Daten für Zwecke des Adresshandels oder der Werbung eine abschließende Spezialregelung darstelle.[48] Nicht mehr in Absatz 3 geregelt sei lediglich die nicht geschäftsmäßig zu eigenen Zwecken erfolgende Markt- und Meinungsforschung, also solche ohne Werbecharakter, für welche statt Absatz 3 dann Abs. 1 Satz 1 Nr. 2 bzw. Abs. 2 Nr. 3 BDSG gelten. Diese Auslegung verkennt aber sowohl den Wortlaut wie die Entstehungsgeschichte der Vorschrift. § 28 Abs. 3 BDSG regelt für die Verarbeitung oder Nutzung personenbezogener Daten zu Zwecken der Werbung das vormals in § 28 Abs. 3 Satz 1 Nr. 3 BDSG a.F. normierte sog. Listenprivileg. Danach ist die Werbewirtschaft zur Verwendung von listenmäßig zusammengefassten Daten – auch ohne Einwilligung des Betroffenen – berechtigt. Insofern handelt es sich nur um eine Spezialregelung für die Werbung mit Listendaten. Die Gesetzesbegründung spricht an keiner Stelle von einer abschließenden Regelung.[49]

Eine solche Annahme wäre auch europarechtswidrig. Wie der *EuGH* in seinem U. v. 24.11.2011[50] festgestellt hat, dürfen „die Mitgliedstaaten weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben Art. 7 der RL 95/46 einführen, noch zusätzliche Bedingungen stellen, die die Tragweite eines der sechs in diesem Artikel vorgesehenen Grundsätze verändern würden." Demnach steht Art. 7 lit. f DS-RL hinsichtlich der Verarbeitung personenbezogener Daten jeder nationalen Regelung entgegen, die bei Fehlen der Einwilligung der betroffenen Person neben den beiden in der vorstehenden Randnummer genannten kumulativen Voraussetzungen zusätzliche Erfordernisse aufstellt. Unter Berücksichtigung der Auslegungsgrundsätze des *EuGH*[51] kann zukünftig davon ausgegangen werden, dass öffentlich zugängliche Daten über eine Person grundsätzlich ohne Einwilligung des Betroffenen erhoben werden können, soweit nicht im Einzelfall die Interessen des Betroffenen der Datenerhebung entgegenstehen. Vorliegend geht es im Kern um die Nutzung öffentlich zugänglicher Kontaktdaten (Name, Anschrift, Telefonnummer). Solche Daten können nach Ansicht des *EuGH* immer verwendet werden, wenn nicht im Einzelfall überwiegende Schutzinteressen des Betroffenen vorliegen.[52] Das ist vorliegend nicht ersichtlich. Auch die Telefonnummer lässt sich (auch i.R.d. Telefonwerbungsregeln des § 7 UWG) so nutzen, dass der Betroffene keine Nachteile oder Beeinträchtigungen über sich ergehen lassen müsste. Von daher ist die Nutzung dieser Daten zulässig.

Die Kontaktaufnahme mit potenziellen Interessenten ist eine (allein) nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG zulässige Verwendung personenbezogener Daten.

IV. Ergebnis

Die Befragung von Kunden über potenzielle weitere Interessenten aus dem Bekanntenkreis des Kunden ist eine nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG zulässige Datenerhebung. Die Datenerhebung darf gem. § 4 Abs. 2 Satz 2 Nr. 2 lit. a) und b) BDSG auch ohne Mitwirkung und Kenntnis des potenziellen Interessenten erfolgen. Dabei muss sich die Datenerhebung aber auf die zur Kontaktaufnahme erforderlichen personenbezogenen Daten beschränken. Werden die so erhobenen Daten zur weiteren Verwendung gespeichert, ist der Betroffene über die Speicherung, die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle zu informieren. Die Kontaktaufnahme ist nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG zulässig, reicht aber zur Information des Betroffenen nicht aus.

Professor Dr. Thomas Hoeren
ist Direktor der Zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) in Münster und Mitherausgeber der ZD.

48 *Gola/Schomerus* (o. Fußn. 1), § 28 Rdnr. 42.
49 S. etwa BT-Drs. 16/2011, S. 32 f.
50 *EuGH* ZD 2012, 33 – ASNEF/FECEMD.
51 *EuGH* ZD 2012, 33 – ASNEF/FECEMD.
52 Dazu auch ausf. *Hoeren*, RDV 2009, 89 ff.; http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/publikationen/hoeren_veroeffentlichungen/novellierungsplaene.pdf.

