Safe-Harbor: Die Entscheidung des Europäischen Gerichtshofs

Ass. iur. Andreas Börding, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Westfälische Wilhelms-Universität Münster

1 Datensammeln ohne Grenzen

Der Transfer von personenbezogenen Daten kennt keine Grenzen. Durch das Internet ist es möglich, riesige Datenmengen in Sekundenbruchteilen über die gesamte Welt zu versenden, zu kopieren und weiterzuverarbeiten.

Dabei treffen unterschiedliche Rechtssysteme mit verschiedenen Anforderungen aufeinander. Der Umgang mit diesen Daten wird in Deutschland und der Europäischen Union kritisch behandelt. Hiernach gilt insbesondere der Grundsatz, dass personenbezogene Daten allein aufgrund einer gesetzlich bestimmten Zweckbindung erhoben, verarbeitet und genutzt werden dürfen. Zudem sollen nur so viele Daten erhoben werden, wie es der verfolgte Zweck rechtfertigt. Dies läuft im Regelfall auf eine umfassende Interessensabwägung der beteiligten Personen und Stellen hinaus.

Seinen Ursprung hat dieses Verständnis u.a. im Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983, in dem Kriterien für den staatlichen Umgang mit personenbezogenen Daten von Bürgern bestimmt wurden.[1] In dauerhafter Fortentwicklung dieser Grundsätze setzte eine Harmonisierung der europäischen Datenschutzstandards ein. Diese begann mit dem Inkrafttreten der europäischen Datenschutzrichtlinie im Jahr 1995 und wird in der Europäischen Datenschutzgrundverordnung – die eine weitgehende Vollharmonisierung des Datenschutzrechts vorsieht – ihren vorläufigen Höhepunkt finden. Dagegen herrscht in den Vereinigten Staaten von Amerika ein vergleichbar freigiebiges Verständnis vom Datenschutz. Ein einheitliches Datenschutzkonzept für personenbezogene Daten gibt es dort derzeit nicht (Börding 2016). Vielmehr finden sich nur bereichsspezifische Regelungskomplexe ohne eine zentrale Datenschutzaufsicht (Börding 2016). Lediglich einige Bundesstaaten sehen Regelungen zum Umgang mit personenbezogenen Daten vor (Jolly 2015). Zudem gilt ein Großteil der US-amerikanischen Datenschutzvorschriften nicht oder nur eingeschränkt für Europäer (Böhm 2015: 69-70).

Die Unterschiede zwischen den Rechtsräumen erfordern, dass der Export von personenbezogenen Daten aus dem europäischen Raum nur unter der Gewährleistung eines hohen Schutzniveaus für zulässig erklärt wird.

Schließlich haben die größten datenverarbeitenden Unternehmen der Welt wie z.B. Facebook, Google oder Amazon ihren Sitz in den USA. Hierbei muss neben sicheren Rahmenbedingungen für private Unternehmen auch im Auge behalten werden, dass die öffentlichen Stellen in den USA weitreichende Auskunftskompetenzen hinsichtlich der Offenlegung von gespeicherten und verarbeiteten Personendaten haben und hiervon auch reichlich Gebrauch machen (Electronic Frontier Foundation 2015).

Auf einen Blick: Safe-Harbor

- Der Transfer von personenbezogenen Daten in die USA ist derzeit höchst problematisch.
- Eine Übermittlung aufgrund des Safe-Harbor-Abkommens der Europäischen Kommission mit den USA scheidet aus.
- Nunmehr können Unternehmen auf das Nachfolgeabkommen namens Privacy Shield zurückgreifen.
- In Zukunft dürften zunehmend vertragliche Regelungen relevant werden.
- Ob eine langfristige Lösung realistisch ist, hängt von der Umsetzung des Urteils des Europäischen Gerichtshofs ab.

[1] BVerfG, NJW 1984, 419.

