US Department of Commerce und die US International Trade Administration vom 19. Februar 2016.

[51] Vgl. Entwurf der Angemessenheitserklärung der Kommission, Rz. 16 ff.; Annex II: Darstellung der Grundsätze des Abkommens (EU-U.S. Privacy Shield Framework Principles) des US-Handelsministeriums, Ziff. II., 4 ff., nachfolgend «Principles».

[52] Principles, Ziff. I.2 und II.7.e.

[53] Principles, Ziff. II.7.b und III.5.d.

[54] Principles, Ziff. II.7.e.

Fraud and Abuse Act», der «Electronic Communications Privacy Act», der «Right to Financial Privacy Act» und der «Freedom of Information Act»[55]. Ferner stehe es auch Personen ausserhalb der USA frei, Ansprüche gegen Mitglieder von US-Behörden wegen widerrechtlichen Überwachungstätigkeiten vor dem FISA-Gericht durchzusetzen, inklusive strafrechtlicher Verantwortlichkeit der betroffenen Beamten. Wenn durch Überwachungsmassnahmen gewonnene Daten widerrechtlich und absichtlich gebraucht oder bekannt gegeben werden, haften die USA für den Schaden und die Verfahrenskosten[56]. Zudem werden eine Ombudsperson eingesetzt und ein Koordinationsverfahren geschaffen, was die Behandlung von Anfragen aus der EU betreffend Datenzugriffen der US-Sicherheitsbehörden erleichtern soll[57].

Die Kommission kommt im Entwurf der Angemessenheitsentscheidung zum Ergebnis, dass der Privacy Shield den Vorhaben des EuGH im Urteil i.S. Schrems entspreche. Ob dies tatsächlich zutrifft, ist heute allerdings offen, wie die folgende erste Gegenüberstellung der einzelnen Kritikpunkte des Urteils und des Privacy Shield zeigt.

b) Zum Vorwurf mangelnder Bindung staatlicher Behörden

Der EuGH kritisierte am Safe-Harbor-Abkommen, dass dieses nur die Unternehmen selbst bindet, die sich dem Abkommen unterstellt haben, nicht aber die amerikanischen Behörden[58].

Dieser Punkt ändert sich durch den Privacy Shield nicht. Auch der Privacy Shield bindet nur die ihm unterstellten Unternehmen. Verschiedene US-Behörden haben im Rahmen des Privacy Shield zwar Zusagen gemacht[59]. Diese Zusagen werden offenbar auch im US Federal Register publiziert[60]. Ob und inwiefern diese Zusagen und die Publikation künftige US-Regierungen zu binden vermögen, wird jedoch nicht erläutert.

Der Vorwurf der mangelnden Bindung staatlicher Behörden betrifft jedoch nicht nur Datenübermittlungen in die USA. Zudem vermögen auch andere Datenübermittlungsgrundlagen wie Konzerndatenschutzregeln oder Standardvertragsklauseln staatliche Behörden nicht zu binden. Dieser «Mangel», wenn man diesen Ausdruck überhaupt verwenden will, ist also systemimmanent und kann ohne eine Überarbeitung der Richtlinie nicht ausgeräumt werden[61].

c) Zum Vorwurf des Vorrangs des inneramerikanischen Rechts

Der EuGH kritisierte sodann, dass zertifizierte Unternehmen an entgegenstehendes inneramerikanisches Recht gebunden bleiben, das den Schutz des Safe-Harbor-Abkommens deshalb unterlaufen kann[62].

Auch dieser Punkt ändert sich mit dem Privacy Shield nicht. Allerdings ist im Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (nachfolgend «Konvention 108»)[63] vorgesehen, dass bestimmte datenschutzrechtliche Grundsätze durch das Recht einer Vertragspartei eingeschränkt werden dürfen, soweit dies auf verhältnismässige Weise erfolgt und notwendig ist zum Schutz bestimmter Güter, namentlich der nationalen Sicherheit[64].

