NETZWERK DATENSCHUTZEXPERTISE

Privacy Shield – Darstellung und rechtliche Bewertung

Stand: 07.03.2016

Inhalt

Thilo Weichert
Waisenhofstr. 41, 24103 Kiel
0431 9719742
weichert@nnetzwerk-datenschutzexpertise
www.netzwerk-datenschutzexpertise.de

Am 29.02.2016 veröffentlichte die Europäische Kommission die Dokumente, die Grundlage für die Angemessenheitsentscheidung personenbezogener Datenübermittlungen von Europa in die USA sein sollen. Der Europäische Gerichtshof (EuGH) hatte mit Urteil vom 06.10.2015 die bisher geltende Entscheidung der EU-Kommission zum sog. Safe-Harbor-Rechtsrahmen aufgehoben und festgestellt, dass dieser nicht grundrechtskonform ist und keine angemessenen Datenschutz in den USA gewährleistet. Die folgende Darstellung beschreibt den aktuellen Diskussionsstand (1), die Planungen zum Privacy Shield (2), die Anforderungen des EuGH sowie der künftigen Europäischen Datenschutzgrundverordnung (EU-DSGVO)(3) und untersucht schließlich, ob das Privacy Shield diesen Anforderungen gerecht wird (4).

Das **Ergebnis der folgenden Untersuchung** ist, dass das Privacy Shield mit europäischem Recht nicht in Einklang steht. Dies hat, kurz zusammengefasst, folgende Gründe:

1. Die Zusagen der US-Seite in Form von Briefen genügen nicht den Anforderungen an die Verbindlichkeit der rechtlichen Verpflichtungen.

2. Das gesamte Regelwerk des Privacy Shield genügt nicht den Transparenzanforderungen, um Betroffenen die Informationen zu geben, die für eine wirksame Durchsetzung ihrer Rechte nötig wäre.

3. Der geplante Kommissionsbeschluss nimmt keinen Rechtsvergleich der Standards des Privacy Shield mit den Standards des EU-Rechts vor und genügt daher nicht den Begründungsanforderungen an eine Angemessenheitsentscheidung.

4. Die für US-Unternehmen geltenden Prinzipien bleiben hinter den materiellen Garantien des europäischen Datenschutzes weit zurück, etwa im Hinblick auf die Zweckbindung, das Auskunftsrecht, die erfassten Verarbeitungsschritte oder wegen des Fehlens von Abwägungsklauseln.

5. Der Rechtsschutz ist für EU-Betroffene in vieler Hinsicht ausgeschlossen und nicht wirksam durchsetzbar,

- weil die Teilnahme an einem nicht rechtsstaatlich organisierten Streitschlichtungsverfahren Voraussetzung für eine Klage nach dem FTC-Gesetz zu sein scheint,

- weil die Vertretung der Betroffeneninteressen im Streitschlichtungsverfahren nicht hinreichend gewährleistet ist,

- weil es keine verbindliche und ausnahmslose Behandlungszusage für Beschwerden, etwa durch die FTC, gibt,

- weil die Aufsichtsbehörden in den USA nicht unabhängig sind.

6. Die Regelungen zum US-behördlichen Zugriff und zu der dortigen Verwendung von Daten aus der EU entspricht nicht den europäischen Datenschutzstandards,

- weil lediglich die Speicherung und die Übermittlung von Daten erfasst werden, nicht aber die weiteren mit Grundrechtseingriffen verbundenen Verarbeitungsschritte (insbesondere die Erhebung, die Auswertung und interne Verarbeitung, die Nutzung),

- weil keine Abwägungsregelungen gelten für Eingriffe in die Datenschutzrechte der Betroffenen,

- weil Massenüberwachungsmaßnahmen in großen Bereichen weiterhin erlaubt bleiben und keine Erforderlichkeits-, geschweige denn eine Verhältnismäßigkeitsprüfung gewährleistet wird,

[Privacy Shield – Darstellung und rechtliche Bewertung

- weil der Rechtscharakter der Datenverarbeitungsregelungen sowie deren Einschränkung nicht die nötige gesetzliche Verbindlichkeit hat,

- weil, ohne dass rechtliche Kompensationen vorgesehen sind, der Wesensgehalt der in der Europäischen Grundrechte-Charta garantierten Rechte auf Privatsphäre und Rechtsschutz betroffen ist.