Auch wenn der bisherige „USA Patriot Act“ im Jahr 2015 durch den „USA Freedom Act“ ersetzt wurde und die Geheimdienste somit strengeren formellen Anforderungen unterliegen, bleibt abzuwarten, welcher praktische Umgang und welche datenschutzrechtlichen Entwicklungen in den USA Einzug halten werden. Daher ist es nötig, dass die Europäische Union sichere und transparente Regelungen im Hinblick auf den Datenaustausch mit den USA festschreibt. Als Rechtsgrundlagen fungieren hierbei die EU-Datenschutzrichtlinie sowie das Bundesdatenschutzgesetz und die jeweiligen Landesdatenschutzgesetze. Letztere wurden aufgrund der EU-Datenschutzrichtlinie in deutsches Recht umgesetzt.

2 Das Safe-Harbor-Abkommen der EU

Im Jahr 2000 entschied die europäische Kommission, dass in den USA ein angemessenes Schutzniveau für übermittelte personenbezogene Daten vorliege. Grundlage dieser Entscheidung war, dass die EU-Datenschutzrichtlinie eine Übermittlung solcher Daten in Drittstaaten zum Zweck der Datenverarbeitung nur in Ausnahmefällen vorsieht.

Hiernach dürfen z.B. weder die Zweckbestimmung der Datenverarbeitung noch Rechtsvorschriften oder ein unzureichendes Sicherheitsniveau in dem Empfängerland dem Schutz der Privatsphäre und den Freiheiten sowie Grundrechten des Datensubjekts zuwiderlaufen. Dieser gesetzliche Rahmen veranlasste das US-Handelsministerium „Grundsätze des sicheren Hafens zum Datenschutz“ (Grundsätze) aufzustellen sowie einen Fragen- und Antwortenkatalog (FAQ) zusammenzufassen, der die konkrete Umsetzung der o.g. Grundsätze behandelt.

Nach den Bestimmungen des Ministeriums konnten Organisationen, welche personenbezogene Daten aus der Europäischen Union für die Datenverarbeitung übermitteln wollten, den Grundsätzen beitreten. Somit sollte im Verhältnis von EU, USA und den datenverarbeitenden Stellen in den USA ein ausreichendes Schutzniveau gewährleistet werden.

Nach den Grundsätzen waren u.a. Informationspflichten, Weitergabe- und Sicherheitsbestimmungen sowie Auskunftsrechte der betroffenen Personen vorgesehen. Die Kommission stellte daraufhin fest, dass die Maßnahmen ausreichen würden, um die Rechte der europäischen Bürger – insbesondere das Recht auf informationelle Selbstbestimmung – zu gewährleisten.

3 Die Entscheidung des EuGH

In der Folgezeit legte der Österreicher Max Schrems bei der irischen Datenschutzaufsicht eine Beschwerde gegen die Tätigkeiten von Facebook ein. Nach den Enthüllungen von Edward Snowden kam er zu der Einsicht, dass die Übermittlung seiner personenbezogenen Daten in die USA durch Facebook unzulässig sei. Schließlich wären die Datensätze nicht ausreichend vor Einsichtnahmen der US-amerikanischen Behörden geschützt.

Nachdem die Datenschutzbehörde sein Ersuchen unter Bezugnahme auf das o.g. Safe-Harbor-Abkommen abwies, klagte Herr Schrems vor dem High Court in Irland gegen diese Entscheidung. Dieser legte dem Europäischen Gerichtshof die Frage vor, ob die Entscheidung der Europäischen Kommission aus dem Jahr 2000 einer eigenen Entscheidung der nationalen Aufsichtsbehörde entgegenstehe, d.h. ob es eine eigene Prüfungskompetenz gebe.

Der Europäische Gerichtshof legte in seinem anschließenden Urteil dar, dass die Kommissionsentscheidung nationale Kontrollbehörden nicht hindere, eine eigene Prüfung der Angemessenheit des Datenschutzniveaus in dem Drittstaat vorzunehmen. Vielmehr würden es die in Art. 7, 8 und 47 der EU-Grundrechtecharta statuierten Rechte auf Achtung des Privatlebens, Schutz der personenbezogenen Daten und des Anspruchs auf effektiven Rechtsschutz gebieten, dass die Mitgliedsstaaten eigenverantwortliche Überprüfungen vornehmen müssten. Gleichwohl bleibe nur der Gerichtshof befugt, über die Wirksamkeit des Unionrechtsakts – hier die Entscheidung der Europäischen Kommission – zu befinden.

