



Sachstand

**Einzelfragen zum Abkommen über eine transatlantische
Handels- und Investitionspartnerschaft (TTIP) im Kontext von
Datenschutz, Datentransfer und Datensicherheit**



Einzelfragen zum Abkommen über eine transatlantische Handels- und Investitionspartnerschaft (TTIP) im Kontext von Datenschutz, Datentransfer und Datensicherheit

Verfasserin: [REDACTED]
Aktenzeichen: WD 10 - 3000 – 094/14
Abschluss der Arbeit: 16.01.2015
Fachbereich: WD 10: Kultur, Medien und Sport
Telefon: [REDACTED]

Ausarbeitungen und andere Informationsangebote der Wissenschaftlichen Dienste geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung.

[REDACTED]

Inhaltsverzeichnis

1.	Einleitung	4
2.	In wie weit waren in den bisherigen TTIP- Verhandlungen die Themen Datenschutz, Datentransfer und/ oder Datensicherheit Gegenstand der Verhandlungen?	5
2.1.	Interoperabilität und Lokalisierung	6
3.	Könnten die Forderungen der USA nach einer Einbeziehung von IT- Produkten mit personenbezogener Datenverarbeitung in die TTIP- Verhandlungen, die Aktivitäten der europäischen Wirtschaft für mehr Datenschutz sowie IT- Sicherheit gefährden?	10
4.	Gibt es Anzeichen dafür, dass Datenschutz und IT- Sicherheitsstandards (z.B. CC EAL) als technische Handelshemmnisse bei den TTIP-Verhandlungen gewertet werden könnten?	12
5.	Inwieweit enthalten die Vorschläge bzw. die Verhandlungspapiere der US-Seite Vorgaben, die die „digitale Souveränität“ Deutschlands oder Europas unterlaufen?	13
6.	Quellenverzeichnis	14

1. Einleitung

Das derzeit zwischen der Europäischen Union und den Vereinigten Staaten von Amerika verhandelte Abkommen über eine transatlantische Handels- und Investitionspartnerschaft (TTIP) steht sowohl hinsichtlich des Verfahrens als auch aufgrund bekannt gewordener Inhalte oder befürchteter Folgen der geplanten Freihandelspartnerschaft zunehmend in der öffentlichen Kritik.¹ Dabei wurde zunächst besonders intensiv die Vertraulichkeit der Verhandlungen kritisiert, die zur Folge hatte, dass im ersten Jahr der Verhandlungen ab Juli 2013 kaum gesicherte Informationen über Ziele und Inhalt des Vorhabens bekannt wurden. Erst im Oktober 2014 veröffentlichte der Rat der EU das Verhandlungsmandat zu TTIP, auf dessen Grundlage die insoweit zuständige Kommission für Handelspolitik der EU die Verhandlungen mit der amerikanischen Seite führt.

Demnach werden mit TTIP weit umfassendere Ziele verbunden als mit traditionellen Freihandelsabkommen, denn über den verbesserten Marktzugang durch Zollabbau hinaus bezieht sich das neue Abkommen auch auf die Bereiche Regulierungsfragen und nicht-tarifäre Handelshemmnisse sowie Regeln.² Besonders schwierig gestaltet sich offenbar der Bereich Regulierung und nicht-tarifäre Handelshemmnisse. Denn dort treffen auch die Erwartungen größten wirtschaftlichen Nutzens der TTIP-Befürworter auf die Befürchtungen der Kritiker, die durch eine Harmonisierung von Standards einen Verlust von Vielfalt und Regulierungsniveau in bestimmten Bereichen sehen (FELBER/FALKE 2014: 29/30).

Während sich die Diskussion in der Öffentlichkeit bislang stark auf Beispiele aus dem Lebensmittelbereich (Stichwort „Chlorhühnchen“) und Pflanzenschutz (Stichwort „Gentechnik“) bezog, werden von Kritikerseite seit einigen Monaten zunehmend auch die Bereiche Datenschutz und IT-Sicherheitsstandards thematisiert (WEICHERT 2014; ALBRECHT 2014). Gerade in diesem Bereich sind die Unterschiede zwischen beiden Seiten besonders groß. Und gerade bezüglich dieser Thematik hat die NSA-Affäre, die fast zeitgleich mit dem Beginn der TTIP-Verhandlungen durch die Enthüllungen des ehemaligen NSA-Mitarbeiters Snowden ausgelöst wurde, in Europa zu einer großen Vertrauenskrise gegenüber den USA geführt.

