ZEITSCHRIFT FÜR DATENSCHUTZ

ZD

EDITORIAL

11/2015

# Safe Harbor: Ein Ende mit Schrecken – Wann kommt Safe Harbor 2.0?

Am 6.10.2015 hat der *EuGH* (Rs. C-362/14, ZD 2015, 549 m. Anm. *Spies* – in diesem Heft) die Entscheidung der *EU-Kommission* zum EU/US-Safe Harbor-Abkommen 2000/520/EG v. 26.7.2000 für ungültig erklärt. Liest man den ein oder anderen Online-Kommentar oder Artikel zur Entscheidung des *EuGH* (z.B. „Kampfansage der Europarichter gegen US-Internetkonzerne", Börsenzeitung v. 7.10.2015) erkennt man vielfach große Freude über die Entscheidung, gepaart mit der Hoffnung, dass die verbliebenen Regelungsmechanismen nun besseren Schutz böten und die USA nachziehen müssten. Teilweise zeigt sich sogar Schadenfreude über die angeblich bösen Unternehmen in den USA, die sich nun endlich an das europäische Datenschutzrecht halten müssten.

So klar und schön ist die Welt durch das Urteil aber nicht geworden. Der Paukenschlag des *EuGH* kann zu einer erheblichen Rechtsunsicherheit führen, da er weit über das Safe Harbor-Abkommen hinausgeht und das Finden neuer Lösungen erschwert. Keineswegs sind von der Entscheidung nur große US-Internetkonzerne betroffen, wie auch so manche Schlagzeile andeutet. Die Entscheidung betrifft uns alle, viele mittelständische und größere Unternehmen, die entweder Datenflüsse im Konzernverbund in die USA benötigen oder mit Geschäftspartnern in den USA zusammenarbeiten, und nicht zuletzt die europäischen Verbraucher, die von Dienstleistungen in den USA im Alltag profitieren und ihre Daten mehr oder weniger freiwillig in die USA schicken. All diese verantworten die mit der Entscheidung verursachte Rechtsunsicherheit nicht. Wenn überhaupt, haben die USA und die *EU-Kommission* diese Situation verschuldet, da beide viel zu lange keine substanziellen Fortschritte in Bezug auf den Schutz personenbezogener Daten erzielt haben.

**Dr. Christian Schröder** ist Rechtsanwalt, Partner und Leiter des Fachbereichs IP/IT & Data Protection Practice Group in der Kanzlei ORRICK, HERRINGTON & SUTCLIFFE LLP in Düsseldorf sowie Wissenschaftsbeirat der ZD.

Man kann jetzt nur hoffen, dass die nationalen Aufsichtsbehörden gemeinsam mit der *EU-Kommission* schnell praktische und verantwortungsvolle Vorgaben entwickeln. Nach einer ersten Stellungnahme der *Kommission* besteht hierauf jeweils eine gewisse Hoffnung (vgl. PM der *EU-Kommission* v. 7.10.2015).

## Was folgt für bisher Safe Harbor-basierte Datenübermittlungen?

Der *EuGH* hat in seiner Entscheidung die Safe Harbor-Entscheidung der *EU-Kommission* für nichtig erklärt und zugleich die Rechte und Pflichten der nationalen Aufsichtsbehörden gestärkt. Unternehmen, die bisher Datenübermittlungen auf Safe Harbor gestützt haben, können sich jetzt nicht mehr auf dieses Abkommen berufen. Für diese liegt der Rat nahe, nun auf Alternativen wie die EU-Standardvertragsklauseln (Entscheidung der *Kommission* v. 5.2.2010, 2010/87/EU), Binding Corporate Rules (BCR) oder die anderen von der RL 95/46/EG (DS-RL) vorgesehenen Rechtfertigungsmöglichkeiten wie z.B. Einwilligungen oder Einzelfallgenehmigungen auszuweichen (vgl. PM der *Kommission* v. 6.10.2015). Für Unternehmen, die über eine Vielzahl von Unterauftragnehmern verfügen, ist der Wechsel von Safe Harbor auf z.B. die EU-Standardvertragsklauseln für Auftragsdatenverarbeiter jedoch schwierig und erfordert einige Anpassungen. Während Safe Harbor keine speziellen Vorgaben für eine Unterbeauftragung machte und insofern den Abschluss von relativ weichen und unspezifischen Unteraufträgen erlaubte, verlangt z.B. Klausel 11 des EU-Standardvertrags für Auftragsdatenverarbeiter (a.a.O.), dass dem Unterauftragnehmer schriftlich die gleichen Pflichten wie dem primären Auftragnehmer auferlegt werden. Vor besonderen Herausforderungen stehen auch Unternehmen, die nicht in der EU niedergelassen sind und Daten z.B. über das Internet direkt von Bewohnern der EU erheben.

