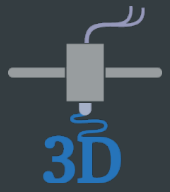


Was ist noch sicher? & Bird & Bird

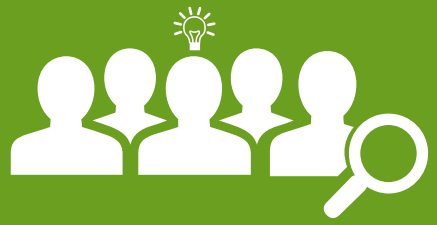
Das Urteil des EUGH zu Safe Harbor und seine Auswirkungen auf Cloud-Angebote

Dr. Fabian Niemann
Bird & Bird LLP

7. IT LawCamp 2016
03. Juni 2016, Frankfurt am Main

Inhaltsverzeichnis

EUGH "Schrems", C-362/14 v. 6. 10. 2015



Der Sachverhalt

- Ausgangsgericht: *High Court of Ireland* ("**High Court**")
- Parteien: Österreicher *Maximilian Schrems* gegen den irischen Datenschutzbeauftragten (*Irish Data Protection Commissioner* – "**Commissioner**")
- Streitgegenstand:
  - Schrems: Beschwerde bei dem Commissioner - Weitergabe von Daten durch Facebook Ireland an Facebook US sei rechtswidrig, insb. da Safe Harbor keinen ausreichend Schutz (mehr) herstelle
  - Commissioner: keine Prüfungskompetenz, da er an die Safe Harbor Entscheidung der EU Kommission gebunden sei
  - High Court: Zweifel an Safe Harbor geäußert, aber Frage europäischen Rechts, daher Vorlage an EUGH

Der Sachverhalt

Vorlagefragen:

1. Ist ein unabhängiger Amtsträger [Commissioner], der von Rechts wegen mit der Handhabung und der Durchsetzung von Rechtsvorschriften über den Datenschutz betraut ist, bei der Prüfung einer bei ihm eingelegten Beschwerde, dass personenbezogene Daten in ein Drittland (im vorliegenden Fall in die Vereinigten Staaten von Amerika) übermittelt würden, dessen Recht und Praxis keinen angemessenen Schutz der Betroffenen gewährleisteten, im Hinblick auf die Art. 7, 8 und 47 der Charta, unbeschadet der Bestimmungen von Art. 25 Abs. 6 der Richtlinie 95/46, absolut an die in der Entscheidung 2000/520 enthaltene gegenteilige Feststellung der Union gebunden?
2. Oder kann und/oder muss der Amtsträger stattdessen im Licht tatsächlicher Entwicklungen, die seit der erstmaligen Veröffentlichung der Entscheidung der Kommission eingetreten sind, eigene Ermittlungen in dieser Sache anstellen?

Der Sachverhalt

Mit anderen Worten:

- Vorlagegegenstand war, ob die Ansicht des Commissioners, dass er an die Safe Harbor Entscheidung 2000/520 gebunden ist, richtig ist oder ob er eigene Ermittlungen anstellen kann oder sogar muss?
- Die Vorlagefragen beschäftigten sich mithin mit Kompetenzfragen.
- Nicht Gegenstand war eigentlich die Frage der Wirksamkeit der Safe Harbor Entscheidung als solche; erst recht nicht die von Transfers in die USA oder unsichere Drittstaaten im Allgemeinen.

Das Urteil

Tenor:

1. Art. 25 Abs. 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr in der durch die Verordnung (EG) Nr. 1882/2003 des Europäischen Parlaments und des Rates vom 29. September 2003 geänderten Fassung ist im Licht der Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass eine aufgrund dieser Bestimmung ergangene Entscheidung wie die Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46 über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, in der die Europäische Kommission feststellt, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, eine Kontrollstelle eines Mitgliedstaats im Sinne von Art. 28 der Richtlinie in geänderter Fassung **nicht daran hindert, die Eingabe einer Person zu prüfen**, die sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten, die aus einem Mitgliedstaat in dieses Drittland übermittelt wurden, bezieht, wenn diese Person geltend macht, dass das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleisteten.
2. Die Entscheidung **2000/520 ist ungültig**.

Das Urteil

Tenor (vollständig und in Deutsch):

1. Die zuständigen Datenschutzbehörden können individuelle Beschwerden prüfen, auch wenn sie sich auf Übermittlungen in Drittländer beziehen, die von der EU Kommission grundsätzlich als sicher eingestuft wurden (wie Safe Harbor). [Für nichtig erklären können Sie diese aber nicht; dies kann nur der EUGH.]
2. Die Safe Harbor Entscheidung **2000/520 ist ungültig**.

