Stellungnahme

der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

zum

Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015 zu Safe Harbor

(C-362/14)

Der Europäische Gerichtshof (EuGH) hat am 6. Oktober 2015 die Angemessenheitsentscheidung der Europäischen Kommission 2000/520/EG vom 26. Juli 2000 hinsichtlich der Datenübermittlung an US-Organisationen, die sich den Safe Harbor-Prinzipien unterwerfen, für unzulässig erklärt. Was auf den ersten Blick lediglich eine Abkehr vom „sicheren Hafen" bedeutet, hat weitreichende Folgen für sämtliche Datenexporte in die Vereinigten Staaten und stellt europäische sowie amerikanische Datenverarbeiter vor ernste Probleme.

1. Zur Ausgangslage

Safe Harbor, der „sichere Hafen", wurde im Jahr 2000 nach zweijährigen Verhandlungen zwischen der Europäischen Union (EU) und den Vereinigten Staaten ins Leben gerufen, um gewährleisten zu können, dass die Übermittlung personenbezogener Daten aus der EU in die USA, trotz der Existenz zweier unterschiedlicher Datenschutz-Systeme, rechtskonform vonstattengehen kann. Hierzu fasste die Europäische Kommission eine so genannte „Angemessenheitsentscheidung", die den USA aus Sicht des europäischen Datenschutzes, mithin der Grundrechtecharta sowie der Datenschutzrichtlinie 95/46/EG, ein angemessenes Schutzniveau für die übermittelten personenbezogenen Daten attestierte. Dies sollte nur für diejenigen Empfänger gelten, die sich den Safe Harbor-Prinzipien bzw. den zugehörigen „Frequently Asked Questions" („FAQs") durch eine Selbstzertifizierung unterworfen hatten. Über die Jahre sah sich das Safe Harbor-Abkommen vermehrt Kritik ausgesetzt, so vor allem seitens der hiesigen Aufsichtsbehörden zum Datenschutz. Grund hierfür lag in der Annahme, dass US-Unternehmen, die sich den Vorgaben von Safe Harbor verpflichtet haben, diese nicht adäquat umsetzen würden. Im Zuge des NSA-Skandals folgte gar die Aufforderung an die Europäische Kom-

mission, ihre Entscheidungen zu Safe Harbor und zu den Standardverträgen vor dem Hintergrund der exzessiven Überwachungstätigkeit ausländischer Geheimdienste bis auf Weiteres zu suspendieren.[1]

Eine europäische Dimension erreichte die Debatte um Safe Harbor im Jahre 2014, als der irische High Court in Dublin mit Beschluss vom 18.06.2014 dem EuGH die Frage nach der Verbindlichkeit des Safe Harbor-Beschlusses der EU-Kommission aus dem Jahr 2000 vorlegte. Geklagt hatte der Österreicher Max Schrems, der die Speicherung personenbezogener Daten auf US-Servern des Betreibers des sozialen Netzwerks Facebook in Anbetracht der weitereichenden Zugriffe amerikanischer Geheimdienste für als nicht zulässig erachtete und diesbezüglich zuvor erfolglos eine Eingabe bei der irischen Aufsichtsbehörde zur weiteren Ermittlung veranlasst hatte. Nachdem sich die irische Aufsichtsbehörde auf Grund fehlender tatsächlicher Anhaltspunkte für die Verletzung von Rechten und Interessen des Betroffenen zur Durchführung weiterer Ermittlungen geweigert hatte, wurde der irische High Court angerufen, der die Sache wiederum dem EuGH zur Entscheidung vorlegte.

