Transatlantischer Datenverkehr … wie geht es nach der Kritik am Entwurf der Privacy Shield-Entscheidung weiter?

Erich Schweighofer

Prof. Mag. Dr. Dr.

https://intlaw.univie.ac.at
https://rechtsinformatik.univie.ac.at

Arbeitsgruppe Rechtsinformatik
universität wien ARI
Centre for Computers and Law

universität wien

Inhaltsverzeichnis

Typisierung der Daten und Datenzugriffe (1)

- Datenarten – grober Konsens, Unterschiede im Detail
  - Personenbezogene Daten: „… alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; …“ (Art. 4 Z. 1 DSGVO)
  - Pseudonymisierte Daten: „… die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, …“ (Art. 4 Z. 5 DSGVO)
  - Sensible Daten: Verarbeitung unterliegt besonderen Vorschriften; Spezfikation durch Mitgliedstaaten (Präambel Abs. 10 DSGVO)
- Verarbeiten: transatlantischer Dissens
  - EU: „… jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; … (Art. 4 Z. 2 DSGVO)

Typisierung der Datenarten und Zugriffe (2)

  - USA (vereinfachende Darstellung unter Verwendung der EU Definition): „ … das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; …“
- Zugriffe auf EU-Daten
  - Mit Privacy Shield (früher: Safe Harbor)
    - Beachtung der EU-Datenschutzgrundsätze
    - Keine unberechtigte Weitergabe bzw. zweckwidrige Nutzung der Daten
  - Ohne Privacy Shield
    - Zustimmung
    - Standardsvertragsklauseln
    - Binding Corporate Rules
    - Genehmigung nationaler Datenschutzbehörden

Typisierung der Datenarten und Zugriffe (3)

- Polizei- und Sicherheitsbehörden
  - Territoriale Souveränität bzw. Interpol (+ Vertragsnetzwerk)
  - Zweck der Verbrechensbekämpfung bzw. Risikoabwehr genügt
- Nachrichten- und Geheimdienste
  - Zunehmende staatliche Regulierung; Tätigkeit jenseits der Grenzen bleibt weitgehend im rechtsfreien Raum bzw. ist illegal („Open Skies“ vs. „Illegals“)
  - Zweck des Schutzes nationaler Sicherheitsinteressen genügt, nach US-Praxis auch für Vorratsdatenspeicherung und Massenüberwachung

Datentransfer mit Privacy Shield

- Art. 1 Abs. 2 Entwurf Privacy Shield-Verordnung, Annex II – Privacy Principles etc.
- Selbstverpflichtung ist erforderlich – Aufnahme in die „Privacy Shield List“
- Rechtsschutz durch Federal Trade Commission (FTC) bzw. Ombudsmann

- Risiko des Eingriffs der Datenschutzbehörde bzw. des EuGH
  - Art. 3 Entwurf Privacy Shield-Verordnung – Suspendierung oder Verbot des Datentransfers gem. Art. 28 Abs. 3 Datenschutzrichtlinie durch die zuständige Datenschutzbehörde
  - Aufhebung der Privacy Shield-Verordnung durch EuGH (Datenschutzaktivisten scharren bereits in den Löchern)

Datentransfer mit Standardvertragsklauseln

- Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2001/497/EG) bzw. Alternative Standardvertragsklauseln (2004/915/EG)
- Standardvertragsklauseln für die Weitergabe personenbezogener Daten an Auftragsverarbeiter in Drittländern (2010/87/EG)
- Bessere Absicherung der Datenschutzgrundsätze und der Nichtweitergabe der Daten

- Vorteil der weiteren Zusicherung hinsichtlich des derzeitigen Datenzugriffs der US-Behörden
  - Der Datenimporteur muss gegenüber dem europäischen Datenexporteur garantieren, dass keine Gesetze ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen.
  - Ob er das zusichern kann, hängt von der Effektivität des amerikanischen Rechtsschutz ab; dies wird derzeit stark angezweifelt.
  - Eine Untersagung des Datenverkehrs durch Datenschutzbehörden ist bei Standardtransaktionen schwer begründbar.