---

[55] Annex VI: Brief des Director of National Intelligence an das US Department of Commerce und die US International Trade Administration vom 22. Februar 2016, 17.
[56] Annex VI, Ziff. V; FISA ist die Abkürzung für «Foreign Intelligence Surveillance Act», Annex VI, Ziff. I.
[57] Vgl. dazu insbesondere Annex III: Brief des US Secretary of State John Kerry an Kommissarin V˘era Jourová vom 22. Februar 2016, 1 ff.
[58] Vgl. vorne II.2.c.
[59] Vgl. dazu vorne III.4.a.
[60] Medienmitteilung der Kommission, Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, 29. Februar 2016.
[61] Vgl. ROSENTHAL/KAISER (Fn. 41), Rz. 3 und 25 f.
[62] Vgl. vorne II.2.c.
[63] Übereinkommen 108 des Europarates vom 28. Januar 1981, für die Schweiz in Kraft getreten am 1. Februar 1998, SR 0.235.1.
[64] Art. 9 Konvention 108; vgl. auch ROSENTHAL/ KAISER (Fn. 41), Rz. 30 m.w.H., insbesondere auf die offenbar beinahe fertig gestellte revidierte Fassung der Konvention 108.

Der Vorbehalt des nationalen Rechts, den auch Mitgliedstaaten der EU kennen[65], sollte ein Abkommen zum Datenschutz – und daher auch die Anerkennung der Gleichwertigkeit eines nationalen Rechts – nicht grundsätzlich infrage stellen.

d) Zum Vorwurf mangelnder Begrenzung von Grundrechtseingriffen

Der EuGH stellte weiter fest, dass die Kommission bei ihrer Entscheidung nicht geprüft hatte, ob US-amerikanische Rechtsvorschriften Grundrechtseingriffe angemessen begrenzen[66]. Diese Bedenken dürften auch für den Privacy Shield gelten. Insbesondere behalten sich die USA Massenüberwachungsmassnahmen vor, wenn auch nur zu bestimmten Zwecken, beispielsweise um terroristische Bedrohungen zu erkennen und abzuwehren[67]. Dass der Vorwurf der fehlenden angemessenen Begrenzung der Grundrechtseingriffe dadurch entkräftet wird, ist unwahrscheinlich. Auch beruht die Begrenzung der Massenüberwachung auf einer Anweisung des Präsidenten[68], die sich ändern lässt und deren Fortbestand auch vom Ausgang der kommenden Wahlen in den USA abhängen dürfte.

e) Zum Vorwurf des fehlenden Rechtsschutzes

Schliesslich kritisierte der EuGH, dass die Kommission nicht festgestellt hat, ob die US-amerikanischen Rechtsvorschriften einen wirksamen gerichtlichen Rechtsschutz vermitteln[69].

In diesem Punkt sehen die «Principles» des Privacy Shield vor, dass die zertifizierten Firmen Beschwerden innerhalb einer Frist von 45 Tagen behandeln müssen und dass sich Unternehmen verpflichten, sich auf Schiedsverfahren mit betroffenen EU-Bürgern einzulassen[70]. Zudem können europäische Datenschutzaufsichtsbehörden Beschwerden dem US-Handelsministerium und der Federal Trade Commission (FTC) weiterleiten. Schliesslich wird für Vorwürfe von Eingriffen im Interesse der nationalen Sicherheit eine Ombudsstelle geschaffen, die allerdings nur koordinative Funktion hat und beispielsweise Vorwürfe überschiessender Überwachungstätigkeiten an die zuständige amerikanische Behörde weiterzuleiten hat[71].