In der Sache bemängelt der Gerichtshof, dass die Kommission bei ihrer Entscheidung nicht festgestellt habe, dass die Gesetze in den Vereinigten Staaten bzw. internationale Abkommen ein vergleichbares Datenschutzniveau sicherstellen würden. Weiterhin reiche es nicht aus, dass die Regelungen der Kommission nur Unternehmen, nicht aber öffentliche Stellen in den USA

erfassen. Eine Regelung, welche es zulasse, dass der Inhalt der elektronischen Kommunikation von den Behörden generell eingesehen werden kann, sei mit dem Wesensgehalt des Grundrechts auf Achtung der Privatsphäre unvereinbar.

Darüber hinaus stellt der Gerichtshof fest, dass die Eingriffsbefugnisse der öffentlichen Stellen in den USA sowie die mangelnden Rechtsschutzmöglichkeiten dem erforderlichen Schutzniveau für die Übermittlung der personenbezogenen Daten entgegenstehen würden. Das Safe-Harbor-Abkommen würde diese Probleme nicht ausräumen.

4 Folgen des Urteils

Als unmittelbare Folge des Urteilsspruchs hat die irische Datenschutzaufsicht angekündigt, dass die Beschwerde von Herrn Schrems gegen Facebook eingehend geprüft werde (Zeit-Online 2015).

Im Übrigen stellt sich zum jetzigen Zeitpunkt der Datenexport aus der Europäischen Union in die USA als höchst problematisch dar. Denn europäische Stellen, welche die Daten übermitteln wollen, können sich nun nicht mehr auf das Safe-Harbor-Abkommen berufen. Soweit in der Zwischenzeit ein neuer Regelungsmechanismus namens „Privacy Shield“ mit den USA eingesetzt wurde, bleiben erhebliche Zweifel an der Wirksamkeit dieser Regelung. Insbesondere werden wesentliche Vorgaben europäischen Datenschutzrechts nicht oder nur unzureichend beachtet (Bördíng 2016). Daher soll im Folgenden ein Fokus auf alternativen Instrumenten liegen.

Das Bundesdatenschutzgesetz sieht vor, dass eine Datenübermittlung insbesondere dann zu unterbleiben hat, wenn die datenverarbeitende Stelle kein angemessenes Schutzniveau gewährleisten kann. Hierbei müssen v.a. die Datenschutzvorschriften am Bestimmungsort berücksichtigt werden. Zwar wird nicht gefordert, dass das Schutzniveau deckungsgleich mit dem deutschen bzw. europäischen Standard ist (Gola, Klug & Körffer 2015: § 4b Rn. 12). Allerdings dürfen Grundprinzipien des hiesigen Datenschutzrechts nicht missachtet werden (ebd.). Insoweit dürfte der Annahme eines angemessenen Schutzniveaus in den USA schon entgegenstehen, dass dort kein einheitliches Datenschutzkonzept auf bundesstaatlicher Ebene existiert.

Ausnahmen werden u.a. zugelassen, wenn der Betroffene seine Einwilligung in die Übermittlung der Daten erteilt hat bzw. dies zur Erfüllung eines Vertrags oder zur Wahrung öffentlicher Interessen erforderlich ist. In Erweiterung dieser Ausnahmen, verbleibt der zuständigen Aufsichtsbehörde die Befugnis, den Datenexport gleichwohl zu genehmigen, wenn der Schutz des Persönlichkeitsrechts und die Ausübung der damit verbundenen Rechte garantiert werden.

5 Praktische Umsetzung

Ausgehend von den vorgenannten Ausnahmebestimmungen, erscheinen **drei Gestaltungsinstrumente** als praktikable Umsetzungslösungen für den Transfer von personenbezogenen Daten in die USA: die Einwilligung des Betroffenen, die Abgabe von Datenschutzgarantien und verbindliche Unternehmensrichtlinien.

a) Einwilligung

Im Einzelfall könnte die **Einwilligung** des Betroffenen zur Datenübermittlung eingeholt werden. Das Gesetz fordert hierzu eine freie, unzweifelhafte und konkrete vorherige Zustimmung. Die datenverarbeitende Stelle hat das Datensubjekt zudem über den Zweck, den Umfang und die Folgen des Datentransfers aufzuklären. Nötig ist, dass dem Betroffenen Risiken aufgrund der Übermittlung in ein Drittland ohne angemessenes Schutzniveau vor Augen geführt werden (Gola, Klug & Körffer 2015: § 4c Rn. 5).

