Internationaler Datentransfer – Was geht, was nicht?

Infobörse 1

Referent: Dr. Sven Polenz, ULD

Moderation: Torsten Koop, ULD

Übersicht

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

1.2 Privacy Shield

1.3 Angemessenes Datenschutzniveau?

2. Datentransfer in andere Drittstaaten

2.1 Vorgaben des EuGH

2.2 Beispiele: Indien und China

3. Alternativen?

3.1 Technische Lösungsansätze?

3.2 Binding Corporate Rules und Standardvertragsklauseln?

3.3 Datenverarbeitung in Europa?

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

ENTSCHEIDUNG DER KOMMISSION

vom 26. Juli 2000

gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA

(Bekannt gegeben unter Aktenzeichen K(2000) 2441)

(Text von Bedeutung für den EWR)

(2000/520/EG)

(ABl. L 215 vom 25.8.2000, S. 7)

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

Selbstzertifizierungsgrundsätze:

a) Informationspflicht (bzgl. Zweck)
b) Wahlmöglichkeit
c) Weitergabe
d) Sicherheit
e) Datenintegrität
f) Auskunftsrecht
g) Durchsetzung

DURCHSETZUNG

Für einen effektiven Schutz der Privatsphäre müssen Mechanismen geschaffen werden, die die Einhaltung der Grundsätze des sicheren Hafens gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens Folgendes umfassen: a) leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, behandelt werden und nach denen Schadenersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen; b) Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Unternehmen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden; c) Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Organisationen die Einhaltung der Grundsätze zwar erklärt, sich aber trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

- **Studie** „The U.S. Safe-Harbor – Fact or Fiction?“ des Beratungsunternehmens Galexia (2008): Von 1.597 der damals registrierten Unternehmen nutzen nur 1.109 das System. Nur 348 Unternehmen hatten die eigenen Selbstzertifizierungsgrundsätze umgesetzt. 206 Unternehmen gaben fälschlich an, eine Selbstverpflichtung abgegeben zu haben. Nur 54 der 1.597 Unternehmen hatten die **Anforderungen zum Punkt „Enforcement“** zumindest formal erfüllt.

- Eine qualitative Überprüfung der Enforcement-Regelungen fand nicht statt.

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

- Die FTC nutzte ihre Aufsichtsbefugnisse bisher nur in den Fällen der „irreführenden und unfairen Praktiken“, wobei erstmals im Jahre 2009 gegen **lediglich sechs Unternehmen** wegen falscher Angaben zu den Selbstverpflichtungen vorgegangen wurde. Es wurde lediglich eine Unterlassung der Falschangaben verfügt. Bußgelder wurden keine verhängt.

- Erforderlich waren auch unabhängige Schlichtungsstellen. Hierfür wurden jedoch private Organisationen (American Arbitration Association und Judicial Arbitration Mediation Service) eingesetzt, welche für eine Schlichtung mehr als 1000 US-Dollar inkl. Verwaltungspauschale verlangten. Durch die Abrechnung auf Stundenbasis konnten teilweise höhere Beträge anfallen.

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover (überarbeitete Fassung vom 23.8.2010)

Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens" (Safe Harbor)[1]. Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Das US-Handelsministerium veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Habor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, ob die Safe Habor-Zertifizierung des Importeurs noch gültig ist. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor[2] gegenüber den von der Datenverarbeitung Betroffenen nachkommt.

89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 18. und 19. März in Wiesbaden

Entschließung:

Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

Maßgebend ist nach Art. 25 der Richtlinie 95/46/EG ein „angemessenes Datenschutzniveau.“

Artikel 25

Grundsätze

(1) Die Mitgliedstaaten sehen vor, daß die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt.

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

Die Kommission kann nach Art. 25 Abs. 6 der Richtlinie 95/46/EG das angemessene Datenschutzniveau für ein Drittland feststellen.