Auf den nachfolgenden Seiten werden verschiedene Einzelfragen behandelt, die zu dem oben genannten Themenkomplex an den Wissenschaftlichen Dienst heran getragen wurden. Dabei wurden die Recherchemöglichkeiten dadurch begrenzt, dass trotz größerer Transparenzbemühungen der EU-Kommission Informationen zum Verlauf der Verhandlungsrunden oder gar zu den Positionen und Vorschlägen beider Seiten nur eingeschränkt – und von amerikanischer Seite gar nicht – zugänglich sind. Die hier zusammen gestellten Informationen können daher nicht mehr als einen aktuellen Sachstand darstellen, der auch schon aufgrund der noch andauernden Verhandlungen noch keine abschließenden Aussagen über die mit dem TTIP Abkommen etwaig für europäische Datenschutzstandards ausgehenden Risiken erlaubt.

1 Hierzu beispielhaft FELBER/FALKE 2014: 25ff.

2 SCHMUCKER zufolge wird mit modernen Freihandelsabkommen auch das Ziel verfolgt, in Bereichen, die bislang vom Regelwerk der Welthandelsorganisation nicht erfasst werden, neue Regeln zu schaffen (SCHMUCKER 2014: 20 und 22).

2. Inwieweit waren in den bisherigen TTIP- Verhandlungen die Themen Datenschutz, Datentransfer und/ oder Datensicherheit Gegenstand der Verhandlungen?

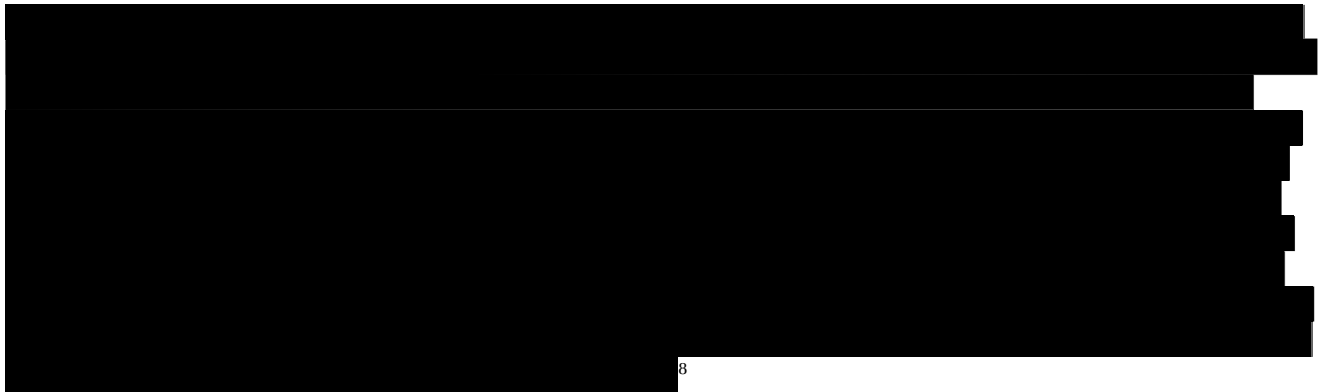
Die Frage, inwieweit Datenschutz und Datensicherheit in den TTIP- Verhandlungen erörterte Themen sind, ist zwischen Befürwortern und Gegnern des Abkommens umstritten. Von Seiten der EU-Kommission wurde wiederholt betont, dass von TTIP keine Gefahr für europäische Standards beim Datenschutz ausgehe und dort auch nicht verhandelt würden, denn die TTIP Verhandlungen seien „nicht der rechte Ort“, um die seit langem bekannten transatlantischen Unterschiede in dieser Hinsicht zu thematisieren. Dafür gäbe es geeignetere Möglichkeiten, wie „beispielsweise das Safe-Harbour-Abkommen“.³ Explizit gegen eine Einbeziehung grundlegender Datenschutzfragen in die TTIP-Verhandlungen hatte sich im Oktober 2013 die damalige EU-Kommissarin für Justiz Viviane Reding ausgesprochen: „I warn against bringing data protection to the trade talks. Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable.“⁴

Dementsprechend findet **Datenschutz als grundsätzliches Thema keine Erwähnung** im offiziellen Verhandlungsmandat, das der EU-Kommission am 17. Juni 2013 vom Europäischen Rat erteilt wurde. Das Thema gehört sogar zu den durch Artikel 18 des Mandats ausdrücklich geschützten Ausnahmen, „on the supply of services justifiable under the relevant WTO rules (Articles XIV and XIVbis GATS).“⁵ In diesen im Allgemeinen Abkommen über den Handel mit Dienstleistungen (GATS) formulierten Ausnahmen wird unter anderem garantiert, dass dieses Abkommen nicht dahingehend ausgelegt werden darf, „dass es die Annahme oder Durchsetzung von Maßnahmen eines Mitglieds verhindert“ ... „zum Schutz der Persönlichkeit bei der Verarbeitung und Weitergabe personenbezogener Daten und zum Schutz der Vertraulichkeit persönlicher Auszeichnungen und Konten.“⁶

Auch die Bundesregierung betont, dass Datenschutzfragen an sich kein Thema in den TTIP-Verhandlungen sind und sogar für eine Behandlung in diesem Rahmen ungeeignet seien. Dennoch berührten auch einige im Rahmen von TTIP behandelte Fragen das Thema, denn

