Luther.

IP/IT

(Intellectual Property/Information Technology)

Europäischer Gerichtshof kippt „Safe Harbor“

Sondernewsletter II

Europäischer Gerichtshof kippt „Safe Harbor“

Am 6. Oktober 2015 hat der Europäische Gerichtshof (EuGH) entschieden, dass die Safe Harbor Entscheidung 2000/520/EG der EU-Kommission vom 26. Juli 2000 ungültig ist. Damit wird der Übermittlung personenbezogener Daten in die USA in zahlreichen Bereichen die rechtliche Grundlage entzogen. Die USA verliert ihren Status als Land, das zumindest im Geltungsbereich der Safe Harbor Zertifizierung über ein mit der EU-Datenschutzrichtlinie 95/46 vergleichbares angemessenes Datenschutzniveau verfügt. Gleichzeitig stärkt der EuGH mit diesem Urteil die Kontroll-Befugnisse der nationalen Datenschutzaufsichtsbehörden.

1. Verfahrensgang

Dem EuGH Urteil liegt ein Vorabentscheidungsersuchen gemäß Art. 267 AEUV des irischen High Court datierend vom 17. Juli 2014 zugrunde. Geklagt hatte ein Österreicher. Dieser hatte sich wegen der Übermittlung seiner persönlichen Daten durch die europäische Facebook Zentrale, Facebook Ireland Ltd., in die USA und wegen des unzureichenden Schutzes seiner Daten in den USA vergeblich an den irischen Beauftragten für Datenschutz gewandt. Dieser hatte eine inhaltliche Prüfung der Anfrage abgelehnt mit der Begründung, er sei an die Feststellungen der EU-Kommission in der sog. „Safe Harbor“ Entscheidung aus dem Jahre 2000 zur Angemessenheit des Datenschutzniveaus in den USA gebunden. An der Geltung dieser Entscheidung habe sich auch durch die Enthüllungen im Zusammenhang mit der NSA Überwachung nichts geändert. Gegen den ablehnenden Bescheid erhob der Österreicher Klage beim irischen High Court. Dieser legte dem EuGH daraufhin die Frage vor, ob eine unabhängige Datenschutzaufsichtsbehörde dahingehend an die Safe Harbor Entscheidung der EU Kommission gebunden sein kann, dass sie keine eigene Prüfung vornehmen und keine neueren Entwicklungen berücksichtigen könne.

Der Generalanwalt teilte in den „Schlussanträgen“ Ende September 2015 mit, dass nach seiner Auffassung die EU-Kommission mit einer Entscheidung wie „Safe Harbor“ die Kontrollbefugnisse der nationalen Datenschutzbehörden nicht einschränken könne. Damit würde deren – nach europäischem Recht ausdrücklich vorgesehene – Unabhängigkeit in Frage gestellt. Es obliege den Mitgliedstaaten dafür zu sorgen, dass die nationalen Datenschutzaufsichtsbehörden die Grundrechte ihrer Bürger schützen können. Das US-Recht erlaube es, persönliche Daten von EU-Bürgern zu speichern, ohne dass diese über wirksamen Rechtsschutz dagegen verfügten. Die EU-Kommission hätte die Anwendung von „Safe Harbor“ nach den neuen Erkenntnissen in Sachen NSA aussetzen müssen. Es genüge nicht, dass die EU-Kommission neue Verhandlungen mit den USA aufgenommen habe, um mögliche Datenschutzverstöße abzustellen.

2. Gegenstand des Urteils

Der Auffassung des Generalanwalts hat sich der EuGH angeschlossen.

