Zur Information

Winter 2015/2016, Nr. 25

Europäischer Gerichtshof kippt Safe Harbor

Übertragung personenbezogener Daten von der Europäischen Union in die USA nach der neuen Rechtsprechung

Nachdem der Europäische Gerichtshof das Safe Harbor-Abkommen zwischen Deutschland und den USA aufgehoben hat, besteht eine erhebliche Rechtsunsicherheit bei Unternehmen, die darauf angewiesen sind personenbezogene Daten von der Europäischen Union in die USA zu transferieren. Die Europäische Kommission und die nationalen Datenschutzbehörden zeigen nun Übergangslösungen bis zum Abschluss eines neuen Abkommens auf.

Am 6. Oktober 2015 erklärte der Europäische Gerichtshof (EuGH) in einem aufsehenerregenden Urteil[1] das Safe Harbor-Abkommen zwischen der EU und den USA für ungültig. Damit entfällt die wichtigste Rechtsgrundlage für einen Export von Daten aus der EU in die USA. Unser Newsletter gibt einen Überblick über die neue Rechtsprechung und zeigt auf, was von nun an beim Transfer von personenbezogenen Daten in die USA zu beachten ist.

I. Hintergrund

Bei Safe Harbor (Sicherer Hafen) handelt es sich um ein Abkommen zwischen der EU und den USA, welches gewährleistet, dass personenbezogene Daten legal an teilnehmende Unternehmen in den USA übermittelt werden können.[2]

Ausgangspunkt dieser Vereinbarung war die europäische Datenschutzrichtlinie 95/46/EG, die einen Datentransfer in Drittstaaten verbietet, in denen kein dem EU-Recht entsprechendes Schutzniveau herrscht. Die Richtlinie regelt allerdings ebenfalls, dass die Europäische Kommission (EU-Kommission) die Angemessenheit des Datenschutzes „feststellen“ kann, wenn bestimmte Auflagen erfüllt werden.

Eine solche Feststellung traf die EU-Kommission im Jahre 2000 für die Datenübermittlung in die USA, welche kein der Europäischen Union entsprechendes Schutzniveau aufweisen, indem sie den Datentransfer an US-Unternehmen, die sich den sog. Safe Harbor Principles („Grundsätze des sicheren Hafens“) unterwerfen, generell gestattete.[3]

Die Safe Harbor Principles bestehen aus sieben Prinzipien. Diese regeln unter anderem, dass Unternehmen ihre Kunden aufklären müssen, welche Daten sie erheben und ihnen die Möglichkeit einräumen müssen, die über sie erhobenen Daten einzusehen. Hinzu kommt, dass die Unternehmen die Antworten auf 15 „häufig gestellte Fragen“ beachten müssen, die vom US-Handelsministerium veröffentlicht wurden.

EuGH erklärt das Safe-Harbor-Abkommen mit den USA für ungültig.

Seitdem sind ca. 5.500 US-Unternehmen, unter anderem Facebook, Google, Amazon, Apple und Microsoft, dem Safe Harbor-Abkommen beigetreten. Der Beitritt erfolgt auf freiwilliger Basis durch eine Selbstzertifizierung der Unternehmen. Hierbei verpflichten sie sich gegenüber der Federal Trade Commission oder einer von ihr benannten Stelle, die im Rahmen des Safe Harbor Abkommens aufgestellten Mindestanforderungen an den Datenschutz einzuhalten. Die Zertifizierung ist von den Unternehmen jährlich zu aktualisieren. Verstößt eine der Firmen gegen die Safe Harbor-Vorgaben, so können Sanktionen verhängt und die Datenverarbeitung gestoppt werden. Dies ist allerdings bis jetzt eher selten geschehen.

1: EuGH, Az.: C-362/14.
2: Siehe „Zur Information“, Ausgabe Nr. 1, Herbst 2009 auf www. phillipsnizer.com.
3: Entscheidung 2000/520/EG.

Steven H. Thal und **Florian von Eyb**

II. Schwachstellen des Safe Harbor

In den letzten Jahren kamen jeddoch immer mehr Schwachstellen des Safe Harbor-Programms zum Vorschein.

1. Unzureichende Kontrolle

Zum einen herrschte keine konsequente Überwachung der Einhaltung der Grundsätze. Es fehlten wirksame Überwachungs- und Kontrollmechanismen, die es erlaubten, in der Praxis etwaige Verstöße gegen Grundrechte, insbesondere des Rechts auf Achtung der Privatsphäre sowie des Rechts auf den Schutz personenbezogener Daten, zu ermitteln und zu ahnden.

