



Hintergrundpapier

Nachfolgeregelung zu Safe Harbor: „EU-US Privacy Shield“

Berlin, 2. Mai 2016

I. Aktueller Stand

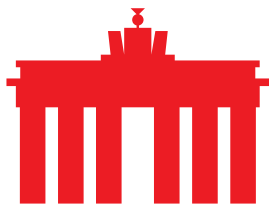
1. Hintergrund

Der Europäische Gerichtshof (EuGH) hatte am 6. Oktober das sogenannte Safe Harbor-Abkommen für ungültig erklärt. Mit der Entscheidung entfiel eine wichtige Rechtsgrundlage für den Datentransfer in die USA. Zuletzt hatten sich über 4000 Unternehmen auf dieses Abkommen berufen.

Darüber hinaus stellte der Gerichtshof fest, dass ein von der Europäischen Kommission vereinbartes Abkommen wie Safe Harbor die nationalen Datenschutzbehörden nicht rechtlich binde; es ihnen also weiterhin möglich sei,“(…) die Eingabe einer Person zu prüfen, die sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten, die aus einem Mitgliedstaat in dieses Drittland übermittelt wurden, bezieht¹ (…).“ Das Urteil ist damit insbesondere als eine Stärkung der europäischen Datenschutzaufsichtsbehörden zu sehen.

In der Folge einigten sich Vertreter der europäischen Datenschutzbehörden mit der sogenannten Art. 29 Datenschutzgruppe – einem unabhängigen Gremium der europäischen Datenschutzaufsichtsbehörden – darauf, bis Ende Januar 2016 auf das Tätigwerden der Kommission zu warten. Sollte bis dahin kein neues Abkommen bzw. eine Vereinbarung mit der amerikanischen Regierung ausgehandelt werden, sollten die europäischen Datenschutzbehörden alle ihnen zur Verfügung stehenden Mittel ergreifen können, um die Einhaltung europäischen Datenschutzrechts durchzusetzen. Konkret: Ab Februar 2016 wäre damit zu rechnen gewesen, dass die Aufsichtsbehörden an die Unternehmen herantreten, ihre Datentransfers überprüfen und ggf. Sanktionen verhängen, wenn sie zu dem Ergebnis kommen, dass europäische Datenschutzstandards nicht eingehalten werden.

¹ Europäischer Gerichtshof, Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14, Rdnr. 66, [\[16\]](#)



Zwar hätte die Datenübertragung nach dem Aus für Safe Harbor auch auf andere Rechtsgrundlagen (informierte Einwilligung, EU-Standardvertragsklauseln, Binding Corporate Rules (BCM) umgestellt werden können. Es war und ist aber sehr umstritten, inwieweit die Feststellungen des EuGH-Urteils Auswirkungen auf derartige Rechtsgrundlagen haben. Denn die vom EuGH problematisierten Zugriffsmöglichkeiten der amerikanischen Geheimdienste bestehen auch bei Daten, die auf Grundlage von Standardvertragsklauseln und BCMs in die USA übertragen wurden. Daher wird oft vertreten, diese seien aus denselben Gründen europarechtswidrig wie das Safe Harbor-Abkommen.

Das Moratorium zeigt Wirkung: Am 2. Februar 2016 gaben die EU-Kommissare Věra Jourová und Andrus Ansip bekannt, dass eine Einigung mit der US-amerikanischen Seite gelungen sei. Die Nachfolgeregelung zum Safe Harbor-Abkommen trägt den Namen „EU-US Privacy Shield“.

Ende Februar 2016 wurden die ausformulierten Leitlinien vorgelegt (im Volltext zu finden unter http://europa.eu/rapid/press-release_IP-16-433_de.htm). Die EU-Mitgliedstaaten müssen dem Kompromiss aber noch zustimmen.

Auch die Artikel-29-Datenschutzgruppe hat Mitte April 2016 zu den Plänen ihre Stellungnahme abgegeben. Diese ist für die EU-Kommission jedoch nicht bindend. Näheres hierzu unter Punkt 5. Stellungnahme der Artikel-29-Datenschutzgruppe.