b) Datenschutzgarantien

Als weitere Option kommt der **Abschluss eines Übermittlungsvertrags** in Frage (Deutlmoser & Filip 2015: Teil 16.6 Rn. 44). In diesem kann die übermittelnde Stelle mit dem Empfänger der Daten vereinbaren, dass wesentliche Grundgedanken der europäischen Datenschutzrichtlinie eingehalten werden (Gola, Klug &

Körffer 2015: § 4c Rn. 10). Im Regelfall findet ein Rückgriff auf die von der EU-Kommission erlassenen Standardvertragsklauseln statt (Gola, Klug & Körffer 2015: § 4b Rn. 16). In der Diskussion steht, ob die Übermittlungsverträge, so sie die Standardvertragsklauseln unverändert übernehmen, überhaupt der Genehmigung der Aufsichtsbehörde bedürfen. Entgegen dem scheinbar eindeutigen Gesetzeswortlaut, wird dies überwiegend abgelehnt (Deutlmoser & Filip 2015: Teil 16.6. Rn. 45). Interessant bleibt abzuwarten, ob die Behörden dieser Linie in Zukunft folgen werden.

Zudem wird die Ansicht vertreten, dass von der übermittelnden Stelle gegenüber der Aufsichtsbehörde der Nachweis zu erbringen sei, dass der Datenempfänger von den Behörden in den USA nicht zum Vertragsbruch – d.h. einem Verstoß gegen die eingeräumte Datenschutzgarantie – gezwungen werden dürfe. Ein fehlender oder untauglicher Nachweis stehe hiernach sonst einer Genehmigung des Datenexports entgegen (Deutlmoser & Filip 2015: Teil 16.6. Rn. 46).

c) Binding Corporate Rules

Schließlich können die Unternehmen sog. Binding Corporate Rules (BCR) erlassen. Diese verbindlichen Unternehmensrichtlinien müssen Garantien im Umgang mit den personenbezogenen Daten enthalten (Deutlmoser & Filip 2015: Teil 16.6. Rn. 47). Maßgeblich ist, dass ein angemessenes Schutzniveau innerhalb als auch außerhalb des Unternehmens gewährleistet wird (Deutlmoser & Filip 2015: Teil 16.6. Rn. 47). Gesetzliche Regelungen zum Umfang der Richtlinien existieren nicht. Gleichwohl sollten sich die Richtlinien an den gesetzlichen Bestimmungen auf nationaler und europäischer Ebene orientieren, um Rechtssicherheit zu garantieren. Hierbei können die o.g. Standardvertragsklauseln der Europäischen Kommission herangezogen werden (Gola, Klug & Körffer 2015: § 4c Rn. 15).

6 Reaktionen zum Urteil

Nachdem das Urteil des EuGH zum Safe-Harbor-Abkommen ergangen ist, haben sich verschiedene Stimmen zum weiteren Vorgehen in der Sache zu Wort gemeldet.

In Deutschland ist die Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein bemerkenswert. Nach dem Positionspapier (ULD 2015) sollen künftig keinerlei Übermittlungen in die USA zulässig sein, soweit hierüber keine völkerrechtliche Vereinbarung zwischen den USA, der EU bzw. den Nationalstaaten abgeschlossen wird. Dabei sei insbesondere die Einwilligung des Betroffenen nicht ausreichend, den Datenexport zu legitimieren, da das Individuum nicht über den Wesenskern des Grundrechts auf Achtung seiner Privatsphäre disponieren könne.

Diese Lösung trifft auf erhebliche Bedenken. Schließlich wird dem Datensubjekt hiermit jede Autonomie und Handlungsfreiheit über die personenbezogenen Daten von vorneherein abgesprochen. Zuzustimmen ist hingegen den Vorbehalten hinsichtlich der Wirksamkeit von Datenschutzgarantien oder dem Abschluss von verbindlichen Unternehmensrichtlinien. Denn der Bezugnahme hierauf könnte entgegenstehen, dass die datenempfangende Stelle in den USA durch die amerikanischen Behörden zum Vertragsbruch und damit zur Offenlegung der Daten gezwungen werden könnte. Insoweit würden die vertraglichen Regelungen ihre Zwecksetzung weitgehend verfehlen.