2. Überwachung durch US-Behörden

Zum anderen bestanden weitreichende Ausnahmen für US-Unternehmen. So mussten sie die Grundsätze des sicheren Hafens in dem Umfang nicht befolgen, in dem sie durch US-Gesetze daran gehindert waren. Im Jahre 2013 wurde, angestoßen von den Enthüllungen des Edward Snowden, bekannt, dass es umfassende Überwachungssysteme der US-Behörden gibt. US-Unternehmen, die dem Safe Harbor beigetreten waren, konnten zur Freigabe von Daten an US-Geheimdienste aufgefordert werden. Dadurch diente das System des sicheren Hafens ungewollt als Kanal für die Übertragung personenbezogener Daten von EU-Bürgern an US-Behörden.

3. Fehlender Rechtsschutz

Zudem beziehen sich sämtliche US-Datenschutzregeln nur auf Daten von US-Bürgern und von Personen, die sich langfristig in den USA aufhalten und nicht auf importierte Daten. EU-Bürger haben bisher keine Möglichkeit, die Rechtmäßigkeit eines Eingriffs in ihre Grundrechte wegen der Übermittlung ihrer Daten an US-Behörden gerichtlich überprüfen zu lassen. Ein Rechtsbehelf für die Löschung oder Berichtigung personenbezogener Daten existiert nicht.

III. Darstellung der neuen Rechtsprechung des Europäischen Gerichtshofs

Anlass für die Entscheidung des EuGH war eine Klage des österreichischen Juristen und Datenschutz-Aktivisten Max Schrems, die sich gegen die Speicherung seiner Daten durch Facebook auf Servern in den USA richtete. Schrems machte insbesondere geltend, dass nach den Enthüllungen von Edward Snowden davon auszugehen sei, dass seine Daten in den USA nicht ausreichend geschützt seien und sie dem Zugriff des US-Nachrichtendienstes NSA unterlägen. Nachdem seine zuvor bei der irischen Datenschutzbehörde erhobene Beschwerde mit der Begründung abgelehnt wurde, dass Facebook in den USA aufgrund seines Beitritts in das Safe Harbor-Programm ein angemessenes Schutzniveau für die Übermittlung personenbezogener Daten gewährleiste, klagte Schrems vor dem irischen High Court.

Die Beschwerde sowie die darauffolgende Klage wurden in Irland erhoben, da Facebooks europäische Tochtergesellschaft, Facebook Irland, ihren Sitz in Dublin hat. Alle im Unionsgebiet wohnhaften Personen, die Facebook nutzen, schließen bei ihrer Anmeldung einen Vertrag mit Facebook Irland ab. Die personenbezogenen Daten der europäischen Facebook-Nutzer werden daraufhin an den Server von Facebook Inc., der sich in den Vereinigten Staaten befindet, übermittelt und dort verarbeitet.

Der irische High Court wandte sich im Juli 2014, im Rahmen eines Vorabentscheidungsverfahrens nach Art. 267 AEUV, an den EUGH. Das europarechtlich normierte Vorabentscheidungsverfahren berechtigt bzw. verpflichtet nationale Gerichte dazu, eine Frage, die in einem anhängigen Rechtsstreit entscheidungserheblich ist, dem EuGH zur abschließenden Klärung vorzulegen. Der irische High Court stellte dem EuGH die Frage, ob die nationalen Datenschutzbehörden an die "Safe Harbor"-Entscheidung der EU-Kommission gebunden seien oder ob ihnen eine eigene Prüfungskompetenz zustehe.

Bundesjustizminister Maas zum EuGH-Urteil: "Ein starkes Signal für mehr Datenschutz"

Der EuGH entschied am 06.10.2015, dass das Safe Harbor-Programm, entgegen der bisherigen Auffassung, kein angemessenes Schutzniveau gewährleiste und erklärte es in Folge dessen für ungültig. Ferner attestierte er den nationalen Datenschutzbehörden die Befugnis, Datenübermittlungen in die USA auf der Basis des Safe Harbor-Abkommens zu untersagen. Der EuGH argumentierte damit, dass die europäische Datenschutzrichtlinie im Lichte der Grundrechtecharta der Europäischen Union auszulegen sei und stellte fest, dass die bisherige Praxis gegen diese verstoße. Zum einen werde durch eine Regelung, die es zulasse, dass Behörden generell auf den Inhalt elektronischer Kommunikation zugreifen können, in das durch Art. 7 der Charta garantierte Grundrecht auf Achtung des Privatlebens eingegriffen. Zum anderen verletze eine Regelung, die keine Möglichkeit für den Bürger vorsieht, durch einen Rechtsbehelf Zugang zu den ihn betreffenden Daten zu erlangen und deren Berichtigung oder Löschung zu erwirken, das in Art. 47 der Charta verankerte Grundrecht auf wirksamen gerichtlichen Rechtsschutz.