AXEL SPIES

Keine „Genehmigungen" mehr zum USA-Datenexport nach Safe Harbor?

Übertragung personenbezogener Daten aus Deutschland in die USA

Überwachung
EU-Standardklauseln
Datenverkehr in Drittstaaten
Datenübermittlung
PRISM

■ Eine Presseerklärung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) zu den gravierenden NSA-Affären hat in der deutschen Industrie und bei einigen US-Unternehmen Staub aufgewirbelt. Die Frage ist, ob die Übertragung von personenbezogenen Daten aus Deutschland in die USA weiter noch rechtssicher möglich ist, wenn der Empfänger in den USA nach dem EU/US-Safe Harbor-Programm registriert ist bzw. wenn zwischen dem Datenexporteur und dem Datenimporteur ein Vertrag nach den EU-Standardklauseln (Standard Contractual Clauses) abgeschlossen worden ist. An der Kompetenz der Datenschutzbeauftragten zu den medienwirksam angekündigten Maßnahmen, diesen Datenverkehr in die USA zu beschränken oder gar zu untersagen, bestehen erhebliche Zweifel.

■ A press release issued by the joint conference of data protection agencies of the Federation and the States – Länder (DSK) regarding the serious NSA-affairs has caused quite a stir in the German industry and in several US companies. The question is whether the transfer of personal data from Germany to the USA is still possible with sufficient legal certainty if the recipient is registered in the USA under the EU/US-Safe Harbor-Program, or, as the case may be, if a contract pursuant to the so-called EU Standard Contractual Clauses has been concluded between the data exporter and the data importer. There must be serious doubt whether the data protection agencies are in fact allowed to impose the measures they announced publicly as picked up by the media to limit this data traffic to the USA, or whether they even can prohibit this data flow.

I. „Diffuse Bedrohlichkeit"

Schneider/Härting[1] haben in ihrem Beitrag „Warum wir ein neues BDSG brauchen" auf eine Passage im Urteil des *BVerfG* zur Vorratsdatenspeicherung hingewiesen, die sich auf die Protokollierung des Nutzerverhaltens bezieht. Der Internetnutzer empfinde eine „diffuse Bedrohlichkeit", wenn er sich vor Augen halte, welche Spuren er im Netz hinterlasse.[2] Diese diffuse Bedrohlichkeit hat sich bei vielen deutschen Internetnutzern durch die Medien in den letzten Monaten verstärkt und durch die verschiedenen publik gewordenen „NSA-Abhörskandale" potenziert.

Über die Abhöraktionen der *NSA* wird auch in den USA ausführlich berichtet, allerdings um einiges besonnener als in Deutschland.[3] Da niemand so recht weiß, was US-Spionage- und Heimatschutzbehörden so alles an Daten kurz- oder langfristig speichern, ist die Büchse der Pandora für Spekulationen und Verschwörungstheorien geöffnet. Durch die erregte und auch vom deutschen Wahlkampf geprägte Debatte hat sich bei den deutschen Datenschutzbehörden einiger Handlungsdruck aufgebaut, die Datenweitergabe an diese Behörden lieber heute als morgen zu unterbinden. Zumindest besteht die öffentliche Erwartungshaltung, dass die „Datenschützer" für Aufklärung und Schutz sorgen sollen – wenn die Politik eher untätig bleibt. So muss man wohl die Ergebnisse der *Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK)* v. 24.7.2013 interpretieren.

II. Inhalt der Erklärung

Ausweislich der Presseerklärung der *DSK* v. 24.7.2013[4] „fordert die Konferenz die Bundesregierung auf, plausibel darzulegen, dass der unbeschränkte Zugriff ausländischer Nachrichtendienste auf die personenbezogenen Daten der Menschen in Deutschland effektiv i.S.d. genannten Grundsätze begrenzt wird. Bevor dies nicht sichergestellt ist, werden die Aufsichtsbehörden für den Datenschutz keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten (z.B. auch zur Nutzung bestimmter Cloud-Dienste) erteilen und prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind."

