HÄRTING

PRIVACY SHIELD – PRAXISFOLGEN FÜR DEN DATENTRANSFER IN DER CLOUD NACH SAFE HARBOR

RA Daniel Schätzle | Berlin, 7. April 2016

SIBB e.V. | Forum Law, Tax & Compliance und Forum Cloud Computing

SIBB
ICT & Digital Business Association
Berlin – Brandenburg

PROGRAMM

- Begrüßung
- Rechtliche Hintergründe, Entwicklungen und Auswirkungen

  Daniel Schätzle (HÄRTING Rechtsanwälte)
- Perspektiven des transatlantischen Datenraumes – Herausforderungen für deutsche Unternehmen

  Ansgar Baums (HP)
- Warum uns Safe Harbor und Privacy Shield nicht interessieren muss

  Philipp Schmolling (YUNICON)
- Diskussion
- Ausklang

Rechtliche Hintergründe, Entwicklungen und Auswirkungen

Worum geht es eigentlich?

PROBLEM: DATENÜBERMITTLUNG IN DIE USA

- Datenschutzrecht: Verbotsprinzip
- Übermittlung von personenbezogenen Daten ins Ausland bedarf zusätzlich einer gesonderten Rechtfertigung
- unproblematisch für
  - Europäische Union und EWR, § 4b Abs. 1 BDSG
  - Drittländer mit angemessenem Datenschutzniveau (z.B. Argentinien, Kanada, Israel, Uruguay und Schweiz)
- USA ist unsicheres Drittland
  - § 4b Abs. 2 BDSG: Datenübermittlung muss unterbleiben, es sei denn angemessenes Schutzniveau
  - Safe Harbor simuliert angemessenes Datenschutzniveau

r9 Wobei bei all diesen Ländern die Einstufung auf feststellenden Entscheidungen der EU-Kommission beruht, die im Lichte der Safe Harbor-Entscheidung zum Teil ebenso angreifbar sein könnten. Insbesondere im Fall von Kanada, wenn man auf Geheimdienstaktivitäten ("Five Eyes") abstellt.
referendare; 06.04.2016

SAFE-HARBOR-ENTSCHEIDUNG DER KOMMISSION

- EU Kommission entschied im Jahre 2000, dass das Datenschutzniveau in den USA ausreichend ist, wenn sich der Dienstleister zur Einhaltung der Safe Harbor Datenschutzkriterien verpflichtet
- Safe Harbor Zertifikat genügte für Compliance des jeweiligen Unternehmens
- Datenschutzbehörden verlangten seit den NSA-Enthüllungen zusätzliche Prüfungen durch die deutschen Auftraggeber (z.B. Prüfung der Privacy Policy des Dienstleisters)
- Kommission entschied sich gegen Aussetzung
- 13 Empfehlungen an die USA zur Optimierung in 11/2013
- Verhandlungen über ein Nachfolgeabkommen

EuGH-Urteil

Was wurde genau entschieden?

EUGH ERKLÄRT SAFE HARBOR FÜR UNGÜLTIG

- Ursprung des Streits in Irland
- Max Schrems verlangte von Facebook Unterlassen der Weitergabe von Daten in die USA und Facebook weigerte sich
- Die angerufene irische Datenschutzbehörde sah sich durch Safe Harbor Entscheidung der Kommission an Untersuchung gehindert
- EuGH hat entschieden, dass die
  - Datenschutzbehörden die Angemessenheit des Schutzniveaus überprüfen dürfen
  - Safe-Harbor-Entscheidung der Kommission ungültig ist

BEGRÜNDUNG DES EUGH-URTEILS

- EU-Kommission habe keine derart weitreichenden Befugnisse, nationalen Aufsichtsbehörden eine Untersagung von Datenschutztransfers zu verbieten
- Keine Untersuchung, inwieweit tatsächlich ein angemessenes Datenschutzniveau in den USA gewährleistet werden kann
- Keine Untersuchung, inwieweit Grundrechtseingriffe auf ein absolut erforderliches Maß begrenzt werden
- Zu weit reichende Ausnahmen
- Vereinbarungen über Safe-Harbor mit den USA schließen einen Zugriff staatlicher Behörden (z.B. NSA) nicht aus
- Gegen Eingriffe in die Rechte von Bürgern seien keine Rechtsbehelfe gegeben

r5

r5 Genauer hat der EuGH gesagt, die Kommission kann nicht verhindern, dass die Aufsichtsbehörden prüfen (Rn. 66 des Urteils).

Die Untersagung von Datentransfers wäre den Behörden wohl weiterhin nicht möglich, wenn es ein neues Abkommen gibt, da dieses zunächst gültig wäre und die Aufsichtsbehörden dieses nicht direkt verwerfen könnten (Rn. 62). Dafür müssten sie sich zunächst wieder an den EuGH wenden.

referendare; 06.04.2016

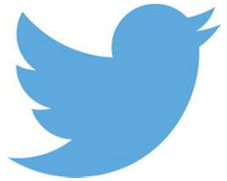
Folgen des Urteils
Wer ist davon betroffen?

