KELLENERS + ALBERT
RECHTS- UND FACHANWÄLTE

Datenschutzabkommen „Safe Harbor“ zwischen EU und USA vom EuGH für ungültig erklärt – Was bedeutet das für Unternehmen in Deutschland?

Das am 06.10.2015 vom Europäischen Gerichtshof – EuGH – verkündete Urteil in der Rechtssache C-362/14 M. Schrems gegen den irischen Datenschutzbeauftragten wegen Facebook zur Ungültigkeit des Safe Harbor-Abkommens hat große Medienaufmerksamkeit gefunden und wurde als Sieg des europäischen Datenschutzrechts gefeiert. Doch gibt es etwas zu feiern? Um das zu verstehen muss man einige datenschutzrechtliche Grundbegriffe kennen und wissen, was das Safe Harbor Abkommen bedeutet hat.

1. Grundbegriffe – Datenschutzrecht, Datenverarbeitung und Drittländer

a) Datenschutzrecht

Das Datenschutzrecht ist auf europäischer Ebene durch die **EU-Datenschutzrichtlinie** von 1995 geregelt, die alle EU-Staaten in ihr nationales Recht umgesetzt haben müssen. Daher wird davon ausgegangen, dass in allen EU-Staaten zumindest im Grundsatz ein gleicher, angemessener **Mindeststandard** an Datenschutzrechten besteht.

Die Datenschutzrichtlinie stammt von 1995 und gibt nicht mehr angemessene Antworten auf die heutigen Formen der Datenverarbeitung, insbesondere auch durch Internetangebot wie Social Media Plattformen (z.B. Facebook). Zudem hat sich gezeigt, dass der erhoffte EU-weite einheitliche Mindeststandard doch in der Praxis recht unterschiedlich ausfällt. Dies beeinträchtigt den freien Waren- und Dienstleistungsverkehr in der EU. Aus diesen Gründen finden sich aktuell die Verhandlungen zu einem neuen EU-Datenschutzrecht, der sogenannten **EU-Datenschutzgrundverordnung,** die dann als Verordnung ohne unterschiedliche nationale Umsetzung direkt in allen EU-Staaten unmittelbar geltendes Recht ist, in der Schlussphase. Links zum Text und Hintergrundinformationen sind auf der Webseite des Berichterstatters (Verhandlungsführers) im Europäischen Parlament und EU-Parlamentsabgeordneten Jan Philipp Albrecht zu finden.

Seit 01.12.2009 schützt die **Grundrechtscharta der EU** Pdf-Fassung im Amtsblatt der EU und Html-Fassung in allen Amtssprachen ausdrücklich auch das **Grundrecht auf Datenschutz** (Grundrechte: Recht auf Schutz personenbezogener Daten (Art. 8) und Recht auf Achtung des Privatlebens (Art. 7))

> ***Artikel 7 – Achtung des Privat- und Familienlebens***
>
> *Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.*

Artikel 8 – Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

In Deutschland ist das Datenschutzrecht im **Bundesdatenschutzgesetz** (BDSG), in den Landesdatenschutzgesetzen und für bestimmte Themen auch noch in speziellen Gesetzen geregelt, z.B. im Telemediengesetz (TMG), im Telekommunikationsgesetz (TKG), im Kreditwesengesetz (KWG), Sozialrecht (SGB) oder in den Landeskrankenhausgesetzen, um nur einige Spezialgesetze zu nennen.

Das Bundesverfassungsgericht hat im Volkszählungsurteil 1983[1] aus der Menschenwürde und dem allgemeinen Persönlichkeitsrecht ein **Grundrecht auf informationelle Selbstbestimmung** entwickelt. In der Entscheidung zur Online-Durchsuchung hat das Bundesverfassungsgericht 2008 ein **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**[2], auch IT-Grundrecht genannt, entwickelt.

Das Datenschutzrecht regelt die Verarbeitung von **Daten natürlicher Personen** – im Gegensatz zu juristischen Personen (z.B. GmbH, AG). Daten juristischer Personen sind nicht schutzlos; deren Schutz ist z.B. im Gesetz gegen unlauteren Wettbewerb (UWG) in Form des Schutzes von Betriebs- und Geschäftsgeheimnissen und durch das von der Rechtsprechung entwickelte allgemeine Persönlichkeitsrecht des Unternehmens bzw. des Unternehmers.

b) Datenverarbeitung

Jegliche Daten bzw. Informationen über eine natürliche Person, mögen sie auch noch so vermeidlich belanglos erscheinen, dürfen nur dann erhoben, verarbeitet oder genutzt werden, wenn entweder die betroffene Person selbst dies erlaubt hat (Erlaubnis, die man vorab erteilt, nennt man **Einwilligung**) oder ein Gesetz dies erlaubt oder angeordnet hat. Liegt keine Einwilligung oder **gesetzliche Erlaubnis** vor, ist die Datenverarbeitung verboten, sogenanntes **Verbot mit Erlaubnisvorbehalt**.

Der Begriff des **Verarbeitens** ist im Datenschutzrecht sehr viel weiter gefasst, als im allgemeinen Sprachverständnis. Die EU-Datenschutzrichtlinie definiert den Begriff folgendermaßen:

*Art. 2 b) "**Verarbeitung personenbezogener Daten**" ("Verarbeitung") jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;*

Im Bundesdatenschutzgesetz, § 3 Abs. 4 BDSG, ist "Verarbeiten" wie folgt definiert:

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. ***Speichern** das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,*
2. *Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,*
3. ***Übermitteln** das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass*
4. *a) die Daten an den Dritten **weitergegeben** werden oder*
5. *b) der **Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten** einsieht oder abruft,*
6. ***Sperren** das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,*
7. ***Löschen** das Unkenntlichmachen gespeicherter personenbezogener Daten.*

Hervorheben möchte ich hier zwei Aspekte:

Speicher – schon das bloße Speichern von Daten auf einem Server, **Hosting**, z.B. in Form der Nutzung eines **Cloud-Anbieters** wie DropBox, iCloud, Amazon-Cloud etc. stellt eine Datenverarbeitung dar, die unter das Datenschutzrecht fällt, und zwar ohne, dass es hierbei auf irgendwelche Arten von Bearbeitung der Daten ankäme.

Übermitteln – Auch wenn die Daten dabei nicht verändert werden, ist das Übermitteln der Daten eine Datenverarbeitung im Rechtssinne. Das für den ein oder anderen vielleicht überraschende ist, dass die Daten auch wenn sie an Ort und Stelle auf dem eigenen Server bleiben, dennoch z.B. im Rahmen eines **Fernwartungszuganges** (Remote Access) an den IT-Dienstleister durch die Einsichtnahmemöglichkeit übermittelt werden.

c) Drittländer

Im Datenschutzrecht sind oft **zwei Prüfungsschritte** zu machen:

1. Dürfen die Daten überhaupt verarbeitet werden, liegt also eine Einwilligung der betroffenen Person, deren Daten verarbeitet werden sollen, vor, oder gibt es eine gesetzliche Erlaubnis, auf die man als Verarbeiter die Verarbeitung stützen kann.
2. Wenn diese Frage mit ja beantwortet ist, stellt sich in einem zweiten Prüfungsschritt die Frage, dürfen die Daten in dem Land verarbeitet werden, in dem das für die Daten verantwortliche Unternehmen (z.B. der Arbeitgeber die Beschäftigtendaten oder der Händler die Kundendaten) die Daten verarbeiten lassen will.