-
- 3 Vgl. EU Kommission. About TTIP (deutsch). Häufig gestellte Fragen. Online unter: http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/questions-and-answers/index_de.htm (Stand: 08.01.2015).
 - 4 Vgl. EU Commission. Viviane Reding, Vice-President of the European Commission and EU Justice Commissioner. “Towards a more dynamic transatlantic area of growth and investment”. Main Messages of a speech on 29th October 2013 in Washington, D.C.. Online unter: [http://europa.eu/rapid/press-release SPEECH-13-867_de.htm](http://europa.eu/rapid/press-release_SPEECH-13-867_de.htm) (Stand: 08.01.2015).
 - 5 Vgl. Council of the European Union. Directives for the negotiation on the Transatlantic Trade and Investment Partnership between the European Union and the United States of America, adopted on 14 June 2013 (Doc. 11103/13 DCL 1). Online unter: <http://data.consilium.europa.eu/doc/document/ST-11103-2013-DCL-1/en/pdf> (Stand: 08.01.2015).
 - 6 Vgl. Artikel XIV. In: Europäische Gemeinschaft. Die multilaterale Verhandlungen der Uruguay-Runde (1986- 1994) - Anhang 1 - Anhang 1B - Allgemeines Übereinkommen über den Handel mit Dienstleistungen (WTO) WTO vom 22.12.1994. Online unter [http://eur-lex.europa.eu/legal-content/DE/NOT/?uri=CELEX:21994A1223\(16\)](http://eur-lex.europa.eu/legal-content/DE/NOT/?uri=CELEX:21994A1223(16)) (Stand: 08.01.2015).

„Datenschutz [betrifft] zum Beispiel auch handelsbezogene Kommunikation, d.h. etwa bei Dienstleistungen im IKT-Bereich auch Fragen, ob und wie Regeln und Vorschriften zusammen passen ("regulative Kompatibilität"). Solche Aspekte werden im Rahmen von TTIP behandelt. Auch Fragen des Datenschutzes beim Dienstleistungshandel, bei E-Commerce oder im IKT-Bereich werden mit dem Ziel einer gemeinsamen Verständigung angesprochen. TTIP hat jedoch keinen Einfluss auf die gegenwärtig laufenden Verhandlungen zur EU-Datenschutzreform.“⁷



So verweist der wissenschaftliche Mitarbeiter des Europaabgeordneten Jan Philipp Albrecht und Datenschutzexperte RALF BENDRATH auf einen derzeit dem US-Senat vorliegenden Gesetzentwurf zum digitalen Handel (*Digital Trade Act of 2013*), der „Vertretern der Vereinigten Staaten ein bindendes Mandat für internationale Verhandlungen zum E-Commerce in die Hand geben [würde].“ (BENDRATH 2014). Gemäß Abschnitt 3 des Gesetzentwurfs, der im Oktober 2013 eingebracht wurde und derzeit dem Finanzausschuss des US-Senats zur Beratung vorliegt, sollen als „Verhandlungsprinzipien“ (*negotiating principles*) für alle künftigen bilateralen, plurilateralen oder multilateralen Abkommen der USA unter anderem die „interoperability of data protection regimes“ und ein Verbot von Maßnahmen zur „localization of data, infrastructure, or investment“ festgelegt werden.⁹

2.1. Interoperabilität und Lokalisierung

Die Begriffe Interoperabilität und Lokalisierung haben sich seit einigen Jahren im Zusammenhang mit Diskussionen zum Thema Datenschutz im transatlantischen Verhältnis sowohl auf politischer Ebene als auch zwischen Unternehmen beider Seiten als zentrale Stichworte für die

7 Vgl. Bundesministerium für Wirtschaft und Energie (BMWi). Häufig gestellte Fragen zur Transatlantischen Handels- und Investitionspartnerschaft (TTIP), Thema Datenschutz / 1. Frage. Online unter: : <http://www.bmwi.de/DE/Themen/Aussenwirtschaft/Ttip/faqs.html> (Stand: 08.01.2015).

8

9 Vgl. 113th Congress (2013-2014). S. 1788 – Digital Trade Act of 2013. Section 3, No. (1) (interoperability) and No. (4) (localization). Online unter: <https://www.congress.gov/bill/113th-congress/senate-bill/1788/text> (Stand: 09.01.2015).

grundlegenden Unterschiede der Standpunkte herausgebildet. Sie sollen deshalb nachfolgend genauer erläutert werden:

Mit dem Begriff **Interoperabilität** wird ein in den USA entwickelter und aus dortiger Sicht als wünschenswert angesehener Lösungsansatz für die derzeit vorhandene grundlegende Unvereinbarkeit der Datenschutzregime zwischen der EU und den USA bezeichnet. Diese Situation wird in einem Bericht der internationalen Handelskommission der Vereinigten Staaten (*U.S. International Trade Commission*) von 2013 erläutert.

