© Marco2811 - Fotolia

DBSC INFOLETTER 2015/12

DIE FOLGEN DES SAFE HARBOR-URTEILS

Die Folgen des EuGH-Urteils zum Safe-Harbor-Abkommen mit den USA

Der Europäische Gerichtshof hatte in seinem Urteil vom 6. Oktober 2015 in der Rechtssache Schrems die Bedeutung des Grundrechts auf Datenschutz insbesondere bei der Übermittlung personenbezogener Daten in Drittländer unterstrichen:

- Auch wenn die EU-Kommission entschieden hat, dass in einem Land ein angemessenes Datenschutzniveau gegeben ist, darf und **muss ggf. eine nationale Aufsichtsbehörde eigene Ermittlungen anstellen, falls bei ihr eine Beschwerde diesbezüglich eingeht**. Kommt die Aufsichtsbehörde zu dem Ergebnis, dass in dem Drittland kein angemessenes Datenschutzniveau vorhanden ist, kann sie den Angemessenheitsbeschluss der Kommission vor einem nationalen Gericht anfechten. Das nationale Gericht hat dann die Möglichkeit, eine Auslegungsfrage an den Europäischen Gerichtshof (EuGH) zu richten. Nur letzterer kann einen EU-Rechtsakt (z.B. die Safe-Harbor-Entscheidung oder Standardvertragsklauseln der Kommission) für ungültig erklären.
- Die **Entscheidung 2000/520 der EU-Kommission** aus dem Jahr 2000, mit der das durch Safe Harbor hergestellte Datenschutzniveau als angemessen anerkannt wurde, **ist ungültig**. Die Kommission hätte vor Inkrafttreten von Safe Harbor ausführlich untersuchen müssen, ob das US-amerikanische Recht ein angemessenes Datenschutzniveau tatsächlich zulässt.

Die Europäische Kommission arbeitet seit Januar 2014 daran, auf der Grundlage von 13 Empfehlungen Datenübertragungen für EU-Bürger sicherer zu machen. Im Anschluss an das Urteil des Gerichtshofes hat die Kommission die Verhandlungen mit den Vereinigten Staaten über einen neuen und sicheren Rahmen für die Übermittlung personenbezogener Daten intensiviert. Ziel der Kommission ist es, die Gespräche **innerhalb von drei Monaten** abzuschließen.

In der Zwischenzeit müssen Unternehmen das **Urteil befolgen** und nach Möglichkeit auf **alternative Datenübermittlungsinstrumente** zurückgreifen. Wie bereits vom ersten Vizepräsidenten Timmermans und von Kommissionsmitglied Jourová am Tage des Urteilsspruches angekündigt, hat die Kommission am 6.11.2015 Leitlinien für die Übergangszeit bis zur Annahme eines neuen Rechtsrahmens veröffentlicht. In der betreffenden Mitteilung der Kommission werden die Folgen des Urteils analysiert und alternative Verfahren für die Übermittlung von personenbezogenen Daten in die Vereinigten Staaten erörtert. Die Kommission wird zudem weiterhin eng mit den unabhängigen Datenschutzbehörden zusammenarbeiten, um eine einheitliche Umsetzung des Urteils sicherzustellen.

[Fortsetztung auf der nächsten Seite.]

Was ist/war "Safe Harbor" überhaupt ?

Die Bundesbeaufrtragte für Datenschutz und Informationsfreiheit (BfDI), Frau Andrea Voßhoff, läßt dazu auf ihrer Web Site veröffentlichen:

"Safe Harbor war eine vom 06.07.2000 bis 6.10.2015 bestehende Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens" (Safe Harbor, Kommissionsentscheidung 2000/520/EG. Ausgangspunkt für diese Vereinbarung bilden die Vorschriften der Art. 25 und 26 der EU-Datenschutzrichtlinie, nach denen ein Datentransfer in Drittstaaten verboten ist, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, da es dort keine umfassenden gesetzlichen Regelungen zum Datenschutz gibt, die dem europäischen Standard entsprechen. Allerdings sieht Art. 25 Abs. 6 der Richtlinie vor, dass die Kommission der Europäischen Gemeinschaft die Angemessenheit des Datenschutzes in einem Drittland "feststellen" kann, wenn dieses bestimmte Anforderungen erfüllt. Ausführliches ist in den Erläuterungen zu Safe Harbor von BfDI nachzulesen.

Am 06.10.2015 erklärte der Europäische Gerichtshof im Urteil zur Rechtssache C-362/14 die Entscheidung 2000/520 der EU-Kommission für ungültig und folgte weitgehend dem Rechtsgutachten des Generalanwaltes. Der EuGH stärkt mit diesem Urteil zum einen die Unabhängigkeit der Datenschutzaufsichtsbehörden, indem er klar feststellt, dass die Kompetenzen und Befugnisse der nationalen Kontrollstellen durch Entscheidungen der EU-Kommission nicht tangiert werden.