In der EU geht man wie dargelegt von einem einheitlichen Mindestdatenschutzstandard aus, so dass innerhalb der EU das Verarbeitungsland frei gewählt werden kann. Bei Ländern außerhalb der EU, sogenannte **Drittstaaten** bzw. **Drittländer**, wird grundsätzlich erst einmal davon ausgegangen, dass dort kein angemessenes Datenschutzniveau besteht. Dann ist die Datenübermittlung nur in bestimmten Fällen zulässig, z.B. wenn der Betroffene seine Einwilligung gegeben hat, § 4c Abs. 1 Nr. BDSG oder die Übermittlung zur Erfüllung des Vertrages mit dem Betroffenen erforderlich ist.

Ob ein **angemessenes Datenschutzniveau** besteht, ist nach § 4b Abs. 3 BDSG „unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland**, die für den betreffenden Empfänger geltenden Rechtsnormen** sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen

Zwar ist jedes übermittelnde Stelle (jedes Unternehmen) selbst für diese Beurteilung verantwortlich, § 4b Abs. 5 BDSG; jedoch sind die wenigsten dazu selbst in der Lage. Daher hat die **EU-Kommission** diese Prüfung für einige Staaten selbst vorgenommen und einzelne wenige Staaten als „**sichere Drittstaaten**“

d) USA als sicherer Datenhafen – Safe Harbor

Da die USA eines der Hauptdrehkreuze des Internet-Datenverkehrs sind und die wesentlichen Betriebssysteme, größten Softwareunternehmen und bedeutendsten Internet-Anbieter aus den USA komme, besteht ein überragendes Bedürfnis, den Datenverkehr der EU-Staaten mit den USA zu regeln. Die EU-Kommission hat hierzu mit dem US-Handelsministerium 2000 ein Abkommen über ein Verfahren zum – aus EU-Sicht – angemessenen Datenschutzstandard abgeschlossen – die Entscheidung der EU-Kommission wird **Safe Harbor** genannt.

Das Safe Harbor Verfahren sah vor, dass sich Unternehmen in den USA auf die Einhaltung eines definierten Datenschutzstandards selbst verpflichten konnte und diese Selbstverpflichtungserklärung an eine Liste im US-Handelsministerium gemeldet haben. Bei den Safe Harbor-Zertifizierten Unternehmen wurde dann davon ausgegangen, dass ein angemessener Schutz für Daten von EU-Bürgern besteht.

Bis Mitte Oktober 2015 waren etwa **5484 amerikanische Unternehmen** dem Safe-Harbor-Abkommen beigetreten, darunter IBM, Microsoft, General Motors, Amazon.com, Google, Apple , Hewlett-Packard, Dropbox und Facebook. Andererseits waren alle wichtigen Unternehmen, die am NSA-Programm PRISM beteiligt waren, auch Safe Harbor zertifiziert. Die **Safe Harbor Unternehmens-Liste** wird auch nach der Entscheidung des EuGH vom US-Handelsministerium weiter gepflegt.

Aus meiner Sicht war schon die Bezeichnung für dieses Verfahren „**Safe Harbor-Zertifiziert**“ irreführend, da man bei einer Zertifizierung üblicherweise von einer regemäßigen und neutralen Überprüfung und Bestätigung der Einhaltung bestimmter Regeln und Standards versteht. Es fand aber weder eine anfänglich noch eine regelmäßige unabhängige Überprüfung oder Sanktion bei Verstößen statt.

e) Folgen und Sanktionen bei Datenschutzverstößen

Werden personenbezogene Daten nicht rechtskonform verarbeitet, also z.B. ohne Rechtsgrundlage in Drittstaaten übermittelt, gibt es verschiedene potentielle (Rechts-)Folgen, die so empfindlich für Unternehmen sein können, dass man das Datenschutzrecht und etwaige Verstöße dagegen nicht auf die leichte Schulter nehmen sollte.

Die Datenschutzbehörden haben in den letzten Jahren ebenso wie die Medien entdeckt, dass die Berichterstattung über Datenschutzverstöße eine teilweise erhebliche Auswirkung haben (**Image-Schaden**), bis hin zum Rücktritt von Unternehmensvorständen. Instrumente sind hierbei **Pressemitteilungen** oder auch die **Tätigkeitberichte** der Datenschutzaufsichtsbehörden.

Neben der Möglichkeit **Auskünfte** zu verlangen, detaillierte **Kontrollen** und **Prüfungen** vorzunehmen, kann eine bestimmte Datenverarbeitung untersagt werden (Untersagungsverfügung), also **die IT stillgelegt werden**, vgl. § 38 BDSG. Zudem kommen insbesondere Bußgelder wegen Ordnungswidrigkeiten in Betracht, § 43 BDSG. Bei formellen Verstößen können **Bußgelder** bis zu 50.000 Euro und bei materiellen Verstößen bis zu **300.000 Euro** verhängt werden, wobei auch die Möglichkeit besteht **einen höheren Gewinn** aus der Datenschutzverletzung durch ein noch höheres Bußgeld **abzuschöpfen**. Vorsätzliche Datenschutzverstöße können sogar als Straftat mit **Freiheitstraße oder Geldstrafe** geahndet werden, § 44 BDSG. Man könnte sogar überlegen, ob die Datenübermittlung in die USA bei besonders sensiblen Daten nach § 42a BDSG eine unrechtmäßige Kenntnisnahme durch unberechtigte Dritte darstellt und eine Meldepflicht an die Aufsicht und die Betroffenen auslöst.

[1] BVerfG, Urteil vom 15.12.1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1.

[2] BVerfG, Urteil vom 27.02,2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 – 350.

2. Die Safe Harbor Entscheidung des EuGH

a) Sachverhalt

Hintergrund der Entscheidung ist die Facebook-Nutzung durch einen österreichischen Juristen Maximillian Schrems, der sich bei der **irischen Datenschutzaufsicht**, dem Sitzland von Facebook Europa, darüber beschwert hatte, dass **Facebook Irland** seine **Daten an Facebook USA weiterleitet** und dort speichert. Es war übrigens die 23ste Beschwerde, weshalb die irische Aufsicht diese auch als „frivoles and vexatious" bezeichnet hat und sich nicht mehr damit befassen wollte. Ziel der Beschwerde war es, Facebook Irland die Datenübermittlung in die USA zu untersagen. Der irische Datenschutzschutzbeauftragte hatte es abgelehnt, sich damit zu beschäftigen, weil sich Facebook auf die Entscheidung der EU-Kommission zu Safe Harbor stützt und diese Entscheidung für die irische Datenschutzaufsicht bindend sei. Herr Schrems erhob daraufhin Klage von dem **High Court in Irland**. Dieses stellte fest, dass die **NSA und das FBI** massenhaft und undifferenziert Zugriff auf personenbezogene Daten nehmen und dies dem Grundsatz der Verhältnismäßigkeit und den durch die irischen Verfassung geschützten Grundrechten widerspricht. Da Herr Schrems mit seiner Klage de facto die Rechtmäßigkeit des Safe Harbor Regelung in Frage stellt, setzte der High Court das Verfahren aus und legte dem EuGH die Frage vor, ob der irische Datenschutzbeauftragte absolut an die Entscheidung zu Safe Harbor der EU-Kommission gebunden ist oder aufgrund der seit der Entscheidung bekannt gewordenen Umstände eigene Ermittlungen anstellen kann bzw. muss.

b) Entscheidung des EuGH

Das Gericht stellt fest, dass die Safe-Harbor-Entscheidung der EU-Kommission solange bindend ist für die Mitgliedsstaaten der EU und ihre Organe einschließlich der Datenschutzaufsichtsbehörden, bis die Entscheidung vom EuGH für ungültig erklärt wurde. Einem nationalen Gericht, wie dem High Court in Irland, steht diese Befugnis nicht zu. Gleichwohl hätte die irische Datenschutzaufsicht die Beschwerde von Herrn Schrems zumindest mit der gebotenen Sorgfalt prüfen müssen.