Zum Thema Safe Harbor/Standardklauseln und zur Aussetzung der Datenübermittlung heißt es in der Erklärung: „Die Europäische Kommission hat in mehreren Entscheidungen Grundsätze des ‚sicheren Hafens' (Safe Harbor) zum Datentransfer in die USA (2000) und Standardvertragsklauseln zum Datentransfer auch in andere Drittstaaten (2004 und 2010) festgelegt.

Die Beachtung dieser Vorgaben soll gewährleisten, dass personenbezogene Daten, die in die USA oder andere Drittstaaten übermittelt werden, dort einem angemessenen Datenschutzniveau unterliegen. Allerdings hat die Kommission stets betont, dass die nationalen Aufsichtsbehörden die Datenübermittlung dorthin aussetzen können, wenn eine ‚hohe Wahrscheinlichkeit' besteht, dass die Safe Harbor-Grundsätze oder Standardvertragsklauseln verletzt sind. Dieser Fall ist jetzt eingetreten."

III. Rechtliche Auswirkungen und Hindernisse

Diese Erklärung wurde teilweise in der deutschen Presse[5] so interpretiert, dass die deutschen Datenschutzbehörden mitgeteilt hätten, dass sie keine „Genehmigungen" mehr nach dem EU/US-Safe Harbor-Abkommen erteilen würden.

Allerdings gibt es für solche Datenexporte in die USA nach deutschem Recht, wie *Voigt*[6] zu Recht betont, kein solches rechtliches Erfordernis: Das Safe Harbor-Abkommen bzw. die sog. EU-Standardvertragsklauseln basieren auf Entscheidungen der *EG-Kommission* und sind damit – rechtlich gesehen – einer weitergehenden Überprüfung durch die nationalen Datenschutzbehörden entzogen. Das hat verschiedene Gründe:

- Die *EU-Kommission* hat in Art. 1 der Entscheidung 2000/520/EG gem. der RL 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) festgestellt: „Es wird davon ausgegangen, dass die dieser Entscheidung als Anhang I beigefügten ‚Grundsätze des ‚sicheren Hafens' zum Datenschutz' ... für alle unter die RL 95/46/EG fallenden Tätigkeiten ein i.S.d. Art. 25 Abs. 2 dieser RL angemessenes Schutzniveau für personenbezogene Daten gewährleisten." Dies ist abschließend zu verstehen. Gem. Art. 3 (1) dieser EU-Entscheidung können die zuständigen Behörden in den Mitgliedstaaten „ihre bestehenden Befugnisse ausüben" und zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung an eine Organisation auszusetzen, die den Grundsätzen, die entsprechend den FAQ umgesetzt wurden, beigetreten ist, wenn „eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden; wenn Grund zur Annahme besteht, dass die jeweilige Durchsetzungsinstanz nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den Fall zu lösen; wenn die fortgesetzte Datenübermittlung für die betroffenen Personen das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde, und wenn die zuständigen Behörden in den Mitgliedstaaten die Organisation unter den gegebenen Umständen in angemessener Weise unterrichtet und ihr Gelegenheit zu Stellungnahme gegeben haben." Es lohnt sich diese Passage genau zu lesen, denn mit „Grundsätzen" sind die Safe Harbor-Prinzipien gemeint, nicht die nationalen Datenschutzgrundsätze. Die Safe Harbor-Grundsätze schließen aber nicht aus, dass Sicherheitsbehörden Zugriff auf die übermittelten Daten in den USA haben. Darauf hätten sich die USA auch nie eingelassen.[7] In der *EU-Kommissions*-Entscheidung 200/520/EWG heißt es deshalb im Anhang 1 (Schreiben vorgelegt vom amerikanischen Handelsministerium am 21.7.2000), auf den Art. 1 der Entscheidung verweist: „Die Geltung dieser Grundsätze kann begrenzt werden a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss ..."