Auch in diesem Punkt ist noch kaum eine verlässliche Aussage über die Belastbarkeit des Privacy Shield möglich. Auch die Bedeutung des «Judicial Redress Act», der inzwischen den amerikanischen Senat und den Kongress passiert hat und die Voraussetzungen schaffen soll, ausländischen Bürgern für Ansprüche gegen US-Behörden unter bestimmten Umständen den Zugang zu US-Gerichten zu öffnen[72], ist noch unklar.

f) Zum Vorwurf fehlender regelmässiger Überprüfung

Anders als Safe Harbor sieht der Privacy Shield eine jährliche Überprüfung durch beide Vertragsparteien vor. Zu diesem Monitoring-Prozess werden neben den europäischen Datenschutzbehörden auch die US-Geheimdienste Zugang haben[73].

Zumindest in diesem Punkt sollte der Privacy Shield also eine Verbesserung bringen. Allerdings ist das Vorgehen unklar, wenn sich die beiden Seiten nicht darüber einig werden, ob und wie neue Umstände zu berücksichtigen sind[74].

---

[65] Vgl. dazu zum Beispiel B. WIDMER, Safe-Harbor – wenn weniger nicht genügt, digma 2015, 152.
[66] Vgl. vorne II.2.c.
[67] Schreiben des Director of National Intelligence an das US Department of Commerce und die US International Trade Administration vom 22. Februar 2016, Annex VI des Privacy Shield, <ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf>.
[68] Presidential Policy Directive no. 28 – Signals Intelligence Activities, Januar 2008, <fas.org/irp/offdocs/ppd/ppd-28.pdf>.
[69] Vgl. vorne II.2.c.
[70] Principles, Ziff. II.11, 21 ff. und Annex I der Principles.
[71] Annex III: Brief des US Secretary of State John Kerry an Kommissarin V˘era Jourová vom 22. Februar 2016, 2.
[72] Dazu vgl. <www.congress.gov/bill/114th-congress/house-bill/1428>.
[73] Kommission, Medienmitteilung Privacy Shield: «To regularly monitor the functioning of the arrangement there will be an annual joint review, which will also include the issue of national security access. The European Commission and the U.S. Department of Commerce will conduct the review and invite national intelligence experts from the U.S. and European Data Protection Authorities to it.»
[74] In diesem Zusammenhang ist an die langwierigen Verhandlungen zu einer Revision des Safe-Harbor-Abkommens zu erinnern, die erst der EuGH mit seinem Urteil beschleunigen konnte, vgl. Memo der Kommission, Fn. 47.

g) Zwischenfazit zum Privacy Shield und nächste Schritte

Die Dokumentation zum Privacy Shield wird nun der Artikel-29-Datenschutzgruppe und Vertretern der EU-Mitgliedstaaten zur Konsultation vorgelegt[75]. Die definitive Feststellung der Angemessenheit obliegt schliesslich der Kommission und folgt den dafür geltenden Regeln[76].

Seitens der USA ist geplant, in der Zwischenzeit die notwendigen Vorkehrungen zur Einrichtung des neuen Rahmens, der neuen Überwachungsmechanismen und der neuen Ombudsstelle zu treffen[77].

Der Privacy Shield verspricht Verbesserungen im Bereich Datenschutz. Zu begrüssen sind insbesondere die Verschärfung der für unterstellte Unternehmen geltenden Regeln und die Durchsetzungsmechanismen mit Beschwerdemöglichkeiten für Betroffene. Ob der Rechtsschutz bei Eingriffen der Behörden im Interesse der nationalen Sicherheit durch die Ombudsstelle effektiv gewährleistet werden kann, scheint hingegen fraglich. Sämtliche Kritikpunkte des EuGH können mit dem Privacy Shield jedenfalls kaum beseitigt werden[78]. Zwar sind gewisse der verbleibenden Mängel systemimmanent, nämlich in der Richtlinie selbst angelegt. Dennoch kann nicht ausgeschlossen werden, dass der EuGH auch den Privacy Shield als unzureichend beurteilen wird.

Ob die Zahl der zertifizierten Unternehmen unter diesen Umständen jemals wieder so hoch wird wie zuvor unter dem Safe-Harbor-Abkommen, ist daher ungewiss und von den weiteren Entwicklungen in den nächsten Wochen und Monaten abhängig[79].