Der EuGH erklärte dann die Regelungen zu Safe Harbor für ungültig.

c) Entscheidungsgründe

Zwar hat die EU-Kommission keine Befugnis im Bezug auf die Verarbeitung von personenbezogenen Daten in einem Drittland. Jedoch stellt die Übermittlung von Daten in ein Drittland (also das „Abschicken") noch eine Datenverarbeitung („Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung") in einem Hoheitsgebiet eines EU-Staates dar. Anerkannt wird die Notwendigkeit von Datenübermittlung für die Entwicklung des internationalen Handels. Voraussetzung für die Zulässigkeit ist jedoch ein angemessenes Schutzniveau. **Besteht kein angemessenes Schutzniveau, dann ist die Datenübermittlung in Drittstaaten zu untersagen**.

Unter "**angemessenem Schutzniveau**" ist nicht das identische Schutzniveau zu verstehen, sondern ein gleichwertiges. Dazu muss das nationale Recht und dessen Praxis im Zielland beurteilt werden und zwar regelmäßig, um etwaige Änderungen feststellen zu können. Der Bewertungsspielraum, den die Kommission dabei hat, ist durch die Grundrechte der EU-Grundrechtscharata eingeschränkt.

Zwar stellt der EuGH das **System der Selbstzertifizierung** der US-Unternehmen für Safe Harbor nicht grundsätzlich in Frage, fordert jedoch wirksame Überwachungs- und Kontrollmechanismen zur Gewährleistung des Grundrechtsschutzes sowie Sanktionsmechanismen bei Verstößen. An diesen Mechanismen fehlt es jedoch im US-Recht.

Zudem können die Datenschutzgrundsätze eingeschränkt werden, soweit es die **nationale Sicherheit der USA** erfordert. Die US-Gesetze zur nationalen Sicherheit haben Vorrang vor den Datenschutzgrundsätzen für Safe Harbor. Diese Regelung ermöglicht einen Eingriff in Grundrechte europäischer Bürger, deren Daten in die USA übermittelt werden. Die Safe Harbor Entscheidung der Kommission enthält keine Feststellung, wie etwaige **Eingriffe begrenzt** werden oder ob **ein wirksamer gerichtlicher Rechtsschutz** gegen derartige Eingriffe besteht. Die Kommission hat selbst festgestellt, dass US-Behörden auf die Daten der Europäer im einem Ausmaß zugreifen, das über die Bedürfnisse der nationale Sicherheit hinausgehen und noch verhältnismäßig wären. Zudem gebe es keine Rechtsbehelfe dagegen und auch keine Möglichkeit, die Berichtigung oder Löschung von Daten zu verlangen. Die US-Regelungen stellen also Grundrechtseingriffe dar, die nicht auf das absolut notwendige Maß begrenzt sind. Insbesondere verletzt die generelle Befugnis, auf Inhalte der elektronischen Kommunikation zuzugreifen, den Wesensgehalt des durch die Grundrechtscharta garantierten Rechts auf Achtung des Privatlebens.

Schließlich hat die EU-Kommission bei Erlass der Entscheidung zu Safe Harbor ihre **Zuständigkeiten überschritten**, indem sie den Datenschutzaufsichtsbehörden die Möglichkeit nimmt, Maßnahmen zum Datenschutz zu ergreifen. Auch dies führt zur Ungültigkeit der Entscheidung zu Safe Harbor.

d) Fortgang vor dem Irish High Court

Der Irish High Court nach dem EuGH Urteil am 20.10.2015 entschieden, dass der irische Datenschutzbeauftragte die Beschwerde von Herrn Schrems prüfen muss.

3. Die Auswirkungen der Safe Harbor Entscheidung

In der Einleitung zu seinen Schlussanträge vor der Entscheidung des EuGH führt der **Generalanwalt** Bot am 23.09.2015 aus:

Siehe zu den Schlussanträgen des Generalanwalts Bot in der Rechtssache C-362/14 Maximilian Schrems / Data Protection Commissioner v. 23.09.2015

1. Wie die Europäische Kommission in ihrer Mitteilung vom 27. November 2013(2) festgestellt hat, stellt „[d]ie **Übermittlung personenbezogener Daten … einen wichtigen und notwendigen Aspekt der transatlantischen Beziehungen dar. Sie ist integraler Bestandteil der transatlantischen Handelsbeziehungen, auch für neu entstehende digitale Geschäftsbereiche wie soziale Medien oder Cloud-Computing**, für die große Datenmengen von der EU in die USA fließen."(3)

In der Konsequenz des Urteils wird aber gerade diese Datenübermittlung grundlegend in Frage gestellt.

a) Handlungsbedarf – Prüfungsphase

Die EuGH Entscheidung stellt für **alle Unternehmen, ob KMU oder Großkonzerne**, erhebliche Herausforderungen im Bereich der **Datenschutz-Compliance** dar. Zwar hat der EuGH seine Entscheidung keine „Aufbrauchsfrist" genannt und die Safe Harbor Entscheidungen der EU Kommission ist mit Verkündung des Urteils **ab sofort unwirksam** geworden. Ab Verkündung und Veröffentlichung des EuGH-Urteils lässt sich also keine Datenübermittlung in die USA mehr auf sie stützen. Darin sind sich alle Datenschutzaufsichtsbehörden, auf EU-Ebene und national, einig. Erfolgte dennoch eine Datenübertragung, so ist diese, sofern nicht andere Rechtfertigungsgründe vorliegen, rechtswidrig mit den eingangs dargestellten Rechtsfolgen. Dies ist jedoch kein Grund in hektischen Aktionismus oder Panik zu verfallen oder gar jegliche Datenverarbeitung einzustellen. Vielmehr ist es angeraten, interne Projekte zur Überprüfung der eigenen Datenverarbeitung aufzusetzen. Es muss zunächst zweierlei im Hinblick auf den Sachverhalt geprüft werden – ist man überhaupt vom Urteil betroffen und wenn ja wie und inwieweit.

Check-Liste

1. **Erfolgt eine Übermittlung personenbezogener Daten in die USA?**

   Hierbei ist zu beachten, dass die Datenübermittlung, wie eingangs dargestellt, bei beauftragten Dienstleistern und auch in Form des Zugriffs bei Fernwartung erfolgen kann. Hierzu ist jede Software, jeder Wartungsvertrag von Software, jede Cloud-Anwendung, jeder Outsourcing Partner und Sub-Unternehmer gesondert zu betrachten und zwar in technischer und rechtlicher bzw. vertraglicher Hinsicht.

2. **Wird diese Datenübermittlung (die eigene oder die der beauftragten Dienstleister) in die USA auf Safe Harbor gestützt?**

Mit diesen beiden Fragen wird das Aufgabenfeld für die nächsten Monate abgesteckt.