IV. Lösungsansätze

Da die bisher vorgenommene Datenübertragung nach den Safe Harbor-Grundsätzen nun nicht mehr zulässig ist, stellt sich für viele Unternehmen daher unweigerlich die Frage, ob und wie der Transfer von personenbezogenen Daten von der EU in die USA in Zukunft möglich sein wird.

Neues Rahmenabkommen für die Übermittlung personenbezogener Daten in die USA wird derzeit verhandelt.

Bereits seit 2013 laufen Verhandlungen zwischen der EU-Kommission und den USA über ein neues Abkommen zur Weitergabe der Daten europäischer Internet-Nutzer in die USA. Nach der Safe Harbor-Entscheidung sind die Verhandlungen mit dem Ziel intensiviert worden, sie innerhalb von drei Monaten abzuschließen. Dass ein neues Abkommen, welches den strengen Vorgaben des EuGH Urteils Rechnung trägt, bis Ende Januar 2016 ausgearbeitet werden wird, erscheint allerdings unwahrscheinlich.

1. EU-Kommission

Für die Übergangszeit, bis zur Schaffung eines neuen Rahmenabkommens, hat die Europäische Kommission im November 2015 Leitlinien vorgelegt, die erläutern, unter welchen Bedingungen Unternehmen auf rechtmäßige Art und Weise vorübergehend Daten übermitteln können. Möglichkeiten sollen demnach EU-Standardvertragsklauseln sowie Binding Corporate Rules („verbindliche Unternehmensregeln“) darstellen.
Standardvertragsklauseln sind Vertragsvorgaben der EU-Kommission zum Datenschutz und müssen vom datenverarbeitenden Unternehmen unverändert übernommen werden. Der Datenimporteur unterwirft sich damit den EU-Datenschutzregeln und verspricht gegenüber dem Datenexporteur, den Datenschutz einzuhalten. Die Standardvertragsklauseln beinhalten bestimmte Pflichten, wie z.B. von den Daten nur innerhalb des angegebenen Verwendungszwecks Gebrauch zu machen, Sicherheitsvorkehrungen bei der Übermittlung sensibler Daten zu treffen und für die Einhaltung der Verpflichtungen zu sorgen.
Binding Corporate Rules (BCR) stellen von den nationalen Datenschutzbehörden genehmigte Regeln für die Datenübertragungen dar. Auf der Grundlage derartiger Vorschriften können personenbezogene Daten unbegrenzt zwischen den Unternehmen einer weltweit operierenden Unternehmensgruppe übermittelt werden.
Die Kommission vertritt die Ansicht, dass die von ihr herausgegebenen Standardvertragsklauseln für die Mitgliedstaaten bindend seien, da diese eine Kommissionsentscheidung darstellten. Daher seien die nationalen Behörden prinzipiell dazu verpflichtet, diese zu akzeptieren. Allerdings betont sie gleichzeitig, dass das Vorgehen der nationalen Aufsichtsbehörden in deren eigenem Ermessen stehe.

2. Deutsche Datenschutzbehörden

Neben der EU-Kommission haben sich mittlerweile auch die deutschen Datenschutzbehörden in einem gemeinsamen Positionspapier zu ihrem weiteren Vorgehen geäußert, welches teilweise noch strengere Anforderungen aufstellt als die Leitlinien der Kommission. Die Datenschutzbehörden äußern in ihrem Positionspapier, dass sie von nun an Datenübermittlungen in die USA untersagen werden, welche sich ausschließlich auf Safe Harbor stützen. Ferner heißt es darin, dass die Datenschutzbehörden derzeit keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregeln oder Datenexportverträgen erteilen werden.

3. Datenschutzkonferenz auf europäischer Ebene (sog. „Art. 29-Datenschutzgruppe“)

Bereits am 16. Oktober 2015 hatte die Art. 29-Datenschutzgruppe ein Statement zu den Konsequenzen der EuGH-Entscheidung herausgegeben. Die Gruppe ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes. Ihrer Einschätzung nach sollen zwischenzeitlich, jedenfalls bis Ende Januar 2016, die EU-Standardvertragsklauseln und Binding Corporate Rules weiter genutzt werden können.