5. Wirtschaftliche Folgen des Urteils

Das Safe-Harbor-Abkommen kann Datenübermittlungen in die USA kaum mehr rechtfertigen. Zurzeit ist hingegen davon auszugehen, dass die weiteren Grundlagen zur Übermittlung von Personendaten in Länder ohne angemessenes Datenschutzniveau weiterhin gelten und Datenübermittlungen auch in die USA rechtfertigen können[80]. Hierzu bietet sich vor allem der Abschluss eines Vertrages gemäss den EU-Standardvertragsklauseln an, weil sich diese in der Praxis bewährt haben und ohne aufwendiges Genehmigungsverfahren implementiert werden können[81]. Bei den Konzerndatenschutzregeln ist demgegenüber zu beachten, dass manche europäische Aufsichtsbehörden zurzeit keine entsprechenden Genehmigungen erteilen.

Davon unabhängig darf man das Urteil des EuGH aber nicht nur in einem datenschutz- sowie einem grundrechtlichen, sondern auch in einem wirtschaftspolitischen Kontext lesen. Die Erschwerung der Datenübermittlung in die USA – nicht zuletzt durch eine Erschütterung des Vertrauens – dürfte näm-

[75] Kommission, Medienmitteilung Privacy Shield: «to prepare a draft ‹adequacy decision› in the coming weeks, which could then be adopted by the College after obtaining the advice of the Article 29 Working Party and after consulting a committee composed of representatives of the Member States».
[76] Siehe <ec.europa.eu/justice/data-protec tion/international-transfers/adequacy/index _en.htm>.
[77] Kommission, Medienmitteilung Privacy Shield: «In the meantime, the U.S. side will make the necessary preparations to put in place the new framework, monitoring mechanisms and new Ombudsman.»
[78] Datenschutzaktivisten bezeichnen den Privacy Shield daher bereits als «Accountability Shield», E. SNOWDEN, Twitter, 2. Februar 2016, <twitter.com/snowden/status/6945 71566990921728> oder «Privacy Fig Leaf», Castlebridge Associates, Privacy Shield or Fig Leaf?, 2. Februar 2016, <castlebridge.ie/news/2016/02/02/privacy-shield-or-fig-leaf>.
[79] Die Liste der Unternehmen, die sich nach dem EU-Safe-Harbor-Abkommen zertifiziert haben, hat über 5500 Einträge; <safeharbor.export.gov/list.aspx>; jene der nach dem CH-Safe-Harbor-Abkommen zertifizierten Unternehmen fast 4000, <safeharbor.export.gov/swisslist.aspx>; vgl. zur Beliebtheit von Safe Harbor auch ROSENTHAL/KAISER (Fn. 41), Rz. 8.
[80] Dies entspricht der Meinung der Mehrheit der Institutionen – auch der Kommission – sowie der Lehre.
[81] Gleicher Meinung ROSENTHAL/KAISER (Fn. 41), Rz. 6 sowie Rz. 46 ff.

lich die Wirkung haben, den europäischen Raum als Datenstandort zu stärken. Europäische Unternehmen werden künftig versuchen, Alternativen zum Datentransfer in die USA zu finden[82]. Amerikanische Firmen wie beispielsweise Facebook bauen deshalb neue Rechenzentren in Europa[83]. Allerdings versuchen die US-Justizbehörden sogar auf Daten von US-Unternehmen zuzugreifen, die ausserhalb der USA gespeichert werden[84].

IV. Rechtslage in der Schweiz

1. Grundsätze des schweizerischen Datenschutzrechts

Wie das europäische Datenschutzrecht erlaubt auch das schweizerische Recht eine Bekanntgabe von Personendaten ins Ausland nur dann, wenn diese Bekanntgabe nicht zu einer schwerwiegenden Gefährdung der Persönlichkeit führt[85]. Eine solche Gefährdung wird fingiert, wenn im Empfängerstaat ein angemessenes Schutzniveau fehlt. Dafür ist – im Sinne einer Vermutung – von der Staatenliste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (nachfolgend «EDÖB») auszugehen[86]. Fehlt im Zielland ein angemessener Schutz, ist eine Übermittlung deshalb nur in den vom Gesetz in Art. 6 Abs. 2 DSG abschliessend aufgeführten Fällen zulässig[87]. Dazu gehören insbesondere hinreichende Garantien des Datenempfängers, in der Praxis zumeist in Datenübermittlungsverträgen (insbesondere in der Form der anerkannten Musterverträge, beispielsweise der EU-Standardvertragsklauseln[88]).