7. Die Datenschutzaufsicht im behördlichen Bereich ist nicht, wie erforderlich, unabhängig.

8. Es gibt keine wirksamen Rechtsschutzmöglichkeiten für EU-Betroffene gegen informationelle Eingriffe durch US-Behörden; die wenigen Rechtsschutzmöglichkeiten betreffen nur Randbereiche des Datenschutzes und entsprechen nicht den europäischen Standards.

1 Der aktuelle Stand

Die am 29.02.2016 von der EU-Kommission[1] veröffentlichten Texte zum EU-U.S. Privacy Shield (EU-US-Datenschutzschild) wurden als Teil eines „*Legislativpakets*“[2] vorgestellt, mit dem das erschütterte Vertrauen in den transatlantischen Datenverkehr wiederhergestellt werden soll. Dabei handelt es sich neben dem Privacy Shield um die Reform des EU-Datenschutzrechts mit der EU-DSGVO, eine Datenschutzrichtlinie für Justiz und Polizei[3] sowie um ein EU-US-Rahmenabkommen, das „hohe Datenschutzstandards für der Strafverfolgung dienende Datenübermittlungen über den Atlantik“ gewährleisten soll.[4] Das US-Wirtschaftsministerium (Department of Commerce, DOC) ging zeitgleich mit einer eigenen Veröffentlichung zum Privacy Shield an die Öffentlichkeit[5].

1.1 Das Privacy Shield

Das Privacy Shield besteht aus einer *Vielzahl von Dokumenten*. Neben einer Presseerklärung werden der Entwurf eines Angemessenheitsbeschlusses der EU-Kommission (künftig: EU-K-Beschluss-E) vorgelegt sowie 7 Annexe, in denen die schriftlichen Garantien der US-Regierung dokumentiert sind:

Annex 1. Zwei Schreiben des US-Department of Commerce (Pritzker u. Selig) v. 23.02.2016 an EU-Kommissarin Vera Jourová

1 Europäische Kommission stellt EU-US-Datenschutzschild vor: verbindliche Garantien zur Wiederherstellung des Vertrauens in den transatlantischen Datenverkehr, http://europa.eu/rapid/press-release_IP-16-433_de.htm.

2 Transatlantic Data Flows: Restoring Trust through Strong Safeguards, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

3 Dazu Weichert, http://www.netzwerk-datenschutzexpertise.de/dokument/eu-datenschutzrichtlinie-für-polizei-und-justiz, 2016.

4 Dazu Schaar, Transatlantische Sicherheitskooperation und Datenschutz – Was bringt das „Umbrella Agreement“, DANA 1/2016, 4-7.

5 US-Wirtschaftsministeriums, Overview of the EU-U.S.- Privacy Shield, https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shield-framework.

[Privacy Shield – Darstellung und rechtliche Bewertung

Annex 2. EU-U.S. Privacy Shield Framework Principles issued by the U.S. Department of Commerce

Annex 3. Schreiben des US-Außenministers John F. Kerry v. 22.02.2016 an EU-Kommissarin Jourová mit EU-U.S. Privacy Shield Ompudsperson Mechanism Regarding Signals Intelligence

Annex 4. Schreiben der United States of America Federal Trade Commission (FTC)(Ramirez) an EU-Kommissarin Jourová v. 23.02.2016

Annex 5. Schreiben des Secretary bzw. des Department of Transportation (DOT)(Foxx) an EU-Kommissarin Jourová v. 19.02.2016

Annex 6. Schreiben des Office of the Director of National Intelligence (ODNI) Office of General Counsel (Litt) an das US-Wirtschaftsministerium v. 22.02.2016

Annex 7. Scheiben des US-Justizministeriums (Swartz) an das US-Wirtschaftsministerium vom 19.02.2016.

Rechtlicher Hintergrund des vorgelegten Privacy-Shield-Rechtsrahmens ist das *Urteil des Europäischen Gerichtshofs vom 06.10.2015*, das die Entscheidung der EU-Kommission aus dem Jahr 2000 zum Safe-Harbor-Rechtsrahmen aufgehoben hatte.[6] Danach hatte die EU-Kommission angekündigt, die schon seit 2013 geführten Verhandlungen mit den USA zu einem „Safe Harbor 2“ zu intensivieren. Die Artikel-29-Arbeitsgruppe, der Zusammenschluss der europäischen Datenschutzbehörden, hatte der EU-Kommission bis Ende Januar 2016 eine Frist gesetzt, um mit den US-Behörden eine angemessene Lösung zu finden.