2. Inhalt der Einigung

Folgende Punkte sind als besonders wichtig zu nennen:

- Zum ersten Mal sollen die USA schriftliche Zusicherungen machen: Es soll keine unterschiedslose Massenüberwachung der europäischen Daten geben, die auf Grundlage des neuen Abkommens in die USA transferiert wurden. Eine solche Überwachung soll nur aufgrund außergewöhnlicher Umstände oder bei technischer Unmöglichkeit eines präzisen Zugriffs möglich sein. Außerdem soll es diesbezüglich Transparenzregeln geben.
- US-amerikanische Firmen, die europäische Daten verarbeiten, müssen sich verpflichten, bestimmte Vorgaben einzuhalten, um die



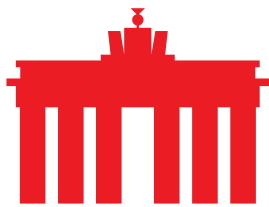
Datenschutzrechte der europäischen Bürger zu garantieren. Das US-Wirtschaftsministerium wird überwachen, ob die Unternehmen ihren Verpflichtungen nachkommen, und dies ggf. nach amerikanischem Recht durchsetzen.

- Das US-Außenministerium will einen Ombudsmann installieren, der für Beschwerden aus Europa zuständig ist. Dieser soll unabhängig von den amerikanischen Geheimdiensten sein. (Richtig klar ist seine Rolle allerdings wohl noch nicht. Er soll die Befugnis haben, über Fälle zu urteilen, in denen Rechte verletzt wurden, aber nicht die Macht, über die Art der Abhilfe zu bestimmen.)
- Es soll einen jährlichen Bericht der EU-Kommission und des US-Wirtschaftsministeriums geben, in dem die Umsetzung des Abkommens überprüft wird. Dieser wird auch die Thematik des Zugriffs nationaler Sicherheitsbehörden beinhalten. Sicherheitsexperten aus den USA und der Europäischen Union sollen daran mitwirken.
- Jeder Bürger, der befürchtet, dass seine Daten verletzt worden seien, wird mehrere Handlungsmöglichkeiten bzw. Rechtsbehelfe haben. US-Unternehmen müssen Beschwerden innerhalb von 45 Tagen nachgehen. Außerdem soll es ein kostenloses Verfahren der alternativen Streitbeilegung geben. Die betroffenen EU-Bürger sollen sich auch an ihre nationalen Datenschutzbehörden wenden können, die dann zusammen mit der Federal Trade Commission dafür sorgen, dass Beschwerden nachgegangen und abgeholfen wird.

Bei diesem Kompromiss handelt es sich wohl wieder nicht um einen Vertrag, sondern wie bei Safe Harbor um eine einseitige Entscheidung der EU-Kommission. Die USA wird auch keine Gesetze ändern und auch die europäischen Datenschutzbehörden behalten weiterhin ihre Befugnisse, könnten also abweichende Entscheidungen treffen.

3. Weitere Schritte

Die USA treffen die notwendigen Vorkehrungen zur Einrichtung des neuen Rahmens, der neuen Überwachungsmechanismen und der neuen Ombudsstelle.



Nach Verabschiedung des von Präsident Obama am 24. Februar unterzeichneten Judicial Redress Act im US-Kongress soll die Kommission in Kürze die Unterzeichnung des Datenschutz-Rahmenabkommens vorschlagen. Über den Abschluss des Abkommens entscheidet der Rat nach Zustimmung des Europäischen Parlaments. Davor werden die Mitgliedstaaten ihre –nicht bindenden – Ansichten zu der Vereinbarung formulieren.

Aufbauend auf der vorliegenden Vereinbarung möchte die EU-Kommission im Juni 2016 eine neue „Angemessenheits-Entscheidung“ für den Datentransfer vorlegen. Hierin sollen die Verpflichtungen für die Firmen und die Verfahren zur Streitschlichtung konkret definiert sein. Außerdem soll sie eine Aufhebungsklausel enthalten, falls die USA die Vereinbarungen nicht erfüllt. Diese „Angemessenheits-Entscheidung“ wird auf drei von der höchsten Ebene der US-Regierung unterzeichneten Schriften basieren. Sie werden im Register der US-Bundesgesetze hinterlegt. Die Kommission stuft die „Angemessenheits-Entscheidung“ als rechtlich bindende Verpflichtung für die amerikanischen Unternehmen ein. Bis zur Präsentation der Vereinbarung im Juni wird sich die Kommission mit einer Kommunikation der Einzelheiten der Vereinbarung allerdings zurückhalten.²

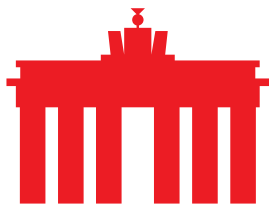
Tritt das Abkommen in Kraft, ist fast sicher, dass vor dem Europäischen Gerichtshof überprüft werden wird, ob es den Anforderungen, die der EuGH in seinem Schrems-Urteil aufgestellt hat, entspricht.