Demnach unterscheiden sich ganz allgemein die Datenschutzregime unterschiedlicher Länder grundlegend dadurch, ob sie ein alle Bereiche umfassendes Datenschutzrecht haben oder je nach Bereich unterschiedlich regeln. Dabei wird die EU mit ihrer Datenschutzverordnung als „primary example“ für den umfassenden Regelungsansatz genannt. Demgegenüber fehle in den USA ein allgemeines Datenschutzgesetz gänzlich. Stattdessen bestünden unterschiedliche Datenschutzregelungen für einzelne Bereiche wie Banken, Krankenversicherungen und für den Kinderschutz im Internet, die ergänzt würden durch „targeted enforcement of privacy requirements by the Federal Trade Commission, the Department of Health and Human Services, and other federal and state regulators“.¹⁰ Insgesamt gesehen sei die datenschutzrechtliche Situation der Verbraucher in den USA trotz des Fehlens eines allgemeinen Gesetzes deutlich stärker, wenn konkrete Regelungen einzelner Unternehmen und die zunehmend aktive Rolle bestimmter Institutionen für den Datenschutz betrachtet würden.¹¹

Die EU dagegen verfolge mit der umfassend geltenden Datenschutzverordnung einen grundsätzlich anderen Ansatz. Da jedoch trotz der allgemein geltenden Regelung jeder Mitgliedstaat der EU seine eigenen, zum Teil stark variierenden Implementierungsgesetze erlassen habe, sei für Firmen, die Daten innerhalb der EU transportieren wollten, eine uneinheitliche und unvorhersagbare Situation entstanden. Betroffene Wirtschaftsvertreter in den USA drängten daher darauf, dass die durch unterschiedliche Datenschutzgesetze in den EU-Mitgliedstaaten entstandene „fragmentation, inconsistency, redundancy and procedural complexity“ ein prioritäres Thema in den TTIP-Verhandlungen sein sollten, denn auch das Safe Harbour Abkommen aus dem Jahr 2000 beseitige nicht die Uneinheitlichkeit der gesetzlichen Situationen in den einzelnen EU-Mit-

10 Diesem sektoralen Ansatz folgen auch andere Länder wie z.B. ¹⁰Brasilien, Indien, Thailand oder Simbabwe. Vgl. U.S. Trade Commission. *Digital Trade in the U.S. and Global Economies*, Part 1. Investigation No. 332-531. USITC Publication 4415. July 2013, p. 5-10. Online unter: <http://www.usitc.gov/publications/332/pub4415.pdf> (Stand: 09.01.2015). Eine sehr kurze Darstellung datenschutzrechtlicher Vorgaben auf den verschiedenen Ebenen des us-amerikanischen Rechtssystems und in den von der FTC erwähnten einzeln geregelten inhaltlichen Bereichen findet sich in einer Zusammenstellung des Wissenschaftlichen Dienstes des Europäischen Parlamentes (*European Parliamentary Research Service*). Jan Baeverstroem. „TTIP and the Question of Data Protection“. 03. November 2014, S. 1-2. Online unter: <http://epthinktank.eu/2014/11/03/ttip-the-question-of-data-protection/> (Stand: 14.01.2015).

11 Vgl. FTC 2013 p. 5-10. Damit stützt sich die FTC auf die Ergebnisse einer Studie von Forschern der Stanford Universität aus dem Jahr 2011, in der dargelegt wird, dass vor allem in Reaktion auf die Verabschiedung der EU-Datenschutzverordnung im Jahr 2000 und damit verbundener Befürchtungen von Umsatzeinbrüchen für us-amerikanische Unternehmen der Elektronikbranche auf dem wichtigen europäischen Markt, unterhalb der Schwelle eines allgemeinen Datenschutzgesetzes eine Vielzahl neuer Regelungen und Verfahren in den USA entwickelt wurden. Diese hätten im Ergebnis die datenschutzrechtliche Situation für Verbraucher in den USA deutlich gestärkt, wobei gerade die FTC und ihre zunehmend aktive Rolle in dieser Hinsicht eine zentrale Rolle gespielt habe (BAMBERGER/MULLIGAN 2011: 281 ff., insbesondere 285-287).

gliedsländern. Anzustreben sei daher eine „Interoperabilität“ zwischen Ländern mit unterschiedlichen Datenschutzregelungen. Im Unterschied zu einer Harmonisierung sei Interoperabilität von der Annahme geleitet,

„that while there are different privacy approaches, the outcomes generally will be similar and thus should be entitled to mutual recognition. More specifically, interoperability requires that organizations take on binding obligations to protect private information based on established criteria; that there are mechanisms to enforce these obligations; and that regulatory agencies can depend on each other to ensure that these obligations are honored when data travels around the world.“ (FTC 2013: 5-11).