Im Übrigen sehen die Datenschutzbehörden des Bundes und der Länder die Übermittlung der Daten aufgrund von Datenschutzgarantien oder Unternehmensrichtlinien derzeit als nicht tragfähige Lösung an (Der Hessische Datenschutzbeauftragte 2015). Neue Genehmigungen würden auf diesen Grundlagen nicht mehr erteilt. Ob und wie mit bereits zuerkannten Genehmigungen zu verfahren sei, bleibt offen. Allerdings könne im Einzelfall und in engen Grenzen die Einwilligung des Betroffenen eingeholt werden.

Die sog. Art. 29-Datenschutzgruppe, welche im Auftrag der Europäischen Kommission Stellungnahmen zum Datenschutz erarbeitet, kommt zu recht vagen Schlussfolgerungen (Art. 29-Datenschutzgruppe 2015). Danach solle die Problematik der Datenübermittlung vorrangig politisch gelöst werden. Zugleich sollten nationale Aufsichtsbehörden vertragliche Regelungen weiterhin als taugliche Instrumente für Datenexporte in

Betracht ziehen. Schließlich sei ein entschiedenes Handeln der europäischen Behörden erforderlich, wenn bis zum Januar 2016 keine tragfähige Lösung erarbeitet worden ist.

Der Unternehmensverband BITKOM hat mittlerweile einen Leitfaden für Unternehmen veröffentlicht. In diesem wird die Feststellung getroffen, dass der Export personenbezogener Daten grundsätzlich auf Datenschutzgarantien gestützt werden solle, wobei die Standardvertragsklauseln der EU-Kommission zu verwenden seien. Zudem könne auf Einwilligungen der Betroffenen zurückgegriffen werden (BITKOM 2015).

7 Ausblick

Wie sich zeigt, herrscht eine erhebliche Unsicherheit im Umgang mit dem Urteil des Europäischen Gerichtshofs. Aufgrund dessen wird mit einer Klärung aller rechtlichen Fragen erst im Laufe der nachfolgenden Monate und Jahre zu rechnen sein. Insbesondere die Nachfolgevereinbarung zum Privacy Shield scheint nicht geeignet zu sein, die Unwägbarkeiten nachhaltig zu beseitigen (Börding 2016).

Eine weitere Problematik tut sich auf, soweit man die Bestrebungen zum Abschluss des Transatlantischen Freihandelsabkommens (TTIP) zwischen der Europäischen Union und den Vereinigten Staaten berücksichtigt (Schnarrenberger 2015). Das Abkommen soll zu Erleichterungen des gemeinsamen Handels führen; somit könnte auch der Austausch von personenbezogenen Daten hierunter fallen. Da Handelsbarrieren beseitigt, nicht aber zusätzliche aufgebaut werden sollen, dürfte die politische und wirtschaftliche Bereitschaft der amerikanischen Administration zum Erlass zusätzlicher Datenschutzvorschriften gering sein.

Ein gemeinsames europäisches Handeln ist hierbei zwingend anzuraten. Denkbar ist schließlich, dass die nationalen Aufsichtsbehörden aufgrund der Vielzahl an Vertragsabreden verschiedene Lösungsansätze im Umgang mit diesen entwickeln werden. Dabei erfordert die Harmonisierung des Datenschutzniveaus in der Europäischen Union, dass gemeinsame Standards festgelegt und eingehalten werden. Es gilt zu vermeiden, dass die Frage der Einhaltung des Datenschutzniveaus im Wesentlichen von der Handhabe der jeweiligen Mitgliedstaaten abhängt. Zugleich würde es einen großen Fortschritt bedeuten, wenn die Vereinigten Staaten eine Nivellierung des Datenschutzrechts hin zu mehr Rechtsschutzmöglichkeiten und Selbstkontrolle vornähmen.

