

Antwort der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Renate Künast,
Dieter Janecek, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 18/7746 –**

Konsequenzen aus dem „Safe Harbor“-Urteil des Europäischen Gerichtshofs

Vorbemerkung der Fragesteller

Der Europäische Gerichtshof (EuGH) hat am 6. Oktober 2015 die sogenannte „Safe Harbor“-Regelung der Europäischen Kommission mit den Vereinigten Staaten von Amerika für unwirksam erklärt, ohne Übergangsfrist. Seit diesem Datum ist damit die notwendige zentrale Rechtsgrundlage der Privatwirtschaft für Informations- bzw. Datentransfers in die USA entfallen. Das Urteil betrifft über 4 000 Unternehmen, darunter auch zahlreiche bundesdeutsche Unternehmen. Nach Ablauf der von der Artikel-29-Gruppe der Datenschutzbeauftragten der EU-Mitgliedstaaten ausgesprochenen Frist präsentierte die Europäische Kommission am 2. Februar 2016 mündlich Inhalte einer Einigung mit den USA unter dem Namen EU-US Privacy Shield.

Über eigene Aktivitäten der Bundesregierung zur Lösung der nach dem EuGH-Urteil eingetretenen, auch nach der jüngsten Einigung unverändert rechtlich unsicheren Situation ist bislang nichts bekannt. Die Bundesregierung baut vielmehr ihre Kooperation mit der für das Urteil ursächlich gewordenen US-amerikanischen National Security Agency (NSA) weiter aus (vgl. Süddeutsche Zeitung vom 8. Januar 2016, BND und NSA kooperieren wieder in Bad Aibling, abrufbar unter: www.sueddeutsche.de/politik/abhoerskandal-bnd-und-nsa-kooperieren-wieder-in-bad-aibling-1.2810828, zuletzt abgerufen am 2. Februar 2016). Dabei wirft die im Lichte der Enthüllungen von Edward Snowden getroffene, in seiner Reichweite kaum zu überschätzende Kernaussage des Gerichts, wonach zu weitgehende Zugriffsmöglichkeiten von Sicherheitsbehörden ein für Datentransfers in dieses Land bzw. das für Übermittlungen in die USA EU-rechtlich erforderliche angemessene Schutzniveau ausschließen, gravierende und weitergehende Fragen auf.

Wirtschaftsverbände auf beiden Seiten des Atlantiks monieren zu Recht die für ihre Unternehmen entstandene Rechtsunsicherheit (vgl. SPIEGEL ONLINE vom 18. Januar 2016, Safe Harbor: Verbände schreiben Brandbrief an EU und Obama, abrufbar unter: www.spiegel.de/netzwelt/netzpolitik/safe-harbor-unternehmer-verbaende-senden-brandbrief-a-1072543.html, zuletzt abgerufen am 2. Februar 2016). Der Ausgang der auf europäischer wie nationaler Ebene anstehenden Gespräche der im EuGH-Urteil gestärkten nationalen Datenschutzbehörden zu einer möglichen gemeinsamen Positionierung bleibt nach wie vor

ungewiss. Auf Nachfragen des Parlamentes zur Positionierung reagiert die Bundesregierung aus Sicht der Fragesteller ausweichend (siehe die Antworten auf die Kleine Anfrage der Fraktion Die Linke. vom 21. Dezember 2016 auf Bundestagsdrucksache 18/7134).

Es erscheint angeraten, den dahinterliegenden, grundlegenden Konflikt zwischen einer ausgefeilten Geheimdienstpolitik westlicher Regierungen einerseits und den menschen- wie grundrechtlichen Gewährleistungen andererseits ebenso wie die Unterschiede zwischen US- und EU-Recht zur Frage der Schutzwürdigkeit von Privatsphäre und Privatheit schnellstmöglich und entschlossen mit allen beteiligten Akteuren anzugehen und die vom höchsten europäischen Gericht monierten Praktiken effektiv abzustellen.

Vorbemerkung der Bundesregierung

Bevor die Kleine Anfrage bei der Bundesregierung eingegangen ist, hat die Europäische Kommission am 29. Februar 2016 als mögliche „Safe Harbor“-Nachfolgeregelung den Entwurf eines Angemessenheitsbeschlusses zu dem neu verhandelten „Privacy Shield“ (EU-US-Datenschutzschild) vorgelegt. Der Entwurf umfasst als Anhänge sieben Schreiben der US-Administration mit von US-Unternehmen einzuhaltenden Datenschutzgrundsätzen sowie Zusicherungen der US-Regierung zu Garantien und Beschränkungen für den behördlichen Datenzugriff und ist auf der Internetseite der Kommission abzurufen (http://europa.eu/rapid/press-release_IP-16-433_en.htm).

