Gemeinsame Stellungnahme zum Safe Harbor-Urteil

Eine Zusammenarbeit von

Arbeitsgruppe Datenschutz des Bundesverband Gesundheits-IT - bvitg e. V.

Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“ der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG) der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V.

Inhalt

1 Zusammenfassung

Der EuGH erklärte mit seinem Urteil vom 06.10.2015 die "Safe Harbor"-Entscheidung der Kommission für ungültig (Az.: C-362/14). Demnach sind auf Safe-Harbor-Verträgen beruhende Datenübermittlungen in die USA rechtswidrig.

Hauptkritikpunkt des EuGH: US Unternehmen können nicht garantieren, dass amerikanische Behörden keinen uneingeschränkten Zugriff auf die übertragenen personenbezogenen Daten haben.

Als alternative Rechtsgrundlage könnte gelten:

1) Die Einwilligung eines jeden Betroffenen.
2) Gesetzliche Ausnahmen: Art. 26 Abs. 1 Ziff. a-f RL 93/46/EG bzw. §4c Abs. 1 BDSG enthält Öffnungstatbestände, welche jedoch i.d.R. nicht die Verarbeitung von Patientendaten durch Dritte erlauben.
3) EU-Standardvertragsklauseln der europäischen Kommission zur Gewährleistung eines angemessenen Datenschutzniveaus in ein Drittland.
4) Binding Corporate Rules (BCR). Verbindliche Richtlinien zur Gewährleistung eines erforderlichen Datenschutzniveaus entsprechend RL 93/46/EG bei konzerninterner Übermittlung personenbezogener Daten in Drittstaaten. Spezielle Processor BCR gelten zwar für Auftragsdatenverarbeiter, werden in Deutschland in Hinblick auf die Verarbeitung in den USA derzeit jedoch nicht mehr genehmigt.

Letztlich kann damit nur durch den Einsatz der EU-Standardvertragsklauseln eine rechtskonforme Datenübermittlung in ein Drittland realisiert werden. Hierbei muss beachtet werden, dass ein derartiger Vertrag ausschließlich zwischen Auftraggeber und Verarbeiter im Drittland geschlossen werden kann; natürlich kann ein im Inland sitzendes Unternehmer rechtlich als Bevollmächtigter auftreten und im Namen eines anderen einen entsprechenden Vertrag abschließen.

Daher wird jedem Auftraggeber, welcher z.B. im Rahmen von Wartungsarbeiten Patientendaten in den USA (beispielsweise durch einen Subunternehmer eines deutschen Herstellers) verarbeiten lässt, empfohlen, einen Vertrag basierend auf den EU-Standardvertragsklauseln mit dem Datenverarbeiter in den USA zu vereinbaren.

Jedoch: Nach dem Urteil des EuGH gibt es in den USA weder bei Standardvertragsklauseln noch BCRs ein dem europäischen Datenschutzrecht entsprechend angemessenes Datenschutzniveau, eine Übermittlung der Daten wäre darauf basierend wahrscheinlich unzulässig.

Die Artikel-29-Datenschutzgruppe forderte die Politik auf, bis Ende Januar 2016 Lösungen herbeizuführen. Bis Ende Januar 2016 sieht sie Datenübermittlungen in die USA beruhend auf den EU-Standardvertragsklauseln und BCR als rechtskonform an.

Ab Februar 2016 behalten sich die europäischen Aufsichtsbehörden vor, entsprechend europäischem Recht unberechtigten Datentransfer in Drittstaaten, insbesondere in die USA zu untersagen, sofern sich bis dahin keine grundsätzliche Lösung abzeichnet.

Die Artikel-29-Datenschutzgruppe schließt jedoch eine anlassbezogene Tätigkeit aufgrund von Beschwerden noch vor Februar 2016 nicht aus. Laut EuGH-Urteil sind die Aufsichtsbehörden dazu auch verpflichtet.

Zum jetzigen Zeitpunkt kann die Frage, wie eine Datenübermittlung in die USA rechtskonform ausgestaltet werden kann, nicht sicher beantwortet werden.

2 Chronik

Der Österreicher Max Schrems, damals noch Rechtsstudent in Wien, heute selbst Jurist, nutzt seit 2008 Facebook. Die Daten, die er Facebook liefert, werden von der irischen Tochtergesellschaft von Facebook ganz oder teilweise an Server übermittelt, die sich im Hoheitsgebiet der Vereinigten Staaten befinden, und dort gespeichert. Er legte eine Beschwerde bei der irischen Datenschutzbehörde ein, da seiner Ansicht nach das Recht und die Praxis in den Vereinigten Staaten in Anbetracht der von Edward Snowden im Jahr 2013 enthüllten Tätigkeiten der Nachrichtendienste der Vereinigten Staaten (insbesondere der National Security Agency - NSA) keinen wirklichen Schutz gegen eine Überwachung der in dieses Land übermittelten Daten durch den amerikanischen Staat bieten.

Die irische Behörde wies die Beschwerde mit der Begründung zurück, dass die Kommission in einer Entscheidung vom 26.07.2000 das von den USA im Rahmen der als "sicherer Hafen" (Safe Harbor[1]) bezeichneten Regelung gewährleistete Schutzniveau der übermittelten personenbezogenen Daten als angemessen eingestuft habe.

Daraufhin wandte sich der Österreicher Max Schrems an den irischen High Court, woraufhin sich dieser an den EuGH mit folgender Fragestellung wandte: Hindert diese Entscheidung der Kommission eine nationale Kontrollstelle daran, eine Beschwerde zu untersuchen, mit der geltend gemacht wird, dass ein Drittland kein angemessenes Schutzniveau gewährleistet, und die beanstandete Übermittlung von Daten gegebenenfalls auszusetzen ist.

Der EuGH-Generalanwalt vertrat die Meinung, dass trotz der Feststellung der Europäischen Kommission, dass personenbezogene Daten in den USA angemessen geschützt sind, nationale Behörden die Übermittlung der Daten europäischer Nutzer von Facebook an Server, die sich in den Vereinigten Staaten befinden, aussetzen dürfen (Schlussanträge vom 23.09.2015).