Am 01.02.2016 kündigte EU-Kommissarin Jourová vor dem Innen- und Rechtsausschuss des EU-Parlaments an, dass man kurz vor einem Ergebnis stehe. Am 02.02.2016 veröffentlichte die *EU-Kommission* eine Presseerklärung, wonach sie und die USA sich auf ein EU-US-Datenschutzschild geeinigt habe, und stellte die wesentlichen Inhalte dieser Einigung dar. Dies führte zu unterschiedlichen Reaktionen dies- und jenseits des Atlantiks bei Politik, Behörden und Wirtschaft.[7]

Anlässlich der Vorlage der Privacy-Shield-Dokumente erklärte EU-Kommissarin Jourová: „Der EU-US-Datenschutzschild bietet eine neue solide Regelung, die auf robuster Durchsetzung und Kontrolle basiert, einem besseren Rechtsschutz für den Bürger und erstmals einer schriftlichen Zusicherung unserer amerikanischen Partner zu den Garantien und Beschränkungen für den Datenzugriff der Behörden aus Gründen der nationalen Sicherheit.“[8]

1.2 Reaktion des Klägers im EuGH-Verfahren

Weniger zuversichtlich äußerte sich Max Schrems, über dessen Beschwerde letztlich der EuGH am

6 EuGH U. v. 06.10.2015, C-362/14 – Schrems, NJW 2015, 3151; siehe hierzu die Dokumente des Netzwerks Datenschutzexpertise unter http://www.netzwerk-datenschutzexpertise.de/dokument/folgen-der-safe-harbor-entscheidung-des-eugh.

7 Zu allem ausführlich und dokumentierend Weichert/Schuler, Privacy Shield – kein grundrechtskonformer Ersatz für Safe Harbor, http://www.netzwerk-datenschutzexpertise.de/dokument/folgen-der-safe-harbor-entscheidung-des-eugh.

8 Europäische Kommission (Fn. 1).

06.10.2015 entschieden hatte: „Man versucht hier mit einigen Behübschungen, das illegale ‚Safe Harbor'-System wiederzubeleben; die grundsätzlichen Probleme der US-Massenüberwachung und der Nonexistenz von US-Datenschutz sind aber nicht gelöst. Der EuGH hat für eine neue Entscheidung massive Verbesserungen verlangt. Das ‚Privacy Shield' bringt zwar einige kleine Fortschritte, ist aber meilenweit von der Vorgabe des Gerichts weg. Auch wenn die EU-Kommission und die USA das mit großem PR-Aufwand überdecken wollen, ist das leider keine Lösung, die sehr stabil aussieht.

Die Kommission sagt, es gäbe keine ‚Massenüberwachung' mehr, obwohl die vorgelegten Dokumente genau das Gegenteil sagen. Das ist eine derart offensichtliche Verletzung der Gesetze und der Gerichtsentscheidung, dass man sich fragen muss, was die EU-Kommission im Hintergrund treibt. Dieses Vorgehen ist jedenfalls keine rationale Umsetzung der Gesetze und des EuGH-Urteils bei dieser Faktenlage.

Die Prinzipien für den privaten Bereich limitieren die Datennutzung nur bei einer sogenannten Zweckänderung und bei der Weitergabe an Dritte. Alles andere – vom Sammeln über das Speichern bis zum Verarbeiten der Daten – ist praktisch unlimitiert erlaubt. Aber selbst die zwei Einschränkungen kann man mit zwei Zeilen in einer Datenschutzrichtlinie umgehen. In der Praxis konnten US-Unternehmen unter ‚Safe Harbor' machen, was sie wollten, und können das auch weiterhin. Das ‚Privacy Shield´ hat nicht mal im privaten Bereich etwas gebracht, auch wenn hier viel mehr Spielraum vorhanden wäre als bei der Massenüberwachung. Die Minimalverbesserungen sind Meilen weit weg von dem ‚gleichwertigen' Datenschutz, den der EuGH verlangt hat.