Bei dieser möglicherweise noch überschaubaren Rechtsunsicherheit belässt es der *EuGH* aber nicht, sondern er stellt mit seiner Argumentation auch viele weitere Übermittlungen in die USA und auch in andere Staaten in Frage.

## Was folgt für Datenübermittlungen in andere „sichere" Drittstaaten?

Neben Safe Harbor kann die Entscheidung des *EuGH* auch Übermittlungen in andere Drittstaaten betreffen. Der *EuGH* hat ausdrücklich festgehalten, dass die Bindungswirkung der Kommissionsentscheidungen nach Art. 25 Abs. 6 DS-RL nationale Aufsichtsbehörden nicht davon entbindet, bei Verdacht einer Verletzung europäischer Grundfreiheiten selbst tätig zu werden. Die insofern überzeugenden Ausführungen des *EuGH* halten fest, dass die nationalen Datenschutzaufsichtsbehörden eine Beschwerde nicht einfach unter Hinweis auf eine von der *Kommission* getroffene Entscheidung verwerfen dürfen. Die Aufsichtsbehörden müssen selbst den Sachverhalt prüfen und ggf. den Rechtsweg beschreiten. Ohne eine solche Kontrolle wären der *Kommission*, die auch in der Vergangenheit selbst bei rechtlichen Zweifeln eher wirtschaftliche bzw. politische Lösungen suchte (s. Aufhebung des PNR-Abkommens zwischen der *EU-Kommission* und den USA durch den *EuGH*, U. v. 30.6.2006 – C-317/04 u. C-318/04),

ein nicht mit den Grundfreiheiten vereinbarer Spielraum eröffnet. Vielleicht, und so hofft vermutlich auch der *EuGH*, wird die nun klargestellte Kontrolle ihr auch helfen, bei Verhandlungen mit anderen Staaten bessere Lösungen zu finden.

Da der kritisierte Zugriff von Geheimdiensten auf personenbezogene Daten in den USA jedoch nicht singulär ist, könnten zukünftig auch Datenübermittlungen in andere von der *EU-Kommission* als sicher eingestufte Drittstaaten von den nationalen Aufsichtsbehörden geprüft werden. Wenn Pressemeldungen zufolge sogar von Mitgliedstaaten innerhalb der EU massenhaft und verdachtslos Daten erhoben werden (s. Berichte über den Britischen Geheimdienst GCHQ, Die Zeit, v. 26.9.2015), müsste konsequenterweise auch die Übermittlung von Daten in solche Staaten innerhalb der EU in Frage gestellt werden.

Entgegen dem Wunsch von Generalanwalt *Yves Bot* in seinen Schlussanträgen v. 23.9.2015 (Rdnr. 81 u. 117) dürften die Ausführungen des *EuGH* jedoch so zu verstehen sein, dass sich die nationalen Aufsichtsbehörden nicht ohne Vorlage an die Gerichte und nachfolgend an den *EuGH* über die jeweilige Kommissionsentscheidung hinwegsetzen und z.B. eine Datenübermittlung unterbinden dürfen (*EuGH* ZD 2015, 549, Rdnr. 61, 62, 64 u. 65). Diese der Rechtsklarheit dienende Auffassung bestätigt daher, dass Unternehmen auf die Entscheidungen der *EU-Kommission* vertrauen dürfen. Erst durch eine Entscheidung des *EuGH* könnte ein Datentransfer verhindert werden. Nationale Aufsichtsbehörden dürften daher nicht bereits heute Datenübermittlungen in andere vermeintlich sichere Drittstaaten und ggf. auch in gewisse EU-Mitgliedstaaten dauerhaft untersagen.