(6) Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, daß ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

→ EuGH, Urteil vom 06.10.2015, C-362/14

- Rückgriff auf System der Selbstzertifizierung verstößt als solcher nicht gegen Art. 25 der Richtlinie 95/46/EG.
- Die Zuverlässigkeit des Systems hängt aber von wirksamen Überwachungs- und Kontrollmechanismen ab, die es erlauben, datenschutzrechtliche Verstöße zu ermitteln und zu ahnden.
- Der Safe-Harbor-Beschluss enthält keine Feststellungen zu staatlichen Regelungen in den USA, welche Grundrechtseingriffe (etwa zum Schutz des nationalen Sicherheit) begrenzen.
- Im Safe-Harbor-Beschluss fehlen Feststellungen zum Bestehen eines wirksamen gerichtlichen Rechtsschutzes.

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

EuGH, Urteil vom 06.10.2015, C-362/14

Art. 7 der Grundrechtecharta

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.“

„Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den **Wesensgehalt** des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens.“

→ Zugriff auf gespeicherte Daten ohne Zweckbindung, Einschränkungen, Differenzierungen

1. Datentransfer in die USA

1.1 Nichtigkeit des Safe-Harbor-Beschlusses

Art. 47 der Grundrechtecharta

Artikel 47

Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht

Jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, hat das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen.

Jede Person hat ein Recht darauf, dass ihre Sache von einem unabhängigen, unparteiischen und zuvor durch Gesetz errichteten Gericht in einem fairen Verfahren, öffentlich und innerhalb angemessener Frist verhandelt wird. Jede Person kann sich beraten, verteidigen und vertreten lassen.

Personen, die nicht über ausreichende Mittel verfügen, wird Prozesskostenhilfe bewilligt, soweit diese Hilfe erforderlich ist, um den Zugang zu den Gerichten wirksam zu gewährleisten.

EuGH, Urteil vom 06.10.2015, C-362/14

„Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den **Wesensgehalt** des in Art, 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz.“

→ „Insoweit ist schon das Vorhandensein einer wirksamen, zur Gewährleistung der Einhaltung des Unionsrechts dienenden gerichtlichen Kontrolle dem **Wesen eines Rechtsstaats** inhärent.“

1. Datentransfer in die USA

1.2 Privacy Shield

DURCHFÜHRUNGSBESCHLUSS (EU) 2016/1250 DER KOMMISSION

vom 12. Juli 2016

gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes

(Bekannt gegeben unter Aktenzeichen C(2016) 4176)

(Text von Bedeutung für den EWR)

1. Datentransfer in die USA

1.2 Privacy Shield

EuGH, Urteil vom 06.10.2015, C-362/14

„Der Erlass einer Entscheidung der Kommission nach Art. 25 Abs. 6 der Richtlinie 95/46/EG erfordert die gebührend begründete Feststellung dieses Organs, dass das betreffende Drittland aufgrund seiner **innerstaatlichen Rechtsvorschriften** oder **internationaler Verpflichtungen** tatsächlich ein Schutzniveau der Grundrechte gewährleistet, das dem in der Rechtsordnung der Union garantierten Niveau (..), der Sache nach gleichwertig ist.“

1. Datentransfer in die USA

1.2 Privacy Shield

a) Innerstaatliche Rechtsvorschriften?

Auf Basis von **Artikel 215 des U.S. Patriot Act** hat die National Security Agency in großem Umfang über Jahre hinweg Telefon- sowie Internet-Metadaten von U.S. Bürgern gespeichert. Art. 215 des U.S. Patriot Act war ab dem 1. Juni 2015 nicht mehr anwendbar: Im U.S. Freedom Act wurde nun normiert, dass die Telefondaten künftig nicht mehr bei den U.S. Behörden, sondern bei den TK-Konzernen gespeichert werden. Geheimdienste sollen für einen Datenzugriffs nun einer richterliche Erlaubnis benötigen (Beschluss vom Foreign Intelligence Surveillance Court).

1. Datentransfer in die USA

1.2 Privacy Shield

a) Innerstaatliche Rechtsvorschriften?

Die Gesetzesänderung im Freedom Act hatte jedoch keinen Einfluss auf die Überwachung von Nicht-U.S. Bürgern. Art. 702 des U.S. Patriot Act ermöglicht den Zugriff auf Nutzerdaten von Nicht-U.S. Bürgern (z.B. von Microsoft und Facebook). Erlaubt wird sogar die **Auswertung der Kommunikationsinhalte**.