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sei im Licht der Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union dahingehend auszulegen, dass eine Entscheidung wie die Safe Harbor Entscheidung eine nationale Datenschutzaufsichtsbehörde nicht an der Prüfung von Eingaben Betroffener hindere, wenn diese geltend machten, dass das Recht und die Praxis des Landes, in das personenbezogene Daten aus der EU übermittelt werden, kein angemessenes Schutzniveau gewährleisteten. Zwar dürften die EU Mitgliedstaaten und ihre zuständigen Aufsichtsbehörden keine der Kommissions-Entscheidung zuwiderlaufenden Maßnahmen – wie etwa Rechtsakte mit verbindlichen Feststellungen zur Angemessenheit des Schutzniveaus – erlassen. Für die Rechtsakte der Unionsorgane gilt grundsätzlich eine Vermutung der Rechtmäßigkeit, so dass sie Rechtswirkungen entfalten, solange sie nicht zurückgenommen, im Rahmen einer Nichtigkeitsklage für nichtig erklärt oder infolge eines Vorabentscheidungsersuchens oder einer Einrede der Rechtswidrigkeit für ungültig erklärt wurden. Trotzdem dürfe eine Kommissionsentscheidung die Datenschutzaufsichtsbehörden nicht an einer Überprüfung hindern.

Der EuGH führt aus, dass die Safe Harbor Entscheidung keine hinreichenden Garantien im Sinne der EU-Datenschutzrichtlinie enthalte. Der den US-Geheimdiensten eröffnete Zugriff bedeute einen Eingriff in die Grundrechte auf Achtung der Privatsphäre und Datenschutz. Die Überwachung sei massiv, nicht zielgerichtet und umfasse auch die Inhalte der Kommunikation ohne jede Differenzierung. EU-Unionsbürger verfügten über keinen effektiven Rechtsschutz gegen derartige Abhör- und Überwachungsmaßnahmen der US-Sicherheitsbehörden. In diesem Zusammenhang hatte der Generalanwalt angemerkt, dass alle am PRISM Programm beteiligten Unternehmen Safe Harbor zertifiziert seien und damit das Safe Harbor Verfahren als ein Zugang für die US-Überwa-

chungsbehörden zu der Erhebung personenbezogener Daten aus der EU fungiere.

3. Hintergrund

Die EU-Entscheidung zu Safe Harbor steht seit längerem in der Kritik.

Die EU-Datenschutzrichtlinie 95/46 fordert, dass die Mitgliedstaaten eine Übermittlung personenbezogener Daten außerhalb der EU nur dann erlauben, wenn dort ein angemessenes Datenschutzniveau besteht. Auf Basis von Artikel 25 der EU-Datenschutzrichtlinie hat die EU-Kommission für bestimmte Staaten mit EU-weiter Gültigkeit festgestellt, dass in diesen Staaten ein „angemessenes Schutzniveau" für dorthin übermittelte Daten besteht. In der sog. Safe Harbor Entscheidung 2000/520/EG vom 26. Juli 2000 hatte die EU-Kommission genau dies für die USA festgestellt. US-Unternehmen im Zuständigkeitsbereich des US-Handelsministeriums können *Safe Harbor* beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die *Safe Harbor Principles* (englisch für „Grundsätze des sicheren Hafens") und die dazugehörenden – verbindlichen – FAQ zu befolgen. Übermittlungen von personenbezogenen Daten aus einem EU-Staat an „Safe Harbor" zertifizierte Unternehmen in den USA bedurften damit im Hinblick auf die Vorgaben für EU-Auslandstransfers bis dato keiner weitergehenden Vorkehrungen mehr. Mehrere tausend US-Unternehmen, unter ihnen Microsoft, IBM, Google und Facebook, sind „Safe-Harbor-zertifiziert".