4. Stellungnahme

Der Vorteil der Standardvertragsklauseln und Binding Corporate Rules besteht darin, dass diese effektive Schutzmechanismen für die Grundrechte betroffener Personen beinhalten, wie z.B. detaillierte Regelungen zur Datensicherheit sowie externe Kontrollen (Audits) und Rechtsschutzmöglichkeiten. Allerdings unterwerfen sich diesen Regeln nur die Unternehmen und nicht die US-Behörden, sodass der Kritikpunkt des Zugriffs auf personenbezogene Daten durch amerikanische Behörden weiterhin bestehen bleibt.

V. Vorgehensweise für Unternehmen

Da Safe Harbor ab sofort keine Rechtsgrundlage für eine Datenübermittlung in die USA mehr bietet, müssen Unternehmen, die bislang Daten auf der Grundlage von Safe Harbor in die USA übermittelt haben, nun auf andere Wege ausweichen.

1. Im Rahmen von Safe Harbor übermittelte Daten?

Zunächst sollte ein Unternehmen prüfen lassen, ob seine Datentransfers in den Anwendungsbereich der bisherigen Safe Harbor-Regelung fallen. Es muss sich um personenbezogene Daten von EU-Bürgern handeln, die gespeichert und übermittelt werden. Hierbei ist zu erwähnen, dass vielerlei Datentransfers auch bis dato unabhängig von Safe Harbor zulässig waren. Beispielsweise unterliegt die Übertragung von Finanzdaten oder Fluggastdaten gesonderten Regelungen und war nie vom Anwendungsbereich des Safe Harbor-Programms erfasst.
Zudem muss es sich um Daten handeln, die von der Europäischen Union aus in die USA übermittelt werden, bzw. um solche, die in der EU gespeichert sind und auf die ein amerikanisches Unternehmen zugreifen kann. Dies ist zum Beispiel der Fall bei der Nutzung von Cloud-Diensten oder Software-as-a-Service-Produkten von US-Dienstleistern.

Unternehmen müssen prüfen, auf welcher rechtlichen Basis sie künftig Daten in die USA übermitteln können.

2. Ausnahmen einschlägig?

Ferner gibt es in begrenztem Umfang gesetzliche Ausnahmeregelungen, die den Datentransfer auch in Länder gestatten, in denen kein den EU-Gesetzen entsprechendes Datenschutzniveau gewährleistet ist. Diese sind in Art. 26 Abs. 1 der EU-Datenschutzrichtlinie sowie in § 4 c Bundesdatenschutzgesetz (BDSG) normiert. Dazu gehört sowohl die Datenübermittlung zur Durchsetzung oder Verteidigung von Rechtsansprüchen als auch bei Zustimmung der betroffenen Person. Die Anforderungen an eine Einwilligung durch den Betroffenen sind jedoch hoch. Der Kunde müsste umfassend über die Risiken der Datenübermittlung in die USA informiert werden und ihm müsste eine echte Wahlmöglichkeit eingeräumt werden, sodass bei Versagen seines Einverständnisses der Datentransfer unterbleiben müsste. Eine bloße Änderung der Datenschutzbestimmungen wird hierfür nicht als ausreichend erachtet.
Überdies bestehen weitere gesetzliche Ausnahmen für Fälle der Erfüllung eines Vertrages oder der Durchführung vorvertraglicher Maßnahmen, wenn der Datentransfer dafür erforderlich ist sowie wenn der Vertrag dem Interesse des Betroffenen dient. Letzteres ist beispielsweise der Fall, wenn ein Arbeitgeber Daten eines Arbeitnehmers an eine Versicherungsgesellschaft im Ausland weitergibt, bei der er zugunsten des Arbeitnehmers eine Versicherung abgeschlossen hat.

Um personenbezogene Daten in die USA zu transferieren können Unternehmen somit momentan zwischen Standardvertragsklauseln, Binding Corporate Rules und der Einholung von Einwilligungen wählen. Wir empfehlen den Unternehmen, sich zeitnah rechtlich beraten zu lassen im Hinblick darauf, ob die Aufhebung von Safe Harbor ihre Datentransfers überhaupt tangiert und wenn ja, welche dieser rechtlichen Lösungen für ihre zukünftigen Datenübertragungen anwendbar und praktikabel sind.

Für weitere Fragen nehmen Sie bitte Kontakt mit uns auf:

Steven H. Thal
J.Dr.; Attorney at Law, New York
Rechtsberater für US Recht,
OLG Frankfurt/ M.
+1 212 841 0742
sthal@phillipsnizer.com

Florian von Eyb
LL.M.; Rechtsanwalt
Attorney at Law, New York
+1 212 841 0720
fvoneyb@phillipsnizer.com

Alan Behr
J.Dr.; Attorney at Law, New York
+1 212 841 0552
abehr@phillipsnizer.com

Mitarbeit: **Sara Afschar-Hamdi** (Rechtsreferendarin)