1. Teilt die Bundesregierung die Auffassung, wonach insbesondere die globale Abkehr der Mitgliedstaaten von der ungezielten Massenüberwachung der Zivilgesellschaften sowie allgemein eine rechtsstaatlich und menschenrechtlich effektive Einhegung von Überwachungseingriffen eine zentrale Grundlage für eine rechtssichere, auf dem globalen Austausch von Informationen und Daten basierende Weltwirtschaft darstellt?

Die Bundesregierung teilt die Auffassung, dass eine Vermeidung ungezielter Massenüberwachung von Zivilgesellschaften sowie allgemein eine rechtsstaatlich und menschenrechtlich effektive Einhegung von Überwachungseingriffen eine zentrale Grundlage für eine rechtssichere, auf dem globalen Austausch von Informationen und Daten basierende Weltwirtschaft darstellt.

2. Welche über das Urteil hinausgehenden Maßnahmen leitet die Bundesregierung national, supranational und international vor dem Hintergrund der Tatsache, dass Entscheidungen des Europäischen Gerichtshofs lediglich die zwingend von den Mitgliedstaaten zu beachtenden rechtlichen (Mindest-) Vorgaben enthalten, in die Wege, um das vom Gericht eindeutig artikulierte, zugrundeliegende Problem sowohl übermäßiger staatlicher Überwachung und mangelhafter rechtlicher Schutzvorkehrungen im Sinne der Menschen- und Grundrechte der Bürgerinnen und Bürger als auch der Wirtschaft konstruktiv und effektiv voranzubringen?

Die Bundesregierung setzt sich sowohl bilateral als auch international für die Wahrung von Menschenrechten online wie offline ein.

Den Vereinten Nationen (VN) kommt dabei eine Schlüsselrolle zu. Auf eine deutsch-brasilianische Initiative hin wurde zum Beispiel im Jahr 2015 das Mandat für einen Sonderberichterstatter für das Recht auf Privatleben im Menschenrechtsrat der VN geschaffen. Zuvor hatte Deutschland ebenfalls zusammen mit

Brasilien 2013 und 2014 Resolutionen zum Recht auf Privatheit im digitalen Zeitalter in die VN-Generalversammlung eingebracht, die dort im Konsens angenommen wurden.

Die Bundesregierung bringt sich intensiv in die Reform der Europaratskonvention 108 ein (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten). Menschenrechtliche Anforderungen haben auch die Verhandlungen zum EU-US-Rahmenabkommen „Umbrella Agreement“ und zum EU-US-Datenschutzschild „Privacy Shield“ geprägt.

3. Unter welche Rechtsnormen des bundesdeutschen als auch des US-amerikanischen Rechts fällt die kürzlich in Bad Aibling wiederaufgenommene Kooperation der Bundesregierung mit der Obama-Administration bzw. von Bundesnachrichtendienst (BND) und National Security Agency (NSA) bei der Telekommunikationsüberwachung von Informationen und Daten (vgl. Süddeutsche Zeitung vom 8. Januar 2016, BND und NSA kooperieren wieder in Bad Aibling, abrufbar unter: www.sueddeutsche.de/politik/abhoerskandal-bnd-und-nsa-kooperieren-wieder-in-bad-aibling-1.2810828, zuletzt abgerufen am 2. Februar 2016), und aufgrund welchen faktischen Prüfverfahrens sowie aufgrund welcher rechtlicher Grundlage bewertet die Bundesregierung diese Normen als auch das Wiederanfahnen dieser Kooperation als mit den Grundsätzen des „Safe Harbor“-Urteils des Europäischen Gerichtshofs für vereinbar?

Die einschlägigen US-amerikanischen Rechtsnormen, unter denen es US-amerikanischen Behörden wie der National Security Agency (NSA) gestattet ist, Kooperationen einzugehen, sind der Bundesregierung im Einzelnen nicht bekannt. Die Kooperation des Bundesnachrichtendienstes (BND) mit ausländischen Behörden in Bad Aibling stützt sich auf § 1 Absatz 2 des BND-Gesetzes (BNDG). Übermittlungen zwischen Nachrichtendiensten waren und sind von dem Regelungsgehalt der Entscheidung der Europäischen Kommission vom 26. Juli 2000 („Safe Harbor“-Entscheidung) nicht erfasst, da sie nicht in den Anwendungsbereich der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) fallen, deren Umsetzung die „Safe Harbor“-Entscheidung diente.

4. Schließt die Bundesregierung auf der Grundlage der von ihr nach den Snowden-Enthüllungen inzwischen angeblich ergriffenen (www.tagesschau.de/inland/bnd-nsa-113.html) tatsächlichen und/oder rechtlichen Maßnahmen aus, dass ihre eigenen Überwachungsmaßnahmen als auch ihre Kooperationen mit ausländischen Nachrichtendiensten die Grundrechte von EU-Bürgerinnen und EU-Bürgern verletzen?

Die Grundrechte binden in ihrem Anwendungsbereich die vollziehende Gewalt als unmittelbar geltendes Recht. Die Nachrichtendienste des Bundes sind zudem für ihre Aufgabenwahrnehmung an das jeweils für sie geltende Fachrecht gebunden.