Nicht erst seit den Enthüllungen über die Reichweite der Überwachungsbefugnisse des US-Geheimdienstes NSA steht die Safe-Harbor Entscheidung in der Kritik. Bereits mit Beschluss vom 28./29. April 2010 hat der Düsseldorfer Kreis als Zusammenschluss der deutschen Datenschutz-Aufsichtsbehörden aus Anlass von Mängeln bei der Umsetzung und Einhaltung des Safe Harbor Standards festgestellt, dass deutsche datenexportierende Unternehmen die Selbst-Zertifizierung des US-Importeurs gemäß den Safe Harbor Vorgaben zu überprüfen haben. Vor dem Hintergrund der massiven Überwachungstätigkeit ausländischer Geheimdienste hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Pressemitteilung vom 24. Juli 2013 die EU-Kommission aufgefordert, ihre Entscheidungen zu Safe Harbor und zu den Standardverträgen bis auf Weiteres zu suspendieren. Die deutschen Datenschutzaufsichtsbehörden kündigten in diesem Zusammenhang an, keine neuen Genehmigungen für Datenübermittlungen in Drittstaaten erteilen und die Aussetzung entsprechender Datenübermittlungen prüfen zu wollen. Unklar blieb, wie diese Forderung in der Praxis umgesetzt werden sollte, soweit Datenübermittlungen in Länder mit angemessenem Datenschutzniveau nach deutschem Recht keiner aufsichtsbehördlichen Genehmigung bedürfen. Ungeachtet dieser Forderung und ihrer praktischen Umsetzbarkeit sowie der von der EU-Kommission daraufhin angekündigten Überprüfung war die Safe Harbor Entscheidung aber bis zum aktuellen EuGH-Urteil in Kraft.

4. Folgen des EuGH-Urteils

Als Folge des EuGH-Urteils sind die nationalen Datenschutzaufsichtsbehörden gehalten, zukünftig aktuelle Entwicklungen im Rahmen von Einzelfallprüfungen zu berücksichtigen.

Die Unwirksamkeit der Safe Harbor Entscheidung hat aber darüber hinaus weitreichende Folgen für europäische Unternehmen, die personenbezogene Daten in die USA übermitteln und die Angemessenheit des Datenschutzniveaus in den USA bislang über die Safe Harbor Zertifizierung des in den USA ansässigen datenempfangenden Unternehmens gewährleistet haben. Dies gilt für konzerninterne Übermittlungen von Personal- und Kundendaten – etwa wenn europäische Tochterunternehmen Daten mit ihrer US-amerikanischen Konzernzentrale austauschen – genauso wie für Übermittlungen von Daten an US-amerikanische IT Dienstleister und Social Media Plattformen. Insbesondere bei cloudbasierten Diensten gehört der globale Datenaustausch zum Geschäftsmodell, so dass diese von dem EuGH-Urteil besonders betroffen sind.

5. Unmittelbarer Handlungsbedarf für Unternehmen

Der Wegfall der Safe Harbor Zertifizierung erfordert andere Instrumente zur Legalisierung der Datenübermittlungen. Eine Alternative besteht im Abschluss der sog. EU-Standardvertragsklauseln. Die Europäische Kommission hat Standardvertragsklauseln für Übermittlungen an sog. Auftragsdatenverarbeiter (Beschluss 2010/87/ EU der Kommission vom 5. Februar 2010) und Standardvertragsklauseln für Übermittlungen an sog. verantwortliche Stellen (Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001 und Entscheidung 2004/915/EG der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln) verabschiedet, die angemessene Garantien bei der Übermittlung personenbezogener Daten von der EU in Drittländer gewährleisten und von den nationalen Datenschutzaufsichtsbehörden

anzuerkennen sind. Unternehmen sollten prüfen, welche der verschiedenen Standardvertragsklauseln für ihre Zwecke sachgerecht sind und wie diese in bestehende vertragliche Absprachen mit Kunden und Dienstleistern integriert werden können. In diesem Zusammenhang sind auch die unterschiedlichen rechtlichen Anforderungen – etwa das gesetzliche Schriftformgebot in § 11 Bundesdatenschutzgesetz – und die im Einzelfall bestehende Komplexität etwaiger Unterauftragnehmerbeziehungen – insbesondere die Aufgabenverteilung sowie die betroffenen Datenaustausch- und Vertragsbeziehungen – zu berücksichtigen.