Die Gründe – Prüfungskompetenz

Punkt 1 – Prüfung durch Datenschutzbehörden, vorliegend der Commissioner:

- Datenschutz ist "hohes Gut" (Grundrecht/EU Charta)
- Datenschutzbehörden als unabhängige Kontrollstellen (zwar beschränkt auf eigenes Territorium, aber Übermittlung erfolgt lokal und ist nur rechtmäßig in Einklang mit Datenschutz-Richtlinie und EU Charta)
- Individuen benötigen effektiven Rechtsschutz; sie müssen Datenschutzbehörden auch im Rahmen von Transfers basierend auf Safe Harbor anrufen können
- Entsprechend Prüfungskompetenz, aber keine Aufhebungskompetenz der Datenschutzbehörden

Die Gründe – Prüfungskompetenz (2)

Verfahren bei Zweifeln:

- Bei Zweifeln an der Rechtmäßigkeit von Kommissionsentscheidungen können Datenschutz-behörden und Betroffene nationale Gerichte anrufen
- Gerichte müssen prüfen; haben sie Zweifel an der Rechtmäßigkeit, müssen sie EUGH vorlegen
- Rechtsakte der EU (wie die Safe Harbor Entscheidung) kann nur der EUGH aufheben; es gilt die "*Vermutung der Rechtmäßigkeit*" von Rechtsakten der EU, die nur der EUGH entkräften kann; auch aus Gründen der einheitlichen Rechtsanwendung

Die Gründe – Safe Harbor

Punkt 2 – Safe Harbor: Warum überhaupt Verfahrensgegenstand?

- Nicht direkt Gegenstand der Vorlage; da aber Gegenstand des Ausgangsverfahrens & nur EUGH beantworten kann, äußert sich EUGH, um „vollständige Antwort" zu geben

Konstrukt Safe Harbor als solches überhaupt zulässig?

- Selbstzertifizierung als solche nicht zu beanstanden, umso mehr ist aber wirksame Überwachungs- und Kontrollmechanismen zur Achtung der Privatsphäre nötig
  - ➢ EU und USA können Safe Harbor II abschließen; allerdings sind Vorgaben des EUGH zu beachten

Exkurs – Privacy Shield

- Entwurf „Privacy Shield“ Feb. 2016 veröffentlicht
  - kritische Stellungnahme Art. 29 Gruppe 12./13. April, substantielle Änderungen angemahnt
  - abzuwarten ob (geändert oder unverändert?) wie geplant im Juni verabschiedet wird und Ende des Jahres in Kraft tritt
  - Wenn es (im Wesentlichen) unverändert in Kraft tritt, ist damit zu rechnen, dass Privacy Shield vor dem EUGH angegriffen wird

Die Gründe – Safe Harbor (2)

Kritikpunkte des EUGH:

- Kritik 1: Safe Harbor betrifft (und Kontrolle der Einhaltung der Regeln trifft) nur Unternehmen, nicht Behörden
- Kritik 2: Safe Harbor Entscheidung enthält keine hinreichenden Feststellungen, wie in den USA das notwendige Schutzniveau i.S.v. Art. 25 Abs. 6 der Datenschutzrichtlinie gewährleistet wird (Safe Harbor basiert auf Art 25 Abs. 6 der Datenschutzrichtlinie; führt mithin zu der Feststellung eines grundsätzlich angemessenen Schutzniveaus vergleichbar einem sicheren Drittstaat wie der Schweiz)

Die Gründe – Safe Harbor (3)

Kritikpunkte des EUGH:

- Kritik 3: Vorbehaltslose Begrenzung des Safe Harbor Datenschutzes durch Erfordernisse der nationalen Sicherheit; in der Safe Harbor Entscheidung 2000/520 fehlt jegliche Abwägung, auch gegenüber Unternehmen, die Safe Harbor beigetreten sind
- Kritik 4: Die Safe Harbor Entscheidung 2000/520 sieht keinen ausreichenden wirksamen gerichtlichen Rechtschutz und keine ausreichende Ansprüche (z.B. Löschungsansprüche) für die betroffenen Datensubjekte aus der EU und für die EU Datenschutzbehörden vor

Die Gründe – Safe Harbor (4)

Kritikpunkte des EUGH:

- Kritik 5: Die Datenspeicherung in den US ist exzessiv, wie es sich aus den Berichten der Kommission selbst 2013 (nach den Snowden-Veröffentlichungen) selbst ergibt
- Kritik 6: Ausreichende Garantien zur Einhaltung eines angemessenen Datenschutzstandards ist in der Rechtsgrundlage (hier Safe Harbor Entscheidung) umso bedeutsamer, wenn automatische Datenverarbeitung erfolgt und erhebliche Gefahr eines unberechtigten Zugriffs erfolgt; ergo: weil in den USA umfangreiche Speicherungen und Zugriffe durch Behörden erfolgen, wären ausreichende Garantien in der Safe Harbor Entscheidung ganz besonders erforderlich gewesen

Ergebnis – Was der EUGH entschieden hat und was er nicht entschieden hat

- Der EUGH hat entschieden:
  1. Safe Harbor ist nichtig.
  2. Datenschutzbehörden haben hinsichtlich EU-Rechtsakten eine umfassende Prüfungs-, aber keine Aufhebungskompetenz
- Der EUGH hat nicht entschieden:
  1. Zu Transfers in die USA im Allgemeinen, insbesondere dass dies grundsätzlich nicht möglich seien.
  2. Andere Mechanismen für internationale Datentransfers wie Standartvertragsklauseln (SCC) oder Binding Corporate Rules (BCRs)

Interpretation

Auswirkungen für Cloud Angebote

Safe Harbor:

- Anbieter können sich nicht mehr (nur) auf Safe Harbor berufen; was viele aber ohnehin jedenfalls in Deutschland nicht getan haben

Standartvertragsklauseln (*Standard Contractual Clauses* – „**SCC**“)

- Nach wie vor in Kraft
- Können auch von Datenschutzbehörden nicht außer Kraft gesetzt werden; ebenso wenig können pauschal Transfers in ein bestimmtes Land verboten werden
- Datenschutzbehörden können aber (wie schon immer) einzelne konkrete Transfers untersuchen und auch untersagen, wenn individuelle Gründe dafür vorliegen

SCC nach EUGH “Schrems”

Kritikpunkte des EUGH:

1. Reichweite: nicht umfassend, insb. nicht Behörden
2. Tatsachengrundlage: keine ausreichenden Feststellungen, dass grundsätzlich sicheres Drittland
3. Schutz vor Behörden: keine Abwägung
4. Rechtsschutz: nicht ausreichend
5. Lokale Praxis: exzessive Datenspeicherung
6. Garantien: nicht ausreichend gerade angesichts Praxis

SCC nach EUGH “Schrems” (2)

Regelungen in den EU-Entscheidungen zu SCC, namentlich 2010/87/EU zu Auftragsdatenverarbeiter:

1. Reichweite: gilt für alle Empfänger; Empfänger (Exporteur) muss bei Weitergabe sicher stellen -> anders als Safe Harbor (besser, ausreichend)
2. Tatsachengrundlage: Standardvertragsklauseln sind keine Entscheidung nach Art. 25 Abs. 6 Datenschutzrichtlinie, die grundsätzliche Aussagen für ein bestimmtes Land treffen und können zu den Empfängern/Empfängerländern naturgemäß nichts sagen -> anders als Safe Harbor (nicht übertragbar)

SCC nach EUGH “Schrems” (3)

3. Schutz vor Behörden: umfassender Schutz in Art. 5 der SCC, insb. umfassende Verpflichtung auf EU Standards ohne Ausnahme bei „nationaler Sicherheit“ und umfassende Informationspflichten; kein Unterschied zu Verarbeitung in EU -> anders als Safe Harbor (besser, ausreichend)
4. Rechtsschutz: umfassend für Datensubjekte und Datenschutzbehörden, inkl. Drittbegünstigungsansprüche für Datensubjekte nach Art. 5, 6, 8 der SCC -> anders als Safe Harbor (besser, ausreichend)

SCC nach EUGH “Schrems” (4)

5. Lokale Praxis: gibt es nicht, SCCs gelten global -> anders als Safe Harbor (nicht übertragbar)
   - Aber: Transfer in die USA auf Basis von SCC?
   - Kritik 5 gilt unabhängig von Mittel
   - Konsequenz wäre nicht Unwirksamkeit von SCC, sondern grds. Verbot Transfer personenbezogener Daten in die USA; das fordert (und will) aber fast niemand
6. Garantien: Standardvertragsklauseln gelten für Transfers in alle Ländern, inklusive Ländern mit im Vergleich zu den USA weit niedrigerem Datenschutzniveau und stärkeren staatlichen Eingriffen (z.B. China) -> anders als Safe Harbor (besser, ausreichend)