Das bedeutet, dass es für Unternehmen keine wirkliche Rechtssicherheit gib. Selbst wenn sie nach ‚Privacy Shield' zertifiziert sind, können nationale Datenschutzbehörden den Datenfluss jederzeit stoppen. Es ist wirklich schade, dass die Kommission diese Situation nicht genutzt hat, um endlich eine stabile Lösung für Unternehmen und Nutzer zu verhandeln. Die meisten Unternehmen werden sich wohl nicht auf ‚Privacy Shield' als rechtliche Grundlage verlassen, wenn man sich diese Situation ansieht. Ich denke eine Reihe von Leuten wird diese Entscheidung beim EuGH bekämpfen – ich könnte einer davon sein."[9]

1.3 Weitere Reaktionen

vVZu der Dokumenten des Privacy Sield äußerte sich u. a. auch die Deutsche Vereinigung für Datenschutz e. V. (DVD) kritisch: „Nach Ansicht der DVD ist der Versuch, die US-Regierung zu Zugeständnissen zu veranlassen, die mit den Anforderungen des Europäischen Gerichtshofs (EuGH) in Bezug auf personenbezogene Datenübermittlungen von Europa in die USA in Einklang stehen, rundherum gescheitert. … Aus den Dokumenten ergeben sich nicht im Ansatz effektive Begrenzungen der Massenüberwachung durch Sicherheitsbehörden wie die NSA und ebenso keine wirksamen Datenschutzinstrumente gegenüber US-Firmen. … Die materiell-rechtlichen Vorgaben des aufgehobenen Safe-Harbors unterscheiden sich nur unwesentlich vom jetzt geplanten Schild. Wer Transparenz sucht, muss – wie bisher bei Safe Harbor – einen Hindernislauf absolvieren, bei dem absehbar das Ziel – die Sicherung eines Grundrechts – nicht erreicht wird. Anstelle von unabhängigen Datenschutzkontrolleuren sollen es das US-Wirtschaftsministerium, die Federal Trade Commission und ein 20-köpfiges „Privacy Shield Panel" richten, das von der EU-Kommission und dem US-Ministerium

9 Schrems, European Commission presents EU-US „Privacy Shield", http://www.europe-v-facebook.org/PA_PS.pdf.

besetzt werden soll. Die für die Geheimdienstkontrolle vorgesehene Ombudsperson soll nicht wirklich unabhängig, sondern keinen Weisungen der Geheimdienst-Community unterworfen sein. Eine unabhängige Rechtskontrolle, wie sie Art. 47 der Europäischen Grundrechtecharta fordert, sieht anders aus“.[10]

Laut der Initiative European Digital Rights (EDRi) hat die Kommission dem Kaiser nur neue Kleider übergestreift. Diese könnten nicht verbergen, dass nicht nur in dem löchrigen Schutzschild schwere Fehler vorhanden seien, sondern auch in damit zusammenhängenden zusätzlichen Rechtsinstrumenten. EDRi verweist insbesondere auf den Entwurf für den Judical Redress Act, der EU-Bürgerinnen und -Bürgern eigentlich ein Klagerecht in den USA in Datenschutzfragen eröffnen soll. Ferner habe der US-Gesetzgeber mit dem Cybersecurity Act Fakten geschaffen, der Unternehmen einen Freibrief zum Datentransfer an nationale Geheimdienste ausstelle. Konstantin von Notz, Vizefraktionschef der Grünen im Deutschen Bundestag, sprach von einer „reinen Mogelpackung“. Die linke EU-Abgeordnete Cornelia Ernst warf der Kommission vor, den Knall der Snowden-Enthüllungen nicht gehört zu haben. Brüssel habe „sich wieder einmal von den USA über den Tisch ziehen lassen“. Die Piraten sehen die Kommission angesichts der unverbindlichen Versprechungen gar „als Wiederholungstäter bei der Verletzung unserer Grundrechte“.

Der Digitalverband Bitkom begrüßte dagegen die Einigung als „wichtigen Schritt zu mehr Rechtssicherheit beim Datenaustausch mit den USA“. Die US-Regierung müsse nun zu ihrem Wort stehen, die Übereinkunft sich „in der Praxis bewähren“. Laut der American Chamber of Commerce in Deutschland haben die USA und die EU mit den überarbeiteten Transferabkommen „politische Handlungsfähigkeit auf einem zentralen wirtschaftspolitischen Feld bewiesen“. Mittelfristig müsse es aber zu einer Reform der transatlantischen Rechtshilfeabkommen kommen, um „gemeinsame Standards für grenzüberschreitend Zugriffsmöglichkeiten zu entwickeln“.[11]

2 Der aktuelle Stand

Die Planungen zum Privacy Shield zielen in zwei Richtungen: Zum einen sollen die *US-Unternehmen*, die personenbezogene Daten aus der EU verarbeiten, materiellen und formellen Anforderungen unterworfen werden, mit denen ein höheres Datenschutzniveau als bisher in den USA erreicht wird. Außerdem sollen über Zusicherungen im Hinblick auf die Nutzung der Daten von EU-Bürgern durch *US-Behörden* vom EuGH festgestellte grundrechtliche und rechtsstaatliche Defizite abgebaut werden.