Sollte diese gegenseitige Anerkennung im transatlantischen Verhältnis nicht gelingen, bestünde die Gefahr eines erheblichen Vertrauensverlustes der Konsumenten in internetbasierte Geschäfte und Produkte, zum Beispiel im Zusammenhang mit Datenanalysen oder Big Data. Auch seien die wegen der divergenten und komplexen Datenschutzsituation erforderlichen Maßnahmen mit erhöhten Kosten für die betroffenen Firmen verbunden, was wiederum eine Begünstigung der marktbeherrschenden großen Firmen mit sich bringe (FTC 2013: 5-11 f.). Aufgrund grundlegender Unterschiede zwischen der EU und den USA in kultureller und rechtlicher Hinsicht sei eine Interoperabilität zudem eher zu erreichen als eine Harmonisierung. Abschließend konstatiert der FTC-Bericht, dass auch unter Einbeziehung derzeit sowohl in den USA wie auch der EU bestehender datenschutzrechtlicher Reformbestrebungen substantielle Unterschiede zwischen beiden Rechtssituationen bestehen blieben. (FTC 2013: 5-15).

Die Obama Administration hat bereits im Jahr 2012 unter dem Titel „Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy“ einen Rahmenplan vorgestellt, mit dem das Datenschutzrecht in den USA umfassend reformiert werden soll. Dessen wichtigste Elemente sind ein vorgeschlagener Katalog von „Datenschutzgrundrechten für Konsumenten“ (*Consumer Bill of Rights*), eine deutliche Stärkung der Kompetenzen der Federal Trade Commission zur Durchsetzung datenschutzrechtlicher Vorschriften (wie auch für Ausnahmeregelungen für Firmen, die sich durch zertifizierte Selbstverpflichtungen (*Codes of Conduct*) gebunden haben sowie ein Ausgleich zwischen Bundes- und Landeszuständigkeiten im amerikanischen Datenschutzrecht (WHITE HOUSE 2012).

Nach Einschätzung der New York Times würde die Umsetzung dieser Initiative der US-Administration amerikanischen Verbrauchern „many of the same baseline protections [geben] that the draft European rule proposes to inforce.“ (NYT 2013). Auch wenn diese Bewertung im Rahmen der vorliegenden Arbeit inhaltlich nicht näher überprüft werden kann, bleibt festzuhalten, dass eine Verabschiedung der nötigen Gesetze durch den 113. U.S. Kongress nicht erfolgte. Ob diese in der gerade begonnenen Legislaturperiode des 114. U.S. Kongresses mit den für den amerikanischen Präsidenten ungünstigeren Mehrheitsverhältnissen gelingen wird und Appelle an den Kongress, den Schutz von Verbraucherdaten an die erste Stelle seiner Tagesordnung zu setzen, erfolgreich sein werden (BREYALD 2014), bleibt abzuwarten. Doch auch im Reformplan der Administration spielt der Begriff der Interoperabilität im Bereich der internationalen Zusammenarbeit eine wichtige Rolle. (WHITE HOUSE 2012: 31-33). Vor diesem Hintergrund kann sicher davon ausgegangen werden, dass die us-amerikanische Seite in den TTIP-Verhandlungen entsprechende Vorschläge unterbreiten wird.

Ein weiterer kritischer Punkt in den Verhandlungen zwischen den USA und der EU zum Thema Datenschutz wird von den USA unter dem Stichwort „**Lokalisierung**“ zusammengefasst. Damit sind Vorschläge gemeint, die vereinzelt bereits im Jahr 2012¹², besonders intensiv jedoch seit Bekanntwerden der Enthüllungen des früheren NSA-Mitarbeiters Edward Snowden im Juli 2013 bekannt wurden und darauf zielen, europäische Daten so weit wie möglich innerhalb des Schengen-Raums zu halten. Insbesondere die Deutsche Telekom hatte sich mit entsprechenden Vorschlägen für ein „Schengen-Netz“ positioniert¹³ und trat auch dafür ein, das Safe Harbour Abkommen mit den USA zu kündigen. Innerhalb des Branchenverbandes Informationstechnik, Telekommunikation und neue Medien (Bitkom), dem sowohl deutsche wie auch amerikanische Unternehmen angehören, war es daraufhin zu intensiven Auseinandersetzungen um ein Positionspapier zu diesen Fragen gekommen.¹⁴ Auch unter deutschen Unternehmen und IT-Experten findet die Idee eines innereuropäischen Netzes jedoch kaum Unterstützung.¹⁵

Die USA wenden sich gegen diese Vorstöße für eine regionale Begrenzung von Datenflüssen und sehen in ihnen „a means of providing protectionist advantage to EU-based ICT suppliers.“¹⁶ Diese Vorschläge wie auch die Drittstaatenregelungen der EU-Datenschutzverordnung, die die Verarbeitung von Daten nur in Staaten mit verlässlichen Datenschutzvorschriften

12 Vgl. Deutsche Telekom. „So zuverlässig wie sonst nirgends: Datenschutz in der EU“. <http://www.telekom.com/medien/medienmappen/104306> (Stand: 09.01.2015).