1. **Wird eine Datenübermittlung in die USA nicht auf Safe Harbor gestützt, so ist zu prüfen, auf welche andere Rechtsgrundlage die Datenübermittlung gestützt wird**, zum Beispiel EU Standardvertragsklauseln, Binding Corporate Rules oder Einwilligungen. Ist keine Rechtsgrundlage gegeben, so ist diese zu schaffen oder die Datenverarbeitung bzw. -übermittlung einzustellen. Ist eine der Rechtsgrundlagen gegeben, so ist zu prüfen, ob dieser dauerhaft tragfähig ist oder bereits vorsorglich mit der Suche nach Alternativen begonnen werden sollte.
2. **Wird eine Datenübermittlung auf Safe Habor gestützt, ist mit der Suche nach einer alternativen rechtlichen oder technischen Lösung zu beginnen.** Streng juristisch betrachtet wäre die Datenübermittlung sofort einzustellen. Auf eine vermeintliche Schonfrist bis Ende Januar 2016 kann man sich nur eingeschränkt verlassen.

Die Entscheidung hat auch Auswirkungen auf

- beliebte Online-Marketing-Angebote
- Web-Analytic-Diensten
- E-Mail-Marketing-Tool, Newsletterversand-PlugIns
- Cloud-Computing Diensten,
- Reisebüro,
- Außendienstmitarbeiter mit eigenem SmartPhone – bring your own device , BYOD,
- Krankenkassen-Apps
- Google-Dienste
- Amazon Hosting
- Oracle Datenbanken, insb. Fernwartung
- Office 365
- Online-Bilddatenbanken
- Software für Webinare
- Software für Videokonferenzen etc.

Aufkunftsverlangen

Betroffene Personen können grundsätzlich von den datenspeichernden Unternehmen Auskunft über die zu ihrer Person gespeicherten Daten, deren Herkunft und Verwendung verlangen, § 34 BDSG. Nach einem Musterbrief der Verbraucherschutzzentrale in NRW wird auch nach dem Ort der Datenspeicherung gefragt. Erste Unternehmen sind bereits kurz nach Bekanntwerden der Safe Harbor-Entscheidung mit einem derartigen Auskunftsverlangen konfrontiert worden. Es ist jedoch keine Rechtsgrundlage für diese Auskunft ersichtlich.

E-Discovery-Verfahren

Ein weiteres Problemfeld sind Offenlegungspflichten im Rahmen von torprozessualen Beweiserhebungen bei Zivilprozessen (Pre-Trail-Discovery), insbesondere die Offenlegung von E-Mails von Beschäftigten aus der EU vor US-Gerichten (E-Discovery). Hierzu hat die Art. 29 Datenschutzgruppe eine 2009 Arbeitsunterlage vorgelegt, in der u.a. Safe Harbor und EU-Standardvertragsklauseln zur Absicherung dieser Datenübermittlung vorgeschlagen wurden. Zumindest Safe Harbor fällt als Rechtsgrundlage definitiv weg. Gerade in den Fällen, in denen Unternehmen aus der EU ihre Ansprüche vor US-Gerichten vertreten müssen, stehen oft erhebliche Summen auf dem Spiel, so dass ein erhebliches und berechtigtes Bedürfnis besteht, in rechtssicherer Weise die hierzu nach US-Recht erforderlichen Beweise vorlegen zu dürfen, auch wenn dies eine Übermittlung personenbezogener Daten aus der EU erfordert.

b) Erste Reaktionen der Datenschutzaufsichtsbehörden

b.1. Hamburg

Der Hamburgische Beauftragte für Datenschutz ließ noch am Tag der Urteilsverkündung verlauten: "*Bei der Umsetzung dieser Entscheidung werden die nationalen und europäischen Datenschutzbehörden künftig eine Schlüsselrolle einnehmen.*" Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Johannes Caspar, wird mit den Worten zitiert: „Dies ist eine historische Entscheidung im Sinne unserer europäischen Werteordnung. Sie markiert einen Wendepunkt im Datenverkehr zwischen der EU und den USA." (PM vom 06.10.2015). Praktisch bedeutet das: „Es ist zu prüfen, ob und inwieweit **Datentransfers in die USA auszusetzen** sind. Dies gilt auch, wenn sie auf andere Rechtsgrundlagen wie Standardvertragsklauseln, Einwilligung oder Binding Corporate Rules gestützt werden."

Am 5.11.2015 hat die Datenschutzaufsicht in Hamburg ein dreistufiges Vorgehen angekündigt.

1. Zunächst wird sie Unternehmen über die EuGH-Entscheidung im November informieren.
2. Im Dezember und Januar wird sie Auskunftsersuchen an die Unternehmen richten, um festzustellen, ob diese noch unter den Safe Harbor-Grundsätzen Daten in die USA übermitteln.
3. Für die dritte Phase ab Februar 2016 hat sie **Untersagungsverfügungen und Bußgelder** denjenigen angedroht, die dann immer noch auf der Grundlage vor für ungültig erklärten Safe Harbor Grundsätze Daten in die USA übermitteln.

b.2. Schleswig-Holstein

In Schleswig-Holstein hat die dortige Datenschutzaufsichtsbehörde, das unabhängige Landeszentrum für Datenschutz, kurz **ULD**, eine Pressemitteilung am 14.10.2015 herausgegeben. Das Positionspapier des ULD kann online abgerufen werden.

Einwilligung

Eine der Kernaussagen ist, dass das ULD sogar **die Einwilligung der Betroffenen** an die Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau **für unzulässig** hält, da die Betroffenen nicht in eine Verletzung des „Wesensgehalts" ihres Datenschutzgrundrechts einwilligen können. Das ULD will also die Betroffenen vor den Konsequenzen ihrer eigenen Entscheidung schützen.

Ich halte diesen weitgehenden Schutz vor sich selbst für zu weitgehend. Mir ist ein derartiger Schutz nur in so extremen Fällen wie „**Zwergenweitwurf**" (VG Neustadt (Weinstraße), Entscheidung vom 21. Mai 1992, Aktenzeichen: 7 L 1271/92.NW, Fundstelle: GewArch 1992, 296–297 oder NVwZ 1993, 98–100) und „**Peepshow**" bekannt. Die Datenübermittlung in die USA halte ich damit aber nicht für vergleichbar, auch in Kenntnis der NSA-Affäre nicht. Außerdem sieht gerade § 4c Abs. 1 BDSG die Einwilligung des Betroffenen für den Fall vor, dass eben kein angemessenes Datenschutzniveau im Drittland besteht. Die freie Entscheidung über eine Einwilligung gehört ihrerseits zu den Grundrechten (vgl. BAG, Az. 8 AZR 1010/13 Rn 32), die das ULD mit seiner Auffassung unzulässig einschränken will.

Datenübermittlung zur Vertragserfüllung

Das ULD hält im Wesentlichen nur die Datenübermittlung zur Erfüllung eines Vertrages mit dem Betroffenen für zulässig. Als Beispiel führt das ULD **Reise- und Flugbuchungen** an. Ergänzen muss man auch noch zahllose andere Fälle mit vertraglichem US-Bezug, z.B. Bestellung englischer Fachliteratur aus den USA, **Überweisung in die USA** oder **Wertpapierorder an den New Yorker Börse**. Unzulässig sei hingegen die Datenübermittlung von **Beschäftigtendaten** zur Leistungs- oder Verhaltenskontrolle – ein Punkt der gerade EU-Tochtergesellschaften von US-Konzernmüttern mit zentraler Personalabteilung in den USA vor erhebliche Probleme stellen dürfte.