5. Welche konkreten innerstaatlichen Rechtsvorschriften und internationalen Verpflichtungen sichern das angemessene Schutzniveau im Umgang des BND und des Bundesamts für Verfassungsschutz (BfV) mit Informationen und Daten der Angehörigen von Drittstaaten, insbesondere von US-Bürgerinnen und US-Bürgern bei Datenerfassungen und Datenverarbeitungen durch die und in der Bundesrepublik Deutschland, um den zwingenden Vorgaben des „Safe Harbor“-Urteils, insbesondere der Pflicht zum Schutz der freien Kommunikation durch hinreichend konkrete und verhältnismäßige gesetzliche Regelungen zu genügen?

Die Erhebung und Verwendung von personenbezogenen Daten von Angehörigen von Drittstaaten durch den BND und das Bundesamt für Verfassungsschutz (BfV) richten sich nach den jeweils anwendbaren Fachgesetzen (BNDG, Bundesverfassungsschutzgesetz – BVerfSchG, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses – G10-Gesetz). Diese gewährleisten einen angemessenen Datenschutz.

6. Teilt die Bundesregierung die Auffassung, dass die deutsche Rechtslage etwa für die Erteilung eines „Freibriefes“ des Bundeskanzleramtes an die Deutsche Telekom für Massenzugriffe auf in Deutschland gelegene Glasfaserkabel sowie das Teilen der Ergebnisse des Abgriffes mit der NSA (vgl. Netzpolitik.org vom 12. Juni 2015, Live-Blog aus dem Geheimdienst-Untersuchungsausschuss, abrufbar unter: <https://netzpolitik.org/2015/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-ex-bnd-praesident-ernst-uhrlau-und-dieter-urmann/>, zuletzt abgerufen am 2. Februar 2016) den im „Safe Harbor“-Urteil niedergelegten, aus Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (GRCh) abgeleiteten Anforderungen des EuGH (siehe insbesondere Rn. 91 des Urteils) standhalten würde, und wenn ja, welche Rechtsschutzmöglichkeiten gab es für die von dem damaligen Abgriff Betroffenen?

Das „Safe Harbor“-Urteil des Europäischen Gerichtshofs (EuGH) vom 6. Oktober 2015 (Rs. C-263/14) findet auf den Datenaustausch zwischen Nachrichtendiensten keine Anwendung; auf die Antwort zu Frage 3 wird insoweit verwiesen. Für den BND lassen sich hieraus keine zwingenden rechtlichen Vorgaben oder Anforderungen ableiten.

7. Auf welche Weise unterstützte die Bundesregierung, wie auch etwa von den Datenschutzbeauftragten des Bundes und der Länder gefordert, konkret das Ziel der Europäischen Kommission, zeitnah ein neues „Safe Harbor“-Abkommen zu erreichen, und was stand einer zeitnahen Vereinbarung entgegen?

Die Europäische Kommission hat am 29. Februar 2016 als mögliche „Safe Harbor“-Nachfolgeregelung den Entwurf eines Angemessenheitsbeschlusses zu dem neu verhandelten „Privacy Shield“ vorgelegt.

Damit hat die Europäische Kommission ihrer mit den USA am 2. Februar 2016 erzielten politischen Einigung zügig ein konkretes Maßnahmenpaket folgen lassen.

8. Zu welchen konkreten Terminen welcher Gremien insbesondere des Rates fand insbesondere seit der Verkündung des Urteils sowie nach der Verkündung der Einigung mit den USA am 2. Februar 2016 auf welcher Rechtsgrundlage eine Einbeziehung der Mitgliedstaaten zum weiteren Vorgehen der Europäischen Kommission statt?

Erfolgte etwa vorab eine inhaltliche Abstimmung bezüglich des Verhandlungsmandats der EU-Kommission für ein „Safe Harbor 2.0“, und wenn ja, welchen konkreten Inhalts?

Das Verhandlungsmandat der Europäischen Kommission ergibt sich direkt aus Artikel 25 Absätze 5 und 6 der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG). Die EU-Mitgliedstaaten sind über den Artikel 31 – Ausschuss (einem Komitologie-Ausschuss gemäß Verordnung EU Nr. 182/2011) im Hinblick auf die Annahme des neuen Angemessenheitsbeschlusses beteiligt. Am 7. April 2016 wird dieser Ausschuss erstmals zum „Privacy Shield“ beraten. Die Europäische Kommission will dort Einzelheiten zum Datenschuttschild erläutern.

9. Bestehen außer den in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. zu Frage 5 genannten Fällen (siehe Bundestagsdrucksache 18/7134) weitere Fälle, insbesondere TK-Provider-Verträge und/oder Outsourcing- und Cloud-Verträge von Stellen im Geschäftsbereich der Bundesregierung, bei denen die beauftragten Unternehmen unter die „Safe Harbor“-Regelung fielen oder nach wie vor fallen?