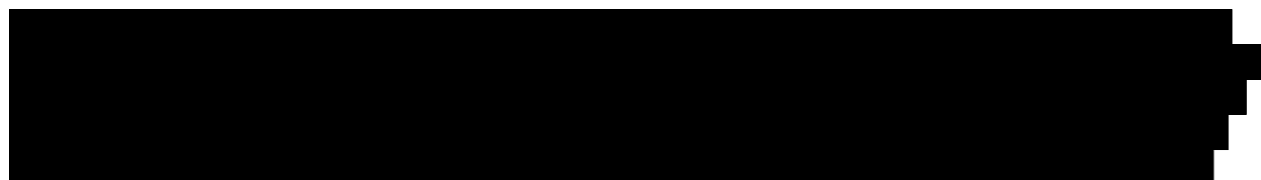
13 Vgl. „Die Telekom und der NSA-Skandal: Auf ins Schengen-Netz“. Heise online vom 11.11.2013. Online unter: <http://www.heise.de/newsticker/meldung/Die-Telekom-und-der-NSA-Skandal-Auf-ins-Schengen-Netz-2043536.html> (Stand: 12.01.2015).

14 Vgl. „Deutsche Telekom und der Abhörskandal: Allein gegen die Amerikaner.“ In: Wirtschaftswoche vom 17.02.2014. Online unter: <http://www.wiwo.de/unternehmen/it/deutsche-telekom-und-der-abhoerskandal-allein-gegen-die-amerikaner-/9481452.html> (Stand: 13.01.2015).

15 Vgl. „Cyber-Security Summit: Wenig Unterstützung für Schengen-Netz.“ Heise online vom 04.11.2014. Online unter: <http://www.heise.de/security/meldung/Cyber-Security-Summit-Wenig-Unterstuetzung-fuer-Schengen-Netz-2441784.html> (Stand: 13.01.2015). Von Expertenseite äußerte sich unter anderem kritisch zu der Idee Ralf Bendrath, IT-Experte und Mitarbeiter des Europaabgeordneten Jan Philipp Albrecht, MdEP. Nicht nur sei ein „Geo-Routing“ technisch schwierig. Selbst wenn es das nicht sei, „kann es doch nicht unser Ziel sein, die Topologie des transnationalen, weltweiten Internets entlang der Ländergrenzen neu zu formen.“ (BENDRATH 2014: 3).

16 Bericht des U.S. Handelsbeauftragten Michael Froman: 2014 Section 1377 Review On Compliance with Telecommunication Trade Agreements, S. 4. Online unter: <http://www.ustr.gov/sites/default/files/04032013%202013%20SECTION%201377%20Review.pdf> (Stand: 13.01.2015).

ten (zu denen die USA nicht gezählt werden) zulassen, fassen die USA in dem Begriff „Lokalisierungsbestrebungen“ zusammen, die sie in ihren Auswirkungen offenbar als ein Handelshemmnis ansehen.¹⁷



¹⁸ Vor dem Hintergrund der vorstehend erläuterten Positionen der USA zu diesen Fragen bleibt abzuwarten, ob sich die EU in den TTIP-Verhandlungen am Ende wird durchsetzen können in ihrem Bestreben, die unterschiedlichen Datenschutzregelungen beider Seiten durch dieses Abkommen unberührt zu lassen und dafür weiterhin bereits vorhandene „geeignete Möglichkeiten zum Umgang mit dem transatlantischen Datenfluss“, wie das Safe-Harbour-Abkommen, zu nutzen.¹⁹

3. Könnten die Forderungen der USA nach einer Einbeziehung von IT- Produkten mit personenbezogener Datenverarbeitung in die TTIP- Verhandlungen, die Aktivitäten der europäischen Wirtschaft für mehr Datenschutz sowie IT- Sicherheit gefährden?

Über „Forderungen der US-Seite, informationstechnische Produkte mit personenbezogener Datenverarbeitung [in die TTIP-Verhandlungen] einzubeziehen“ berichtete das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein in einer Pressemitteilung vom 08.09.2014 und bezog sich dabei auf eine Analyse von Unterlagen über die 5. Verhandlungsrunde zu TTIP im Mai 2014. Insbesondere handele es sich dabei um Forderungen der USA nach Einbeziehung „von

17 Entsprechende Äußerungen zitiert Jan Philipp Albrecht, MdEP aus der Vorstellung des Berichts des US-Handelsbeauftragten zu Handelsabkommen für den Telekommunikationsmarkt am 4. April 2014. (ALBRECHT 2014: 3). Siehe hierzu auch das von den Vorsitzenden des Finanz- und des *Ways-and-Means*-Ausschusses unterzeichnete Schreiben an den Präsidenten des Europäischen Parlamentes Martin Schulz vom 25.11.2014. Darin äußern die Abgeordneten ihre Sorge über einen „trend in the European Union towards discriminating against foreign companies with respect to the digital economy.“ Auch die Vorschläge zur „localization of cloud services“ werden explizit erwähnt. (Congress of the United States. Letter to President Martin Schulz, European Parliament. Washington, D.C. 2015: 25 November 2014. Online unter: <https://placelux.files.wordpress.com/2014/11/lettre-du-congres-americain-a-martin-schulz.pdf> (Stand: 14.01.2015).