UNMITTELBARE FOLGEN

- Safe-Harbor-Entscheidungen der Kommission sind ungültig
- Übermittlung von personenbezogenen Daten in die USA ist illegal, soweit allein auf Safe Harbor gestützt
- Übermittlung meint sowohl die echte Weitergabe als auch die Gewährung von Zugriff auf personenbezogene Daten
- Theoretisch: Bußgelder bis zu 300.000,- Euro drohen
- Betroffen sind sowohl der deutsche Datenexporteur als auch der U.S.-Datenimporteur

Immer dann, wenn ein US-Dienstleister genutzt wird, der auf personenbezogene Daten zugreifen kann.

WER IST BETROFFEN



Alternativen
Welche Möglichkeiten gibt es?

r10

r10 Als weitere Alternative kämen Garantien nach § 4c II BDSG in Betracht, wobei das wegen des Genehmigungserfordernisses natürlich aufwändig ist.

referendare; 06.04.2016

NUTZUNG VON ANBIETERN INNERHALB DER EU

- Wechsel zu Anbieter in Deutschland/EU/EWR
- Wechsel zu Anbieter in einem sicheren Drittland
- U.S.-Anbieter gründet EU-Gesellschaft
- Anforderungen an eine Datenübermittlung im Inland müssen erfüllt sein:
  - Verbotsprinzip mit Erlaubnisvorbehalt
  - Einwilligung oder
  - Gesetzlicher Erlaubnistatbestand

AUSNAHMEN FÜR BESTIMMTE FÄLLE

- Einwilligung rechtfertigt Datenübermittlung auch in unsicheres Drittland, § 4c Abs. 1 Nr. 1 BDSG
  - Anforderungen an Einwilligung sind hoch
  - ULD: Zweifelhaft, ob überhaupt in die anlasslose Massenüberwachung durch Geheimdienste eingewilligt werden kann
- Zur Vertragserfüllung notwendige Datenübermittlungen
  - Bspw. Hotelbuchung

INDIVIDUALLÖSUNG

- Abschluss eines individuellen Vertrages
  - Verpflichtung, die wesentlichen Bestimmungen dt. Deutschen Datenschutzrechtes einzuhalten
  - Abgaben entsprechender Garantien
- Verbindliche Unternehmensregelungen
  - Binding Corporate Rules
  - Interne Datenschutzvorschriften für den internationalen Datentransfer innerhalb einer Gruppe
- Genehmigung durch Aufsichtsbehörde erforderlich
- Genehmigungen sollen derzeit jedoch grundsätzlich nicht erteilt werden

STANDARDVERTRAGSKLAUSELN

- Entscheidungen der EU-Kommission über Standardvertragsklauseln
- Unternehmen, mit denen EU-Standardvertragsklauseln („Model Clauses“) vereinbart werden, haben angemessenes Schutzniveau
- eine Art Safe Harbor im Einzelfall
- Keine Genehmigung der Aufsichtsbehörde erforderlich
- Privilegierung gilt nur, wenn die Klauseln unterschiedslos übernommen werden
- 3 Versionen:
  - Standardvertragsklauseln 2001
  - Standardvertragsklauseln 2004
  - Standardvertragsklauseln für die Übermittlung an Auftragsdatenverarbeiter

STANDARDVERTRAGSKLAUSELN

- ULD:
  - In Konsequenz aus dem EuGH-Urteil können diese nicht mehr zulässig eingesetzt werden
- Art. 29-Gruppe
  - Bis zu einer abschließenden Detailprüfung weiterhin einsetzbar, aber DSB können im Einzelfall prüfen
- Dt. DSB
  - Ähnlich wie Art. 29-Gruppe, teilw. wird seit Februar geprüft
  - Verantwortung des Datenexporteuers wird betont
- EU-Kommission
  - Weiterhin einsetzbar
  - DSB können Entscheidung der Kommission lediglich auf Rechtmäßigkeit prüfen und ggf. den Rechtsweg bestreiten
  - Verantwortung des Datenexporteuers wird betont
- Bundesregierung
  - Weiterhin einsetzbar

STANDARDVERTRAGSKLAUSELN

- Weitgehende Einigkeit dahingehend, dass eine Überprüfung der Standardvertragsklausel an den Maßstäben des EuGH-Urteils, zu deren Unwirksamkeit führen würde
- Hier bedarf es jedoch einer Entscheidung des EuGH
- Aufsichtsbehörden können allenfalls im Einzelfall eine Datenübermittlung untersagen, wobei die genauen Möglichkeiten umstritten sind
- Fazit:
  - Standardvertragsklauseln stellen derzeit die einzig praxistaugliche Rechtfertigungsmöglichkeit für einen Datentransfer in die USA dar
  - Unterzeichnung ist nicht ausreichend
  - Regelungen müssen auch eingehalten werden
  - Ggf. Umsetzung besonderer Maßnahmen, um ein angemessenes Datenschutzniveau zu gewährleisten
  - Ansonsten droht eine (berechtigte/unberechtigte?) Untersagungsverfügung