EU-Standardvertragsklausel

Das ULD vertritt folgerichtig die Auffassung, dass die US-Unternehmen, die mit den Standardvertragsklauseln verbundenen Pflichten aufgrund des US-Rechts nicht erfüllen können. Praktische Konsequenz laut ULD: die **deutschen Unternehmen sollen ihre Datenübermittlung in die USA auf der Grundlage von Standard-Vertragsklausel sofort aussetzen** oder noch besser sogar den **Vertrag kündigen**.

Handeln die Unternehmen nicht selbst, so kündigt das ULD an, die Datenübermittlung in die USA per verwaltungsrechtlicher Anordnung zu verbieten. Es liefert auch gleich die Argumentation mit – denn noch sind die EU-Standardvertragsklauseln nicht für ungültig erklärt worden und die dahingehende Kommissionsentscheidung ist noch wirksam. Das ULD meint, dass sich die US-Unternehmen nicht an ihre Pflichten nach den Standardvertragsklauseln halten können und daher der Datenübermittlung

die Rechtsgrundlage entzogen ist. Das ULD weißt auf dem **Bußgeldrahmen bis 300.000 Euro** hin und droht an Ordnungswidrigkeiten entsprechend zu ahnden.

b.3) EU – Artikel 29 Arbeitsgruppe

Auf europäischer Ebene hat am 16.10.2015 der Zusammenschluss der Datenschutzaufsichtsbehörden, die Artikel 29 Arbeitsgruppe der EU-Kommission einen Frist für Verhandlungen mit den USA bis Ende Januar 2016 gesetzt (Pressemitteilung). Bis dahin will die Art. 29 Arbeitsgruppe die Bindung Corporate Rules und die EU-Standardvertragsklauseln weiterhin aus rechtmäßige Grundlage für die Datenübermittlung in die USA akzeptieren, siehe Statement der Art. 29. Datenschutzgruppe vom 15.10.2015 – deutsche Fassung, englische Fassung.

b.4) Deutsche Datenschutzaufsicht – Datenschutzkonferenz

Die deutschen Datenschutzaufsichtsbehörden habe ihre Ansicht in einem Positionspapier vom 26.10.2015 veröffentlicht.

Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)

- Nach dem Safe-Harbor-Urteil des EuGH vom 6. Oktober 2015 ist eine Datenübermittlung aufgrund der **Safe-Harbor**-Entscheidung der Kommission vom 26. Juli 2000 (2000/520/EG) **nicht zulässig**.
- Im Lichte des Urteils des EuGH ist auch die Zulässigkeit der Datentransfers in die USA auf der Grundlage der anderen hierfür eingesetzten Instrumente, etwa **Standardvertragsklauseln oder verbindliche Unternehmensregelungen (BCR), in Frage gestellt**.
- Der EuGH stellt fest, dass die Datenschutzbehörden der EU-Mitgliedstaaten ungeachtet von Kommissions-Entscheidungen nicht gehindert sind, in völliger Unabhängigkeit die Angemessenheit des Datenschutzniveaus in Drittstaaten zu beurteilen.
- Der EuGH fordert die Kommission und die Datenschutzbehörden auf, das Datenschutzniveau in den USA und anderen Drittstaaten (Rechtslage und Rechtspraxis) zu untersuchen und gibt hierfür einen konkreten Prüfmaßstab mit strengen inhaltlichen Anforderungen vor.
- Soweit Datenschutzbehörden Kenntnis über ausschließlich auf Safe-Harbor gestützte Datenübermittlungen in die USA erlangen, werden sie diese untersagen.
- Die Datenschutzbehörden werden bei Ausübung ihrer Prüfbefugnisse nach Art. 4 der jeweiligen Kommissionsentscheidungen zu den Standardvertragsklauseln vom 27. Dezember 2004 (2004/915/EG) und vom 5. Februar 2010 (2010/87/EU) die vom EuGH formulierten Grundsätze, insbesondere die Randnummern 94 und 95 des Urteils, zugrunde legen.
- Die Datenschutzbehörden werden derzeit **keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen**
- Unternehmen sind daher aufgerufen, unverzüglich ihre Verfahren zum Datentransfer datenschutzgerecht zu gestalten. Unternehmen, die Daten in die USA oder andere Drittländer exportieren wollen, sollten sich dabei auch an der Entschließung der DSK vom 27.03.2014 "**Gewährleistung der Menschenrechte bei der elektronischen Kommunikation**" und an der **Orientierungshilfe "Cloud Computing"** vom 09.10.2014 orientieren.
- Eine **Einwilligung** zum Transfer personenbezogener Daten kann unter engen Bedingungen eine tragfähige Grundlage sein. Grundsätzlich darf der Datentransfer jedoch nicht wiederholt, massenhaft oder routinemäßig erfolgen.
- Beim **Export von Beschäftigtendaten** oder wenn gleichzeitig auch Daten Dritter betroffen sind, kann die Einwilligung nur in Ausnahmefällen eine zulässige Grundlage für eine Datenübermittlung in die USA sein.
- Die Datenschutzbehörden fordern die Gesetzgeber auf, entsprechend dem Urteil des EuGH den **Datenschutzbehörden** ein **Klagerecht** einzuräumen.
- Die Kommission wird aufgefordert, in ihren Verhandlungen mit den USA auf die Schaffung ausreichend weitreichender Garantien zum Schutz der Privatsphäre zu drängen. Dies betrifft insbesondere das Recht auf gerichtlichen Rechtsschutz, die materiellen Datenschutzrechte und den Grundsatz der Verhältnismäßigkeit. Ferner gilt es, zeitnah die Entscheidungen zu den Standardvertragsklauseln an die in dem EuGH-Urteil gemachten Vorgaben anzupassen.
- Insoweit begrüßt die DSK die von der Art. 29-Gruppe gesetzte Frist bis zum 31. Januar 2016.
- Die DSK fordert die Bundesregierung auf, in direkten Verhandlungen mit der US-Regierung ebenfalls auf die Einhaltung eines angemessenen Grundrechtsstandards hinsichtlich Privatsphäre und Datenschutz zu drängen.

Die DSK fordert Kommission, Rat und Parlament auf, in den laufenden Trilog-Verhandlungen die strengen Kriterien des EuGH-Urteils in Kapitel V der **Datenschutzgrundverordnung** umfassend zur Geltung zu bringen.

Zwei Punkte seien hervorgehoben:

1. Die Einwilligung als Rechtsgrundlage wird im Gegensatz zur Auffassung des ULD nicht gänzlich abgelehnt.
2. Die Datenschutzbehörden werden wohl nicht vor Ende Januar 2016 aktiv Prüfung durchführen, um Datenübermittlungen auf der Safe Harbor-Grundlage zu entdecken, zu untersagen und zu ahnden. Aber wenn sie z.B. aufgrund von Beschwerden und Hinweisen davon erfährt, werden sie die Datenübermittlung auf dieser unzulässigen Rechtsgrundlage untersagen und ggf. auch sanktionieren.

b.5) EU-Kommission – Leitlinien für die Übergangszeit

Die EU-Kommission hat am 06.11.2015 Leitlinien für transatlantische Datenübermittlungen veröffentlich.