### Betrifft die Entscheidung auch andere Rechtfertigungen für Übermittlungen von Daten in die USA?

Da der *EuGH* seine Kritik an der Safe Harbor-Entscheidung der *EU-Kommission* an dem verdachtslosen massiven Zugriff auf Daten ohne Rechtsbehelf (a.a.O., Rdnr. 90 unter Berufung auf Analysen der *EU-Kommission*, COM(2013) 846 und 847 final) festmacht und diese für mit Art. 7 und 8 GRCh unvereinbar hält (a.a.O., Rdnr. 91), dürfte diese Kritik auch Datenübermittlungen in die USA treffen, die z.B. auf den Standardvertragsklauseln basieren. Die vom *EuGH* gesehene Gefahr trifft daher diese Daten im gleichen Maße wie Daten, die über Safe Harbor in die USA übermittelt worden sind. Zwei Überlegungen mögen jedoch den betroffenen Unternehmen derzeit helfen:

#### ■ Das Gefährdungspotenzial ist nicht für alle Daten gleich

Es gibt keinerlei Anlass zur Annahme, dass sämtliche in die USA übermittelten Daten tatsächlich einem massiven und verdachtslosen Zugriff durch US-Geheimdienste ausgesetzt sind. Es gibt z.B. keine Informationen darüber, dass bei US-Muttergesellschaften gespeicherte Mitarbeiterdaten regelmäßig an US-Geheimdienste herausgegeben werden müssen. Dies dürfte auch für eine Vielzahl anderer Übermittlungen von Daten gelten, die kein mit Kommunikationsdaten vergleichbares Interesse der Geheimdienste auf sich ziehen.

#### ■ Bindungswirkung der Kommissionsentscheidungen zu den Standardvertragsklauseln

Die Entscheidungen der *EU-Kommission* zu den Standardvertragsklauseln (*Kommission,* E. v. 15.6.2001 – 2001/479/EG; v. 27.12.2004 – 2004/915/EG u. v. 5.2.2010 -2010/87/EU) folgen der Vorgabe des Art. 26 Abs. 2 DS-RL, wonach Datenübermittlungen in unsichere Drittstaaten übermittelt werden dürfen, wenn die empfangende Stelle einen Vertrag mit hinreichendem Schutz für personenbezogene Daten mit der datenexportierenden Stelle schließt. Um den wirtschaftlich gebotenen Datenaustausch zu erleichtern und den Unternehmen mehr Verlässlichkeit zu geben (*Kommission*, E. v. 15.6.2001 – 2001/479/EG, Begründungserwägung 4), sieht Art. 26 Abs. 4 vor, dass die *EU-Kommission* Standardverträge beschließen kann, die – wie bei Art. 25 Abs. 6 – von den nationalen Aufsichtsbehörden zu beachten sind. Von dieser Ermächtigungsnorm hat die *Kommission* Gebrauch gemacht und derzeit drei Vertragswerke als ausreichend bewertet (a.a.O).

Angesichts der grundsätzlichen Kritik des *EuGH* an einem verdachtslosen Zugriff durch Behörden im Empfängerland könnten jedoch nun die nationalen Aufsichtsbehörden daran denken, auch grundsätzlich Datenübermittlungen auf Basis der Standardvertragsklauseln in Frage zu stellen und gar auszusetzen. Dies stünde jedoch nicht nur im Gegensatz zu der Festlegung der RL in Art. 26 Abs. 2, wonach Verträge offenbar einen ausreichenden Schutz bieten können, sondern würde ebenfalls die erwünschte begrenzte Bindungswirkung der Kommissionsentscheidung in Frage stellen. Insofern spricht viel dafür, dass jedenfalls bei einer grundsätzlichen Kritik der Aufsichtsbehörden an den Standardvertragsklauseln zunächst ebenfalls eine Entscheidung des *EuGH* einzuholen wäre.