- Im Endeffekt geht es den Datenschutzbehörden um die Auslegung und Reichweite von US-Recht, an das sich die US-Datenimporteure allgemein halten müssen. Der *Irische Datenschutzbeauftragte* und auch hierzulande *Schuppert/von Reden*[8] (stellvertretend für viele) glauben nicht, dass Safe Harbor durch PRISM verletzt ist. Konkrete Anmahnungen an möglicherweise betroffene Unternehmen hat es bislang nicht gegeben. Wenn sich ein individuell Betroffener in seinen Rechten nach Safe Harbor verletzt fühlt, kann er ggf. eine Beschwerde bei einem be-

1 *Schneider/Härting*, ZD 2011, 63 ff.
2 *BVerfG* MMR 2010, 356.
3 Vgl. *Spies*, MMR 2013, 549.
4 Die PM ist abrufbar unter: http://www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.9283.de.
5 Vgl. hierzu: http://www.golem.de/news/konferenz-der-datenschuetzer-datentransfers-in-die-usa-werden-nicht-mehr-genehmigt-1307-100589.html.
6 *Voigt*, ZD-Aktuell 2013, 03165; s.a. die Diskussion im Beck-Blog v. 25.7.13, abrufbar unter: http://blog.beck.de/2013/07/25/keine-genehmigungen-mehr-zum-usa-datenexport-nach-dem-safe-harbor-abkommen-geht-das-berhaupt.
7 Alle US-Unternehmen sind allgemein nach den US-Gesetzen zur Kooperation mit den Sicherheitsbehörden nach Einhaltung der einschlägigen US-Vorschriften verpflichtet – s. insb. Sec. 215 USA Patriot Act (50 USC § 1861), abrufbar mit weiteren Information auf der Webseite des *US-Department of Commerce (DoC)* unter: http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf; http://www.justice.gov/archive/ll/subs/add_myths.htm.
8 Vgl. http://www.europe-v-facebook.org/Response_23_7_2013.pdf; *Schuppert/von Reden*, ZD 2013, 210, 212 f.

sonderen EU-Gremium einreichen (dem *Data Protection Panel* – einer hochkarätig besetzten Schiedsstelle),[9] also gerade nicht direkt bei einer deutschen Datenschutzbehörde.

■ Wenn es zu einer massiven Verletzung der Safe Harbor-Prinzipien und „unmittelbaren schweren Schäden" durch beim *US Department of Commerce* registrierte US-Unternehmen als Datenimporteure käme, wozu es derzeit keine wirklich greifbaren Anhaltspunkte gibt, müsste die *Federal Trade Commission (FTC)* oder das *Department of Transport (DoT)* in den USA tätig werden. Nur wenn sich auf diesem Wege nichts bewegt, könnte die *EU-Kommission* tätig werden. Das diplomatische EU-Schreiben zu Safe Harbor sieht in diesen Fällen die Anrufung des *Ausschusses nach Art. 31 DS-RL* vor – gem. Art. 31 Abs. 1 DS-RL sitzen dort Repräsentanten der EU-Mitgliedstaaten und der *EU-Kommission* am Tisch, nicht die Vertreter der nationalen Datenschutzbehörden.[10] Zu diskutieren wäre dann an diesem Tisch, ob „Beweise" vorliegen, dass die *FTC* oder das *DoT* nicht gegen Verletzungen von Safe Harbor durch massive NSA-Überwachungen und „unmittelbare schwere Schäden" für die Betroffenen einschreiten. Das Ausklammern der nationalen Datenschutzbehörden auf dieser Ebene entspricht voll und ganz dem Sinn und Zweck von Safe Harbor: Ob Safe Harbor – eine diplomatisch über Jahre hinweg sorgsam austarierte Kompromisslösung für Datenübermittlungen – als eine völkerrechtliche Vereinbarung einzuordnen ist, ist umstritten. Es ist jedenfalls kaum vorstellbar, dass die *EU-Kommission* mit den genannten Erklärungen den nationalen Datenschutzbehörden Hintertürchen für medienwirksame Ausflüge ins US-Recht eröffnen wollte, zumal es bislang keine „unmittelbare Unterrichtung" von unter Safe Harbor registrierten Unternehmen von etwaigen Rechtsverstößen gem. Entscheidung 2000/520/EG der *Kommission* gegeben hat.[11]