4. Kritik an der Einigung

Die Vereinbarung stößt bei vielen Datenschützern und Politiker auf große Kritik. Es wird befürchtet, dass sich die Daten europäischer Bürger auch in Zukunft nicht vor dem Zugriff der US-amerikanischen Geheimdienste werden schützen lassen, da alles, was die Datenverarbeitung im angeblichen Interesse der nationalen Sicherheit betrifft, gar nicht unter das Privacy Shield fallen solle.³ Außerdem wird an der Durchsetzung der Zusicherungen durch die USA gezweifelt. Die EU-Kommission ist sich nach offiziellen Aussagen

² Diese Informationen basieren auf den Aussagen der Kommissare Ansip, Jourová und Oettinger anlässlich einer Veranstaltung von EuroISPA am 8.2.2016.

³ <http://www.ksta.de/politik/safe-harbor-nachfolger--privacy-shield--scharfe-kritik-an-abkommen-zum-transatlantischen-datenaustausch,15187246,33708018.html>



aber sicher, dass die Abmachung den Anforderungen des EuGH genügen wird.

5. Stellungnahme der Artikel-29-Datenschutzgruppe

Als beispielhaft für die Befürchtungen der Gegner des Abkommens können die Ausführungen der Artikel-29-Datenschutzgruppe angesehen werden.

Das Privacy Shield fällt bei den Datenschützern in wesentlichen Punkten durch: Schlüsselprinzipien des europäischen Datenschutzes seien nicht enthalten.

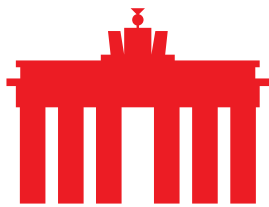
Die Gruppe kritisiert vor allem wirtschaftliche und sicherheitstechnische Punkte: Nach europäischem Recht muss sichergestellt sein, dass ein Drittland ein Schutzniveau aufweist, das dem der EU entspricht. In der Stellungnahme der Datenschützer heißt es, das Privacy Shield verfehle dieses Ziel, da es einige wichtige Prinzipien des europäischen Datenschutzes nicht enthalte.

Zum einen tauchten Zusicherungen, dass die USA das europäische Prinzip der Datenspeicherung respektieren werde, in der Vereinbarung nicht auf. Dieses Prinzip besagt, dass Daten nur so lange gespeichert werden dürfen, bis das Ziel erreicht ist, für das sie gesammelt wurden.

Außerdem gebe es keine Absicherung, die sicherstelle, dass auch dann adäquate Schutzmaßnahmen für die Daten europäischer Bürger ergriffen würden, wenn sie in ein weiteres Land außerhalb der USA ausgeleitet würden. Auch die als entscheidende Verbesserung zum Vorgänger Safe Harbor konzipierten Entschädigungsmechanismen seien ineffektiv: In der Praxis werde sich zeigen, dass die Regelungen derart komplex und schwierig seien, dass sie von einzelnen EU-Bürgern kaum genutzt werden dürften.

Große Bedenken hat die Datenschutzgruppe auch bezüglich der vorgesehenen Regelungen, die die Befugnisse amerikanischer Sicherheitsbehörden betreffen.

Die Vorschriften, die den Behörden den Zugriff auf die Daten ausnahmsweise erlauben, seien zu vage und schädeten deshalb den Sicherungsvorkehrungen gegen die massive und diskriminierende Sammlung von persönlichen Daten aus der EU.



Auch sei davon auszugehen, dass die neue Ombudsperson nicht ausreichend unabhängig und ausreichend mächtig sein werde, um EU-Bürger effektiv bei Entschädigungsbegehren unterstützen zu können.

Die Meinung der Artikel 29 – Datenschutzgruppe ist nicht bindend für die EU-Kommission.