18 A small black rectangular redaction box.

19 Vgl. Europäische Kommission. Generaldirektion für Handel. TTIP - Häufig gestellte Fragen: Bedeutet TTIP, dass die US-amerikanischen Standards beim Datenschutz Vorrang vor den Standards der EU haben oder diese untergraben? Online unter: http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/questions-and-answers/index_de.htm (Stand: 14.01.2015).

Diensten der Telekommunikation, der Telemedien, des Online-Handels, zu E-Health, zu Verschlüsselung und Cloud-Services, von Finanzdienstleistungen, Medien- und Beratungsleistungen.“²⁰

[REDACTED]

[REDACTED]²¹

[REDACTED]

[REDACTED]²²

20 „Kein Freihandelsabkommen bei personenbezogenen Dienstleistungen“. Pressemitteilung des UNABHÄNGIGEN LANDESZENTRUMS FÜR DATENSCHUTZ SCHLESWIG- HOLSTEIN vom 08.09.2014.; Online unter: <https://www.datenschutzzentrum.de/presse/20140908-freihandelsabkommen-ttip.htm>, (Stand 14.01.2015).

21 [REDACTED]

22 [REDACTED]

4. Gibt es Anzeichen dafür, dass Datenschutz und IT-Sicherheitsstandards (z.B. CC EAL) als technische Handelshemmnisse bei den TTIP-Verhandlungen gewertet werden könnten?

Die **Common Criteria for Information Technology Security Evaluation**, kurz: „Common Criteria (CC)“, sind ein internationaler Standard zur **Bewertung und Zertifizierung der Sicherheit von IT-Systemen**. Er wurde ab 1993 von europäischen Staaten, Kanada und den USA entwickelt und ist seit 1999 ein weltweit anerkannter Standard. Das Ziel einer Evaluierung eines Produkts nach den Common Criteria ist die Bestätigung, dass die vom Hersteller behauptete Sicherheitsfunktionalität wirksam ist.

Innerhalb der *Common Criteria* wird auch die Vertrauenswürdigkeit einer Sicherheitsleistung bewertet und dies geschieht anhand eines Klassifizierungsschemas in sieben Stufen: **Evaluation Assurance Levels – EAL**. Dabei bezeichnet EAL 7 die Stufe mit den höchsten Anforderungen an eine IT-Sicherheitsprüfung in Bezug auf ihre Prüftiefe, die somit in der Regel auch am aufwändigsten und kostenintensivsten ist.²³

Um die Mehrfachzertifizierung des gleichen Produkts in verschiedenen Staaten zu vermeiden, werden unter Beteiligung nationaler Zertifizierungsbehörden internationale Abkommen ausgehandelt, die dann von den jeweiligen Staaten unterzeichnet werden. Für die Koordinierung und Umsetzung des jeweiligen Abkommens ist dann jeweils ein Management Committee zuständig.

Für die europäische Anerkennung von Sicherheitszertifikaten auf Basis der CC ist das *Senior Officials Group Information Systems Security - Mutual Recognition Arrangement – (SOGIS-MRA)*, dem die zehn Staaten Frankreich, Niederlande, Italien, Deutschland, Spanien, das Vereinigte Königreich, die Vereinigten Staaten, Österreich, Finnland und Norwegen angehören. Die weltweite Anerkennung erfolgt dagegen auf der Basis des **Common Criteria Recognition Agreement (CCRA)**. Diesem gehörten bei seiner Gründung im Jahr 1998 Kanada, Frankreich, Deutschland, das Vereinigte Königreich und die Vereinigten Staaten sowie Australien und Neuseeland an. Zwischenzeitlich ist die Zahl der Mitglieder auf 26 angestiegen und umfasst neben den oben genannten Gründungsmitgliedern auch Dänemark, Finnland, Griechenland, Indien, Israel, Italien, Japan, Malaysia, Niederlande, Norwegen, Österreich, Pakistan, Südkorea, Schweden, Singapur, Spanien, die Türkei, Tschechien und Ungarn.²⁴

Bis zum Jahr 2014 galt für beide Anerkennungsabkommen eine Zertifizierung gemäß den Common Criteria bis zur Prüftiefe EAL 4 als gegenseitig anerkannt. Bei der jährlichen CCRA-Konferenz im Jahr 2012 jedoch wurde ein „Vision Statement“ verabschiedet, das einen Übergangsprozess zu einem konzeptionell veränderten Evaluierungsverfahren und die Senkung der gegenseitig

23 Nähere Informationen hierzu finden sich auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/ITSicherheitskriterien/CommonCriteria/eal_stufe.html (Stand: 14.01.2015).