■ Selbst wenn die deutschen Datenschutzbehörden der Datenübermittlung in die USA nachgehen und die Unternehmen eventuelle Verstöße vorab melden, hat die Rechtsauffassung Bestand, dass die deutschen Aufsichtsbehörden i.R.d. NSA-Skandals keine eigene Befugnis zur Aussetzung des Datenflusses bei Safe Harbor haben. Dies wird durch den Wortlaut des § 4c Abs. 1 BDSG gestützt. Nach dieser Vorschrift ist i.R.v. Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 BDSG genannten Stellen zulässig, wenn bei ihnen ein angemessenes Datenschutzniveau gewährleistet ist. Genau diese Angemessenheit wird durch Safe Harbor bzw. durch die EU-Standardvertragsklauseln bereits für Deutschland gewährleistet. Allein aus der Tatsache, dass gem. § 4c Abs. 2 BDSG „unbeschadet des Absatzes 1 Satz 1 die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen genehmigen" kann, ergibt sich nichts anderes. Im Gegenteil: Die Vorschrift zeigt im Umkehrschluss, dass es keine Untersagungsbefugnis der nationalen Aufsichtsbehörden gibt, wenn die Angemessenheit des Schutzniveaus einmal bindend durch die *EU-Kommission* festgestellt wird. Anderenfalls würde die vom BDSG gewollte Befugnis der *Kommission* zur Bestimmung der Angemessenheit des Schutzniveaus national unterlaufen.

■ Das genannte Kompetenzproblem scheinen auch die deutschen Aufsichtsbehörden nicht so einfach „umschiffen" zu können, denn es heißt in der o.g. Presserklärung weiter: „Schließlich fordert die Konferenz die Europäische Kommission auf, ihre Entscheidungen zu Safe Harbor und zu den Standardverträgen vor dem Hintergrund der exzessiven Überwachungstätigkeit ausländischer Geheimdienste bis auf Weiteres zu suspendieren." Diese Aufforderung spielt den Ball nach Brüssel. Wenn jemand irgendwelche belastbare Kompetenz in diesem Bereich hat, dann die *EU-Kommission* bzw. der *Ausschuss nach Art. 31 DS-RL*. Bisher gibt es keine konkreten Anhaltspunkte, dass die *EU-Kommission* den massiven und für Unternehmen schmerzhaften Eingriff befürwortet, Safe Harbor oder die EU-Standardklauseln einseitig zu suspendieren. Die zuständige EU-Kommissarin *Reding* scheint klugerweise erst einmal abwarten zu wollen.[12]

■ Dies ist nicht das erste Mal, dass bei Safe Harbor mit Platzpatronen geschossen wird: Eine Initiative der deutschen Datenschutzbeauftragten gegen Safe Harbor gab es schon mehrmals, zuletzt in der „Orientierungshilfe – Cloud Computing" der *Arbeitskreise Technik und Medien der DSK*.[13] Dort heißt es: „Solange jedoch 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." Ähnliche (weniger konkrete) zusätzliche Erfordernisse für deutsche Datenexporteure hatten die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich in einem Beschluss v. 28/29.4.2010[14] aufgestellt. Darüber, ob dieses Aufsatteln von Pflichten den zitierten EU-Regeln und internationalen Abmachungen zu Safe Harbor entspricht, kann man vielleicht geteilter Meinung sein. Es hat bis dato bezeichnenderweise keine Sanktionen der Aufsichtsbehörden gegen deutsche Unternehmen gegeben, die diesen Nachprüfungspflichten nicht oder unzureichend Folge geleistet haben. Fest steht, dass die Bestrebungen der deutschen nationalen Aufsichtsbehörden, Erkundigungspflichten für deutsche Datenexporteure auf die Safe Harbor-Prinzipien „aufzusatteln", nie von der amerikanischen Seite akzeptiert worden sind. Dies hat das *US-Handelsministerium* zuletzt in seinem Memorandum v. 12.4.2013 „Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing"[15] zum Ausdruck gebracht.[16]

■ Allenfalls könnte die Erklärung der Datenschutzbeauftragten in zwei Fällen Bedeutung und nach deutschem Recht Bestand haben:

---

9 Vgl. http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_safe_harbour_en.pdf; zu denken ist an den Fall des unzulässigen „Onward-Transfers".

10 S. Schreiben der *EU-Kommission* an US-Handelsminister *La Russa* v. 28.1.2000, Az. 4074; DG Markt/E-1 D(2000)168: "As indicated by Article 2 of the decision, evidence that any enforcement body in the United States responsible for compliance with the principles is failing to secure compliance may trigger action by the Commission, in consultation with the Member States through the Article 31 Committee…", abrufbar unter: http://export.gov/static/sh_en_EUletter27JulyHeader_Latest_eg_main_018403.pdf.