2. Zum Urteil

Der EuGH widmete sich in seinem Urteil nicht nur der Frage der Zulässigkeit von Safe Harbor selbst, sondern hatte auch darüber zu entscheiden, inwieweit nationale Aufsichtsbehörden an eine Entscheidung der Kommission hinsichtlich des angemessenen Datenschutzniveaus in einem Drittland gebunden sind. Zu Letzterem stellt der EuGH zunächst fest, dass eine nationale Aufsichtsbehörde zwar keine Maßnahmen ergreifen dürfe, die einer Angemessenheitsentscheidung der Kommission entgegenstünden, sie aber nichtsdestoweniger im Einzelfall und im Rahmen einer Eingabe eines Betroffenen selbst beurteilen können müsse, ob eine Datenübermittlung in ein unsicheres Drittland im Einklang mit den Vorgaben europäischer Datenschutzgrundsätze stehe. Dies sei beim Vorliegen tatsächlicher Anhaltspunkte, die eine gegenteilige Annahme begründen würden, auch geboten. Entsprechend hätte die irische Aufsichtsbehörde die Eingabe des Betroffenen Max Schrems entgegennehmen und prüfen müssen. Die Angemessenheitsentscheidung der Kommission hindere sie daran nicht.

Die Überprüfung der Zulässigkeit der Angemessenheitsentscheidung aus 2000 selbst erfolgte seitens des EuGH anhand der Vorgaben der Richtlinie 95/46/EG sowie der EU-Grundrechtecharta als wesentliche Vorgaben zur Bestimmung eines „angemessenen Datenschutzniveaus“ in Ermangelung einer gesetzlichen Definition. Die Beurteilung eines angemessenen Datenschutzniveaus müsse dabei nach Art. 25 Abs. 2 der Richtlinie 95/46/EG unter Berücksichtigung aller Umstände erfolgen, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Hierbei nimmt der EuGH aus guten Gründen zunächst die Europäische Kommission als Entscheidungsfinderin in die Pflicht, anhand der einschlägigen nationalen Vorschriften im Drittland zum Schutz personenbezogener Daten oder auf Basis internationaler Verpflichtungen, das notwendige Schutzniveau zu prüfen. Darüber hinaus obliege der Kommission die Pflicht einer regelmäßigen Prüfung, ob eine getroffene Entscheidung zu Gunsten des Schutzniveaus eines Landes noch faktisch bzw. rechtlich zu rechtfertigen sei. Dies habe vor allem dann zu erfolgen, wenn Hinweise dies in Zweifel zögen. Insofern kritisiert der EuGH die Vorgehensweise der Kommission, die lediglich Empfehlungen[2] für eine Verbesserung der Safe Harbor-Grundsätze ausgesprochen hatte, ohne die Enthüllungen um die Datenzugriffe ame-

[1] Vgl. Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2013 vom 24. Juni 2013.

[2] Vgl. Memo der Europäischen Kommission “Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA“ vom 27. November 2013.

rikanischer Geheimdienste zum Anlass einer Überprüfung der Angemessenheitsentscheidung aus dem Jahre 2000 zu nehmen.

Die Unzulässigkeit von Safe Harbor folgt für das Gericht zum einen aus der fehlenden Bindungswirkung für staatlich veranlasste Datenzugriffe. Im Übrigen beziehe sich die Angemessenheitsentscheidung lediglich auf die Einhaltung der Prinzipien und der „FAQs" und enthalte keine ausreichenden Maßnahmen nach Art. 25 Abs. 6 der Richtlinie 95/46/EG, inwieweit die Vereinigten Staaten mittels nationaler Rechtsvorschriften oder internationaler Verpflichtungen ein solches Niveau gewährleisten würden. Hierdurch wird der in der Literatur für Safe Harbor verwendete Begriff der „unechten Angemessenheitsentscheidung" bestätigt, zumal sich die übrigen Kommissionentscheidungen auf nationale Vorschriften zum Datenschutz beziehen. Im Übrigen müssten Organisationen - so der EuGH - die Vorgaben von Safe Harbor nicht einhalten, wenn diese im Konflikt zu einem US-Gesetz stünden. Diese Beschränkungen würden auch nicht durch eine nationale Vorschrift zum Schutz Betroffener begleitet. Auch die über Safe Harbor vorgesehene Möglichkeit einer Streitschlichtung beziehe sich nur auf die Einhaltung seiner Prinzipen durch US-Organisationen und fände keine Anwendung auf Maßnahmen des Staates.