Am 06.10.2015 erklärte der EuGH die "Safe Harbor"-Entscheidung der Europäischen Kommission für ungültig (Az.: C-362/14). Laut EuGH kann die "Safe Harbor"-Entscheidung der EU-Kommission die den nationalen Datenschutzbehörden in der EU-Grundrechte-Charta und der Richtlinie eingeräumten Befugnisse weder beseitigen noch beschränken. Die nationalen Datenschutzbehörden müssten im Fall einer Beschwerde völlig unabhängig prüfen können, ob bei der Übermittlung der Daten einer Person in ein Drittland die in der Richtlinie aufgestellten Anforderungen gewahrt werden.

3 Urteilsbegründung

Die Kommission habe lediglich die Safe-Harbor-Regelung geprüft, die nur für diejenigen amerikanischen Unternehmen gelte, die sich ihr unterwürfen, nicht aber für die US-Behörden. Außerdem hätten die Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses und der Durchführung von Gesetzen der USA Vorrang vor der Safe-Harbor-Regelung, sodass die amerikanischen Unternehmen die Schutzregeln unangewendet lassen müssen, wenn sie in Widerstreit zu solchen Erfordernissen stehen. Die amerikanische Safe-Harbor-Regelung ermögliche daher Eingriffe der amerikanischen Behörden in die Grundrechte der Personen. In der Kommissionsentscheidung werde weder festgestellt, dass es in den USA eingriffsbegrenzende Regeln noch einen wirksamen gerichtlichen Rechtsschutz gegen solche Eingriffe gibt. Damit ist eine Übermittlung von Daten europäischer Bürger in die USA rechtswidrig.

[1] Safe Harbor Website des US-Handelsministeriums. [Online, zitiert am 2015-10-26]; Verfügbar unter http://www.export.gov/safeharbor

4 Folgerungen aus dem Urteil

Zum Erfordernis eines angemessenen Schutzniveaus stellt der EuGH fest, dass das Grundrecht auf Achtung des Privatlebens eine Begrenzung der Speicherung personenbezogener Daten auf das absolut Notwendige verlangt.

Laut EuGH verletzt insbesondere eine Regelung, die es den Behörden gestatte, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens.

Außerdem verletze eine Regelung den Wesensgehalt des Grundrechts auf wirksamen gerichtlichen Rechtsschutz, wenn sie für den Bürger keine Möglichkeit vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken.

Neben der Unwirksamkeit der Safe-Harbor-Regelung wird durch diese Urteilsbegründung letzten Endes auch jede andere Datenübertragung in die USA in Frage gestellt. Denn auch bei anderen Möglichkeiten einer Datenübertragung von z. B Unternehmensdaten unter Anwendung der Standardvertragsklauseln der EU-Kommission oder BCR besteht die nahezu unbeschränkte Zugriffsmöglichkeit US-amerikanischer Behörden auf diese Daten.

4.1 Safe Harbor

Ein Datentransfer mit Bezugnahme auf Safe Harbor[2] ist seit der vorliegenden Urteilsverkündung des EuGH vom (06. Oktober 2015) rechtswidrig.

4.2 EU-Standardvertragsklauseln

Die von der europäischen Kommission veröffentlichten Standardvertragsklauseln[3] vom 05. Februar 2010 für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern (bekannt gegeben unter Aktenzeichen K(2010) 593) beinhalten unter Klausel 5 die Pflichten des Datenimporteurs.

Hierbei muss der Datenimporteur u. a. garantieren, dass

- er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen,
- er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen.

Beide Vertragspflichten kann ein unter der Gesetzgebung der USA fallender Datenverarbeiter nicht einhalten: die amerikanische Gesetzgebung erlaubt einerseits staatlichen Stellen nahezu unbegrenzten Zugriff auf Daten, wobei der durch staatliche Behörden erfolgte Zugriff ggfs. nicht mitgeteilt werden darf. Da diese Gesetze Stand heute existieren, kann ein in den USA befindlicher Datenimporteur auch nicht unterschreiben, dass er keinen entsprechenden Gesetzen unterliegt.

Grundsätzlich sind die europäischen Vertragsklauseln aber auch weiterhin gültig. Der EuGH stellte zudem in seinem Urteil unter Rn 193 und 202 fest, dass über die Gültigkeit von durch Unionsorganen verfügten Rechtsakten letztlich nur der EuGH entscheiden kann[4]. Somit kann über die Gültigkeit der von der EU-Kommission verabschiedeten Standardvertragsklausen oder der Gültigkeit von BCR nur der EuGH entscheiden, eine Einzelfallprüfung steht jedoch gemäß

[2] Safe Harbor Website des US-Handelsministeriums. [Online, zitiert am 2015-10-26]; Verfügbar unter http://www.export.gov/safeharbor/

[3] EU-Kommission: Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern. [Online, zitiert am 2015-10-26]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445851652852&uri=CELEX:32010D0087

[4] EuGH-Urteil vom 6. Oktober 2015 · Az. C‑362/14. [Online, zitiert am 2015-10-26]; Verfügbar unter http://openjur.de/u/859036.html

Art. 4 des Beschlusses der Kommission über Standardvertragsklauseln3 den unabhängigen nationalen Aufsichtsbehörden zu.

Nach dem Safe Harbor Urteil sind die EU-Standardvertragsklauseln der einzige legale Weg, um Daten in die USA zu übermitteln. Beachtet werden muss hier natürlich, dass diese Vertragsklauseln zwischen dem eigentlichen Auftraggeber und dem im Drittland die Daten verarbeitenden Unternehmen abgeschlossen werden müssen. Eine Vertragsgestaltung zwischen einem Auftragsdatenverarbeiter und einem im Drittland beschäftigten Subunternehmer erfüllt diese Bedingung nicht.