Datentransfer mit Binding Corporate Rules (BCN) (1)

- Datentransfer innerhalb von Transnationalen (Multinationalen) Unternehmen
- Beachtung der Prinzipien des Datenschutzes
- Maßnahmen zur Durchsetzung und Verbindlichkeit der Regeln
- Haftungsregeln
- Details zu Übermittlungsvorgängen

- Arbeitsdokumente der Artikel 29-Gruppe

- Vorteil der weiteren Zusicherung hinsichtlich des derzeitigen Datenzugriffs der US-Behörden:
  - Der Datenimporteur muss gegenüber dem europäischen Datenexporteur garantieren, dass keine Gesetze ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen.

Datentransfer mit Binding Corporate Rules (BCN) (2)

- Nach der amerikanischen Praxis des Zugriffs auf alle Einheiten eines in den USA ansässigen Konzerns ist diese Zusicherung anzuzweifeln.
- Ein Fall einer gerichtlichen Abwägung zwischen einem „National Security Letter“ und BCN ist noch nicht bekannt.
- Eine Untersagung des Datenverkehrs durch Datenschutzbehörden ist bei Zugriff der US-Behörden auf alle Daten des Konzerns wahrscheinlich.

- Langes Genehmigungsverfahren
  - Zuständigkeit der «Zentralen Datenschutzbehörde»
  - System der gegenseitigen Anerkennung mit 19 Mitgliedsstaaten
  - Stellungnahme der anderen Mitgliedsstaaten erforderlich

Problem des Datenzugriffs staatlicher Behörden für Zwecke der Verbrechensbekämpfung, Gefahrenabwehr und nationalen Sicherheit (1)

- Völkerrechtlicher Grundsatz, abgeleitet aus der staatlichen Souveränität auf dem jeweiligen Territorium; bestätigt durch eine Vielzahl internationaler Abkommen
- Sonderregeln für Datennutzung und Datenschutz, z.B. Interpol
- EuGH Rs. Schrems, C-362/14, 6.10.2015
  - Rz 94: „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 (vgl. in diesem Sinne Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 39).“

Problem des Datenzugriffs staatlicher Behörden für Zwecke der Verbrechensbekämpfung, Gefahrenabwehr und nationalen Sicherheit (2)

- Rz 95: „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.“
- Prinzipien für Datenzugriff von Sicherheitsbehörden
- Rechtliche Determinierung der Eingriffsbefugnisse mit Beachtung des Verhältnismäßigkeitsgebots
- Ausreichender Rechtsschutz
- Problem anlasslose Massenüberwachung: Nach dem EuGH bzw. EGMR ist diese immer unzulässig, weil sie in den Wesensgehalt von Art. 7 EU-Grundrechtscharta bzw. Art. 8 EGMR eingreift.

Problem des Datenzugriffs staatlicher Behörden für Zwecke der Verbrechensbekämpfung, Gefahrenabwehr und nationalen Sicherheit (3)

- Verbrechensverhütung: ja, aber Verhältnismäßigkeitsgrundsatz
- Gefahrenabwehr: ja (?), aber strenger Verhältnismäßigkeitsgrundsatz
- Überwachung wegen Gefährdung nationaler Sicherheit: eher nein (?), weil ausreichende gesetzliche Determinierung und Rechtsschutzerfordernisse schwerlich zu erbringen sind
- Explizite Zustimmung zu Zugriffsrisiko in Drittstaat: eher ja bei bloß möglichen Zugriffen, eher nein bei realen Zugriffen (Datenimporteur hat „Praxis“)
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): nicht möglich, weil Einwilligung unzulässig ist, wenn Wesensgehalt von Art. 7 EU Grundrechtecharta verletzt wird; Sittenwidrigkeit nach § 138 BGB

Beschluss der Privacy Shield-Entscheidung ?