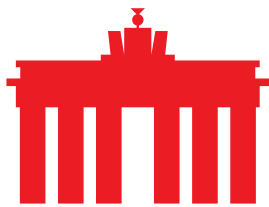
6. Bedeutung/Ausblick

Die Einigung auf ein neues Abkommen bedeutet für die Unternehmen der Internetwirtschaft zunächst relative Rechtssicherheit. Zwar haben einzelne Datenschutzaufsichtsbehörden in Aussicht gestellt, bald Verstöße gegen das europäische Recht ahnden zu wollen. Es ist aber schwer vorstellbar, dass die Datenschutzaufsichtsbehörden in Anbetracht der angekündigten neuen Regeln Sanktionen gegen die Unternehmen verhängen werden, die ihren Datentransfer in die USA bisher auf Safe Harbor gestützt haben. Die Kommission befindet sich momentan auch noch in dem angekündigten Zeitplan, das neue Abkommen ist damit in greifbarer Nähe. De facto wird höchstwahrscheinlich der ursprünglich bis Ende Januar 2016 gewährte Vertrauensschutz für die Unternehmen (und damit die Regelungen des alten Abkommens) aufrechterhalten, bis die neuen Verfahrensregeln des Privacy Shield in Kraft sind, mithin bis mindestens Juni 2016.

7. Forderung eco

eco hat stets betont, dass eine neue Regelung den hohen europäischen Datenschutzstandards genügen und damit die Grundrechte der EU-Bürger ausreichend schützen, gleichzeitig aber auch eine praktikable Lösung für die Unternehmen darstellen muss. Mit Blick auf berechnete Interessen von Sicherheitsbehörden und Geheimdiensten müssten zwischenstaatliche Vereinbarungen gefunden werden, die der Realität des Internet und weltweiter Datenströme gerecht werden.

Als positiv zu bewerten ist, dass EU und USA sich zu einem Kompromiss durchgerungen haben, der auf Rechtssicherheit für Unternehmen hoffen lässt. Denn diese müssen sich auf geltende Regelungen verlassen können. Wird eine Übereinkunft – wie Safe Harbor am 6. Oktober 2015 – gekippt, ist unerlässlich, dass die Politik zügig eine belastbare Neuregelung findet, um



die wirtschaftliche Grundlage der Unternehmen nicht zu gefährden. Es kann nicht angehen, dass private Unternehmen plötzlich in die Situation kommen, für Versäumnisse der Politik bezahlen zu müssen. Deshalb muss der Weg der Einigung konsequent weiter beschritten werden.

Im Folgenden wird es darauf ankommen, eine im Detail so belastbare Regelung auszuarbeiten, dass für die Wirtschaft auf Jahre Rechtssicherheit besteht. Dafür muss die Einigung die Balance zwischen den datenschutzrechtlichen Vorgaben des EuGH und den ökonomischen Interessen der Staaten und Unternehmen finden.

II. Historie

1. Was ist Safe Harbor?

Nach europäischem Datenschutzrecht dürfen personenbezogene Daten europäischer Bürger grundsätzlich nur dann in Staaten außerhalb der Europäischen Union (sog. Drittstaaten) übertragen werden, wenn in dem Drittstaat ein „angemessenes“ Datenschutzniveau gewährleistet wird. In vielen Drittstaaten, insbesondere in den USA, gibt es jedoch kein Datenschutzrecht, das mit dem der EU vergleichbar wäre. Um aufgrund der wirtschaftlichen Bedeutung des transatlantischen Datenaustauschs jedoch trotzdem eine relativ unbürokratische Datenübertragung in die USA zu ermöglichen, hatte die Europäische Kommission im Jahre 2000 mit der US-amerikanischen Handelsbehörde F.T.C das sogenannte Safe-Harbor-Abkommen ausgehandelt. Demnach können Unternehmen, die Daten europäischer Bürger in den USA verarbeiten, sich gegenüber der F.T.C. zur Einhaltung eines „angemessenen“ Datenschutzniveaus im Sinne des europäischen Rechts verpflichten. Bei diesen Unternehmen wird auf Grundlage des Abkommens dann angenommen, dass sie ein „angemessenes“ Datenschutzniveau gewährleisten, also quasi einen „sicheren Hafen“ für die Daten europäischer Bürger darstellen.