2.1 Regeln für US-Unternehmen

US-Unternehmen, die personenbezogene Daten aus der EU unter dem Regelungsrahmen des Privacy Shield importieren wollen, müssen sich über eine *Selbstzertifizierung* zur Einhaltung von vom US-Wirtschaftsministerium (Department of Commerce – DOC)[12] festgelegten Prinzipien verpflichten. Diese Prinzipien wurden vom DOC in Kooperation mit der Kommission, der Industrie und anderen

10 DVD, https://www.datenschutzverein.de/wp-content/uploads/2016/03/2016-03-01-DVD_schockiert_ueber_EU-US-Privacy_shield.pdf.

11 Nachweise bei Weichert/Schuler, Dokumentation und Bewertung Privacy Shield, http://www.netzwerk-datenschutzexpertise.de/dokument/folgen-der-safe-harbor-entscheidung-des-eugh.

Interessierten erarbeitet. Sie sind nur anwendbar, wenn aus der EU importierte Daten betroffen sind; dies gilt auch nach Ausscheiden aus dem Privacy Shield, wenn die Daten noch nicht gelöscht wurden.[13]

2.1.1 Prinzipien

Die materiellen Datenschutzgrundsätze entsprechen im Wesentlichen denen von Safe Harbor[14]:

1. Informationspflicht (notice)

2. Wahlmöglichkeit (choice)

3. Datenweitergabe (accountability for onward transfer)

4. Sicherheit (security)

5. Datenintegrität und Zweckbindung (data integrity and purpose limitation)

6. Auskunftsrecht (access)

7. Durchsetzung (recourse, enforcement and liability)

Gegenüber Safe Harbor sind die Prinzipien teilweise konkreter gefasst.

Die *Informationspflicht* (notice) erstreckt sich u. a. auf die Teilnahme am Privacy Shield, einen Hinweis auf das Auskunftsrecht und die Benennung einer „unabhängigen Konfliktlösungseinrichtung".

Über die *Wahlmöglichkeit* (choice) soll gewährleistet werden, dass Personendaten gemäß den Erwartungen und der Entscheidung des Betroffenen verarbeitet werden. Vorgesehen ist ein „Opt-out" zur Verwendung für Werbung bzw. Direktmarketing. Bezug genommen wird auf „ein zentrales ´Opt-out`-Programm" wie das des „Direct Marketing Association´s Mail Preference Service". Erweise es sich als unpraktikabel, die Opt-out-Möglichkeit vor Nutzung der Personeninformation zu eröffnen, dann müsse dies zumindest zeitgleich und auch jederzeit später möglich sein.[15]

In Bezug auf die *Weitergabe* (onward transfer) wird gefordert, dass eine Stelle, die europäische Daten von einem Privacy-Shield-Unternehmen erhält, den europäischen Angemessenheitsanforderungen voll unterworfen wird.[16] Bei einer Auftragsdatenverarbeitung müssten in den USA die europäischen Regeln hierfür beachtet werden. Auch innerhalb einer kontrollierten Unternehmensgruppe ist eine vertragliche Regelung notwendig.[17] Handelt ein Bevollmächtigter bzw. ein beauftragter Dritter (agent) eigenverantwortlich entgegen einer Weisung, so soll das dem US-Unternehmen nicht zugerechnet

12 Annex 2; die folgenden Nachweise beziehen sich v. a. auf dieses Dokument.

13 Annex 2 III.6.f-h.

14 Annex 2 II. 1-7.

15 Annex 2 III.12.

16 Annex 2 II.5.

17 Annex 2 III.10.a, b.

werden.[18]