11 So auch *A. Schneider*, vgl. https://www.telemedicus.info/article/2613-Die-Drohung-mit-der-Aussetzung-von-Safe-Harbor.html.

12 EU-Kommissarin *Reding* will lt. Medienberichten eine solide Einschätzung („solid assessment") von Safe Harbor abwarten: http://dataguidance.com/news.asp?id=2078; der Schwerpunkt der *EU-Kommission* scheint derzeit eher auf der EU-Datenschutzreform zu liegen, s. *Reding*, RBB-Podcast v. 6.9.13, abrufbar unter: http://mediathek.rbb-online.de/inforadio/interviews?documentId=16933700.

13 Vgl. http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf (Stand: 26.9.2011).

14 Überarbeitete Fassung v. 23.8.2010, abrufbar unter: http://www.bfdi.bund.de/cae/servlet/contentblob/1103868/publicationFile/88848/290410_SafeHarbor.pdf; der Kernsatz in diesem Beschluss lautet: „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 Harbor-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."; s.a. *Schuppert/von Reden*, ZD 2013, 210, 213 m.w.Nw.

15 Vgl. http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf.

16 Zur Erläuterung im Einzelnen s. *Spies/Schröder*, ZD-Aktuell 2013, 03566.

■ ■ **Binding Corporate Rules (BCR):** Die sog. Binding Corporate Rules (BCR)[17] – also konzernweite Datenschutzregeln – bedürfen der Genehmigung der beteiligten Datenschutzbehörden. Es ist damit zu rechnen, dass die Aufsichtsbehörden bei BCR verstärkt Fragen nach dem Datenzugang Dritter in den USA stellen und detailliert Auskunft verlangen werden. Die deutschen Behörden werden BCR wohl dann nicht (mehr) genehmigen, wenn die *NSA* und andere ausländische Geheimdienste nach den gegenwärtigen Erkenntnissen umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf personenbezogene Daten zugreifen, die von Unternehmen in Deutschland an Stellen in den USA übermittelt werden. Die wenig wünschenswerte Konsequenz wird wohl sein, dass noch weniger große Unternehmen die Genehmigung von BCR beantragen werden. Bislang scheint die *Deutsche Post/DHL* das einzige deutsche Unternehmen zu sein, das den recht mühevollen und teuren Prozess erfolgreich abgeschlossen hat.

■ ■ **Individualvertragliche genehmigungspflichtige Vereinbarungen gem. § 4c Abs. 2 BDSG:** Nach der Presseerklärung zu urteilen werden die Aufsichtsbehörden für den Datenschutz keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten erteilen. Damit können die Fälle gemeint sein, wenn der Transfer auf der Grundlage einer genehmigungspflichtigen individualvertraglichen Vereinbarung erfolgt. Das passiert relativ selten.

IV. Kurzes Fazit

Die o.g. Presseerklärung könnte eine neue Eskalationsstufe in der Auseinandersetzung mit den Amerikanern über den Datenfluss in die USA einläuten oder die gerade mit „Pomp and Circumstances" angelaufenen transatlantischen TTIP-Verhandlungen insgesamt verzögern.[18] Zumindest führt die Initiative (parallel zu den politischen Bemühungen der *deutschen Bundesregierung* auf mehreren Ebenen um Klärung im NSA-Skandal) zu Rechtsunsicherheit bei den vielen Datenexporteuern und – importeuren, die sich seit Jahren auf die Geltung der Safe Harbor-Prinzipien bzw. der Standardklauseln verlassen.[19]

Präsident *Obama* hat am 9.8.2013 einige Reformen bei der NSA-Überwachung[20] angekündigt. Es gibt dennoch keine Anhaltspunkte, dass sich hierdurch die Einschätzung der deutschen Datenschützer ändert. Sollten die Aufsichtsbehörden auf Grund der – an sich rechtlich belanglosen – Presseerklärung Taten (konkret: Sanktionen) folgen lassen, ist mit Klagen der betroffenen Unternehmen zu rechnen.

Darüber hinaus ist zu bedenken: Wie eine solche Sanktion, den Datenfluss in die USA nach Safe Harbor oder den Standardklauseln auszusetzen, praktisch aussehen soll und wer sie in Deutschland verhängen soll, ist offen. Viele große Unternehmen haben Server in vielen Ländern und nicht nur in Deutschland.