1. Datentransfer in die USA

1.2 Privacy Shield

a) Innerstaatliche Rechtsvorschriften?

Werden persönliche Daten durch U.S. Behörden willkürlich verarbeitet, so können U.S. Bürger hiergegen einen Rechtsbehelf nach dem U.S. Privacy Act einlegen. Für Nicht-U.S. Bürger gilt diese Befugnis über den **Judicial Redress Act**, mit folgenden **Einschränkungen**:

- Das U.S. Justizministerium entscheidet, für welche Länder das Gesetz gelten soll.
- Es können nur Rechtsverletzungen gegen Bestimmungen des U.S. Privacy Act geltend gemacht werden. Datenverarbeitungen auf Basis anderer Vorschriften sind nicht erfasst.
- Es werden darüber hinaus nur Datenverarbeitungen im Zusammenhang mit einer Strafverfolgung einbezogen.

1. Datentransfer in die USA

1.2 Privacy Shield

a) Innerstaatliche Rechtsvorschriften?

(Auszug aus Erwägungsgrund 109 der Adäquanzentscheidung)

(109) Hingegen autorisiert das FISC nach § 702 des FISA ([144]) keine individuellen Überwachungsmaßnahmen; vielmehr genehmigt es Überwachungsprogramme (wie PRISM oder UPSTREAM) auf der Grundlage jährlicher Zertifizierungen, die vom Justizminister und dem Director of National Intelligence vorgenommen werden. § 702 des FISA gestattet die gezielte Überwachung von Personen, die sich mit hinreichender Bestimmtheit außerhalb der Vereinigten Staaten aufhalten, um Auslandsaufklärungsdaten zu erlangen ([145]). Die gezielte Überwachung durch die NSA erfolgt in zwei Schritten: Zunächst identifizieren Analysten der NSA Nicht-US-Bürger, die sich im Ausland befinden und deren Überwachung nach Einschätzung der Analysten zu den in der Zertifizierung angegebenen Auslandsaufklärungsdaten führt. Sobald diese Personen identifiziert sind und ihre gezielte Überwachung nach einem gründlichen Kontrollverfahren innerhalb der NSA genehmigt wurde ([146]), werden Selektoren, die Kommunikationseinrichtungen (wie E-Mail-Adressen) identifizieren, „aktiviert" (d. h. erstellt und angewandt) ([147]). Wie bereits angemerkt, enthalten die vom FISC zu bestätigenden Zertifizierungen keine Informationen über die einzelnen zu überwachenden Personen, sondern beziehen sich auf Kategorien von Auslandsaufklärungsdaten ([148]). Das FISC beurteilt nicht — anhand eines hinreichenden Verdachts oder sonstigen Kriteriums —, ob die Personen vorschriftsgemäß als Zielpersonen für die Beschaffung von Auslandsaufklärungsdaten ausgewählt wurden ([149]), sondern überprüft die Einhaltung der Bestimmung, dass „ein wesentlicher Zweck der Datenerhebung darin besteht, Auslandsaufklärungsdaten zu erlangen" ([150]). Laut § 702 des FISA ist es nämlich der NSA nur dann gestattet, den Datenverkehr von Nicht-US-Bürgern außerhalb der USA zu erheben, wenn die begründete Annahme besteht, dass ein bestimmtes Kommunikationsmittel verwendet wird, um Daten zu übermitteln, die für die Auslandsaufklärung von Interesse sind (z. B. weil sie mit dem internationalen

1. Datentransfer in die USA

1.2 Privacy Shield

a) Innerstaatliche Rechtsvorschriften?

- Zweckbindung?

- Erforderlichkeit?

- Verhältnismäßigkeit?

- Betroffenenrechte?

1. Datentransfer in die USA

1.2 Privacy Shield

a) Innerstaatliche Rechtsvorschriften?