Die Schweiz hat mit den USA ebenfalls ein Safe-Harbor-Abkommen geschlossen[89], das dem europäischen Abkommen weitgehend entspricht[90]. In der Folge haben sich fast 4000 Unternehmen nach den Safe-Harbor-Grundsätzen der Schweiz zertifiziert[91]. Gestützt auf das Schweizer Safe-Harbor-Abkommen war davon auszugehen, dass das US-Recht für zertifizierte Unternehmen ein angemessenes Schutzniveau i.S.v. Art. 6 Abs. 1 DSG bietet, und zwar für Personendaten natürlicher wie auch juristischer Personen[92]. Massnahmen gemäss Art. 6 Abs. 2 DSG (Gründe für die ausnahmsweise Übermittlung trotz fehlendem angemessenem Datenschutzniveau) waren daher für solche Übermittlungen nicht erforderlich.

2. Reaktion des EDÖB auf das Urteil des EuGH

Der EDÖB hat sich wiederholt zum Urteil geäussert. In einer ersten Stellungnahme hielt er am 7. Oktober 2016 fest[93], dass durch das Urteil auch das Abkommen zwischen der Schweiz und den USA infrage gestellt sei und Daten daher wenn immer möglich im europäischen Raum gespeichert werden sollten und dass bei Datenübermittlungen in die USA «Zusatzvereinbarungen zum besseren Schutz der betroffenen Personen und ihrer Daten» getroffen werden müssen.

---

[82] Das gilt auch für Datentransfers in andere Staaten mit übermässigen Überwachungssystemen, vgl. dazu WIDMER (Fn. 65), 153, und A Clash of EU privacy standards – European countries could face charges of hypocrisy over data protection, Politico, 13. Februar 2016, <www.politico.eu/article/chash-over-data-protection-standards-privacy-safe-harbor-europe>.

[83] Frankfurter Allgemeine, Facebook baut ein Öko-Rechenzentrum in Europa, 4. Februar 2016, <www.faz.net/aktuell/wirtschaft/facebook-baut-ein-zweites-rechenzentrum-in-europa-14033002.html>; siehe auch Policito, Customer demand drives a jump in Europe-only data handling solutions, 13. Februar 2016, <www.politico.eu/article/cus tomer-demand-europe-data-handling-soluti ons-privacy-shield>.

[84] So geschehen im Fall Microsoft Corporation vs. United States of America, vor dem United States Court of Appeals for the Second Circuit pendent; vgl. dazu WIDMER (Fn. 65), 152, sowie <en.wikipedia.org/wiki/Microsoft_Corporation_v._United_States_of_America>.

[85] Art. 6 Abs. 1 Bundesgesetz über den Datenschutz (nachfolgend «DSG»), SR 235.1.

[86] Art. 7 Verordnung zum Bundesgesetz über den Datenschutz (nachfolgend «VDSG»), SR 235.11; Die «Staatenliste» ist abrufbar auf <www.edoeb.admin.ch/datenschutz/00626/ 00753/index.html> (nachfolgend «Liste»).

[87] Art. 6 Abs. 2 DSG.

[88] Art. 26 Abs. 4 der Richtlinie und Beschluss der Kommission vom 5. Februar 2010 (2010/87/EU), Amtsblatt der Europäischen Union L 39 vom 12. Februar 2010, 5 ff.; vgl. aber auch die auf <www.edoeb.admin.ch/datenschutz/00626/00753/index.html> abrufbaren Dokumente «Europarat Mustervertrag (auf Französisch)» inklusive «Anleitungen des Europarats (auf Französisch)» sowie «Mustervertrag für das Outsourcing von Datenbearbeitungen ins Ausland» des EDÖB.