Falls ja, welche Konsequenzen hat die Bundesregierung zwischenzeitlich daraus gezogen?

Das Bundesministerium für Arbeit und Soziales (BMAS) hat zum 1. Januar 2016 einen neuen Vertrag mit dem Unternehmen Microsoft über Premier Support Services abgeschlossen, bei dem als Standard für den Datenschutz das „Safe Harbor“-Modell galt. Aufgrund der „Safe Harbor“-Entscheidung des EuGH wurde mit dem Unternehmen Microsoft ein EEA Data Privacy Offering als Add-On abgeschlossen. Über die EEA Data Privacy Services kann sichergestellt werden, dass im Rahmen des Problemlösungssupports anfallende Daten ausschließlich im Europäischen Wirtschaftsraum verarbeitet und gespeichert werden.

Auch das Bundesministerium für Wirtschaft und Energie (BMWi) hat am 16. Juli 2015 eine Auftragsdatenvereinbarung mit Microsoft geschlossen, die festlegt, dass die Datenverarbeitung ausschließlich auf dem Gebiet der Bundesrepublik Deutschland zu erfolgen hat.

10. Teilt die Bundesregierung die Auffassung, wonach die Gesetzeslage in Großbritannien und in Frankreich, die dort jüngst verabschiedeten Sicherheitsgesetze sowie die durch die Snowden-Dokumente bekanntgewordene Überwachungspraxis digitaler Kommunikation etwa des britischen Geheimdienstes GCHQ (Government Communications Headquarters) ein den Datenschutzrisiken für EU-Bürger mit den USA vergleichbares, unangemessenes Schutzniveau schafft, und mit welchen Mitteln beabsichtigt die Bundesregierung, gegen diese die Grundrechte der EU-Bürgerinnen und EU-Bürger ebenfalls und in ähnlich starkem Maße beeinträchtigende Situation vorzugehen?

Gemäß Artikel 51 Absatz 1 Satz 1 Charta der Grundrechte der Europäischen Union (GRCh) gilt diese für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union. Gemäß Artikel 4 Absatz 2 Satz 3 Vertrag über die Europäische Union (EUV) fällt die nationale Sicherheit in die alleinige Verantwortung der einzelnen Mitgliedstaaten.

11. Was hat die Bundesregierung konkret seit der Entscheidung des EuGH getan, um konstruktiv auf wirksame Schutzvorkehrungen für Verbraucherinnen und Verbraucher und Unternehmen hinzuarbeiten und damit den schwebenden Konflikt zwischen EU und USA zu entschärfen?

Die Bundesregierung hat stets deutlich gemacht, dass zur Wiederherstellung einer sicheren Rechtslage die zügige Vorlage eines Vorschlags für ein konkretes Maßnahmenpaket durch die Europäische Kommission erforderlich ist, das im Einklang mit den vom EuGH aufgestellten Kriterien steht. Im Übrigen obliegt es den unabhängigen Datenschutzaufsichtsbehörden sicherzustellen, dass die Datenverarbeiter im Einklang mit den Vorschriften des Bundesdatenschutzgesetzes Daten in Drittstaaten übermitteln.

12. Teilt die Bundesregierung die Auffassung, dass die Glaubwürdigkeit der EU-Verhandlungsposition eine Schwächung erfährt, wenn einige EU-Mitgliedstaaten selbst im Hinblick auf den aus Artikel 7 und 8 GRCh gebotenen, ableitbaren Grundrechtsschutz dringenden Nachholbedarf in ihrer Sicherheitsgesetzgebung aufweisen, und wenn ja, welche Schritte unternimmt sie, um diesen Missstand zu beheben?

Auf die Antwort zu Frage 10 wird verwiesen.

13. Welche EU-Rechtsgrundlagen für Informations- bzw. Datenübermittlungen in die USA könnten nach Ansicht der Bundesregierung von dem jüngsten EuGH-Urteil zu „Safe Harbor“ ebenfalls betroffen sein (bitte konkrete Auflistung einschließlich gesonderter Datenabkommen wie PNR, SWIFT usw.), und was hat die Bundesregierung unternommen, um diese Frage zu klären und ggf. auch weitere Abkommen schnellstmöglich auf ihre Rechtskonformität hin zu überprüfen?

Es wird auf die Antwort der Bundesregierung zu Frage 26 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/7134 vom 21. Dezember 2015 verwiesen. Die Rechtskonformität des Entwurfs eines PNR-Abkommens zwischen der Europäischen Union und Kanada wird derzeit vom EuGH auf Antrag des Europäischen Parlaments gemäß Artikel 218 Absatz 11 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) überprüft.