(Erwägungsgrund 111 der Adäquanzentscheidung)

(111) Nach amerikanischem Recht steht Betroffenen in der EU eine Reihe von Möglichkeiten offen, wenn sie in Erfahrung bringen wollen, ob ihre personenbezogenen Daten von US-Nachrichtendiensten verarbeitet (erhoben, genutzt usw.) wurden, und sofern dies der Fall ist, ob die im amerikanischen Recht geltenden Einschränkungen befolgt wurden. Diese betreffen im Wesentlichen drei Bereiche: Eingriffe gemäß FISA; der vorsätzliche gesetzwidrige Zugriff auf personenbezogene Daten durch Regierungsbeamte; und der Zugang zu Informationen gemäß dem Freedom of Information Act (FOIA) ([157]).

1. Datentransfer in die USA

1.2 Privacy Shield

a) Innerstaatliche Rechtsvorschriften?

(Erwägungsgrund 115 der Adäquanzentscheidung)

(115) Auch wenn Privatpersonen, einschließlich Betroffene in der EU, eine Reihe von Rechtsschutzinstrumenten zur Verfügung steht, wenn sie aus Gründen der nationalen Sicherheit rechtswidrig (elektronisch) überwacht wurden, steht doch fest, dass zumindest einige Rechtsgrundlagen, die US-Nachrichtendienste nutzen können (z. B. E.O. 12333), nicht dazu gehören. Selbst wenn Nicht-US-Bürger im Prinzip auf gerichtliche Rechtsbehelfe zurückgreifen können, beispielsweise auf der Grundlage des FISA im Falle der Überwachung, sind die verfügbaren Klagemöglichkeiten begrenzt ([169]), denn Klagen von Einzelpersonen (auch US-Bürgern) werden abgewiesen, wenn diese ihre „Klagebefugnis" nicht nachweisen können ([170]), was den Zugang zu den ordentlichen Gerichten einschränkt ([171]).

1. Datentransfer in die USA

1.2 Privacy Shield

a) Innerstaatliche Rechtsvorschriften?

Ein **Ombudsmechanismus** soll dafür sorgen, dass Beschwerden von Bürgern ordnungsgemäß geprüft werden.

Eine Unabhängigkeit, welche dem europäischen Recht gleichwertig ist, ist damit **nicht** verbunden.

(zur Unabhängigkeit einer Datenschutzaufsicht EuGH, Urt. v. 09.03.2010, C 518(07)

Es ist nicht erkennbar, mit welchen **Befugnissen** ein Ombudsmann sich gegenüber datenschutzrechtlichen Verstößen von U.S. Geheimdiensten durchsetzen soll.

Für den Ombudsmann besteht keine erkennbare **Sanktionsbefugnis**.

1. Datentransfer in die USA

1.2 Privacy Shield

a) Innerstaatliche Rechtsvorschriften?

(Erwägungsgrund 124 der Adäquanzentscheidung)

(124) In diesem Zusammenhang nimmt die Kommission das Urteil des Gerichtshofs in der Rechtssache Schrems zur Kenntnis, in dem es heißt: „Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz." ([178]) Die Analyse der Kommission hat bestätigt, dass derartige Rechtsbehelfe in den Vereinigten Staaten vorhanden sind, auch durch die Einrichtung des Ombudsmechanismus. Dieser Mechanismus ermöglicht eine unabhängige Kontrolle mit Ermittlungsbefugnissen. Im Rahmen der ständigen Überwachung des Datenschutzschilds durch die Kommission, wozu auch die gemeinsame jährliche Überprüfung gehört, an der sich die Ombudsperson beteiligen soll, wird die Wirksamkeit dieses Mechanismus überprüft.

1. Datentransfer in die USA

1.2 Privacy Shield

b) Internationale Verpflichtungen?

Nach Art. 25 Abs. 6 der Richtlinie 95/46/EG können zur Beurteilung des angemessenen Schutzniveaus auch internationale Verpflichtungen zur Grundlage einer Adäquanzentscheidung dienen.

Solche Verpflichtungen resultieren aus **völkerrechtlichen Abkommen** und **Verträgen**.

Einseitige Zusicherungen sind dafür nicht ausreichend, auch wenn diese im U.S. Federal Register veröffentlicht werden.

1. Datentransfer in die USA

1.2 Privacy Shield

b) Internationale Verpflichtungen?