SCC nach EUGH “Schrems” (5)

Zusammenfassender Vergleich Safe Harbor – SCC anhand EUGH Kritikpunkten:

EUGH	Safe Harbor	SCC
Reichweite	begrenzt	umfassend
Tatsachen-grundlage	nicht ausreichend	n/a
Behörden	ungenügender Schutz	wie in EU
Rechtsschutz	nicht ausreichend	umfassend, wie in EU
Lokale Praxis	exzessiv	n/a (P: USA allgemein?)
Garantien	nicht ausreichend	ausreichend

Stellungnahmen Datenschutzbehörden

EU Art. 29 Gruppe

Stellungnahme vom 16. Oktober 2015:

- Safe Harbor ungültig
- Aufforderung an Politik/Kommission bis Ende Januar 2016 neuen Rechtsrahmen zu finden
  - ➢ Privacy Shield“ Feb. 2016 veröffentlicht, Stellungnahme Art. 29 Gruppe 12./13. April kritisch
- Auswirkungen auf andere Mittel (wie SCC) werden untersucht (ob und, wenn ja, welche); derzeit werden sie als wirksam angesehen
- Ziel ist einheitliche europäische Handhabung, aber Recht, nationaler Datenschutzbehörden individuelle Transfers zu untersuchen, bleibt unberührt

Deutsche Datenschutzbehörden

Konferenz deutscher Datenschutzbehörden am 21. Oktober:

- Safe Harbor ungültig; bei „Kenntnis über ausschließlich auf Safe-Harbor gestützte Datenübermittlungen in die US erlangen“, werden diese untersagt
- Auch Zulässigkeit der Datentransfers in die USA mit anderen Mitteln, wie SCC oder BCRs, sei „in Frage gestellt“
- Eigene Prüfungskompetenz; derzeit keine „neuen Genehmigungen“ für BCRs und „Datenexportverträge“
- Unternehmen aufgefordert, US-Transfers unverzüglich Datenschutzkonform zu gestalten; ausdrücklicher Bezug auf Orientierungshilfe Cloud Computing (Version 2, 9.10.2014)
- Aufforderung an Politik, unverzüglich zu handeln

Deutsche Datenschutzbehörden

Was nicht gesagt wurde:

- Selbstständige Ermittlungen der Datenschutzbehörden
- Dass SCC oder BCRs oder Transfers in die USA grundsätzlich unzulässig sind; oder dass bestehende BCRs/SCC nicht mehr genutzt werden dürfen
- Dass SCC genehmigungsbedürftig sind oder untersagt werden (in Orientierungshilfe explizit als Mittel genannt)
- Abstimmung mit Artikel 29 Gruppe bzw. anderen europäischen Datenschutzbehörde, mit dem Ziel einheitlicher Handhabung (anders noch der Bundesdatenschutzbeauftragte am 6. Oktober 2015)
  - ➢ Maximaler politischer Druck

Deutsche Datenschutzbehörden – einzelne Stellungnahmen

Hamburg, 5. November 2015:

- Safe Harbor fällt weg; etwaige weitere Auswirkungen werden in Abstimmung mit anderen (dt. und europ.) Datenschutzbehörden untersucht; derzeit können (und müssen) SCC und BCRs weiter genutzt werden
- Dez/Jan Evaluierungsphase; Durchsetzung ab Februar (erfolgt in einigen Bundesländern, z.B. Hamburg); wer bisher Safe Harbor genutzt hat, muss bis dahin (auf SCC) umgestellt haben

Schleswig-Holstein (ULD), 14. Oktober 2015:

- Übermittlungen in die USA außerhalb Vertragszwecks unzulässig (inklusive Einwilligung, BCRs und SCC)

Deutsche Datenschutzbehörden – einzelne Stellungnahmen (2)

Meisten anderen Datenschutzbehörden:

- Keine eigene schriftliche Stellungnahme
- Überwiegend aber wohl „Hamburger Linie“, insbesondere bezüglich Weitergeltung SCC
- Allerdings viele (bisher) keine aktive Durchsetzung gegenüber Unternehmen, die sich immer noch auf Safe Harbor verlassen
- Aas mag sich jetzt ändern (da Entwurf Privacy Shield aus Sicht der Datenschutzbehörden "enttäuschend" ist)