2.1.2 Zusatzprinzipien

In Zusatzprinzipien werden *Konkretisierungen* der sehr allgemeinen o. g. Prinzipien vorgenommen. Entlang der Regelung in Art. 8 Abs. 2 EG-DSRl werden für sensitive Daten vom Einwilligungserfordernis Ausnahmen zugelassen.[19] In Bezug auf die Pressefreiheit gemäß dem 1. Zusatzartikel zur US-Verfassung ist eine Abwägungsklausel aufgenommen.[20] Durchleitende Telemedienanbieter werden von einer Verantwortung freigestellt.[21] Dem europäischen Datenschutzrecht unbekannt ist die explizite Privilegierung beim „Due Diligence“: Ist ein Privacy-Shield-Unternehmen von einer Fusion oder einer Übernahme betroffen, so dürfen Personendaten von „Schlüsselpersonal“ vor Übergang mit Investment-Bänkern ausgetauscht werden.[22]

Einen Spezialfall stellen *Arbeitnehmerdaten* (human ressources personal information) dar. Insofern unterwerfen sich die US-Unternehmen der europäischen Datenschutzaufsicht und dem Recht des exportierenden europäischen Unternehmens. Die Verantwortung für die Beschäftigtendaten verbleibt im Rahmen des Arbeitsverhältnisses beim EU-Unternehmen. Bei Beschwerden soll sich der Beschäftigte in der EU an seine örtliche Datenschutzaufsicht wenden, auch wenn der Datenschutzverstoß durch das US-Unternehmen erfolgte. Das US-Unternehmen unterliegt voll den europäischen Kooperationspflichten. Die verarbeitenden US-Unternehmen dürfen aber die erhaltenen Daten für andere Zwecke gemäß den Notice- und Choice-Prinzipien verwenden. Es wird darauf hingewiesen, dass eine strengere Zweckbindung gelten kann und dass Schutzmaßnahmen wie die Pseudonymisierung genutzt werden können.[23]

Die Verarbeitung von Flugpassagierdaten sowie von sonstigen *Reiseinformationen*, etwa zu Hotelreservierungen oder bestimmten Reisendenwünschen (z. B. religiös bedingte Speisewünsche, Hilfsbedürftigkeit), soll, wenn dies zur Erfüllung der Betroffenenwünsche erfolgt, nicht von einer Privacy-Shield-Zertifizierung abhängig sein. In Fall einer Zertifizierung wird darauf hingewiesen, dass insofern sensible Daten betroffen sein können und das Recht der EU-Mitgliedstaaten zu respektieren sei.[24] Das US-Verkehrsministerium (DOT) wird auf der Grundlage seiner Zuständigkeit in 49 U.S.C 41712 hinsichtlich „unfairer oder betrügerischen Marktmethoden“ in den Bereichen Fluglinien und

18 Annex 1 S. 4.

19 Annex 2 III.1 und II.2.c.

20 Annex 2 III.2.

21 Annex 2 III.3.

22 Annex 2 III.4.

23 Annex 2 III.9.

24 Annex 2 III.13.

Reisebüros tätig, auch soweit der Datenschutz betroffen ist, und verpflichtet sich, in seinem gesetzlichen Rahmen die Beachtung des Privacy Shield zu überwachen.[25]

Pharmazeutischen und medizinischen Produkten wird in den Zusatzprinzipien große Aufmerksamkeit gewidmet.[26] Empfohlen wird, wenn möglich, eine Anonymisierung; eine Pseudonymisierung ist bei Forschungsprojekten, wo möglich, Pflicht. Daten aus spezifischen Studien dürfen für weitere Studien verwendet werden, wenn den Betroffenen zu Beginn diese „Information" (notice) und „Wahlmöglichkeiten" (choice) eingeräumt wurden. Eine erneute Einwilligung ist einzuholen, wenn der ursprüngliche Forschungszweck der Datenverarbeitung mit der geplanten Verwendung nicht vereinbar ist. Zieht ein Betroffener eine Einwilligung zurück, so können die Daten in der Gesamtheit einer klinischen Studie weiterverwendet werden, was den Betroffenen zu Beginn mitgeteilt werden muss. Datenweitergaben zu Aufsichts- und Kontrollzwecken werden generell erlaubt, ebenso solche an Unternehmens-Niederlassungen und andere Forschende, wenn dies mit den Prinzipien Information und Wahlmöglichkeit vereinbar ist. Weiter werden Regelungen zu Blindstudien und zu Pharma- und Medizinproduktkontrollen getroffen.