(Erwägungsgrund 73 der Adäquanzentscheidung)

→ Zusicherung über das Amt des Director of National Intelligence

(73) Den Erklärungen des ODNI zufolge sind die Nachrichtendienste bemüht, auch wenn sie nicht auf zielgenaue Suchkriterien zurückgreifen können, die Datenerhebung „so weit wie möglich" einzugrenzen. Dazu setzen sie „Filter und andere technische Mittel ein, um die Datensammlung auf solche Kommunikationsvorgänge zu konzentrieren, die nachrichtendienstliche Erkenntnisse versprechen" (und berücksichtigen damit die von US-Politikern gemäß dem im Erwägungsgrund 70 dargestellten Prozess aufgestellten Anforderungen). Im Ergebnis wird die Sammelerhebung zumindest auf zweierlei Weise zielgerichtet eingesetzt: Erstens werden damit immer konkrete Ziele der Auslandsaufklärung verfolgt (z. B. Signalaufklärung zur Erlangung von Erkenntnissen über Terroristengruppen, die in einer bestimmten Region operieren) und vor allem diesbezügliche Kommunikationsdaten erhoben. Wie das ODNI dazu ausführte, ist dies auch daran abzulesen, dass „die Signalaufklärung der Vereinigten Staaten nur einen Bruchteil der Kommunikationsvorgänge im Internet erfasst" ([73]). Zweitens ist den Erläuterungen des ODNI zu entnehmen, dass die Filter und sonstigen technischen Mittel so konzipiert sind, dass die Erhebung „so präzise wie möglich" erfolgt, um den Anteil „nichtrelevanter" Informationen auf ein Mindestmaß zu reduzieren.

1. Datentransfer in die USA

1.2 Privacy Shield

b) Internationale Verpflichtungen?

(Erwägungsgrund 82 der Adäquanzentscheidung)

(82) Überdies hat die Regierung der USA der Europäischen Kommission in ihren Erklärungen ausdrücklich zugesichert, dass die Intelligence Community der USA „keine systematische anlassunabhängige Überwachung von Personen betreibt, was normale europäische Bürger einschließt“ ([88]). Was in den USA erhobene personenbezogene Daten anbelangt, wird diese Erklärung durch empirische Erkenntnisse untermauert, wonach die *Zugriffsanfragen* über NSL und gemäß FISA sowohl einzeln betrachtet als auch zusammengenommen nur eine relativ kleine Anzahl von Zielpersonen betreffen, wenn man den Datenverkehr im Internet insgesamt betrachtet ([89]).

(69) Die am 17. Januar 2014 erlassene Presidential Policy Directive 28 („PPD-28“) bringt eine Reihe von Einschränkungen für die „Signalaufklärung“ mit sich ([60]). Diese Verordnung ist für die Nachrichtendienste der USA verbindlich ([61]) und bleibt auch bei einem Regierungswechsel in Kraft ([62]). Die PPD-28 ist für Personen außerhalb der USA, darunter Betroffene in der EU, von besonderer Bedeutung. Sie enthält unter anderem folgende Festlegungen:

a) Die Signalaufklärung muss gesetzlich geregelt oder vom Präsidenten autorisiert sein und muss im Einklang mit der Verfassung der USA (insbesondere dem 4. Zusatzartikel) und dem amerikanischen Recht stehen;

b) alle Personen sind unabhängig von ihrer Nationalität oder ihrem Wohnort würde- und respektvoll zu behandeln;

c) alle Personen haben berechtigte Datenschutzinteressen beim Umgang mit ihren personenbezogenen Informationen;

d) die Privatsphäre und die bürgerlichen Freiheiten sind integraler Bestandteil aller Überlegungen bei der Planung der signalerfassenden Aufklärung in den USA;

e) die Signalaufklärung der USA muss daher angemessene Garantien für die personenbezogenen Informationen aller Privatpersonen unabhängig von ihrer Nationalität oder ihres Wohnorts einschließen.

1. Datentransfer in die USA

1.2 Privacy Shield

b) Internationale Verpflichtungen?

(Auszug aus Erwägungsgrund 90 der Adäquanzentscheidung)

mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen." ([99]) Auch wird es keine unbeschränkte Sammlung und Speicherung von Daten aller Personen geben. Die der Kommission gegenüber abgegebenen Erklärungen, darunter die Zusicherung, dass die US-Aktivitäten zur Signalaufklärung nur einen Bruchteil der Kommunikationsvorgänge im Internet berühren, schließen zudem die Möglichkeit aus, „generell" ([100]) auf den Inhalt elektronischer Kommunikation zuzugreifen.