24 Vgl. CCRA-Website. Online unter: <https://www.commoncriteriaportal.org/ccra/members/> (Stand: 15.01.2015). Die Mitgliedstaaten werden „Certificate Producers“ und „Certificate Consumers“ unterschieden.

anerkannten Prüftiefe auf EAL 2 avisierte.²⁵ Schließlich wurde bei der ICCC im Jahr 2014 ein neues Abkommen verhandelt, das EAL 2 als gegenseitig anerkannte Evaluierungsstufe festlegte.²⁶

Es trifft zu, dass damit nunmehr innerhalb des europäischen Anerkennungsabkommens SOGIS-MRA mit EAL 4 ein höherer Zertifizierungsstandard zugrunde gelegt wird als im weltweiten Abkommen, dem auch die USA angehören. Inwieweit diese Unterschiede im Rahmen der TTIP-Verhandlungen thematisiert werden oder zu welchen konkreten Vereinbarungen sie führen könnten, bleibt abzuwarten. Konkrete Hinweise hierzu liegen derzeit nicht vor.

5. Inwieweit enthalten die Vorschläge bzw. die Verhandlungspapiere der US-Seite Vorgaben, die die „digitale Souveränität“ Deutschlands oder Europas unterlaufen?

Die Unterlagen der US-Verhandlungsdelegation beim TTIP sind öffentlich nicht zugänglich, so dass über die vorangegangenen Ausführungen (insbesondere zu Frage 2) hinaus keine weiteren Informationen hierzu gegeben werden können.

25 CCRA. Vision statement for the future direction of the application of the CC and the CCRA. September 2012. Online unter: http://www.commoncriteriaportal.org/files/ccfiles/2012-09-001_Vision_statement_of_the_CC_and_the_CCRAv2.pdf (Stand: 15.01.2015).

26 CCRA. Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security. 2. Juli 2014. Zur EAL siehe Article 2: Scope. Online unter: <http://www.commoncriteriaportal.org/files/CCRA%20-%20July%202014%20-%20Ratified%20September%202014.pdf> (Stand: 15.01.2015). Zur Beschreibung des veränderten Verfahrens mit sogenannten “Protection Profiles” siehe WIKIPEDIA. Common Criteria. Online unter: http://en.wikipedia.org/wiki/Common_Criteria (Stand: 15.01.2015).

6. Quellenverzeichnis

ALBRECHT, JAN PHILIPP (2014). Datenschutz ist nicht verhandelbar. Heinrich-Böll-Stiftung: 21.05.2014. Onlinedossier zum Thema TTIP. Online unter <http://www.boell.de/de/2014/05/07/datenschutz-ist-nicht-verhandelbar>, (Stand 15.12.14).

BAMBERGER, KENNETH A. / MULLIGAN, DEIRDRE K. (2011). Privacy on the Books and on the Ground. Stanford Law Review, Vol. 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385. Online unter: <http://ssrn.com/abstract=1568385> (Stand: 09.01.2015).

BENDRATH, RALF (2014). TTIP und TISA: USA wollen Datenschutz wegverhandeln. In: Beckedahl, Markus / Biselli, Anna / Meister, André. Jahrbuch Netzpolitik 2014.

BREYHAULT, JOHN (2014). Protecting Consumer's Data should be at Top of new Congress' Agenda. In: Congress Blog. The Hill's Forum for Lawmakers and Policy Professionals. Eintrag vom 18.12.2014. Online unter: <http://thehill.com/blogs/congress-blog/homeland-security/227507-protecting-consumers-data-should-be-at-top-of-new> (Stand: 12.01.2015).

FELBER, CHRISTIAN / FALKE, ANDREAS (2014). TTIP kontrovers. In: Aus Politik und Zeitgeschichte , Heft 50-51/2014, S. 25 – 33.

SCHMUCKER, CLAUDIA (2014). TTIP im Kontext anderer Freihandelsabkommen. In: Aus Politik und Zeitgeschichte , Heft 50-51/2014, S.17 – 23.

WEICHERT, THILO (2014). Freihandelsabkommen contra Datenschutz? Herausgegeben vom Unabhängigen Datenschutzzentrum Schleswig-Holstein. Kiel: 08.09.2014. Online unter <https://www.datenschutzzentrum.de/internationales/20140908-freihandelsabkommen-ttip-contra-datenschutz.html> (Stand 12.12.14).

WHITE HOUSE (2012). „Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy”. The White House. Washington, D.C.: February 2012. Online unter: <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> (Stand: 12.01.2015).