Allgemein, d. h. *öffentlich zugängliche Daten* dürfen privilegiert verwendet werden. Weist der europäische Datenexporteur darauf hin, so müssen dennoch die Prinzipien (notice, choice, accountability, onward transfer) beachtet werden. Keine Privilegierung besteht, wenn die öffentlichen mit nicht-öffentlichen Daten zusammengeführt werden.[27]

2.1.3 Auskunftsanspruch

Der in Prinzip 6 bekräftigte *Auskunftsanspruch* unterliegt relevanten Einschränkungen. Dies gilt nicht nur, wenn Rechte Dritter verletzt würden, sondern auch, wenn die Kosten für die Auskunftserteilung im Verhältnis zu dem Betroffeneninteresse, das als „Datenschutzrisiko für den Betroffenen" definiert wird, unverhältnismäßig wären.[28] Ein weiterer Auskunftsverweigerungsgrund sind Betriebs- und Geschäftsgeheimnisse, deren Kenntnis Wettbewerbern im Markt helfen würden.[29]

„Wie in der Richtlinie kann ein Unternehmen die Auskunft in dem Maße beschränken, wie damit voraussichtlich der Schutz entgegenstehender öffentlicher Interessen verletzt würde, etwa die nationale Sicherheit, die Verteidigung oder die öffentliche Sicherheit. Die Auskunft kann verweigert werden, wenn Personeninformationen ausschließlich für Zwecke der Forschung oder der Statistik verarbeitet werden. Weitere Gründe für die Auskunftsbeschränkung sind

1. die Behinderung der Um- und Durchsetzung von Gesetzen oder privaten Ansprüchen, einschließlich

25 Annex 5.

26 Annex 2 III.14.

27 Annex 2 III.15.

28 Annex 2 III.8.b.

29 Annex 2 III.8.c.

der Verhinderung, der Ermittlung oder der Feststellung von Verstößen oder des Rechts auf ein faires Gerichtsverfahrens,

2. die Verletzung von legitimen Rechten oder wichtigen Interessen anderer durch die Offenlegung,

3. die Verletzung einer rechtlichen oder anderen beruflichen Verpflichtung oder eines solchen Privilegs,

4. die Beeinträchtigung von Sicherheitsuntersuchungen, von Beschwerdeverfahren oder im Rahmen von Einsatzplanungen oder der unternehmerischen Reorganisation im Arbeitsbereich,

5. die Beeinträchtigung der nötigen Vertraulichkeit bei Kontrollmaßnahmen, der Überprüfung von Regelungsfunktionen für ein gesundes Management oder bei künftigen oder stattfindenden, die Organisation betreffenden Verhandlungen."[30]

Für die Auskunft soll für den Betroffenen gebührenfrei sein; es darf eine nicht übermäßige Gebühr verlangt werden.[31]

2.1.4 Selbstzertifizierung

Um eine *Selbst-Zertifizierung* vornehmen zu können, die jährlich zu wiederholen ist, muss das US-Unternehmen der Datenschutzaufsicht der Federal Trade Commission (FTC, zuständig für viele Bereiche des Verbraucherschutzes), des Verkehrsministeriums (Department of Transportation - DOT, zuständig v. a. für Fluggesellschaften) oder einer anderen Behörde unterliegen. In den Privacy Shield-Dokumenten verpflichten sich mit Schreiben an die EU-Kommissarin Jourová die FTC[32] und das DOT[33] zur Überprüfung von Beschwerden über die Missachtung des Privacy Shield.

Die Einhaltung der Privacy-Shield-Verpflichtungen ist nach einer internen *Bewertung durch das Unternehmen schriftlich zu dokumentieren*. Die Bewertung muss auf Anfrage von Bürgern zur Verfügung gestellt werden. Sie kann von einem externen Unternehmen erstellt werden.[34] Das Unternehmen muss seine Datenschutzrichtlinien (Privacy Policies) veröffentlichen, die mit den Prinzipien in Einklang zu stehen haben.