Safe Harbor entwickelte sich in der Vergangenheit, insbesondere im Zuge der aufgrund der Entwicklung des Internet stetig zunehmenden weltweiten Datenströme, zwar nicht zur einzigen, aber zu einer sehr wichtigen rechtlichen Grundlage für den transatlantischen Datenaustausch.



2. Hauptkritikpunkte an Safe Harbor

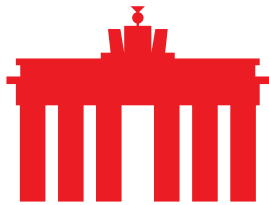
Allerdings waren das Abkommen und die darauf basierende Entscheidung der EU-Kommission auch starker Kritik ausgesetzt. Kritisiert wurde insbesondere die mangelnde Überprüfung der Unternehmen durch die amerikanische F.T.C sowie die unklaren Rechtsschutzmöglichkeiten der europäischen Bürger in den USA. Spätestens seit den Spionage-Enthüllungen durch Edward Snowden war jedoch Hauptkritikpunkt, dass die US-amerikanischen Sicherheitsbehörden und Geheimdienste aufgrund des US Patriot Act immer und auch ohne Benachrichtigung der Dateninhaber Zugriff auf in den USA gespeicherte Daten nehmen darf. Diese Praxis stehe im diametralen Gegensatz zu europäischen Datenschutzrechtbestimmungen.

3. Das Urteil vom 6. Oktober 2015

Das Urteil des EuGH hat seinen Ausgangspunkt in einer Beschwerde des Österreicher Max Schrems über die Praxis der Datenübermittlung von Facebook. Max Schrems argumentierte gegenüber der für Facebook zuständigen irischen Datenschutzbehörde, das Unternehmen könne in den USA eben kein „angemessenes“ Datenschutzniveau gewährleisten, was insbesondere die Enthüllungen durch Edward Snowden offenbaren würden. Die irische Datenschutzbehörde lehnte ein Vorgehen gegen Facebook jedoch mit Verweis auf die Safe-Harbor-Entscheidung der EU-Kommission ab. Solange die Kommission aufgrund des Safe-Harbor-Abkommens von einem „angemessenen“ Datenschutzniveau ausginge, könne die irische Datenschutzbehörde keine abweichende Entscheidung treffen. Mit dieser Begründung war Schrems nicht einverstanden und zog bis vor den EuGH.

Der EuGH entschied, dass die Safe-Harbor-Entscheidung der EU-Kommission ungültig ist:

Zentrale Begründung für die Ungültigkeit ist die Feststellung des Gerichts, der fehlende Schutz der Daten europäischer Bürger vor dem Zugriff US-amerikanischer Sicherheitsbehörden in den USA stehe einer positiven Angemessenheitsentscheidung grundsätzlich entgegen. Denn US-amerikanische Behörden sind nicht verpflichtet, die Safe-Harbor-Grundsätze einzuhalten, da US-Sicherheitsgesetze diesen Grundsätzen vorgehen. US-Sicherheitsbehörden können ohne Einschränkungen, Differenzierungen oder Ausnahmen Daten sammeln und generell auf den Inhalt elektronischer



Kommunikation zugreifen. Die Safe-Harbor-Entscheidung enthält insoweit keine ausreichenden Feststellungen zu Maßnahmen der USA z.B. durch innerstaatliche oder internationale Verpflichtungen, die das durch Safe Harbor vereinbarte „angemessene Schutzniveau“ für die Daten europäischer Bürger gewährleisten würden. Das heißt, solange die USA die Daten der EU-Bürger nicht besser vor dem Zugriff ihrer Sicherheitsbehörden schützen, kann die USA kein „sicherer Hafen“ für diese Daten sein.

Darüber hinaus stellte der Gerichtshof fest, dass eine von der Europäischen Kommission getroffene Entscheidung, wie die Safe-Harbor-Entscheidung, die nationalen Datenschutzbehörden nicht rechtlich bindet, eine gegenüber der Kommission abweichende Entscheidung zu treffen. Die Befugnis nationaler Aufsichtsbehörden zur Kontrolle könnte durch EU-Kommissionsentscheidungen nicht berührt werden. Diese müssen bei Beschwerden von EU-Bürgern prüfen, ob die Voraussetzungen für die Datenübermittlung auch tatsächlich eingehalten werden. Das Urteil ist damit insbesondere auch als eine Stärkung der europäischen Datenschutzaufsichtsbehörden zu sehen.