Weiterhin muss innerhalb Deutschlands beachtet werden, dass nach Auffassung der deutschen Aufsichtsbehörden die EU-Standardvertragsklauseln deutsches Recht nur dann abbilden, wenn ein Passus hinzugefügt wird, welcher der Erfüllung der Voraussetzungen des § 11 Abs. 2 BDSG dient[5]. Die Aufsichtsbehörden erstellten einen Abgleich zwischen den Anforderungen von §11 Abs. 2 BDSG und den EU-Standardvertragsklauseln, sodass man daraus ableiten kann, worum man sich zusätzlich kümmern muss[6]. Eine diesbezügliche Änderung der Klauseln führt nach Auffassung der deutschen Aufsichtsbehörden nicht zu einer Genehmigungspflicht[7]. Denn innerhalb von Deutschland muss eine auf den EU-Standardvertragsklauseln basierende Übermittlung personenbezogener Daten nicht von den Aufsichtsbehörden genehmigt werden, in den meisten anderen EU-Staaten jedoch schon.

4.3 Binding Corporate Rules

Binding Corporate Rules (BCR) sind ein Konstrukt für verbindliche Richtlinien zum Umgang mit den eigenen personenbezogenen Daten innerhalb der eigenen Konzernstruktur[8][9]. Basierend auf diesen Richtlinien dürfen internationale Institutionen, Organisationen und Firmen nach geltendem europäischem Recht, intern personenbezogene Daten in Drittstaaten mit nicht angemessenem Datenschutzniveau transferieren. Firmen, deren BCR genehmigt wurden, werden auf der Homepage der Artikel-29-Datenschutzgruppe gelistet[10].

Im Juni 2012 veröffentlichte die Artikel-29-Datenschutzgruppe Working Paper 195, in denen die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter festgelegt wurden[11]. Diese „Processor BCR“ sollen Datenschutz und Datensicherheit beim Transfer personenbezogener Daten zu einem Dienstleister außerhalb des EWR gewährleisten. D.h. sie dienen der Gewährleistung der Angemessenheit des Datenschutzniveaus beim Auftragsdatenverarbeiter in einem Drittland. Auch Processor BCR gelten nur konzernintern, d.h. können nur verwendet werden, wenn ein Konzernunternehmen innerhalb der EU Daten an ein Konzernunternehmen außerhalb der EU im Rahmen einer konzerninternen Verarbeitung übermittelt, d.h. das Konzernunternehmen innerhalb der EU ist im Rahmen einer ADV tätig und bedient sich zur Vertragserfüllung der Tätigkeit eines Konzernunternehmens außerhalb der EU. Beim Abschluss eines Dienstleistungsvertrages sollten Processor BCR als Anhang Vertragsbestandteil sein, wenn man diese zur Darstellung der Angemessenheit des Datenschutzniveaus in einem Drittland verwenden will.

---

[5] Bayerisches Landesamt für Datenschutzaufsicht: Umsetzung des § 11 BDSG bei Auftragsdatenverarbeitung in Drittstaaten. [Online, zitiert am 2015-10-26]; Verfügbar unter https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_11bdsg_drittstaaten.htm

[6] Bayerisches Landesamt für Datenschutzaufsicht: Abgleich Standardvertragsklauseln [Online, zitiert am 2015-10-26]; Verfügbar unter http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Abgleich_Standardvertragsklauseln-11.pdf

[7] Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises. Version 2.0, Stand 09.10.2014. Rn 35 [Online, zitiert am 2015-10-30]; Verfügbar unter http://www.lfd.niedersachsen.de/download/61457/Orientierungshilfe_Cloud-Computing_AK_Technik_AK_Medien_-_Stand_09.10.2014_.pdf

[8] Artikel-29-Datenschutzgruppe: Letters and other documents. [Online, zitiert am 2015-10-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm

[9] Artikel-29-Datenschutzgruppe: Binding Corporate rules. [Online, zitiert am 2015-10-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm

[10] Artikel-29-Datenschutzgruppe: List of companies for which the EU BCR cooperation procedure is closed. [Online, zitiert am 2015-11-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

[11] Artikel-29-Datenschutzgruppe: Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities. [Online, zitiert am 2015-11-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195a_application_form_en.doc

Die BCR müssen von den zuständigen europäischen Datenschutzaufsichtsbehörden geprüft und genehmigt werden. Hierzu wird unter Leitung einer federführenden Aufsichtsbehörde unter Beteiligung von zweier beisitzenden Aufsichtsbehörden, die BCR geprüft („Mutual Recognition[12]“). Bei positivem Prüfungsergebnis erkennen die Aufsichtsbehörden aller 21 EU-Länder, die von den BCR-Regularien involviert sind, diese an. Sind BCR genehmigt, so müssen auf BCR basierende Datenübermittlungen vor Beginn der Übermittlung ebenfalls von der für die Übermittlung zuständige Behörde genehmigt werden. D.h. es ist nicht möglich, sich beispielsweise in Italien BCR genehmigen zu lassen um dann in Deutschland Datenübermittlungen auf Grundlage der BCR durchzuführen, ohne das zuvor die zuständige deutsche Aufsichtsbehörde die Datenübermittlung genehmigte.

Um Aufsichtsbehörde und Unternehmen den Umgang mit BCR zu erleichtern, veröffentlichte die Artikel-29-Datenschutzgruppe einige Leitlinien (siehe 6.5 BCR Working Paper der Artikel 29 Gruppe).

Letztlich kann der europäische Datenschutzstandard in den USA aber auch durch die Regelung mittels BCR nicht gewährleistet werden. Ebenso wie die Standardvertragsklauseln sind BCRs privatrechtliche bilaterale Verträge zwischen Konzernbeteiligten, die keinerlei Auswirkungen auf US-Behörden besitzen.