[89] Briefwechsel vom 1. und 9. Dezember 2008 zwischen der Schweiz und den Vereinigten Staaten von Amerika über die Schaffung eines Datenschutzrahmenwerkes zur Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika, SR 0.235.233.6.

[90] Tätigkeitsbericht des EDÖB 2008/2009, 18 ff.

[91] Vgl. U.S. Government, U.S. – Swiss Safe Harbor List, <safeharbor.export.gov/swisslist.aspx>.

[92] Mitteilung des EDÖB vom 1. Mai 2013, <www.edoeb.admin.ch/datenschutz/0062 6/00753/00970/index.html>.

[93] EDÖB, Safe-Harbor-Urteil des Europäischen Gerichtshofs: Stellungnahme des EDÖB, <www.edoeb.admin.ch/datenschutz/0062 6/00753/00970/01323/index.html>.

Am 14. Oktober hat der EDÖB sodann dem Bundesrat empfohlen, das Schweizer Safe-Harbor-Abkommen mit den USA zu kündigen oder wenigstens zu sistieren[94]. Begründet wird dies einerseits mit der fehlenden Vereinbarkeit des Schweizer Safe-Harbor-Abkommens mit dem Recht auf Privatsphäre, aber vor allem auch mit der Sorge, dass das schweizerische Datenschutzniveau aus Sicht der EU andernfalls nicht mehr anmessen sein könnte[95]. Die bereits erwähnte Staatenliste wurde zudem entsprechend angepasst[96].

Am 22. Oktober 2015 veröffentlichte der EDÖB auf seiner Webseite eine etwas umfassendere Stellungnahme mit den folgenden Kernpunkten[97]:

– Das Safe-Harbor-Abkommen biete keine Grundlage mehr für Übermittlungen von Personendaten in die USA.
– Bis Ende Januar 2016[98] seien beim Datenaustausch mit US-Unternehmen Datenübermittlungsverträge bzw. -klauseln zu vereinbaren.
– Zudem seien betroffene Personen «klar und umfassend über die möglichen Behördenzugriffe» zu informieren, damit diese ihre Rechte wahrnehmen können[99].
– Der schweizerische Datenexporteur und der US-amerikanische Importeur hätten sich zudem zu verpflichten, «betroffenen Personen die für einen wirksamen Rechtsschutz notwendigen Behelfe zur Verfügung zu stellen, entsprechende Verfahren tatsächlich durchzuführen und darauf ergehende Urteile zu akzeptieren».

Schliesslich sah sich der EDÖB unter anderem durch kritische Reaktionen veranlasst, eine weitere Stellungnahme zu veröffentlichen[100]. Darin hielt er fest:

– Neben Datenübermittlungsverträgen stehen die weiteren Massnahmen von Art. 6 Abs. 2 DSG ebenfalls offen für Übermittlungen von Personendaten in die USA. Ob die EU-Standardvertragsklauseln weiterhin verwendet werden dürften, werde aktuell gesamteuropäisch geprüft.
– Bis Ende Januar 2016 würden zudem keine Untersuchungen durchgeführt.
– Betroffene Personen müssten in genereller Weise (bei regelmässigen oder wiederholten Übermittlungen einmal vor der ersten Übermittlung und nicht bei jeder einzelnen Übermittlung) darüber informiert werden, dass die US-Behörden auf die Daten zugreifen können.
– Der schweizerische Datenexporteur und der US-amerikanische Importeur seien verpflichtet, «betroffene Personen bei der Geltendmachung ihrer Rechte gegenüber ausländischen Behörden […] zu unterstützen und bei hängigen Verfahren in der Schweiz geplante Datenlieferungen aufzuschieben resp. bereits stattfindende einstweilen auszusetzen». Dabei lehnt sich der EDÖB ausdrücklich an seine Vorgaben für die Übermittlung von Bankmitarbeiterdaten in die USA an.