14. Welche nationalen Rechtsgrundlagen, bilateralen Abkommen sowie anderweitige US-Vorgaben und US-Anforderungen, die zwingend zu Datenübermittlungen von Behörden oder Unternehmen an US-Stellen führen oder Datenübermittlungen zwischen Behörden oder Unternehmen in Deutschland und den USA rechtlich legitimieren, könnten nach Ansicht der Bundesregierung von dem jüngsten EuGH-Urteil zu „Safe Harbor“ ebenfalls betroffen sein (bitte konkrete Auflistung), und was hat die Bundesregierung unternommen, um diese Frage zu klären und ggf. auch weitere Abkommen oder Vereinbarungen schnellstmöglich auf ihre Rechtskonformität hin zu überprüfen?

Eine Ressortabfrage hat ergeben, dass keine anderen Regelungen, die einen Datentransfer zwischen Behörden oder Unternehmen in Deutschland mit US-Behörden legitimieren, von dem EuGH-Urteil betroffen sind.

15. Teilt die Bundesregierung die Auffassung des Europäischen Gerichtshofs, wonach Regelungen, die in allgemeiner und nicht näher bestimmter Art und Weise den Zugriff auf Inhaltsdaten elektronischer Kommunikation ermöglichen, als Beeinträchtigung des Kernbereichs („essence“) von Artikel 7 GRCh anzusehen sind, und entspricht die derzeitige gesetzliche Regelung der sogenannten „strategischen“ BND-Rasterfahndung (nach dem Artikel 10-Gesetz als auch die sog. „Routineerfassung“ nach dem Gesetz über den Bundesnachrichtendienst) nach Ansicht der Bundesregierung den aus Artikel 7 GRCh abgeleiteten gesetzlichen Anforderungen des EuGH?

Mit Blick auf die GRCh wird auf die Antwort zu Frage 10 verwiesen. Soweit die in der Charta verbrieften Grundrechte dem Grundrechte-Kanon des Grundgesetzes entsprechen, wird auf die Antwort zu Frage 4 verwiesen.

16. Teilt die Bundesregierung den Ansatz des Europäischen Gerichtshofs, wonach unabhängig vom tatsächlichen Bestehen oder vom tatsächlichen Ausmaß von „Five Eyes“-Überwachungsprogrammen wie PRISM oder TEMPORA bereits die Untersuchung des geltenden US-Rechts im Hinblick auf den Schutz von Nicht-US-Bürgerinnen und -Bürgern Grundrechtsbeeinträchtigungen zumindest der Artikel 7 und 8 GRCh belegt und schon deshalb entsprechende, wie im Urteil dargelegte Schutzvorkehrungen zum Schutz des Telekommunikationsgeheimnisses und der Privatheit zu treffen sind, und wenn nein, warum nicht?

Die Bundesregierung begrüßt, dass mit dem von der Europäischen Kommission vorgeschlagenen EU-US-Datenschutzschild „Privacy Shield“ u. a. im US-Außenministerium eine Ombudsstelle eingerichtet wird, an die sich Unionsbürgerinnen und -bürger mit Rechtsschutzbegehren wenden können, die den Bereich der nationalen Sicherheit der USA betreffen und sie begrüßt, dass von der US-amerikanischen Presidential Policy Directive 28 aus dem Jahr 2014, die datenschutzrechtliche Grundsätze für den gesamten Bereich der Fernmeldeaufklärung etabliert, grundsätzlich auch Unionsbürgerinnen und -bürger erfasst werden (die nicht dem Schutz des Vierten Zusatzartikels zur Verfassung der Vereinigten Staaten unterfallen).

17. Teilt die Bundesregierung die Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (www.datenschutz.rlp.de/de/grem_dsbkonferenz/sonstiges/20151021_Positionspapier_DSK_Safe_Harbor.pdf), wonach den Datenschutzbehörden gesetzlich ein eigenes Klagerecht einzuräumen ist, und wenn ja, bis wann wird sie dazu einen Entwurf vorlegen?

Wenn nein, warum nicht?

Die Bundesregierung prüft diese Frage im Zusammenhang mit der Anpassung des nationalen Datenschutzrechts an die EU-Datenschutzgrundverordnung.

18. Teilt die Bundesregierung die Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (www.datenschutz.rlp.de/de/grem_dsbkonferenz/sonstiges/20151021_Positionspapier_DSK_Safe_Harbor.pdf), wonach insbesondere die Entscheidungen der Europäischen Kommission zu Standardvertragsklauseln nach Fristablauf ebenfalls unwirksam sind bzw. umgehend an die im EuGH-Urteil gemachten Vorgaben anzupassen sind, und wenn ja, auf welche Weise plant die Bundesregierung, dies durch welche konkrete gesetzgeberische Tätigkeit zu berücksichtigen?

Die Überprüfung von Entscheidungen der Europäischen Kommission zu Standardvertragsklauseln fällt nicht in die Zuständigkeit der Bundesregierung, sondern der Kommission selbst. Zukünftig sieht Artikel 42 der EU-Datenschutzgrundverordnung vor, dass Feststellungen der Europäischen Kommission zu Standardvertragsklauseln durch Beschluss der Europäischen Kommission geändert, ersetzt oder aufgehoben werden.