Zudem kündigten die deutschen Datenschutzbehörden in ihrer Stellungnahme vom 26. Oktober 2015 unter Ziffer 7 an, keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen zu erteilen[13]. Die grundsätzliche Genehmigung von BCR entsprechend der Mutual Recognition kann ein Unternehmen auch in einem anderen Mitgliedsland beantragen und auch die Anerkennung wird dann wohl problemlos erfolgen. Jedoch muss jeder auf BCR beruhende Datentransfer bei der zuständigen Aufsichtsbehörde beantragt werden. Bei deutschen Arbeitnehmerdaten wäre hier also die deutsche Aufsicht spätestens bei diesem Schritt zu konsultieren.

[12] Artikel-29-Datenschutzgruppe: What is mutual recognition? [Online, zitiert am 2015-10-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm

[13] Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder. [Online, zitiert am 2015-10-30]; Verfügbar unter https://www.datenschutz.hessen.de/ft-europa.htm#entry4521

5 Übermittlung von Gesundheitsdaten in ein unsicheres Drittland

Bei jeder Datenübertragung von personenbezogenen oder personenbeziehbaren Gesundheitsdaten muss gewährleistet sein, dass die grundlegenden Rechte eines Betroffenen wie z.B. Informationspflicht oder Widerspruchsmöglichkeit gewahrt bleiben. Daher ist eine Übermittlung personenbezogener Daten in ein Drittland - sei dieses nun die USA, Indien, China oder ein anderes Drittland - nur statthaft, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet (siehe Erwägungsgrund Absatz 56 der Richtlinie 95/46/EG).

Die Standardvertragsklauseln oder auch die Binding Corporate Rules sollen in „unsicheren" Drittländern ein entsprechendes Schutzniveau gewährleisten. Dies setzt jedoch voraus, dass die gesetzlichen Grundlagen im Drittland durch eine entsprechende vertragliche Gestaltung dies ermöglichen. Eine nahezu unumschränkte Zugriffsmöglichkeit des Staates auf Daten verhindert jedoch, dass vertraglich ein entsprechendes Schutzniveau erzielt werden kann.

Weiterhin stellte der EuGH fest, dass Entscheidungen der Kommission so lange gültig sind, bis der EuGH diese für ungültig erklärt; Mitgliedstaaten und ihre Organe, zu denen auch die Datenschutzaufsichtsbehörden zählen, können keine einer Entscheidung der Kommission zuwiderlaufenden Maßnahmen treffen, wie beispielsweise einen Rechtsakt erlassen, mit welchem verbindlich festgestellt wird, dass das Drittland, auf das sich die Entscheidung bezieht, kein angemessenes Schutzniveau gewährleistet. Somit bleiben die Entscheidungen der Kommission bzgl. Standardvertragsklauseln und Binding Corporate Rules bestehen, bis entweder die Kommission die Entscheidung widerruft oder ein entsprechendes Gerichturteil vorliegt.

Jedoch können bzw. müssen nationale Aufsichtsbehörden den jeweiligen Einzelfall hinsichtlich der Einhaltung des Schutzniveaus prüfen. D. h eine Aufsichtsbehörde kann zwar weder Standardvertragsklauseln noch Binding Corporate Rules im allgemeinen für ungültig erklären, jedoch kann die Aufsichtsbehörde feststellen, dass in einem vorliegendem Einzelfall ein ausreichendes Schutzniveau durch diese Mechanismen nicht erzielt werden kann, z. B. weil die Gesetze im betreffenden Drittland ein entsprechendes Schutzniveau verhindern.

Bei der Beurteilung muss die nationale Aufsichtsbehörde jedoch beachten, dass lediglich ein „angemessenes" Schutzniveau gewährleistet sein muss, denn ein Drittland muss nach europäischem Recht kein dem in der Unionsrechtsordnung garantiertes „identisches" Schutzniveau gewährleisten (Art. 25 Abs. 6 der Richtlinie 95/46/EG). Hier gibt das Urteil Leitlinien, wie die Angemessenheit beurteilt werden kann.

5.1 (Grund-) Voraussetzungen

Entsprechend §4b Abs. 1 BDSG gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30a BDSG für die Übermittlung. Eine Übermittlung muss entsprechend den Vorgaben von §4b Abs.2 S.2 BDSG unterbleiben, wenn „der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist".

Zunächst muss daher immer die Wahrung der Angemessenheit des Datenschutzniveaus beurteilt werden. Hierzu gibt §4b Abs.3 BDSG vor, dass die Angemessenheit des Schutzniveaus unter Berücksichtigung aller Umstände beurteilt werden muss, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind. Insbesondere sind bei der Beurteilung des Datenschutzniveaus zu berücksichtigen:

- Art der Daten
- Zweckbestimmung der Datenverarbeitung
- Dauer der geplanten Verarbeitung
- Herkunfts- und das Endbestimmungsland
- Die für den betreffenden Empfänger geltenden Rechtsnormen
- Die für den betreffenden Empfänger geltenden Standesregeln und Sicherheitsmaßnahmen.

Bei Patientendaten gelten neben datenschutzrechtlichen Schutzvorschriften auch Schutzvorgaben aus dem Strafrecht (z.B. §203 StGB) und dem Standesrecht (z.B. Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte), so dass bei diesen Daten vom höchsten Schutzbedarf ausgegangen werden muss. Entsprechend gut muss der Schutz der Rechte der Betroffenen beim Datenempfänger im Drittland gewährleistet sein, die

Angemessenheit des Datenschutzniveaus also entsprechend nah am europäischem Recht liegen.

5.2 Zwingend notwendig: Rechtsgrundlage

Liegt kein Widerspruch eines Betroffenen vor und wird die Angemessenheit des Datenschutzniveaus im Drittland unter den beschriebenen Bedingungen als ausreichend beurteilt, so muss entsprechend §4 Abs.1 BDSG für die Übermittlung der Daten eine datenschutzrechtlich wirksame Einwilligung des Betroffenen vorliegen oder eine Rechtsnorm muss dies erlauben oder anordnen.