1. Datentransfer in die USA

1.3 Angemessenes Datenschutzniveau?

- Fehlende Garantien durch innerstaatliche Rechtsvorschriften oder internationale Verpflichtungen

- Verletzungen von Art. 7 und 47 der Grundrechtecharta

- Kritik der Art. 29-Datenschutzgruppe: (mangelhafte Zweckbindung, fehlende Rechtsgrundlagen für eine Weiterverarbeitung personenbezogener Daten, keine klaren Speicherbegrenzungen, nicht ausreichender Streitbeilegungsmechanismus, fehlende Unabhängigkeit des Ombudsmannes)

1. Datentransfer in die USA

1.3 Angemessenes Datenschutzniveau?

Die Gewährleistung eines angemessenen bzw. gleichwertigen Datenschutzniveaus durch den Privacy Shield unterliegt hohen Bedenken.

Es ist wahrscheinlich, dass etwa im Zusammenhang mit Beschwerden von Einzelpersonen auch die Adäquanzentscheidung zum Privacy Shield mittelfristig vom EuGH überprüft wird.

2. Datentransfer in andere Drittstaaten

2.1 Vorgaben des EuGH

Die Ausführungen des EuGH zur Verletzung von Art. 7 und 47 der Grundrechtecharta müssen auch beim Transfer personenbezogener Daten in andere Drittstaaten berücksichtigt werden.

Dies kann sich auf weitere Adäquanzentscheidungen auswirken, welche von der Kommission für andere Länder bereits getroffen wurden.

Wesentliche Kriterien bleiben (EuGH, Urt. v. 06.10.2015, C 362/14, Rz. 93-95) demnach

- die Begrenzung des Zugangs/der Nutzung personenbezogener Daten nur zu bestimmten, strikt begrenzten Zwecken,
- kein genereller Zugriff auf den Inhalt elektronischer Kommunikation auf Basis innerstaatlicher Vorschriften,
- wirksamer gerichtlicher Rechtsschutz und
- die Berechtigung eines Zugangs sowie eines Berichtigungs- und Löschrechts für Betroffene.

2. Datentransfer in andere Drittstaaten

2.2 Beispiele: China und Indien

a) Indien

- **Information Technology Act 2000/Amendment 2008** - Geltung im gesamten indischen Staat (Bei rechtswidriger Veröffentlichung personenbezogener Daten können Schadensersatzpflichten entstehen. Verstöße können auch durch nicht-indische Staatsbürger geltend gemacht werden.)
- **Information Technology Rules 2011** – Verstöße können nur durch indische Staatsbürger geltend gemacht werden und erfassen nur besonders sensible Informationen (etwa Zugangsdaten für Online-Banking und Daten ähnlich dem Katalog des § 3 Abs. 9 BDSG). Vorgesehen ist zudem nur, dass die Unternehmen eine Privacy Policy veröffentlichen müssen.
- Ein Recht auf Löschung ist nicht bekannt.

2. Datentransfer in andere Drittstaaten

2.2 Beispiele: China und Indien

a) China

- **Verbraucherschutzgesetz 1994** (Schutz des Rechts am eigenen Bild, des Namens und anderer personenbezogener Daten; keine Rechte auf Auskunft, Berichtigung oder Löschung der Daten)
- **Entscheidung des Ständigen Ausschusses des Nationalen Volkskongresses 2012** (Stärkung des Online-Datenschutzes; Nutzer sind bei Online-Plattformen zur Registrierung mit Klarnamen verpflichtet.)
- **Leitlinie zum Schutz personenbezogener Daten in öffentlichen und kommerziellen Systemen 2012** (Charakter einer unverbindlichen Richtlinie; Unternehmen können die geregelten Grundsätze als Selbstverpflichtung etablieren;
- Keine datenschutzrechtlichen Regelungen mit **Betroffenenrechten** erkennbar.