Auch im Hinblick auf die Datenschutzgrundverordnung entfällt der Regulierungsbedarf nicht. Hiernach soll wiederum auf die Angemessenheit des Datenschutzniveaus in dem Drittstaat abgestellt werden. Zugleich sind vertragliche Vereinbarungen und Garantien zur Einhaltung von Datenschutzstandards wie auch die Einholung der Einwilligung des Betroffenen möglich.

All diese Überlegungen zeigen: wer sich vor Datenmissbrauch schützen möchte, sollte von vorneherein jede Datenweitergabe an Dritte sorgfältig überdenken.

Literaturnachweise

Jolly, I. (2015). Data Protection in United States: Overview. Online verfügbar unter: http://uk.practicallaw.com/6-502-0467.

Böhm, F. (2015). A comparison between US and EU Data Protection Legislation for Law Enforcement: Study for the LIBE Committee.

Börding, A. (2016). Ein neues Datenschutzschild für Europa – Warum auch das überarbeitete Privacy Shield den Vorgaben des Safe Harbor-Urteils des EuGH nicht gerecht werden kann. *Computer und Recht*, *431-441*.

Electronic Frontier Foundation (2015). Who Has Your Back? : Protecting your data from Government. Online verfügbar unter: https://www.eff.org/who-has-your-back-government-data-requests-2015#results-summary.

ZEIT-Online (2015). Irisches Gericht ordnet Ermittlungen gegen Facebook an. Online verfügbar unter: http://www.zeit.de/digital/datenschutz/2015-10/safe-harbor-facebook-irland-ermittlungen.

Gola, P. , Klug, C. & Körffer, B. (2015). Kommentar zum Bundesdatenschutzgesetz (Hrsg. Gola, P.& Schomerus, R.). München: C.H. Beck.

Deutlmoser, R. & Filip, A (2015). Hoeren, T./Sieber, U./Holznagel, B. (2015). *Handbuch Multimedia-Recht*. München: C.H. Beck

Unabhängiges Landeszentrum für Datenschutz (2015). Positionspapier des ULD zum Safe-Harbor-Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14. Online verfügbar unter: https://www.datenschutzzentrum.de/artikel/967-Positionspapier-des-ULD-zum-Safe-Harbor-Urteil-des-Gerichtshofs-der-Europaeischen-Union-vom-6.-Oktober-2015,-C-36214.html.

Der Hessische Datenschutzbeauftragte (2015). Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen: Datenschutz-Richtlinie im Bereich von Justiz und Inneres. Online verfügbar unter: https://www.datenschutz.hessen.de/ft-europa.htm.

Art. 29-Datenschutzgruppe (2015). Statement of the Article 29 Working Party. Online verfügbar unter: http://www.cnil.fr/fileadmin/documents/Communications/20151016_wp29_statement_on_schrems_judgement.pdf.

BITKOM (2015). Das Safe-Harbor-Urteil des EuGH und die Folgen: Fragen und Antworten. Online verfügbar unter: https://www.bitkom.org/Publikationen/2015/Leitfaden/Das-Safe-Harbor-Urteil-des-EuGH-und-die-Folgen/151110_SafeHarbour_FAQ.pdf.

Schnarrenberger, N. (2015). Wann kommt ein „sicherer Hafen" für TTIP: Die Folgen der EuGH-Entscheidung. Online verfügbar unter: https://netzpolitik.org/2015/wann-kommt-ein-sichererer-hafen-fuer-ttip-die-folgen-der-eugh-entscheidung/.

ABIDA (Assessing Big Data)
Über die Dossiers

Das Projekt ABIDA, gefördert vom Bundesministerium für Bildung und Forschung, lotet gesellschaftliche Chancen und Risiken der Erzeugung, Verknüpfung und Auswertung großer Datenmengen aus und entwirft Handlungsoptionen für Politik, Forschung und Entwicklung. Dabei nähert ABIDA sich dem Thema Big Data aus einer grundlegend interdisziplinären Perspektive. Mehr Informationen finden Sie auf www.abida.de.

In den ABIDA-Dossiers werden regelmäßig ausgewählte Big Data-Themen kurz und prägnant dargestellt, um dem Leser einen Überblick zu liefern und einen Einstieg in die Thematik zu ermöglichen. Weitere Dossiers sind verfügbar unter www.abida.de/content/dossiers.