Für konzerninterne Datenübermittlungsvorgänge in großen oder global aufgestellten Unternehmen sind sog. Binding Corporate Rules eine weitere Alternative. Hier schafft das europaweite Abstimmungsverfahren zwischen den Datenschutzaufsichtsbehörden der betroffenen EU- und EWR Mitgliedstaaten, das in dem Entwurf der EU-Datenschutzgrundverordnung zukünftig weiter vereinfacht werden soll, erhebliche Erleichterungen. Abhängig vom betroffenen Geschäftsmodell ist die Einholung einer Einwilligung der von den Datenübermittlungen Betroffenen zwar grundsätzlich auch eine denkbare Alternative. Eine derartige Einwilligung müsste sich aber ausdrücklich auf die Übermittlung in ein Drittland mit nicht angemessenem Datenschutzniveau beziehen. Zudem bestehen häufig Zweifel an der erforderlichen Freiwilligkeit derartiger Einwilligungen und die jederzeitige Widerrufbarkeit der Einwilligung führt zu Schwierigkeiten in der praktischen Umsetzung.

Das EuGH Urteil ist unmittelbar wirksam. Eine Übergangsfrist, bis zu deren Ablauf der Datentransfer noch – wie bisher – stattfinden kann, wurde nicht vorgesehen. Die EU-Kommission will in den nächsten Tagen gemeinsam mit den nationalen Datenschutzaufsichtsbehörden Vorgaben erarbeiten, um die entstandene Rechtsunsicherheit zu beseitigen. Es bleibt abzuwarten, inwieweit in diesem Zusammenhang faktische Übergangsfristen eingeführt werden, indem zumindest für einen Übergangszeitraum seitens der Datenschutzaufsichtsbehörden keine Sanktionen für unzulässige Datenübermittlungen verhängt werden. In der EU ansässige Unternehmen sind für die Zulässigkeit von Datenübermittlungen an US-Unternehmen unmittelbar verantwortlich. Dies gilt vor allem, wenn es sich bei den eingeschalteten (US-)Dienstleistern um sog. Auftragsdatenverarbeiter handelt, die die Daten nur im Auftrag und auf Weisung der verantwortlichen Stelle verarbeiten. Das Risiko aufsichtsbehördlicher Sanktionen und der Durchsetzung von Ansprüchen der Betroffenen trägt in diesem Fall das in der EU ansässige datenübermittelnde Unternehmen als verantwortliche Stelle.

Soweit IT-Dienstleister nicht bereits aus eigener Initiative Auffangmaßnahmen eingeleitet oder angekündigt haben, ist den betroffenen Unternehmen zu empfehlen, diese ausdrücklich einzufordern, und die vertraglichen Absprachen entsprechend anzupassen.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Stefanie Hellmich, LL.M.
Luther Rechtsanwaltsgesellschaft mbH, An der Welle 10,
60322 Frankfurt a.M., Telefon +49 69 27229 24118
stefanie.hellmich@luther-lawfirm.com

Haftungsausschluss

Die Luther Rechtsanwaltsgesellschaft mbH berät in allen Bereichen des Wirtschaftsrechts. Zu den Mandanten zählen mittelständische und große Unternehmen sowie die öffentliche Hand. Die Luther Rechtsanwaltsgesellschaft mbH ist das deutsche Mitglied von Taxand, einem weltweiten Zusammenschluss unabhängiger Steuerberatungsgesellschaften.

Berlin, Brüssel, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Köln, Leipzig,
London, Luxemburg, München, Shanghai, Singapur, Stuttgart

Luther Corporate Services: Delhi-Gurgaon, Kuala Lumpur, Shanghai, Singapore, Yangon

Ihren Ansprechpartner finden Sie auf www.luther-lawfirm.com

Auf den Punkt. Luther.

JUVE 2014 AWARDS
Kanzlei des Jahres
für Regulierte Industrien

JUVE 2014 AWARDS
Kanzlei des Jahres
für Energiewirtschaftsrecht

JUVE 2014 AWARDS
Kanzlei des Jahres
für Privates Baurecht

www.luther-lawfirm.com

Taxand