Neben der Europäischen Kommission können die Standardvertragsklauseln nur vom EuGH für ungültig oder nichtig erklärt werden. Im Einzelfall kann die Rechtmäßigkeit einer Datenübermittlung auf der Grundlage alternativer Instrumente jederzeit durch die Datenschutzbehörden der Mitgliedstaaten überprüft werden. Nationalen gesetzgeberischen Handlungsbedarf sieht die Bundesregierung daher nicht.

19. Teilt die Bundesregierung die Auffassung, dass die Einholung individueller Einwilligungen kaum eine praktikable, vor allem aber eine in vielerlei Hinsicht rechtlich fragwürdige alternative Rechtfertigung für den Wegfall des „Safe Harbor“-Abkommens darstellt (so etwa wegen der stets bestehenden Widerspruchsmöglichkeit) und deshalb kaum als Ersatz in Frage kommen kann?

Der EuGH hat sich in seinem „Safe Harbor“-Urteil nicht zum Instrument der Einwilligung geäußert. Sowohl das Bundesdatenschutzgesetz als auch die EU-Datenschutzrichtlinie 95/46/EG und zukünftig die EU-Datenschutzgrundverordnung sehen die Übermittlung aufgrund Einwilligung vor. Die Einwilligung kann als Rechtsgrundlage eines Datentransfers herangezogen werden, in denen keine Angemessenheitsentscheidung bzw. kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt.

20. Teilt die Bundesregierung die Auffassung, wonach das sogenannte Umbrella Agreement und der nach Auskunft der US-Regierung geplante und im US-Kongress anhängige Judicial Redress Act schon deshalb nicht den vom EuGH verlangten individuellen Rechtsschutz für EU-Bürgerinnen und -Bürger bieten können, weil diese Instrumente Streitigkeiten zu den von Unternehmen in die USA übermittelten Daten entweder überhaupt nicht mitumfassen, sondern sich ausschließlich auf Übermittlungen zwischen behördlichen Stellen von EU und USA beziehen (Umbrella Agreement) oder deren Anwendungsbereich allenfalls einen geringen Bruchteil der im europäischen Datenschutz möglichen Rechte der von Datenverarbeitung Betroffenen in den USA verfolgbar machen würde?

Der EuGH hat in seinem „Safe Harbor“-Urteil ein Schutzniveau gefordert, das dem EU-Niveau gleichwertig ist, welches sich „aufgrund der Richtlinie 95/46 im Licht der Charta“ (der Grundrechte) ergibt.

Vom Anwendungsbereich der Richtlinie sind gemäß Artikel 3 Absatz 2 der EU-Datenschutzrichtlinie Verarbeitungen ausgenommen, die die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des

Staates im strafrechtlichen Bereich betreffen. Das „Umbrella Agreement“ bezieht sich auf der Strafverfolgung dienende Datenübermittlungen, unterfällt damit nicht dem Anwendungsbereich der Datenschutzrichtlinie und folglich auch nicht den im „Safe Harbor“-Urteil vom EuGH aufgestellten Anforderungen.

21. Teilt die Bundesregierung die vom früheren Landesdatenschutzbeauftragten von Berlin vertretene Auffassung, wonach durchgehende und starke Verschlüsselungen der in die USA übermittelten Daten als technisch-organisatorische Schutzmaßnahme, neben anderen Maßnahmen, bei der Frage der rechtlichen Zulässigkeit der Datenübertragung positiv zu berücksichtigen sind, und wenn nein, warum nicht?

Die Bundesregierung teilt diese Auffassung.

22. Teilt die Bundesregierung die Auffassung der Fragesteller, wonach besonderer Handlungsdruck für die Erzielung EU-grundrechtskonformer Ergebnisse auch deshalb geboten erscheint, weil aufgrund der voraussichtlich erst im Jahr 2018 zur Anwendung kommenden Europäischen Datenschutzverordnung und des darin geregelten Abstimmungsverfahrens der nationalen Datenschutzbeauftragten zwischenzeitlich für die Frage der transatlantischen Datenübermittlungen ein sogenanntes „forum shopping“ zum Nachteil der Rechte der Bürgerinnen und Bürger droht?

Falls nein, warum nicht?

Die Bundesregierung hat stets die Notwendigkeit einer zügigen Nachfolgeregelung zu der „Safe Harbor“-Entscheidung deutlich gemacht. Wichtig ist eine stabile Rechtsgrundlage für den transatlantischen Datenaustausch, die den Anforderungen des EuGH gerecht wird und europaweit einheitlich angewandt wird.

23. Wird die Bundesregierung die Gelegenheit der Vorgaben des EuGH-Urteils auch nutzen, um europäische und nationale Vorschläge und Lösungen beispielsweise im Bereich der IT- und Datensicherheit voranzutreiben?

Falls ja, welche konkret?

Falls nein, warum nicht?