Eine Ausnahme hiervon kann sich aus §4 Lit. c BDSG ableiten. Entsprechend §4 Lit. c BDSG ist eine Übermittlung personenbezogener Daten an ein Drittland, auch wenn dort ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, wenn

1. der Betroffene seine Einwilligung gegeben hat,
2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,
3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Keiner dieser Ausnahmetatbestände wird i.d.R. auf die Patientenversorgung zutreffen, so dass eine andere Erlaubnisnorm für eine legale Datenübermittlung in ein Drittland gefunden werden muss. Eine rechtliche Grundlage kann sich aus §§ 28 bis 30a und §32 BDSG ableiten. Im Bereich der „besondere Arten personenbezogener Daten“ (3 Abs. 9 BDSG) kann nur §28 Abs. 7 bis 8 BDSG betrachtet werden.

Da die Einholung einer Einwilligung des Betroffenen zur Datenübermittlung in ein unsicheres Drittland aus Praxisgründen nicht anwendbar ist[14], kann die Legalität einer Übermittlung sich daher i.d.R. nur auf §28 Abs. 7 bis 8 BDSG beziehen, wenn kein spezialgesetzlicher Erlaubnistatbestand vorliegt.

5.3 Information des Patienten

Gemäß §4b Abs. 4 BDSG muss die verantwortliche Stelle den Betroffenen von der Übermittlung seiner Daten unterrichten, es sei denn,

- es ist damit zu rechnen, dass er davon auf andere Weise Kenntnis erlangt, oder
- wenn die Unterrichtung die öffentliche Sicherheit gefährden oder
- sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

Im Rahmen der Patientenversorgung ist nicht davon auszugehen, dass einer der drei Gründe zutrifft, so dass grundsätzlich die verantwortliche Stelle gemäß §4b Abs.4 BDSG verpflichtet ist, den Patienten bzgl. der Übermittlung seiner Daten zu unterrichten.

Dies entspricht auch den Vorgaben der Standardvertragsklauseln. Gemäß Klausel 4 Lit. f muss „bei der Übermittlung besonderer Datenkategorien“ (= entspricht unseren besonderen Arten von Daten, beinhaltet also Gesundheitsdaten) der Betroffene „vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt werden, dass seine Daten in ein Drittland übermittelt werden (bzw. wurden), welches kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet.

[14] Wenn ein Geschäftsbetrieb von der Einwilligung abhängt, würde der Geschäftsbetrieb letztlich bei Nicht-Erteilung einer Einwilligung oder dem Rückruf einer Einwilligung nicht durchgeführt werden können, d.h. die Patientenversorgung wäre gefährdet.

5.4 Angemessenes Datenschutzniveau im Zielland

Generell gilt, dass alle Staaten des Europäischen Wirtschaftsraumes (EWR) ein angemessenes Datenschutzniveau aufweisen, d.h. das eine Übermittlung in diese Länder rechtmäßig durchgeführt werden kann. Neben den Mitgliedsstaaten der EU gehören Island, Norwegen und Liechtenstein zum EWR.

Die europäische Kommission attestierte auf Basis von Artikel 25 Abs. 6 der Richtlinie 95/46/EG verschiedenen Staaten die Angemessenheit ihres Datenschutzniveaus[15]. Stand heute sind dies die folgenden Staaten:

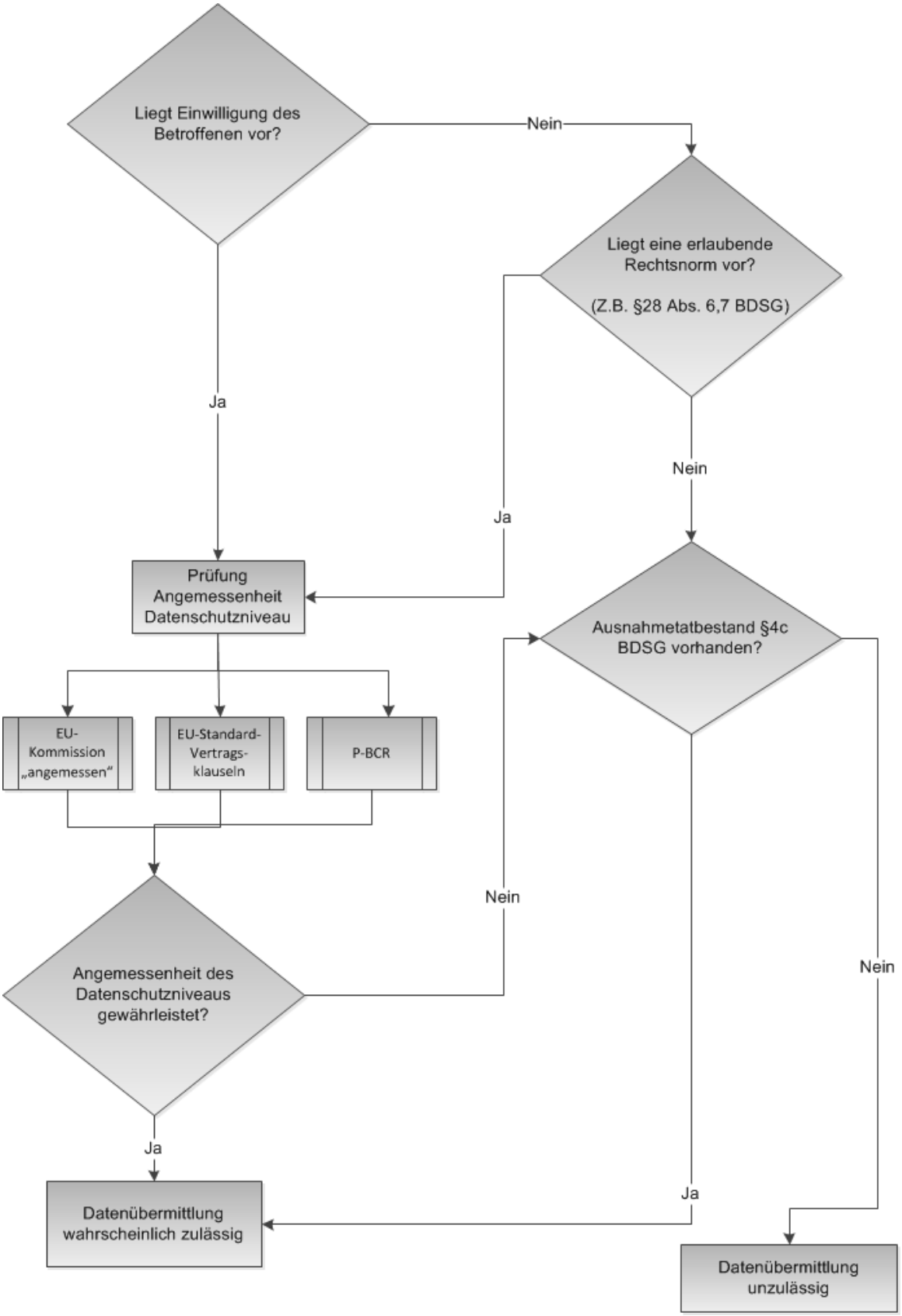
- Andorra
- Argentinien
- Färöer
- Guernsey
- Isle of Man
- Israel
- Jersey
- Kanada
- Neuseeland
- Schweiz
- Uruguay.