Siehe Pressemitteilung und siehe Leitlinien

Die Kommission betont die **Bedeutung der transatlantischen Handelsbeziehungen**, zu denen essentiell und in zunehmendem Maße auch der Austausch von Daten gehört. Andererseits erkennt sie die Stärkung der Datenschutzgrundrechte durch die Safe Harbor-Entscheidung des EuGH an. Nach dem Bekanntwerden des NSA-Skandals hat die Kommission bereits selbst 13 Empfehlungen erarbeitet, auf deren Grundlage sie seit Januar 2014 mit den USA über eine erneuertes und stärker datenschützendes Abkommen verhandelt. Diese Verhandlungen sollen jetzt intensiviert und **binnen 3 Monaten zum Abschluss** gebracht werden.

Hierzu ist anzumerken: da müsste dann auch die andere Seite, die USA, eine entsprechende Verhandlungsbereitschaft über die Datenzugriffsrechte ihrer Geheim- und Sicherheitsdienste und die Klagerechte von EU-Bürgern in den USA dagegen haben. Hieran sind jedoch gewisse Zweifel angebracht.

Die Kommission möchte den Forderungen der Wirtschaft nach einer rechtskonformen Fortsetzung des Datentransfers entsprechen und die rechtlichen Möglichkeiten aufzeigen. Zunächst wird auf die Position der Art. 29 Arbeitsgruppe vom 16.10.2015 verwiesen:

- EU-Standard Vertragsklauseln – Standard Contractual Clauses (SCC) und
- verbindliche unternehmensinterne Vorschriften für unternehmensgruppeninterne Datenübermittlungen, sog. Binding Corporate Rules (BCRs)

können zwischenzeitlich weiter zur Rechtsfertigung des Datentransfers genutzt werden. Zudem sollen von den Unternehmen dringend alle **technischen Möglichkeiten zur Vermeidung von Risiken für die Daten** ergriffen werden.

Aus meiner Sicht bedeutet dies praktisch zweierlei:

1. entweder werden die Daten künftig sicher verschlüsselt oder
2. es werden innereuropäische IT-Lösungen implementiert.

Gerade bei großen Unternehmen und komplexen IT-Landschaften halte ich aber auch das bis Ende Januar 2016, noch dazu über Weihnachten und Neujahr, für völlig unrealistisch.

Vor diesen Hintergrund schlägt die EU-Kommission ihre **Leitlinien für die Übergangszeit** vor. Dabei schreibt sie elegant, dass sie damit nicht die Unabhängigkeit der nationalen Datenschutzaufsichtsbehörden in Frage stellen will selbst zu untersuchen, ob eine bestimmte Datenübermittlung rechtmäßig ist. Ebenso wenig kann sie in die Kompetenzen nationaler Gericht eingreifen oder die Vorlage an den EuGH verhindern.

Mit anderen Worten: die Unternehmen können sich nicht auf das verlassen, was die EU-Kommission verlautbart, insbesondere nicht in Deutschland in Anbetracht der von den Aufsichtsbehörden bereits geäußerten strengeren Ansichten. **Die Rechtsunsicherheit bleibt also bestehen**.

EU-Standardvertragsklauseln

Die EU-Kommission meint, dass Unternehmen (Datenexporteure) sich weiter auf die **EU-Standardvertragsklauseln** stützen könnten, aber selbst dafür verantwortlich wären, dass dabei die Datenschutzrichtlinie eingehalten wird. Die Entscheidung der EU-Kommission, dass die EU-Standard-Vertragsklauseln ein angemessenes Sicherheitsniveau schaffen, sei bindend und können nicht ohne weiteres von nationalen Aufsichtsbehörden in Frage gestellt werden. Bei Bedenken müsse Klage vor einem nationalen Gericht erhoben werden, welches die Frage dem EuGH zur Entscheidung vorlegt.

Da die Aufsichtsbehörden in Deutschland noch **kein derartiges Klagerecht** habe, bedeutet das, dass sie gegen ein Unternehmen eine belastende Verfügung erlassen, gegen die sich dann das Unternehmen mit einer Klage zur wehr setzt, damit dann das angerufene Gericht die Frage dem EuGH zur Vorabentscheidung vorlegen kann.

Binding Corporate Rules

sind konzerninternen verbindliche Datenschutzregelungen. Diese BCR sollen den Datenaustausch innerhalb eines internationalen Konzerns auf der Grundlage des durch die BCR geschaffenen angemessenen Datenschutzniveaus erlauben. Die Artikel 29 Datenschutzgruppe hat hierzu 2008 ein Arbeitsdokument herausgegeben.

Aber auch hierbei gilt die gleiche logische Konsequenz aus dem EuGH-Urteil: auch die BCR sind letztendlich nur zivilvertragliche Regelungen, durch die sich die vorrangigen US-Gesetze, die der EuGH als nicht mit den EU-Datenschutzgrundrechten für vereinbar hält, nicht aushebeln lassen.

Gleichwohl hält die EU-Kommission die BCRs auf der Grundlage ihrer dahingehenden Entscheidung weiterhin für anwendbar. Das ist aber nichts, worauf man auf Dauer setzen kann. Zumal die deutschen Aufsichtsbehörden angekündigt haben, keine neuen BCRs mehr zu genehmigen.

Ausnahmevorschriften

Die Leitlinien der Kommission listen noch weitere mögliche Rechtsgrundlagen auf (als Ausnahme von dem Übermittlungsverbot), u.a.:

- **Einwilligung** der betroffenen Person (freiwillig und verständlich informiert)
- Datentransfer zur **Vertragserfüllung** (z.B. zur Hotelreservierung oder im Zahlungsverkehr)
- Datentransfer ist im öffentlichen Interesse erforderlich oder **Ausübung bzw. Verteidigung von rechtlichen Ansprüchen** (Gerichtsprozesse)
- Datentransfer zum Schutz lebenswichtiger Interessen der betroffenen Person

Die Einwilligung

Hervorgehoben werden die **strengen Anforderungen an eine Einwilligung**:

- sie muss vorab erfolgen;
- sie muss ausdrücklich und bewusst erfolgen;
- sie muss freiwillig und ohne Druck oder gar Zwang erfolgen;
- die Hervorhebung durch eine Kasten wird empfohlen und ein Ankreuzfeld darf nicht vorausgefüllt sein;
- die der Einwilligung vorausgehende Information muss zwingend auch die Risiken, die sich aus dem unangemessenen Schutz im Drittstaat ergeben, beinhalten (es fragt sich, wer dann noch einwilligt);
- die Einwilligung muss widerrufbar sein (und ist damit auch keine dauerhaft verlässliche Verarbeitungsgrundlage).

In Anbetracht dieser hohen und engen Voraussetzungen hält die Art. 29 Arbeitsgruppe die Einwilligung **nicht für massenverkehrstauglich**, sondern allenfalls für im Einzelfall anwendbar.

Die Kommission stellt ergänzend klar, dass die genannten alternativen Rechtsgrundlagen für den Drittstaatentransfer voraussetzen, dass auf der **ersten Prüfungsstufe** die Daten überhaupt erhoben und verarbeitet werden durften. Zudem bleibt das datenexportierende Unternehmen verpflichtet, ausreichende Sicherheitsvorkehrungen zu treffen, seien es technische, organisatorische, rechtliche oder das Geschäftsmodell betreffende Maßnahmen.

b.6) EU-Parlament

Das **EU-Parlament** hat in einer Entschließung am 29.10.2015 festgestellt, dass zu wenig unternommen werde, um die Datenschutzrechte von EU-Bürgern infolge der digitalen Massenüberwachung durch die USA zu schützen. Die EU-Kommission solle umgehend die erforderlichen Maßnahmen zum Schutz der in die USA übermittelten Daten ergreifen. Das Parlament fordert die Kommission auf, die Auswirkungen des Safe Harbor Urteils auf andere Instrumente für die Übermittlung personenbezogener Daten in die USA bis Ende 2015 zu prüfen und darüber zu berichten. (Anm. dies deutet darauf hin, dass das Parlament auch auf Standardvertragsklauseln und die BCRs kritisch sieht) Zudem fordert das Parlament das **SWIFT-Abkommen** (Abkommens über das Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP)) auszusetzen.