Die Bundesregierung evaluiert stetig die Rechtsentwicklung und passt die Rechtslage an Entwicklungen aufgrund neuester Rechtsprechung oder Vorgaben der Europäischen Union an.

24. Wie lautet konkret der Rat der Bundesregierung für bundesdeutsche Unternehmen, bzw. auf welche Weise unterstützt die Bundesregierung aktuell die Unternehmen, damit sie sobald als möglich die notwendige Rechtssicherheit für ihre transatlantischen Datenverkehre erlangen können?

Wie auch die Europäische Kommission mehrfach erläutert und ausgeführt hat, standen und stehen den deutschen Unternehmen nach der Ungültigerklärung der „Safe Harbor“-Entscheidung alternative Instrumente gemäß Bundesdatenschutzgesetz und Richtlinie 95/46 EG zur Verfügung, auf die ein Datentransfer gestützt werden kann. Neben der bereits erwähnten Einwilligung sind dies derzeit insbesondere die Standardvertragsklauseln, welche die Europäische Kommission nach Artikel 26 Absatz 4 der Richtlinie 95/46 EG vorgelegt hat. Auf nationaler Ebene hat die Bundesregierung beispielsweise im BMWi Round-Table-Gespräche mit Vertretern der Wirtschaft und Datenschutzbehörden zu den Regeln für Datentransfers aus der Europäischen Union in die USA geführt.

25. Gehen nach Auffassung der Bundesregierung die Regelungen des Umbrella Agreements allen sekundärrechtlichen Bestimmungen der EU vor, also auch den Bestimmungen des jüngst ausgehandelten Datenschutzreformpakets und wenn ja, weshalb?

Nach der Rechtsprechung des EuGH sind völkerrechtliche Verträge der Europäischen Union integrierende Bestandteile der Unionsrechtsordnung. Rechtswirksam gewordene völkerrechtliche Verträge im Kompetenzbereich der Europäischen Union gehen im Verhältnis zur Vertragspartei entgegenstehendem sekundärem Unionsrecht vor.

26. Teilt die Bundesregierung die Auffassung, dass das Umbrella Agreement den primärrechtlichen Vorgaben insbesondere der Artikel 7 und 8 GRCh genügen muss, und wenn nein, weshalb nicht?

Die Unionsorgane müssen die GRCh auch beim Abschluss völkerrechtlicher Verträge beachten.

27. Teilt die Bundesregierung die Auffassung, wonach Artikel 5 Absatz 3 des Umbrella Agreements die Adäquanz-Entscheidung eines internationalen Abkommens an die Stelle der Adäquanz-Entscheidung der Europäischen Kommission setzt und damit Möglichkeiten der Beanspruchung gerichtlichen Rechtsschutzes vor dem EuGH abschneidet, und wenn nein, warum nicht?

Die Bundesregierung sieht den von den Fragestellern gezogenen Schluss nicht als zwingend an. Das Vertragsschlussverfahren zum „Umbrella Agreement“ wurde noch nicht abgeschlossen, bislang wurden noch nicht einmal die Ratsgremien mit den Inhalten des „Umbrella Agreement“ befasst. Die Bundesregierung will diesen Verhandlungen, die mutmaßlich auch die Frage des Verhältnisses zwischen Artikel 5 Absatz 3 des „Umbrella Agreement“ und Adäquanzbeschlüssen der Europäischen Kommission auf Grundlage von Sekundärrecht betreffen werden, und der Entscheidungsfindung im Rat nicht vorgreifen.

28. Teilt die Bundesregierung die Auffassung, wonach die Glaubwürdigkeit von Zusagen der Einhaltung von Datenschutzbestimmungen durch US-Geheimdienstverantwortliche gering zu veranschlagen ist angesichts der Tatsache, dass diese veranlassten, z. B. heimlich den Telefonverkehr der Bundeskanzlerin abzuhören, und selbst gegenüber ihrem eigenen Parlament ein nach Auffassung der Fragesteller stark taktisches Verhältnis zur Wahrheitspflicht offenbaren (vgl. etwa www.politifact.com/truth-o-meter/article/2014/mar/11/james-clappers-testimony-one-year-later/), und wenn nein, worauf stützt sich konkret das Vertrauen der Bundesregierung in die Zusagen von US-Geheimdiensten?

Die Bundesregierung teilt nicht die Auffassung der Fragesteller. Das Vertrauen der Bundesregierung stützt sich auf Zusagen der US-Regierung auf höchster politischer Ebene.

29. Welche gesetzlichen Veränderungen der US-Rechtslage sind nach Auffassung der Bundesregierung zwischenzeitlich erfolgt, die unmittelbare Einschränkungen der durch die globalen NSA-Überwachungsprogramme bestehenden Zugriffsmöglichkeiten von US-Sicherheitsbehörden auf die Daten von EU-Bürgern nach sich ziehen?