3. Alternativen?

3.1 Technische Lösungsansätze?

a) Verschlüsselung (Stichwörter: Transportverschlüsselung, Verschlüsselung von Inhalten, Notwendigkeit der Entschlüsselung)

b) Pseudonymisierung

c) Protokollierung

- Protokolldaten müssen darüber Auskunft geben können, **wer wann welche personenbezogenen Daten in welcher Weise** verarbeitet hat.
- Protokolldaten dürfen **nicht nachträglich verändert** werden können und **nur Berechtigten** zugänglich sein.
- Die Nutzung administrativer Rechte muss zu einem Protokolleintrag führen.
- Protokolldaten müssen Auskunft geben zu: Zeitpunkt einer Tätigkeit/eines Ereignisses, Bezeichnung von Tätigkeit/Ereignis, mit Tätigkeit/Ereignis befasste Person bzw. Systemkomponente, Zweck der Tätigkeit
- **Aufbewahrungsdauer** von Protokollen muss definiert werden.

3. Alternativen?

3.2 Standardvertragsklauseln?

Beispiel: 2010/87/EU

BESCHLUSS DER KOMMISSION

vom 5. Februar 2010

über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates

(Bekannt gegeben unter Aktenzeichen K(2010) 593)

(Text von Bedeutung für den EWR)

(2010/87/EU)

3. Alternativen?

3.2 Standardvertragsklauseln?

Beispiel: 2010/87/EU

Klausel 5: Garantie des Datenimporteurs, dass er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen

Berechtigungen des Datenexporteurs bei Verstößen:
-**Aussetzung der Datenübermittlung / Rücktritt vom Vertrag**

3. Alternativen?

3.2 Standardvertragsklauseln?

Beispiel: 2010/87/EU

Artikel 4

(1) Unbeschadet ihrer Befugnisse, tätig zu werden, um die Einhaltung nationaler Vorschriften gemäß den Kapiteln II, III, V und VI der Richtlinie 95/46/EG zu gewährleisten, können die zuständigen Kontrollstellen in den Mitgliedstaaten ihre Befugnisse ausüben und zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung in Drittländer verbieten oder aussetzen, wenn

a) feststeht, dass der Datenimporteur oder Unterauftragsverarbeiter nach den für ihn geltenden Rechtsvorschriften Anforderungen unterliegt, die ihn zwingen, vom anwendbaren Datenschutzrecht in einem Maß abzuweichen, das über die Beschränkungen hinausgeht, die im Sinne von Artikel 13 der Richtlinie 95/46/EG für eine demokratische Gesellschaft erforderlich sind, und dass sich diese Anforderungen wahrscheinlich sehr nachteilig auf die Garantien auswirken würden, die das anwendbare Datenschutzrecht und die Standardvertragsklauseln bieten,

3. Alternativen?

3.2 Standardvertragsklauseln?

Die irische Datenschutzbehörde hat eine gerichtliche Prüfung der Standardvertragsklauseln veranlasst.

Mit hoher Wahrscheinlichkeit wird auch der EuGH im Fortgang des Verfahrens über die Anwendbarkeit der Standardvertragsklauseln entscheiden.

3. Alternativen?

3.3 Datenverarbeitung in Europa?

Fall:

Ein Bezirksgericht in New York erließ einen Durchsuchungsbeschluss, welcher Microsoft verpflichtete, E-Mails herauszugeben, die auf einem Server in Irland gespeichert sind. Grundlage war der Stored Communications Act.

Das Bundesberufungsgericht in New York hat die entsprechende Entscheidung aus dem Jahre 2014 zwischenzeitlich aufgehoben. Mircosoft ist demnach nicht verpflichtet, die E-Mails herauszugeben.

3. Alternativen?

Fazit:

- Die Adäquanzentscheidung zum Privacy Shield könnte kurz- oder mittelfristig Gegenstand einer gerichtlichen Prüfung durch den EuGH sein.

- Die Anwendbarkeit der Standardvertragsklauseln wird mit großer Wahrscheinlichkeit vom EuGH geprüft werden.

- Eine Datenverarbeitung in Europa sollte in Erwägung gezogen werden.

Vielen Dank für Ihre Aufmerksamkeit!