3. Zu den Folgen

Die vom EuGH vorgenommene Klarstellung hinsichtlich der Kompetenz nationaler Aufsichtsbehörden zur Möglichkeit der Überprüfung eines einzelnen Datenexports in ein unsicheres Drittland im Falle tatsächlicher Anhaltspunkte hinsichtlich eines nicht mehr vorhandenen angemessenen Datenschutzniveaus ist eine im Ergebnis richtige und wichtige Feststellung, um eine wirksame und flexible behördliche Kontrolle gewährleisten zu können. Wichtig für datenverarbeitende Stellen ist jedoch auch die Aussage des EuGH, dass Angemessenheitsentscheidungen der Kommission durchaus eine Bindungswirkung entfalten, die erst auf Grund konkreter Anhaltspunkte erschüttert werden kann und letztlich nur durch den EuGH selbst aufgehoben werden kann. International agierende Stellen sind auf verlässliche Instrumente für einen Datenexport in Drittländer wie die Vereinigten Staaten angewiesen.

Hinsichtlich der Zulässigkeit von Safe Harbor vermag der EuGH nachvollziehbare Gründe anführen, warum die Angemessenheitsentscheidung der Europäischen Kommission nicht im Sinne der Vorgaben von Art. 25 Abs. 6 der Richtlinie 95/46/EG ergangen ist. Er dürfte jedoch verkennen, wie weitreichend die Unzulässigkeitserklärung in transatlantische Datenflüsse eingreift. Denn die Urteilsgründe veranlassen zur Annahme, dass sich nicht nur Datenübermittlungen von europäischen Stellen an Safe Harbor zertifizierte Unternehmen in den USA nunmehr ohne rechtliche Erlaubnis vollziehen, sondern alle Werkzeuge betreffen könnten, die auf ein angemessenes Datenschutzniveau in den USA abzielen. Denn den Vereinigten Staaten werden insgesamt unzureichende Schutzvorkehrungen im Falle staatlich veranlasster Zugriffe attestiert, mit der Folge, dass die Europäische Kommission in Zusammenarbeit mit der amerikanischen Regierung diese regulatorischen Maßnahmen erst vereinbaren muss. Dass dies eine gewisse Zeit in Anspruch nehmen wird, liegt auf der Hand. In der Zwischenzeit wird jeglicher Datenexport in die Vereinigten Staaten in Frage gestellt. Dementsprechend prüfen hiesige Aufsichtsbehörden ob und inwieweit Datentransfers in die USA, die auf andere Rechtsgrundlagen wie Standardvertragsklauseln, Einwilligung oder Binding Corporate Rules gestützt werden, auszusetzen sind. Diesbezüglich ist jedoch festzuhalten, dass die Entscheidung des EuGH an die Vorlagefragen des irischen High Courts gebunden ist und insoweit andere Instrumente für den Datenexport in ein unsicheres Drittland nicht für unzulässig erklärt hat. **Demnach können hiesige Datenverarbei-**

ter mit transatlantischen Beziehungen formal gesehen weiterhin auf alternative Maßnahmen wie Standardvertragsklauseln, Binding Corporate Rules oder die informierte Einwilligung des Betroffenen setzen. Hierbei ist zu erwägen, ob ein Datenexport durch zusätzliche technische Maßnahmen, so über eine Verschlüsselung, abgesichert werden kann.

Die GDD fordert die Europäische Kommission und die amerikanische Regierung jedoch dazu auf, schnellstmöglich eine novellierte Vereinbarung hinsichtlich des Exports personenbezogener Daten von europäischen Datenverarbeitern an US-amerikanische Stellen zu treffen, um hiesigen verantwortlichen Stellen, die um einen datenschutzkonformen Umgang mit personenbezogenen Daten bemüht sind, eine Sicherheit zu geben, dass ein Datenexport in die Vereinigten Staaten ohne eine Sanktionierung durch Aufsichtsbehörden weiterhin möglich ist. Hierbei sollten die Vorgaben des EuGH hinsichtlich der Erarbeitung angemessener Vorschriften zum Schutz Betroffener vor staatlichen Zugriffen oder seitens der Geheimdienste beachtet werden.

Bonn, den 08.10.2015