Aufgrund der aktuellen Ereignisse sollte im Moment höchste Sorgfalt angewendet werden und die aktuelle Fach-Berichterstattung sowie die Handlungsempfehlungen der Aufsichtsbehörden zu Rate gezogen werden, da Safe Harbor keine gültige Rechtsgrundlage für Datenübermittlungen in die USA ist. "

[*Fortsetzung auf der nächsten Seite.*]

DBSC Ruban GmbH
Otto-Lilienthal-Str. 36
D-71034 Böblingen
www.dbsc.de

V.i.S.d.P.: Gernot Ruban

In der Pressemitteilung IP/15/6015 hebt die EU-Kommission folgende Punkte hervor:

- Das Safe-Harbor-Abkommen kann nicht mehr als Rechtsgrundlage für die Übermittlung personenbezogener Daten in die Vereinigten Staaten dienen.
- Die Kommission wird die Verhandlungen über einen neuen und soliden Rahmen für transatlantische Übermittlungen personenbezogener Daten fortsetzen und zum Abschluss bringen, wobei dieser Rahmen die Anforderungen des Urteils erfüllen muss, insbesondere in Bezug auf die Beschränkungen und Garantien bezüglich des Zugriffs auf personenbezogene Daten durch die US amerikanischen Behörden;
- Darüber hinaus werden weitere Angemessenheitsbeschlüsse geändert werden müssen, damit die Datenschutzbehörden der Mitgliedstaaten auch künftig Beschwerden von Einzelpersonen ungehindert nachgehen können.

In der Mitteilung werden alternative Grundlagen für die Übermittlung personenbezogener Daten in die Vereinigten Staaten dargelegt, ohne der Unabhängigkeit und den Befugnissen der Datenschutzbehörden der Mitgliedstaaten zur Prüfung der Rechtmäßigkeit einer solchen Datenübermittlung vorzugreifen. Datenübertragungen von Unternehmen können derzeit auf folgenden Grundlagen erfolgen:

- vertragliche Regeln: Vertragliche Regeln müssen bestimmte Pflichten (z.B. Sicherheitsmaßnahmen, Benachrichtigung der betroffenen Person, Sicherheitsvorkehrungen bei der Übermittlung sensibler Daten usw.) vorsehen. Mustervertragsklauseln sind hier verfügbar.
- verbindliche unternehmensinterne Vorschriften für unternehmensgruppeninterne Datenübermittlungen: Auf der Grundlage derartiger Vorschriften können personenbezogene Daten unbegrenzt zwischen den Unternehmen einer weltweit operierenden Unternehmensgruppe übermittelt werden. Die Übermittlungen bedürfen jeweils der Zustimmung der Datenschutzbehörde des Mitgliedstaats, aus dem das multinationale Unternehmen Daten übermitteln möchte.
- Ausnahmeregelungen:
  - Datenübermittlung zum Abschluss oder zur Erfüllung eines Vertrags [einschließlich vorvertraglicher Situationen, beispielsweise zur Buchung eines Flugs oder eines Hotelzimmers in den Vereinigten Staaten];
  - Durchsetzung oder Verteidigung von Rechtsansprüchen;
  - (falls kein anderer Grund besteht:) Datenübermittlung bei aus freien Stücken und in voller Sachkenntnis erfolgender Zustimmung der betroffenen Person.

Die Pressemitteilung verweist auf **13 Empfehlungen**, die bereits im November 2013 ausgesprochen wurden:

Transparenz

1. Selbstzertifizierte Unternehmen sollten ihre Datenschutzbestimmungen öffentlich bekanntmachen.
2. Die Datenschutzbestimmungen auf den Websites selbstzertifizierter Unternehmen sollten stets einen Link zur Safe-Harbor-Website des US-Handelsministeriums enthalten, auf der eine Liste aller aktuellen Mitglieder des Safe-Harbor-Programms abgerufen werden kann.
3. Selbstzertifizierte Unternehmen sollten die Datenschutzbestimmungen aller mit Unterauftragnehmern (z. B. mit Cloud-Computing-Diensten) geschlossenen Verträge veröffentlichen.
4. Auf der Website des US-Handelsministeriums sollten alle Unternehmen benannt werden, die aktuell nicht Mitglied des Systems sind.

Rechtsschutz

5. Die Datenschutzerklärungen auf den Websites von Unternehmen sollten einen Link zu einem Anbieter alternativer Streitbeilegungsdienste enthalten.
6. Der alternative Streitbeilegungsmechanismus sollte leicht zugänglich und seine Inanspruchnahme erschwinglich sein.
7. Das US-Handelsministerium sollte Anbieter alternativer Streitbeilegungsdienste systematischer überwachen, was die Transparenz und Zugänglichkeit der von ihnen bereitgestellten Informationen über das angewandte Verfahren und die Behandlung von Beschwerden betrifft.