Hintergrundinfos zum

SWIFT-Abkommen

SWIFT steht Society for Worldwide Interbank Financial Telecommunication und ist eine belgische Gesellschaft, die einen Standard zur weltweiten Übertragung von Zahlungsverkehrsdaten geschaffen hat. Das SWIFT-Abkommen von 2001 sah vor, dass US-Behörden europäische Zahlungsverkehrsdaten nach Terrorverdächtigen durchsuchen durften.

2006 wurde aufgedeckt, dass US-Dienste auf die SWIFT-Daten weitergehend zugreifen, als von EU-Seite aus gedacht. Von EU-Datenschützern gedrängt, wickelte der Belgische Zahlungsverkehrskommunikationsdienstleister SWIFT die Kommunikation von innereuropäischem Zahlungsverkehr seit dem ausschließlich in der Europa ab und hat das Back-Up-Rechenzentrum in den USA, auf das US-Dienste nach dortigem Recht weitgehend Zugriff hatten, nach Niederlanden und in die Schweiz verlegt. Die US-Ermittler waren vom Datenstrom abgeschnitten und wollten schnellstens wieder Zugriff.

Daraufhin hatte das EU-Parlament die Fassung des Abkommens vom Februar 2010 gekippt.

Wenige Monate später kam das neue SWIFT-Abkommen zustanden: 24.06.2010 – Abkommen zwischen USA und EU über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus

Das **SWIFT-Abkommen** wurde 2013 vom EU-Parlament wegen der durch Edward Snowden aufgedeckte NSA Affäre ausgesetzt vom 23.10.2013

Schließlich kritisiert das EU-Parlament die Überwachungsgesetze in Mitgliedsstaaten wie Frankreich, Großbritannien und Niederlanden.

Merkwürdigerweise wird das **Fluggastdatenabkommen** mit den USA nicht angesprochen. Hier will vermutlich aus politischen Gründen das Parlament nicht aktiv werden, auch wenn man sich mit guten Gründen fragen kann, ob der dort geregelte Umfang an zu übermittelnden Passagierdaten dem Grundsatz der Verhältnismäßigkeit entspricht.

Hintergrundinfo

Abkommen für Fluggastdaten zwischen USA und EU – 2013

Der Europäische Gerichtshof hatte bereits 2006 entschieden, dass es für die Weitergabe von Flugpassagierdaten durch EU-Mitgliedsstaaten an die USA keine geeignete Rechtsgrundlage gibt. Damit verstößt die Datenweitergabe gegen EU-Recht. Das EU-Parlament war zuvor im Jahr 2004 gegen ein am 28. Mai 2004 geschlossenes Abkommen zur Freigabe der Daten zwischen der EU-Kommission und den USA vor Gericht gegangen.[8][9]

Im März 2012 stimmte das Europäische Parlament für das *transatlantische Abkommen zum Transfer von Flugpassagierdaten*: Text des Abkommens

b.7) Datenschutzaufsicht Rheinland-Pfalz

Die Datenschutzaufsicht in Mainz (LfDI) hat am 26.10.2015 ihr Folgerungen aus dem Safe-Harbor-Urteil des EuGH veröffentlicht.

Die Kriterien des EuGH sind nicht nur auf die USA, sondern auf alle Drittstaaten anzuwenden:

> "Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes."

Die Aufsicht stellt ab sofort alle Datenübermittlungen in die USA unter ein Genehmigungserfordernis und hält die Exporte nur noch in Ausnahmefällen für zulässig.

Zu den EU-Standardvertragsklauseln stellt die Datenschutzaufsicht in Rheinland-Pfalz fest:

> "Jedenfalls wird der LfDI RLP im Einzelfall prüfen, ob Datenimporteure in den USA ihrer vertraglichen Verpflichtung nachgekommen sind, zu garantieren, dass sie *keinen Gesetzen unterliegen*, die ihnen die Befolgung der Anweisungen des Datenexporteurs oder die Einhaltung ihrer vertraglichen Pflichten unmöglich machen und nachteilige Gesetzesänderungen in den USA (hier: USA Patriot Act 2001 und seine Folgeregelungen) dem Datenexporteur mitzuteilen."

Da kein US-Unternehmen garantieren kann, dass sie nicht den US-Gesetzen wie dem **US-Patriot Act 2001** unterliegen, ist mit dieser Prüfungsfrage auch der Exportweg über die EU-Standardvertragsklauseln "tot". Das Aufsicht will sogar prüfen, ob die Unternehmen (Datenexporteure) angemessene Konsequenzen aus dieser Sachlage gezogen und von ihrem Kündigungsrecht gebraucht gemacht haben. Anderes ausgedrückt: die **Unternehmen** (zumindest die in Rheinland-Pfalz) **sollen die Datenübermittlungen auf der Grundlage von EU-Standardvertragsklauseln einstellen und die Verträge kündigen**. Das kann aber kein Unternehmen ohne nicht eine alternative Lösung gefunden zu haben. Und das genau dürfte das praktische Problem sein und auf absehbare Zeit bleiben.

Neue Genehmigungen von **Binding Corportate Rules** werden nicht mehr erteilt (Ziff 4). Auch **Einwilligungen** sind nur in seltenen Fällen eine zulässige Übermittlungsgrundlage. Für **Beschäftigtendaten** seien Einwilligungen generell keine zulässige Datenübermittlungsgrundlage (Ziff. 5). Letzteres steht m.E. im Widerspruch zur vom BAG auch im Beschäftigungsverhältnis ausdrücklich anerkannten Einwilligungsmöglichkeit.

Die Aufsicht weist auf ihre Instrumente wie Untersagungsverfügungen und Bußgelder hin, betont aber, dass sie zunächst im Wege der Beratung den Unternehmen helfen wolle. Dies gelte auch für die praktische wichtigen Supportleistungen (Fernwartung, Remote Access) aus Drittstaaten und für 24/7-Dienstleistungen. Man darf gespannt sein, was der Aufsicht dazu einfällt und wo sie die Dienstleister in der EU finden will. Die Datenschutzaufsicht gibt den Unternehmen einen **Check-Liste** aus "Hausaufgaben" mit, die bis zum 31.01.2016 abzuarbeiten ist (Ziff III.4):

- auf welcher Rechtsgrundlage bislang Datenübermittlungen in die USA stattfinden,
- insbesondere ob bisher Übermittlungen auf Grundlage der jetzt für ungültig erklärten Safe Harbor-Entscheidung der EU-Kommission erfolgten,
- ob die Entscheidung des EuGH Grundlage einer außerordentlichen Kündigung bestehender Vertragsbeziehungen zu Safe Harbor-zertifizierten Unternehmen in den USA ist und
- welche alternativen Übermittlungsmöglichkeiten in die USA bestehen

Ab 01.02.2016 kündigt der LfDI stichprobenartige Prüfungen an und scheint auch die Lösung eher auf technischer Eben wie Verschlüsselung, Pseudonymisierung und "gekapselter Verarbeitung" zu sehen.

c. Ausblick: Safe Harbor 2.0?