Gesetzliche Veränderungen der US-Rechtslage erfolgten durch den USA Freedom Act of 2015, der der NSA die bis dahin nach Section 215 USA Patriot Act vorgenommene Erhebung von Metadaten untersagt. Die NSA kann auf die entsprechenden Daten unter den im Freedom Act geregelten Voraussetzungen nur noch mittelbar, durch gezielte Anfragen an US-Telekommunikationsunternehmen, zugreifen. Die entsprechenden Vorschriften des Freedom Act of 2015 sind am 29. November 2015 in Kraft getreten. Sie betreffen alle Telefonate, deren Ausgangs- oder Endpunkt in den USA liegt. Auf untergesetzlicher Ebene wurden mit der Presidential Policy Directive 28 vom 17. Januar 2014 zudem datenschutzrechtliche Grundsätze für den gesamten Bereich der Fernmeldeaufklärung etabliert, die, soweit mit nationalen Sicherheitsbelangen vereinbar, unterschiedslos auf US-Bürger und Ausländer Anwendung finden sollen.

30. Teilt die Bundesregierung die Auffassung, wonach jegliche Zusagen einer US-Regierung keine Bindungswirkungen über die jeweilige Amtszeit hinaus entfalten können, und hält sie die damit verbundene Rechtsunsicherheit im Hinblick auf den gebotenen Schutz der EU-Grundrechte gleichwohl für hinreichend, wenn ja, weshalb?

Die Europäische Kommission ist verpflichtet, ihre Feststellung eines angemessenen Datenschutzniveaus regelmäßig zu überprüfen und ggf. anzupassen bzw. aufzuheben, so der EuGH in seiner „Safe Harbor“-Entscheidung (Rn. 76). Daran anknüpfend sieht auch der von der Europäischen Kommission vorgelegte Entwurf des Angemessenheitsbeschlusses vor, dass das „Privacy Shield“ jährlich gemeinsam überprüft wird und die Kommission zudem ein Verfahren zur Aussetzung ihres Angemessenheitsbeschlusses initiieren kann. Daraus, dass US-amerikanische Zusagen im Zusammenhang mit der Amtszeit der jeweiligen US-Regierung stehen, ergibt sich daher keine Rechtsunsicherheit.

31. Teilt die Bundesregierung die Auffassung, wonach eine mit jeder Veränderung des US-Umgangs mit den vereinbarten Vorgaben und bei jedem Regierungswechsel notwendig werdende Neuverhandlung des Privacy-Shield weder praktikabel erscheint noch die gebotene Rechtssicherheit für Bürgerinnen und Bürger als auch Unternehmen erbringen kann, und wenn nicht, warum nicht?

Wendete die US-Administration Regelungen des „Privacy Shield“ nicht an, trüge dies nicht zur Rechtssicherheit bei. Die Bundesregierung befürwortet, dass das „Privacy Shield“ regelmäßig auf den Prüfstand gebracht wird – sei es im Wege der gemeinsamen jährlichen Kontrolle durch die Europäische Union und den USA, sei es durch ein Verfahren der Europäischen Kommission, mit der sie ggf. einen Angemessenheitsbeschluss aussetzen kann. Diese regelmäßige Überprüfung ist Ausfluss des gebotenen Ausgleichs zwischen dem Grundrechtsschutz Betroffener und dem Rechtssicherheitsinteresse der Datenverarbeitenden.

32. Lag oder liegt der Bundesregierung, etwa im Rahmen des Prüfverfahrens im Artikel 31-Ausschuss gem. Artikel 5 der Verordnung (EU) 182/2011 der Entwurf eines Verhandlungsmandats oder bereits der Entwurf der Adäquanzenentscheidung der Europäischen Kommission selbst vor, und wenn ja, wie hat die Bundesregierung sich dazu gegenüber der Europäischen Kommission verhalten bzw. darüber abgestimmt?

Die Europäische Kommission hat am 29. Februar 2016 den Entwurf eines Angemessenheitsbeschlusses zu dem neu verhandelten „Privacy Shield“ veröffentlicht. Die Bundesregierung hat sich weder gegenüber der Europäischen Kommission dazu verhalten, noch im Artikel 31-Ausschuss darüber abgestimmt.

33. Kann es nach Auffassung der Bundesregierung vor dem Hintergrund der Entscheidungsgründe des „Safe Harbor“-Urteils eine tragfähige, rechtssichere Adäquanzenentscheidung der Europäischen Kommission geben (Safe Harbor 2 oder EU-US Privacy Shield), ohne dass die USA Veränderungen an ihren materiellrechtlichen Befugnisnormen für den sicherheitsbehördlichen Zugriff auf Daten von EU-Bürgern vornimmt, und wenn ja, aufgrund welcher konkreten Argumente?

Die USA haben gesetzliche Veränderungen vorgenommen (auf die Antwort zu Frage 29 wird verwiesen). Ihren Entwurf eines Angemessenheitsbeschlusses zum „Privacy Shield“ stützt die Europäische Kommission unter anderem auf die geänderte Gesetzeslage.