Die Nutzung der Standardvertragsklauseln (siehe Abschnitt 4.2) ist eine weitere Möglichkeit, die Angemessenheit des Datenschutzniveaus in einem Drittland zu gewährleisten. Allerdings kann der Vertrag entsprechend Klausel 5 Lit. b nur rechtsgültig abgeschlossen werden, wenn der Datenimporteur im Drittland „keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen“. D.h. der Vertrag kann nur mit Datenimporteuren in Drittländern abgeschlossen werden, deren nationale Gesetzgebung die Rechte des Betroffenen nicht unzulässig einschränken.

Prinzipiell sind auch Processor BCR ein geeignetes Instrument um die konzerninterne Angemessenheit des Datenschutzniveaus in einem Drittland zu gewährleisten, sofern die nationale Gesetzgebung im Drittland dies ermöglicht. Man muss auch beachten, dass bei Nutzung von Processor BCR ggfs. ein Konzernunternehmen der EU für Datenschutzverstöße von Konzernunternehmen außerhalb der EU einstehen muss.

[15] EU-Kommission. Commission decisions on the adequacy of the protection of personal data in third countries. [Online, zitiert am 2015-11-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

5.5 Ablaufschema für die Prüfung



6 Ausblick auf das Jahr 2016

Bis Ende Januar 2016 kann niemand einen rechtskonformen Weg zur Übermittlung personenbezogener Daten benennen. Danach will die Artikel-29-Gruppe entweder gegen aus ihrer Ansicht nach unzulässigen Datentransfer europaweit vorgehen oder die gesetzgebenden Institutionen in Europa erarbeiten bis dahin einen mit dem Europarecht konformen Lösungsweg zum Datentransfer in die USA[16].

Zwangsmittel und Sanktionen der deutschen Datenschutzbehörden ergeben sich in den deutschen Datenschutzgesetzen insbesondere aus §§ 38, 43 und 44 BDSG[17]:

- Kontrolle der Einhaltung von Vorschriften über den Datenschutz
  (§ 38 Absatz 1 Satz 1 BDSG)
- Auskunftsverlangen
  (§38 Absatz 3 Satz 1 BDSG)
- Prüfung und Besichtigung
  (§ 38 Absatz 3 Satz 1 BDSG)
- Einsicht in geschäftliche Unterlagen, gespeicherte personenbezogene Daten und Datenverarbeitungsprogramme
  (§38 Absatz 3 Satz 2 BDSG)
- Anordnung von Maßnahmen zur Beseitigung festgestellter Verstöße, insbesondere Verbote einzelner Datenverarbeitungen bzw. -übermittlungen
  (§38 Absatz 5 Satz 1 BDSG)
- Verhängung eines Zwangsgelds
  (§38 Absatz 5 Satz 2 BDSG)
- Untersagung einzelner Verfahren bzw. Übermittlungen
  (§38 Absatz 5 Satz 2 BDSG)
- Androhung und Verhängung von Bußgeldern
  (§ 43 Absatz 2 BDSG)
- Abschöpfung von durch Datenschutzverstöße bezogenen Gewinnen
  (§43 Absatz 3 Satz 3 BDSG)
- Strafanträge
  (§44 Absatz 2 BDSG)
- Veröffentlichungen von Pressemeldungen über festgestellte Verstöße.

[16] Artikel-29-Datenschutzgruppe: Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14). http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

[17] Wybitul T (2015) Stellungnahme Art. 29-Datenschutzgruppe: Überblick, Checkliste und Bewertung der Lösungsmöglichkeiten. ZD-Aktuell 2015: 04856

7 Empfehlungen

Grundsätzlich - und insbesondere derzeit - sollte ernsthaft die Möglichkeit des Verzichts auf eine Übermittlung/Offenbarung in ein unsicheres Drittland erwogen werden.

Ansonsten sieht nach derzeitigem Stand eine Empfehlung zum Datentransfer in die USA wie folgt aus:

1) Vor einer Übermittlung von Daten muss, sofern keine Einwilligung (des Betroffenen) vorliegt, ein grundlegender Erlaubnistatbestand vorhanden sein. Dies galt vor der Safe Harbor Entscheidung und dies gilt auch nach der Safe Harbor Entscheidung. Da ggfs. mit einer Prüfung der Aufsichtsbehörden zu rechnen ist, wird empfohlen, diesen Erlaubnistatbestand schriftlich festzuhalten, sofern dies bisher noch nicht geschehen ist. Als Rechtfertigungstatbestände kommen insbesondere die §§ 28 ff. BDSG (z.B. bei der Übermittlung von Kundendaten) oder § 32 BDSG (etwa für Beschäftigtendaten) in Betracht.
    a. Cave: Für Patientendaten kann nur §28 Abs. 6,7,8 BDSG, nicht aber die anderen Absätze verwendet werden.
2) Führen Sie eine Überprüfung Ihrer Datenübermittlungen in die USA durch, um festzustellen, welche personenbezogenen Daten aus der EU in die USA derzeit übermittelt werden:
    a. Welche nutzen als Berechtigungsgrundlage Safe Harbor?
    b. Welche EU-Standardvertragsklauseln?
    c. Welche BCR?
3) Räumen Sie Datenübermittlungen, die aufgrund der Art der Daten und deren Nutzung besonders wichtig für Ihr Geschäft sind, einen klaren Vorrang ein.
4) Identifizieren Sie alle Unternehmen, die an konzerninternen Datentransfers oder Übermittlungen an Geschäftspartner beteiligt sind, und prüfen Sie die zweckmäßigste Alternative zu Safe Harbor.
    a. EU-Standardvertragsklauseln lassen sich kurzfristig vertraglich vereinbaren, bieten aber wenig Flexibilität. Zudem erfordern die verbindlich vorgeschriebenen Anlagen, in denen die Datentransfers genau beschrieben werden müssen, einigen Aufwand.
        i. Um Patientendaten der Kunden in den USA zu verarbeiten, sind die EU-Standardvertragsklauseln Stand heute der einzig legale Weg.
        ii. Bei Verwendung der EU-Standardvertragsklauseln muss in Deutschland ein Passus hinzugefügt werden, welcher der Erfüllung der Voraussetzungen des § 11 Abs. 2 BDSG dient; ohne diese Anpassung genügen die Klauseln nach Ansicht der deutschen Aufsichtsbehörden nicht deutschem Recht (Hinweis: diese Änderung führt nicht zur Genehmigungspflicht[18]).
        iii. Die EU-Standardvertragsklauseln müssen zwischen Datenhalter (Datenexporteur) und Datenverarbeiter (Datenimporteur) im Drittland abgeschlossen werden. Die Kombination eines Abschlusses zwischen Auftraggeber und Auftragnehmer im Inland und eines EU-Standardvertrags zwischen Auftragnehmer und Datenimporteur ist nicht statthaft.
            1. Hinweis: Wohl nicht statthaft ist es, wenn der Auftragnehmer eine Bevollmächtigung als Vertreter zum Vertragsabschluss bekommt. Nach deutschem Recht würde der Auftraggeber die Datenhoheit aus der Hand geben. Weiterhin stellt sich die Frage, ob es hierbei nicht zu einem Vertrag zu Lasten Dritter (= Patient) kommt.
            2. Lösungsweg: Der Datenimporteur im Drittland kann den Auftragnehmer als Vertretungsbevollmächtigten benennen, sodass der Auftragnehmer im Namen des Datenimporteurs mit dem Auftraggeber einen Vertrag abschließen kann. Dieses Vorgehen dürfte den Umgang mit den EU-Standardvertragsklauseln erleichtern.

[18] Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises. Version 2.0, Stand 09.10.2014. Rn 35 [Online, zitiert am 2015-10-30]; Verfügbar unter http://www.lfd.niedersachsen.de/download/61457/Orientierungshilfe_Cloud-Computing_AK_Technik_AK_Medien_-_Stand_09.10.2014_.pdf

b. BCRs müssen mit den Datenschutzbehörden im Vorfeld abgestimmt werden. Dafür bieten sie derzeit das höchste Maß an Rechtssicherheit und können an die Bedürfnisse des Unternehmens angepasst werden. Zu beachten:
    i. BCR gelten nur für (konzern-) interne personenbezogene Daten und sind somit keine Lösung für die Verarbeitung von zu Kunden gehörenden Patientendaten.
    ii. BCR einzuführen ist ein langwieriger Prozess und stellt daher keine kurzfristige Lösung dar.
    iii. Innerhalb Deutschlands kündigten die Aufsichtsbehörden zudem an, keine Datentransfers auf Grundlage von BCR zu genehmigen.
    iv. Vorhandene Genehmigungen gelten jedoch weiter.

5) Bei dem Transfer von Patientendaten im Rahmen der Erbringung von Dienstleistungen (z. B. Wartungsarbeiten an einem Informationssystem) für einen Kunden werden die Daten dergestalt verschlüsselt, dass die unverschlüsselten Daten in den USA nicht verarbeitet (insbesondere dort auch nicht gespeichert) werden können. Gleichwohl gilt nach Datenschutzrecht allein schon das „Sehen“ der Daten auf einem Bildschirm als Übermittlung. D. h. im Supportfall erfolgt eine Übermittlung von Patientendaten, sodass hier eine Verschlüsselung der Daten nicht greift.
6) Nutzung technisch-organisatorischer Maßnahmen, die insbesondere berücksichtigen
    a. Nutzung von Verschlüsselungstechnologien
        - Verschlüsselter Transport unter gegenseitiger Authentifizierung in Kombination von Ende-zu-Ende-Verschlüsselung
        - Nutzung von Verfahren zur Erschwerung nachträglicher Entschlüsselung abgeschöpften Datenverkehrs (Perfect Forward Security) auf möglichst kurzen, lokalen, selbst bestimmten und kontrollierten Transferrouten
        - Verschlüsselte Speicherung unter Verwendung eigener Schlüssel, auf welche der Auftragsdatenverarbeiter keinen Zugriff erhält
    b. Eindeutige vertragliche Festlegung der Verarbeitungsorte inklusive Unterverarbeitungen
    c. Informationspflicht mit Widerspruchsmöglichkeit des Betroffenen beim Einsatz von Unterverarbeitern in Drittländern
    d. Auswertbare, lückenlose und unverfälschte Protokollierung mit konfigurierbarer Aufbewahrungszeit, deren Auswertung wiederum zu einem Protokolleintrag führt

8 Weblinks

8.1 Urteil

- EuGH: Rechtsprechung des Gerichtshofs, Az.: C-362/14:
  http://curia.europa.eu/juris/documents.jsf?pro=&lgrec=de&nat=or&oqp=&lg=&dates=&language=de&jur=C,T,F&cit=none%2CC%2CCJ%2CR%2C2008E%2C%2C%2C%2C%2C%2C%2C%2C%2C%2Ctrue%2Cfalse%2Cfalse&num=C-362%2F14&td=;ALL&pcs=Oor&a
- openJur e.V.: EuGH · Urteil vom 6. Oktober 2015 · Az. C‑362/14
  http://openjur.de/u/859036.html