Die Annahme, dass in den laufenden Verhandlungen der EU mit den USA (kurzfristig) die Vorgaben des EuGH umgesetzt werden können:

- kein Vorrang von US-Sicherheitsgesetzen vor Datenschutz von EU-Bürgern,
- begrenzter, verhältnismäßiger Datenzugriff und
- Rechtsmittel gegen Datenzugriff –

halte ich für eher unwahrscheinlich, um nicht zu sagen sogar naiv.

Beispiel **Klagerecht**:

In den USA wird gerade ein Klagerecht für EU-Bürger gegen Datenschutzverletzung verhandelt, welches jedoch in der hiesigen Presse wegen der zahlreichen Voraussetzungen und Ausnahmen als Farce bezeichnet wird: **Judicial Regress Act.**

Eine Studie im Auftrag des EU-Parlaments, Abteilung für Bürgerrechte, vom September 2015 zum Vergleich des Datenschutzrechts von USA und EU zur Rechtsdurchsetzung, individuelle Rechte und Sicherheitsinteressen – Autorin Prof. Franziska Boehm, Uni Münster, kommt unter Ziff 3.3, S. 54 zum Ergebnis, dass das Gesetz (Judicial Redress Act) weit hinter den vergleichbaren Rechte von EU-Bürgern zurückbleibt und schwammig formuliert ist.

Da die Attentäter vom 11. September aus Deutschland kamen, werden die USA wohl aufgrund ihrer nationalen Sicherheitsinteressen kaum den Zugriff auf die Daten der EU-Bürger einschränken und sich den europäischen Vorstellungen von Datenschutzgrundrechten anpassen und ihre Sicherheitsbehörden den Klagen von Europäern aussetzen wollen.

Das ist zwar alles Spekulation, aber wenn man mal diese Position als **Arbeitshypothese** unterstellt und die vom EuGH in der Safe Harbor-Entscheidung entwickelten Grundsätze auch auf die **EU-Standard-Vertragsklauseln** und **Binding Corporate Rules** anwendet, kommt man leicht zu dem **Ergebnis**, dass Safe Harbor 2.0 wohl so schnell nicht kommen dürfte und es wahrscheinlicher ist, dass auch die EU-Standardvertragsklauseln und Binding Corporates Rules noch für ungültig erklärt werden. Die EU-Justizkommissarin Vera Jourova will noch im November zu Verhandlungen über eine neuen Vereinbarung nach Washington reisen. Ein Erfolg wäre ihr im Interesse der Wirtschaft und der Bürger zu wünschen.

Folgt man jedoch meiner kritischen Einschätzung, kann **die mittel- und langfristige Strategie** für betroffene Unternehmen in der EU nur sein, allenfalls als Übergangslösung auf EU-Standard-Vertragsklauseln und Binding Corporate Rules zu setzen, es aber als „sinkendes Schiff“ zu verstehen und nach anderen Lösungen zu suchen. Die Position von einigen US-IT-Firmen in Vertragsverhandlungen ist: wir wollen Eure Daten gar nicht sehen können, trennt die Daten vom Programm, verschlüsselt die Daten, aber belastet uns nicht mit Eurem Datenschutz. Die Position zeigt also in die Richtung, dass das was sich rechtlich nur sehr schwer lösen lasst, durch technische Mittel gelöst wird.

Das ULD hilft Unternehmen bei der Suche nach alternativer Software – angeführt wird als Beispiel statt Doodle zur Terminplanung den DFN-Terminplaner zu nutzen. Ganz verständlich ist dieses Beispiel nicht, da Doodle eine Schweizer Anwendung ist und die Schweiz im Bereich Datenschutz nach wie vor als sicherer Drittstaat angesehen wird.

Die eine Lösung ist es, nicht mehr auf US-Software zu setzen und nur EU-Software zu verwenden bzw. nur auf EU-Dienstleister ohne US-Subunternehmer zuzugreifen und Daten nur in der EU zu speichern und dabei Dienstleister zu wählen, die nicht Töchter oder Niederlassungen von US-Unternehmen sind, über die die US-Dienste dann mit Hilfe von **US-(Geheim-)Gerichten** doch wieder auf die Daten der Europäer zugreifen können.

Hintergrundinfo zu diesem Punkt: nach Auffassung von US-Gerichten haben US-Sicherheitsbehörden auch **Zugriff auf in Europa** gelagerte Daten von US-Unternehmen (US-District Court Southern District of New York, Entscheidung vom 25. 4. 2014 – Aktenzeichen 13 Mag. 2814 – zur Herausgabe von E-Mail aus Irland von den dortigen Servern von Microsoft.

Die andere Lösung könnte in einer **starken Verschlüsselung** bestehen, die sich allerdings eine Verschlüsselungssoftware und Algorithmen bediente, zu der die US-Dienste keinen „Nachschlüssel“ haben.

In bestimmten Fällen kommt auch eine **juristische Lösung** in Betracht, etwa eine Einwilligung oder die Datenübermittlung zur Erfüllung des Vertragszwecks (bei entsprechender vertraglich deutlicher Gestaltung des Vertragszwecks).

Das ULD wirft bereits die Frage auf, ob der Datentransfer nicht auch innerhalb der EU eingeschränkt werden soll. Z.B. weil der britische Geheimdienst GCGQ eng mit den US-Diensten zusammenarbeitet.

d. Einschätzung

Die EuGH-Entscheidung und die Auffassung(-en) der Datenschutzaufsichtsbehörden mögen in sich rein nach der juristischen Logik stimmig sein, nur bedeutet das konsequent zu Ende gedacht die Einstellung den Datenaustauschs mit den USA einschließlich der Verzicht auf die Nutzung von Dienstleistungsangeboten (inkl. Cloud-Diensten, Internetdiensten, Software) von US-Unternehmen und deren EU-Tochterfirmen. Das geht jedoch an den **Interessen der Bürger und der Wirtschaft** vorbei und

berücksichtigt nicht, dass **die Internet- und IT-Welt weit überwiegend US-dominiert** ist (Apple, Goolge, IBM, Microsoft, Oracle, Cisco, Facebook, Amazon, Ebay, PayPal etc.) und es oft keine vergleichbaren oder gleichwertigen europäischen Angebote gibt. Der rechtspolitische Diskussionsprozess, das Datenschutzgrundrecht auch mit anderen Grundrechten abzuwägen und in einen vernünftigen Einklang zu bringen, steht noch aus.

Negativ formuliert könnte man sagen, dass die Entscheidung weltfremd im juristischen Elfenbeinturm gefällt wurde.

Weckruf an die EU-IT-Industrie

Positiv formuliert kann man die Entscheidung als ein selbstbewusstes Vertreten europäischer Grundwerte und Grundrechte gegen die US-Dominanz und zugleich im Effekt als **Weckruf an die EU-IT-Wirtschaft** verstehen, kurzfristig eigene Angebot den US-Unternehmen entgegen zu stellen.

Rechtsanwalt David Seiler, Cottbus den 7.11.2015

Rechtsanwalt David Seiler, externer Datenschutzbeauftragter, berät bundesweit zu Fragen des Datenschutzrechts.

KANZLEI COTTBUS Töpferstraße 2 in D-03046 Cottbus

T 03 55/ 479 20 10, F 03 55/ 479 20 11

cottbus@ka-rechtsanwalt.de, www.ka-rechtsanwalt.de