### Eine grundsätzliche Verständigung ist dringend notwendig

Die aufgezeigte erhebliche Rechtsunsicherheit ist für beide Seiten des Atlantiks schädlich, denn wie aufgezeigt gibt es derzeit kaum wirklich sichere Alternativen. Wir brauchen daher dringend eine Art Safe Harbor 2.0 und darüber hinaus eine grundsätzliche Verständigung zwischen der EU und den USA über einen hinreichenden Schutz von übermittelten personenbezogenen Daten im privaten Rechtsverkehr.

Positiv ist daher zu vermerken, dass der *EuGH* nicht grundsätzlich die Möglichkeit eines Safe Harbor 2.0 ausgeschlossen hat. Der *EuGH* hat ausdrücklich das aus Art. 25 Abs. 5 und 6 DS-RL folgende Mandat der *EU-Kommission* bestätigt, ähnlich wie bei ihrer nun aufgehobenen Safe Harbor-Entscheidung nur sektorale oder auch einen bestimmen Kreis von Unternehmen betreffende Vereinbarungen sowie Vereinbarungen über Selbstzertifizierungen mit Drittstaaten zu verhandeln (a.a.O., Rdnr. 81). Allerdings verlangt der *EuGH* nun, dass die Entscheidung der *EU-Kommission* auch den Schutz vor Zugriff durch Sicherheitsbehörden einschließt (a.a.O., Rdnr. 75, 86). Außerdem, und in dieser Feststellung dürfte das größte Problem liegen, sollen die Drittländer einen mit den europäischen Grundfreiheiten gleichwertigen Schutz für personenbezogene Daten bieten (a.a.O., Rdnr. 73). Der *EuGH* hat zwar betont, dass gleichwertig nicht mit identisch gleichzusetzen sei. Diese Forderung des *EuGH* könnte jedoch gleichwohl als Gebot einer weitgehenden Angleichung fremder Rechtsordnungen an diejenige der EU zu verstehen sein. Das würde keine Berücksichtigung der Wertungen und Rechtsvorstellungen des Empfängerlands ermöglichen und könnte sich auf die Bereitschaft fremder Staaten, sich den europäischen Anforderungen zu nähern, eher negativ auswirken. Eine kleine Abschwächung dieser Anforderungen kann vielleicht in den Satz hineingelesen werden, wonach es im Wesentlichen auf die praktische Wirksamkeit der Maßnahmen ankomme (a.a.O., Rdnr. 74). Vielleicht schafft diese richtige Erkenntnis den notwendigen Raum für Regelungen, die zwar nicht unseren rechtsdogmatischen Vorstellungen entsprechen, aber gleichwohl in der Praxis zu einem deutlich besseren Schutz der Daten führen (a.a.O., Rdnr. 74).

Wenn die EU nicht ernsthaft die Wirtschaftsbeziehungen mit den USA, aber auch mit anderen Drittstaaten gefährden will, sollte der Schwerpunkt der Anforderungen folglich eher auf der Umsetzung der praktischen Wirksamkeit und des Rechtsschutzes liegen und in Bezug auf die Quantität des Zugriffs etwas mehr Verständnis für andere Vorstellungen gezeigt werden. Man kann daher nur hoffen, dass die USA und die *EU-Kommission* schnellstmöglich eine vertretbare Lösung zum Schutz von personenbezogenen Daten entwickeln. Das ist keine leichte Verhandlungsaufgabe und man kann der *Kommission* bei aller Kritik an früheren Entscheidungen und an ihrem Abwarten dieser ihre Position nicht erleichternden Entscheidung des *EuGH* nur viel Erfolg wünschen.