3. Zwischenfazit zur Rechtslage in der Schweiz

Obwohl das Safe-Harbor-Abkommen der Schweiz bisher weder gekündigt noch sistiert wurde und sich Unternehmen an und für sich weiterhin darauf berufen könnten, ist in der Praxis nicht zu empfehlen, das Abkommen als Grundlage für weitere Datenübermittlungen in die USA beizuziehen[101].

---

[94] EDÖB, Bericht und Empfehlungen an den Bundesrat vom 14. Oktober 2015, 1, <www.edoeb.admin.ch/datenschutz/00626/00753/ 00970/index.html>, nachfolgend «EDÖB Bericht und Empfehlungen».
[95] EDÖB Bericht und Empfehlungen, 2.
[96] Die USA werden nun unter den Staaten mit ungenügendem Rechtsschutz aufgeführt, vgl. Nr. 11 der Liste; zuvor fielen Datenexporte an zertifizierte US-Unternehmen unter Art. 6 Abs. 1 DSG.
[97] EDÖB, Nach Safe-Harbor-Urteil: Hinweise zur Datenübermittlung in die USA, 22. Oktober 2015, zuletzt aktualisiert am 27. Januar 2016, <www.edoeb.admin.ch/daten schutz/00626/00753/00970/01320/index.html>.
[98] Der EDÖB übernahm somit die Frist der Artikel-29-Datenschutzgruppe.
[99] Diese Pflicht wird nicht aus Art. 6 DSG abgleitet, sondern aus dem allgemeinen Transparenzgrundsatz von Art. 4 Abs. 4 DSG.
[100] EDÖB, Weiterführende Hinweise zur Datenübermittlung in die USA, 28. Oktober 2015, <www.edoeb.admin.ch/datenschutz/00626/ 00753/00970/01325/index.html>.
[101] Vgl. ROSENTHAL/KAISER (Fn. 41), Rz. 33 ff.

Alle weiteren Massnahmen nach Art. 6 Abs. 2 DSG können Datentransfers in die USA aber weiterhin rechtfertigen. Dies gilt – gemäss überwiegender Lehrmeinung – auch für die EU-Standardvertragsklauseln[102]. Mehrere Safe-Harbor-zertifizierte US-Dienstleister haben ihren schweizerischen Kunden denn auch angeboten, EU-Standardvertragsklauseln abzuschliessen, so etwa Salesforce[103] oder Mailchimp[104].

Die Forderungen des EDÖB nach einer besonderen Transparenzpflicht bei Datenübermittlungen in die USA[105] und nach zusätzlichen Rechtsschutzpflichten sind gleichermassen umstritten. Stellungnahmen des EDÖB sind für private Firmen zudem nicht verbindlich[106]. DAVID ROSENTHAL und BARBARA KAISER[107] vertreten mit überzeugenden Argumenten die Auffassung, dass weder eine besondere Informationspflicht besteht noch Zusatzklauseln zu vereinbaren sind. Auch aus Praktikabilitätsgründen wird der vom EDÖB geforderten besonderen Transparenzpflicht daher höchstens bei der Datenübermittlung in konkreten Einzelfällen nachgelebt oder vielleicht im Rahmen einer ohnehin geplanten AGB-Revision. Eine Ergänzung von Datenübermittlungsvereinbarungen ist vielfach ebenfalls nicht praktikabel.

Zusammenfassend gilt für die Schweiz deshalb nach unserer Auffassung, dass schweizerische Datenexporteure im Wesentlichen gleich vorzugehen haben wie europäische Exporteure. Ihnen stehen sämtliche weiteren Massnahmen nach Art. 6 Abs. 2 DSG zur Verfügung, wobei sich in der Praxis die EU-Standardvertragsklauseln am einfachsten umsetzen lassen. Zudem ist zu erwarten, dass die Zusagen der USA auch an die Adresse der Schweiz erfolgen und die Schweiz damit erneut ein paralleles Datenschutzabkommen erreichen wird, ein CH-EU Privacy Shield.