- Art. 29-Gruppe (Leiter der Datenschutzbehörden der EU-Mitgliedstaaten) Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 13.04.2016 + Europäischer Datenschutzbeauftragter Opinion 4/2016, 30.05.2016
  - Anerkennung der Verbesserung der US-Regulierung hinsichtlich des Zugriffs von Polizei- und Sicherheitsbehörden bzw. Nachrichten- und Geheimdiensten auf Daten
  - Der Entwurf der Privacy Shield-Verordnung ist eine Verbesserung, aber beinhaltet nicht alle wesentlichen Rechtsschutzgarantien (Notwendigkeit, Verhältnismäßigkeit, unabhängiger Rechtsschutz etc.)
  - Selbstregulierungsprinzip wird in Frage gestellt
  - Nachverhandlung erforderlich
  - US-Gesetz wird für „wesentliche Gleichwertigkeit“ mittelfristig eingefordert
  - Keine Anpassung an EU-Datenschutzgrundverordnung; Auftraggebern kann nicht zugemutet werden, dass sich schon 2018 die Regeln wieder ändern.
- Europäisches Parlament
  - Entwurf ist unzureichend; Nachverhandlung eingefordert
  - Es ist daher fraglich, ob die Kommission den Entwurf schon im Juni 2016 beschließen wird.

Schlussfolgerungen (1)

- Der Entwurf der Privacy Shield-Verordnung bringt wesentliche Verbesserungen bei Rechten europäischer Datensubjekte, ist aber noch ungenügend und sollte weiter verhandelt werden.
- Spätestens 2018 müsste eine dann geltenden Privacy Shield-Verordnung an die dann in Kraft tretendende Datenschutzgrundverordnung angepasst werden.
- Das Europäische Parlament, die Datenschutzbehörden sowie die Datenschutzaktivisten sind mit dem Entwurf unzufrieden.
- Es ist fraglich, ob die Europäische Kommission den Entwurf bis Ende Juni 2016 beschließen wird.
- Die Lage europäischer Datenexporteure bleibt schwierig; diese bleiben gefangen zwischen den Notwendigkeiten des Datenaustausches und der nunmehrigen Rechtswidrigkeit vieler Datentransfers.
- Eine (informelle) Kooperation mit der zuständigen Datenschutzbehörde ist entscheidend, um plötzliche Suspendierungen bzw. Untersagungen zu vermeiden. Die Datenschutzbehörde hat einen Ermessensspielraum, sie kann abwartend, pragmatisch oder auch offensiv agieren.

Schlussfolgerungen (2)

- Nur das Instrument der Vertragserfüllung erscheint unproblematisch; bei allen anderen Instrumenten – Zustimmung, Standardvertragsklauseln, Binding Corporate Rules – müsste die Regelung des Datenzugriffs US-staatlicher Behörden als europäischen Grundsätzen entsprechend angesehen werden. Dies ist aber derzeit nicht der Fall. Es ist aber auch richtig, dass die EU-Mitgliedstaaten sich nicht immer an die Grundsätze des EuGH bzw. EGMR halten und die EU hier keine Kompetenz hat.
- Eine vertragliche Lösung bzw. BCN werden empfohlen, weil diese die Rechtsrisiken minimieren und die gute Praxis des Datenschutzes fördern.

Merci für Ihre Aufmerksamkeit!

Erich Schweighofer

Universität Wien

Arbeitsgruppe Rechtsinformatik

Wiener Zentrum für Rechtsinformatik

erich.schweighofer@univie.ac.at

http://rechtsinformatik.univie.ac.at

Jusletter IT

http://www.jusletter-it.eu

Fragen sind sehr willkommen!

- **Fachtagung Verwaltungsinformatik und Rechtsinformatik, 22.-23. September 2016, Dresden, DE; www.ftvi.de**

- **INFORMATIK2016, 26.-30.9.2016, Klagenfurt, AT; http://www.informatik2016.de/**
  - **Workshop Datenschutz, 27.9.2016**
  - **Workshop Risikomodelle, 30.9.2016**

- **IRIS2017, 23.-25. Februar 2017, Salzburg, AT; www.univie.ac.at/RI/IRIS17**