Der Nachfolger:
EU-US Privacy Shield

SAFE HARBOR WIRD PRIVACY SHIELD

- Verhandlungen zu Nachfolgeabkommen wurde nach EuGH-Urteil vorangetrieben
- Am 2.2.2016 wurde eine Einigung verkündet
- Einzelheiten wurden am 29.2. mit dem Entwurf einer neuen Angemessenheitsentscheidung der EU-Kommission veröffentlicht
- Abkommen muss erst noch umgesetzt werden
- Judicial Redress Act für Klagerecht von EU-Bürgern wurde bereits unterzeichnet
- Anhörungen stehen noch aus
- Verabschiedung der Kommissionsentscheidung steht noch aus

EU-US PRIVACY SHIELD: INHALTE

- Verpflichtung zur Einhaltung von EU-Datenverarbeitungsstandards durch US-Unternehmen
- Strengere Kontrolle der zertifizierten Unternehmen
- Schriftliche Zusicherungen der US-Regierung (u.a. Beschränkungen für den Datenzugriff durch Behörden)
- Mehr Rechtsschutzmöglichkeiten für EU-Bürger: Judicial Redress Act, neuer Ombudsmann und alternative Streitbeilegung
- Beschwerdemöglichkeiten für EU-Aufsichtsbehörden
- Jährliche Überprüfung des neuen Abkommens

EU-US PRIVACY SHIELD: KONSEQUENZEN

- EU-Unternehmen sollten (wenn es soweit ist)
  - Prüfen, ob ein US-Unternehmen tatsächlich (noch) auf der Privacy-Shield-Liste des US-Handelsministeriums steht
  - Nachvollziehen, ob ein US-Unternehmen tatsächlich seinen Verpflichtungen nachkommt, z.B.:
    - Informationspflichten (z.B. Veröffentlichung von Datenschutzbestimmungen)
    - Beachtung von Betroffenenrechten (z.B. entsprechende Beschwerden eigener Kunden ernst nehmen)
    - Beschränkung von Datenweitergaben (z.B. Abschluss entsprechender Verträge)
    - Beachtung von Datenschutzprinzipien wie Zweckbindung (z.B. Datenverarbeitung nur zu den vorgesehenen Zwecken)
    - Einrichtung von Maßnahmen zur Datensicherheit (z.B. Abfrage von Zertifikaten)
- Bis dahin Standardvertragsklauseln
- Diskussionen verfolgen

EU-US PRIVACY SHIELD: KRITIK

- Es bleibt bei dem Modell Selbstzertifizierung
- Halten die Garantien für den Datenschutz auch nach den US-Wahlen im November?
- Die Geheimdienstaktivitäten an sich ändern sich nicht
- Auch der Vorrang von US-Regelungen zur Gewährleistung der nationalen Sicherheit ist nicht völlig ausgeschlossen
- Die Einigung basiert auf bloßen Zusicherungen, deren rechtliche Bindung fraglich ist
- Formulierungen sind vage und lassen Interpretationsspielräume

- Ankündigung der Art-29 Gruppe bereits am 3.2.2016, die Einzelheiten zu prüfen
- Heute: Stellungnahme der dt. DSB „zahlreiche Fragen offen“

EU-US PRIVACY SHIELD: PERSPEKTIVEN

- Ein Verfahren vor dem EuGH zur Prüfung der Gültigkeit des Privacy Shield ist zu erwarten
- Abzuwarten ist auch, wie konsequent Mechanismen zu Kontrolle, Sanktionierung und Rechtsschutz umgesetzt werden
- Jährliche Überprüfung führt zu Rechtsunsicherheit, da eine Aussetzung möglich ist
- Unklar, was die DS-GVO für das Privacy Shield bedeutet
  - Zunächst ist vorgesehen, dass die Angemessenheitsentscheidung bestehen bleibt
  - Da die Anforderungen an ein angemessenes Datenschutzniveau unter der DS-GVO jedoch deutlich strenger sind, wäre eine neue Angemessenheitsentscheidung konsequent

Ausblick DS-GVO

EU-DATENSCHUTZGRUNDVERORDNUNG

- Abschließender Entwurf liegt seit heute in dt. Sprachfassung vor
- Inkrafttreten Mitte 2018
- Standardvertragsklauseln und BCR werden auch weiterhin vorgesehen sein, ebenso wie die Möglichkeit einer individualvertraglichen Regelung
- Möglichkeit der Zertifizierung von Unternehmen aus Drittländern auf die Standards des EU-Datenschutzrechtes
- Genehmigte Verhaltensregeln von Verbänden, denen sich US-Unternehmen unterwerfen können
- Sonderregelungen für risikoarme Übermittlungen im Einzelfall
  - Instrumente sind lediglich angelegt und bedürfen oftmals noch zu entwickelnder Details
  - Instrumente können etwaige grundsätzliche Bedenken zum US-Datenschutzniveau nicht beseitigen

FAQ Safe Harbor

haerting.de/neuigkeit/faq-safe-harbor

HÄRTING

Daniel Schätzle

Rechtsanwalt

@dschaetzle

HÄRTING Rechtsanwälte

Chausseestraße 13, 10115 Berlin

Tel. +49 30 28 30 57 40

Fax. +49 30 28 30 57 44

www.haerting.de