Zusammenfassung

- Durchsetzung Ungültigkeit Safe Harbor:
  - Uneinheitliches Bild: teilweise wird durchgesetzt, teilweise nicht
  - Irrelevant, soweit ohnehin SCC genutzt werden
- Auswirkungen auf andere Mittel:
  - Art. 29 Gruppe und meisten deutsche und internationalen Datenschutzbehörden: erst einmal keine, können (müssen) derzeit genutzt werden; weitere Auswirkungen werden noch untersucht
  - ULD Schleswig Holstein: Außerhalb engen Vertragszwecks keine Übermittlung in die USA

Zusammenfassung (2)

- Im Lichte der EUGH-Entscheidung:
  - Safe Harbor ist ungültig
  - Auswirkungen auf andere Mittel:
    - Unmittelbar keine
    - (Einzel)meinung ULD europarechtswidrig und widerspricht EUGH
    - Aber: Prüfung im Einzelfall möglich, erfolgt auch teilweise, insbesondere ab Februar
    - Aber: Neues Verfahren gegen SCC in Ireland ("Schrems reloaded")

Auswirkungen für die Praxis

Schlußfolgerungen für die Praxis

- SCC sind nach wie vor ein rechtmäßiges Tool für Transfers in die USA (z.B. Cloud Computing)
- Wie stets muss Kunde im Einzelfall Anbieter sorgfältig auswählen, um so mehr wenn er in einem „unsicheren Drittstaat“ ist
- Kein Unterschied zu anderen Ländern (Russland, China, Indien etc.)

Schlussfolgerungen für die Praxis (2)

- De Facto Effekt
- Bereits vor dem Urteil waren viele EU Kunden zögerlich, Daten außerhalb der EU, insb. in den USA, zu speichern
- Verstärkter Bedarf für "EU Clouds“
- Viele Anbieter bieten "EU Clouds" an
- Aber: das sind (derzeit) Business-Gründe (nicht rechtlich)
- Es gibt (derzeit) jedenfalls datenschutzrechtlich keine Notwendigkeit für eine „European Cloud“ oder „German Cloud“
- Entwicklung ("Schrems reloaded") muss abgewartet werden

Quellen

- EUGH-Urteil: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117de.pdf
- Safe Harbor / Privacy Shield: http://www.twobirds.com/en/practice-areas/privacy-and-data-protection/eu-us-privacy-shield
- Cloud Computing App: http://www.twobirds.com/en/hot-topics/cloud-computing/cloud-computing-app

Ihr Ansprechpartner

Dr. Fabian Niemann
Partner
Düsseldorf & Frankfurt

Direct: +49 (0)69 74222 6123
Tel: +49 (0)69 74222 6000
Fax: +49 (0)69 74222 6011
fabian.niemann@twobirds.com

„Unschlagbar", "guter Praktiker, sehr zielorientiert", "sehr kompetent", "strukturiert und fokussiert"
JUVE IT 2015/2016

"Without question one of the finest practitioners in data protection law and cloud computing", "The go-to guy for legal issues relating to new technology and convergence topics."
Who's Who Legal IT 2014 & 2015

Dr. Fabian Niemann ist in den Bereichen IT, Technologie, Digitale Medien, Urheber- und Datenschutzrecht tätig. Er berät Anbieter und Kunden in Technologietransaktionen und IT-, Cloud-, Outsourcing und Konvergenzprojekten. Daneben ist er spezialisiert auf das Entwerfen und Verhandeln komplexer Verträge, auf software-, hardware-, urheber- und lizenzrechtliche Fragestellungen und Streitigkeiten sowie auf regulatorische Fragen in den Bereichen M-/E-Commerce, Social Media, Konvergenz, Digitale Medien sowie IT Sicherheit und Datenschutz.

Fabian Niemann wird regelmäßig für IT, TMT, Datenschutz- und Urheberrecht in den führenden Handbüchern empfohlen und hat eine besondere Reputation bei Rechtsfragen neuer Technologien und Geschäftsmodelle wie Cloud Computing, Big Data und IoT. Er ist Co-Leiter der internationalen Cloud Computing Gruppe von Bird & Bird.

Fabian Niemann ist Co-Autor der Cloud Computing, Datenschutz & Compliance Richtlinien des Verband der deutschen Internetwirtschaft e.V. (eco). Er veröffentlicht und referiert regelmäßig zu IT-, Outsourcing-, Cloud Computing, Datenschutz- und Urheberrechtsthemen. Er hat in Bonn und London studiert , über "Urheberrecht und elektronisches Publizieren" promoviert und seine Referendarzeit in Köln und den USA absolviert.

Vielen Dank & Bird & Bird

Dr. Fabian Niemann

Bird & Bird LLP

fabian.niemann@twobirds.com