Die Androhung von Sanktionen steht auch nicht im Einklang mit den kürzlich vom *BMWi* (*Task Force IT*) am 31.7.2013 veröffentlichten 10 Punkten für einen sicheren Umgang mit Unternehmensdaten im Internet.[21] Dort heißt es unter Punkt 7: „Bei Cloud-Service-Providern aus anderen Staaten kann ein angemessenes Schutzniveau dadurch gewährleistet werden, dass der Cloud-Service-Provider mindestens am Safe Harbor-Programm teilnimmt." Mit anderen Worten, die deutsche *Task Force IT* empfiehlt den Unternehmen einen Dienstleister, der nach Safe Harbor zertifiziert ist, während die eigenen Datenschutzbehörden den Datenfluss dorthin am liebsten noch heute unterbinden möchten.

Nur am Rande: Was meint die *Task Force* mit „mindestens"? Gibt es für die *Task Force* noch zusätzliche Verpflichtungen? Was ist mit Dienstleistern, die anderswo außerhalb der EU/des EWR ansässig sind? Was ist, wenn ein Dienstleister aus rechtlichen Gründen nicht an Safe Harbor teilnehmen kann?

In aller Kürze zum Schluss: Noch mysteriöser ist die in der Presseerklärung angesprochene potenzielle Suspendierung oder gar Sanktionsverhängung bei Nutzung der EU-Standardklauseln.[22] Für die Nutzung dieser in der Praxis beliebten EU-Standardklauseln gibt es keinerlei Registrierungspflicht in Deutschland oder den USA. Für viele US-Unternehmen ist das ein handfester Vorteil gegenüber der öffentlichen Safe Harbor-Liste. Wie die Aufsichtsbehörde deren Nutzung trotz der fehlenden Registrierung dem Gleichheitsgrundsatz entsprechend aussetzen will, bleibt offen.

Auf der anderen Seite des Atlantiks hat *Damon Greer*, der langjährige und international erfahrene ehemalige Leiter des Safe Harbor-Programms beim *US-Department of Commerce* die Position der USA klar umrissen: „Die Verachtung der EU-Datenschutz-Gemeinde für Safe Harbor basiert heute nicht sehr auf Bedenken beim Grundrechtsschutz der Bürger, sondern wird an der Dominanz der US-multinationalen [Großkonzerne] im High-Tech-Sektor in Europa und in den USA festgemacht. Unser Rechtssystem ist nicht das ihrige, sie verstehen es nicht, oder sie ziehen es vor, nicht zuzuhören, wenn unser System erklärt wird; sie schmälern so die Bemühungen von allen Parteien, Kompromisse zwischen den USA und der EU zu erreichen."

Bis heute, also über einen Zeitraum von fast 13 Jahren, sei es auf EU-Seite trotz aller Kritik zu keinem abschließenden „Audit" des bestehenden EU/US-Safe Harbor-Systems gekommen, beklagt der *Autor*.[23] Wie immer die Debatte ausgeht – etwas mehr Besonnenheit statt eines Griffs an den Revolverholster hätte den deutschen Aufsichtsbehörden bei diesem politisch im Wahlkampf aufgeladenen NSA-Thema gut getan.

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Bingham McCutchen in Washington, D.C. und Mitherausgeber der ZD.
Der Aufsatz ist eine erweiterte Fassung des Kurzbeitrags aus ZD-Aktuell 2013, 03691.

17 Vgl. *Filip*, ZD 2013, 51.
18 Vgl. *EDRI*-Erklärung v. 13.6.13, abrufbar unter: http://www.edri.org/nodpinttip.
19 *Schuppert/von Reden*, ZD 2013, 210, 215: „sichere Methode"; lesenswert zum Vergleich sind die dort geschilderten Befugnisse zum Datenzugriff der deutschen Behörden (a.a.O., 218).
20 Vgl. http://blog.beck.de/2013/08/09/usa-nsa-berwachung-und-kritik-neuer-vier-punkte-plan-von-pr-sident-obama.
21 Vgl. http://www.bmwi.de/DE/Themen/digitale-welt,did=587382.html.
22 Vgl. http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.
23 *Grier*, Safe Harbor May Be Controversial in the European Union, But It Is Still the Law, abrufbar unter: https://www.privacyassociation.org/publications/safe_harbor_may_be_controversial_in_the_european_union_but_it_is_still_the.