Durchsetzung

8. Nach einer Zertifizierung oder Neuzertifizierung von Unternehmen im Rahmen der Safe-Harbor-Regelung sollten für einen bestimmten Prozentsatz dieser Unternehmen von Amts wegen (über eine bloße Kontrolle der Erfüllung formaler Anforderungen hinausgehende) Untersuchungen zur effektiven Einhaltung ihrer Datenschutzbestimmungen vorgenommen werden.
9. Wird aufgrund einer Beschwerde oder einer Untersuchung festgestellt, dass die einschlägigen Bestimmungen nicht eingehalten werden, sollte das betreffende Unternehmen nach einem Jahr einer gezielten Folgeuntersuchung unterworfen werden.
10. Bestehen Zweifel daran, ob ein Unternehmen die Bestimmungen einhält, oder liegen Beschwerden vor, sollte das US-Handelsministerium die zuständige EU-Datenschutzbehörde unterrichten.
11. Im Falle falscher Erklärungen zum Safe-Harbor-Beitritt sollten weitergehende Ermittlungen durchgeführt werden.

Zugang für US-Behörden

12. Die Datenschutzbestimmungen selbstzertifizierter Unternehmen sollten Informationen darüber enthalten, inwieweit das US-Recht es öffentlichen Stellen gestattet, die im Rahmen der Safe-Harbor-Regelung übermittelten Daten zu sammeln und zu verarbeiten. Insbesondere sollten Unternehmen dazu angehalten werden, in ihren Datenschutzbestimmungen anzugeben, ob sie aus Gründen der nationalen Sicherheit, des öffentlichen Interesses oder der Rechtsdurchsetzung Ausnahmen von den Grundsätzen anwenden.
13. Es sollte sichergestellt werden, dass die in der Safe-Harbor-Entscheidung vorgesehenen Ausnahmeregelungen aus Gründen der nationalen Sicherheit nur zur Anwendung gelangen, wenn dies unbedingt notwendig bzw. angemessen ist.

Quelle: Pressemitteilungen der EU-Kommision zu Leitlinien für transatlantische Datenübermittlungen nach dem Schrems-Urteil, Datenschutz-Wiki des Bundesbeauftragten für den Datenschutz.

Auszug aus der vom EuGH für ungültig erklärten Entscheidung der EU-Kommision:

2000/520/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG über die Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglichen "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA .

Artikel 1

1. Es wird davon ausgegangen, dass die dieser Entscheidung als Anhang I beigefügten "Grundsätze des 'sicheren Hafens' zum Datenschutz", im Folgenden "die Grundsätze" genannt, die gemäß den in den vom US-Handelsministerium am 21. Juli 2000 herausgegebenen, dieser Entscheidung als Anhang II beigefügten, "Häufig gestellten Fragen" (FAQ) enthaltenen Leitlinien umgesetzt werden, für alle unter die Richtlinie 95/46/EG fallenden Tätigkeiten ein im Sinne des Artikels 25 Absatz 2 dieser Richtlinie angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die von der Europäischen Union an in den Vereinigten Staaten niedergelassene Organisationen übermittelt werden, unter Berücksichtigung folgender vom US-Handelsministerium veröffentlichter Dokumente:

a) die "sicherer Hafen Durchsetzungsmechanismen" (Anhang III),

b) ein Memorandum über Entschädigungen für die Verletzung der Privatsphäre und ausdrückliche Ermächtigungen gemäß dem US-Recht (Anhang IV),

c) ein Schreiben der Federal Trade Commission (Anhang V),

d) ein Schreiben des US-Verkehrsministeriums (Anhang VI).

2. Im Hinblick auf jede Datenübermittlung müssen folgende Voraussetzungen erfuellt sein:

a) Die Organisation, die die Daten erhält, hat sich eindeutig und öffentlich verpflichtet, die Grundsätze einzuhalten, die entsprechend den FAQ umgesetzt wurden; und

b) die Organisation unterliegt den gesetzlichen Befugnissen einer in Anhang VII dieser Entscheidung aufgeführten staatlichen Einrichtung in den Vereinigten Staaten, die berechtigt ist, im Fall der Nichtbeachtung der Grundsätze, die entsprechend den FAQ umgesetzt wurden, Beschwerden zu prüfen und Abhilfe wegen unlauterer und irreführender Praktiken sowie Schadenersatz für Privatpersonen zu erwirken, und zwar ungeachtet des Landes, in dem sie ihren Wohnsitz haben, oder ihrer Nationalität.

3. Die Voraussetzungen des Absatzes 2 gelten ab dem Zeitpunkt als erfuellt, zu dem die Organisation, die ihren Beitritt zu den entsprechend den FAQ umgesetzten Grundsätzen bescheinigt, dem Handelsministerium der USA (oder der von ihm benannten Stelle) die öffentliche Bekanntgabe ihrer Verpflichtung nach Absatz 2 Buchstabe a) und die Identität der staatlichen Einrichtung nach Absatz 2 Buchstabe b) mitteilt.

Artikel 2

Die vorliegende Entscheidung betrifft nur die Angemessenheit des Schutzes, der in den Vereinigten Staaten nach den entsprechend den FAQ umgesetzten Grundsätzen gewährt wird, um die Anforderungen des Artikels 25 Absatz 1 der Richtlinie 95/46/EG zu erfuellen. Die Anwendung anderer Bestimmungen der Richtlinie, die sich auf die Verarbeitung personenbezogener Daten in den Mitgliedstaaten beziehen, einschließlich Artikel 4, bleiben von dieser Entscheidung unberührt.