Zusammenfassung

Das hier diskutierte Urteil ist ein weiterer Meilenstein in der datenschutzrechtlichen Rechtsprechung des EuGH nach den Entscheiden zur Vorratsdatenspeicherung und zum Recht auf Vergessen. Der EuGH hielt fest, dass ein Land (wie hier die USA), das die Speicherung sämtlicher personenbezogener Daten erlaubt, dem nationalen Recht Vorrang einräumt, Zugriffe von Behörden nicht beschränkt und keinen Rechtsschutz zur Verfügung stellt, aus europäischer Warte kein angemessenes Datenschutzniveau hat. Infolgedessen hob es den Entscheid der EU-Kommission auf, der das Safe-Harbor-Abkommen als angemessen anerkannt hatte. Vorläufig sind für Datenübermittlungen in die USA deshalb andere Grundlagen wie beispielsweise Datenübermittlungsverträge erforderlich. Dies gilt nicht nur für Datenübermittlungen aus der EU, sondern auch für solche aus der Schweiz.

In der Folge des Urteils kam es zu einer Einigung zwischen der EU und den USA über einen verbesserten Nachfolger des Safe-Harbor-Abkommen mit dem Titel «EU-US Privacy Shield». Nach einer ersten Auswertung der Dokumentation zum Privacy Shield scheint es heute allerdings zweifelhaft, ob damit allen wesentlichen Kritikpunkten des EuGH begegnet werden kann. Für eine abschliessende Stellungnahme sind die weiteren Entwicklungen abzuwarten.

Résumé

La décision discutée dans la présente contribution constitue une nouvelle étape dans la jurisprudence de la CJUE relative à la protection des données, après les décisions concernant la conservation des données et le droit à l'oubli. La CJUE a jugé qu'un pays (comme en l'espèce les États-Unis) qui autorise l'enregistrement de toutes les données personnelles, qui prévoit la primauté du droit national, qui ne limite pas l'accès des autorités et qui ne prévoit aucune protection juridique, ne confère pas de protection suffisante aux données du point de vue européen.

[102] Vgl. dazu eingehend ROSENTHAL/KAISER (Fn. 41), Rz. 46 ff.
[103] Vgl. <www.salesforce.com/company/privacy/data-processing-addendum-faq-de.jsp>.
[104] Vgl. <kb.mailchimp.com/accounts/manage ment/about-mailchimp-and-eu-safe-harbor>; dabei ist die Informationspflicht nach Art. 6 Abs. 3 DSG zu beachten; vgl. dazu ROSENTHAL/KAISER (Fn. 41), Rz. 50.
[105] Für bereits übermittelte Daten scheint dagegen auch der EDÖB keine Informationspflicht zu vertreten, vgl. ROSENTHAL/KAISER (Fn. 41), Rz. 39 ff.
[106] Eine Ausnahme besteht nur nach DSG 29 Abs. 4.
[107] Fn. 41.

C'est pour ces raisons que la CJUE a annulé la décision de la Commission européenne, qui avait considéré l'accord relatif au Safe-Harbor comme approprié. Pour le moment, le transfert de données vers les USA doit donc se baser sur d'autre fondements, tels que par exemple des accords sur la transmission de données. Cela ne vaut pas uniquement pour les transmissions de données depuis l'Union européenne, mais également pour celles en provenance de la Suisse.

La décision a permis à l'UE et aux USA de se mettre d'accord sur une version améliorée de l'Accord Safe-Harbor, le «EU-US Privacy Shield». Après un premier examen de la documentation relative au Privacy Shield, on peut toutefois douter que ce dernier ait pu corriger les principaux points de critiques formulés par la CJUE. Il faut attendre les développements futurs avant de pouvoir prendre position de façon définitive.