8.2 Stellungnahme Datenschutzaufsichtsbehörden

- Communication from the commission to the European Parliament and the council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)
  http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf
- Artikel-29-Datenschutzgruppe: Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)
  http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf
  Deutsche Fassung:
  https://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/StatementOfTheArticle29WorkingParty_DeutscheFassung.pdf?__blob=publicationFile&v=1
- Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26.10.2015
  https://www.datenschutz.hessen.de/ft-europa.htm#entry4521
- Positionspapier des unabhängiges Landeszentrum für Datenschutz (ULD) zum Safe-Harbor-Urteil
  https://www.datenschutzzentrum.de/artikel/967-Positionspapier-des-ULD-zum-Safe-Harbor-Urteil-des-Gerichtshofs-der-Europaeischen-Union-vom-6.-Oktober-2015,-C-36214.html

8.3 Stellungnahme Kommission, Unternehmen, Verbände

- Bitkom
  https://www.bitkom.org/Presse/Presseinformation/Bitkom-zur-EuGH-Entscheidung-zum-Safe-Harbor-Abkommen.html
- Bundesverband Digitale Wirtschaft (BVDW)
  http://www.funkschau.de/telekommunikation/artikel/123784/
- Bundesverbant IT-Mittelstand
  http://www.bitmi.de/php/evewa2.php?menu=019901&newsid=2808
- Bundesverband IT-Sicherheit e.V. (TeleTrusT
  https://www.teletrust.de/uploads/media/PM-151012-TeleTrusT-Safe_Harbor.pdf
- Eco Verband
  http://ikt.nrw.de/news/einzelmeldung/article/eugh-entscheidung-zum-safe-harbor-abkommen/
- EU-Kommission
  http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm
- Gesellschaft für Datenschutz und Datensicherheit (GDD)
  https://www.gdd.de/downloads/stellungnahme-der-gdd-zum-urteil-des-eugh-vom-06-10-2015-zu-safe-harbor
- SAP
  http://news.sap.com/germany/2015/10/07/stellungnahme-der-sap-zum-gerichtsurteil-des-eugh-zum-safe-harbor-abkommen/

- TeleTrusT-AG "Cloud Security"
  https://www.omnisecure.berlin/index.php/de/news/organisationen/6019-safe-harbor-urteil-stellungnahme-der-teletrust-ag-cloud-security

8.4 Kommentierungen

- delegedata.de
  https://www.delegedata.de/2015/10/safe-harbor-urteil-des-eugh-die-kommission-hat-ihre-kompetenzen-unter-und-ueberschritten/
- Dirks & Diercks Rechtsanwälte Partnerschaftsgesellschaft
  http://www.socialmediarecht.de/2015/10/14/safe-harbor-die-erste-stellungnahme-des-unabhaengigen-landeszentrums-fuer-datenschutz-s-h-uld-und-die-damit-verbundenen-konsequenzen-fuer-unternehmen/
- Heise online: Nach dem EuGH-Urteil: Alternativen zu Safe Harbor
  http://www.heise.de/newsticker/meldung/Nach-dem-EuGH-Urteil-Alternativen-zu-Safe-Harbor-2837700.html
- Heise RegioConcept: Safe Harbor: Sofortmaßnahmen nach dem EuGH-Urteil
  http://www.heise-regioconcept.de/social-media/safe-harbor-urteil-folgen
- Kanzlei Lachenmann
  http://kanzlei-lachenmann.de/safe-harbor-urteil-eugh-setzt-zeichen-gegen-massenausspaehung-mit-wirrer-argumentation/
- Kanzlei Schwenke: Was bedeutet das Safe-Harbor-Urteil des EuGH für Sie?
  https://www.jurablogs.com/go/was-bedeutet-das-safe-harbor-urteil-des-eugh-fuer-sie
- Netzwerk Datenschutzexpertise
  http://www.netzwerk-datenschutzexpertise.de/dokument/folgen-der-safe-harbor-entscheidung-des-eugh
- Telemedicus
  http://www.telemedicus.info/article/3001-5-Fragen-zum-Safe-Harbor-Urteil-des-EuGH.html

8.5 BCR Working Paper der Artikel 29 Gruppe

- Working Paper 212 (2014-02): Anforderungen an verbindliche unternehmensinterne Regelungen, die den nationalen Datenschutzbehörden der EU vorgelegt werden, und an Regelungen für den grenzüberschreitenden Datenschutz, die den von der APEC anerkannten „CBPR Accountability Agents“ vorgelegt werden (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_de.pdf)
- Working Paper 204 (2013-04): Erläuterndes Dokument zu verbindlichen unternehmensinternen Datenschutzregelungen für Auftragsverarbeiter (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_de.pdf)
- Working Paper 195 (2012-06): Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_de.pdf)
- Working Paper 155 (2008-06): FAQ zu Binding Corporate Rules (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp155_rev.04_de.pdf)
- Working Paper 154 (2008-06): Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_de.pdf)
- Working Paper 153 (2008-06): Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_de.pdf)
- Working Paper 133 (2007-01): Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp133_en.doc)

- Working Paper 108 (2005-04): Muster-Checkliste für Anträge auf Genehmigungen verbindlicher unternehmensinterner Datenschutzregelungen (BCR) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_de.pdf)
- Working Paper 107 (2005-04): „Festlegung eines Kooperationsverfahrens zwecks Abgabe gemeinsamer Stellungnahmen zur Angemessenheit der verbindlich festgelegten unternehmensinternen Datenschutzgarantien (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_de.pdf)
- Working Paper 102 (2004-11): Muster-Checkliste „Antrag auf Genehmigung verbindlicher Unternehmensregelungen (BCR)“ (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp102_de.pdf)
- Working Paper 74 (2003-06): Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_de.pdf)