Das US-Wirtschaftsministerium (DOC) veröffentlicht eine *Liste* aller selbstzertifizierten Unternehmen. Von dieser Liste werden die Unternehmen vom DOC gestrichen, die ihre Zertifizierung nicht erneuern oder fortdauernd die Prinzipien verletzen. Auf einer zweiten zu veröffentlichenden DOC-Liste werden die Unternehmen aufgeführt, die nicht mehr unter das Privacy Shield fallen.[35] Die Prinzipien sind nicht

30 Annex 2 III.8.e.i.

31 Annex 2 III.8.f.

32 Annex 4.

33 Annex 5.

34 Annex 2 III.7.c, d.

35 Annex 1 S. 5 f.

zwingend zu beachten, soweit dies aus Gründen der nationalen Sicherheit, des öffentlichen Interesses oder der Strafverfolgung nötig ist, sowie in gesetzlich oder durch die US-Regierung geregelten Fällen.[36] Es gilt US-Recht.

Auch wenn keine Beschäftigtendaten tangiert sind, kann sich ein US-Unternehmen für Beschwerden der jeweiligen *europäischen Aufsichtsbehörde freiwillig unterwerfen*, was es dann auch öffentlich zum Ausdruck bringen muss.[37]

Hinsichtlich der „Durchsetzung" ist vorgesehen, dass *Betroffenenbeschwerden* aufgeklärt und unverzüglich ohne Kosten für den Betroffenen geklärt werden.[38] Unternehmen müssen innerhalb von 45 Tagen nach Erhalt einer Beschwerde reagieren.[39] Über den Konfliktlösungsmechanismus soll umfassend öffentlich, insbesondere über eine Internetseite, informiert werden.[40]

2.1.5 Streitschlichtungsverfahren

Die Unternehmen müssen sich einem für sie bindenden *Streitschlichtungsverfahren* unterwerfen, das sie selbst auswählen können.[41] Als Beispiele werden „AAA or JAMS" genannt. Es handelt sich dabei um die American Arbitration Association[42] sowie die JAMS-Foundation[43]. Das Verfahren wird in einem Annex 1 zum Annex 2 beschrieben. Inwieweit die Teilnahme an der Streitschlichtung für die Betroffenen verpflichtend ist, bleibt unklar. Die Teilnahme durch den Betroffenen schließt die Inanspruchnahme anderer Instrumente (außer Finanzforderungen) aus. Die FTC wird durch ein Schlichtungsverfahren nicht an einem eigenen Vorgehen gehindert.

Vor der *Anrufung* ist es nötig, dass sich der Betroffene unter Berufung auf die Privacy-Shield-Prinzipien erfolglos an das US-Unternehmen gewendet hat und über die europäische Datenschutzbehörde der Fall dem DOC vorgetragen wurde, das eine Lösung innerhalb von 90 Tagen anstrebt.[44] Europäische Datenschutzbehörden dürfen den Betroffenen vorbereitend unterstützen, aber nicht an dem Verfahren teilnehmen. Die Schlichtung erfolgt in den USA. Der Betroffene muss nicht teilnehmen, ihm wird eine

36 Annex 2 I.5.

37 Annex 1 S. 6, Annex 2 III.6.c.

38 Annex 2 II.7.a.i.

39 Annex 2 III.11.d.i.

40 Annex 2 III.11.d.ii.

41 Annex 2 II.7.c.

42 https://www.adr.org.

43 http://www.jamsadr.com/rules-comprehensive-arbitration/.

44 Annex 1 C. zu Annex 2, Annex 1 S. 8.

kostenfreie Telefon- oder Videokonferenzschaltung angeboten. Verhandlungssprache ist Englisch. Ausnahmsweise kann das Panel (siehe dazu nächster Absatz), wenn die Kosten nicht zu hoch werden, Übersetzungen vorsehen. Die Verhandlungen sind innerhalb von 90 Tagen abzuschließen.

Bei der Streitschlichtung geht es ausschließlich um die Behandlung des konkreten Beschwerdefalls in Bezug auf die Prinzipien, nicht jedoch die in Annex 2 I.5 vorgesehenen Ausnahmen (nationale Sicherheit, öffentliches Interesse, Strafverfolgung, gesetzliche od. administrative US-Regelung). Die Schlichtung wird von einem „Privacy Shield Panel“ mit einem oder drei Schlichtern wahrgenommen, über die sich die Konfliktparteien einigen müssen. Die möglichen Schlichter werden in einer Liste mit mindestens 20 Personen aufgeführt, die vom DOC und der EU-Kommission ausgewählt werden. Inhalt des Schlichtungsspruchs sind die Betroffenenansprüche, nicht jedoch finanzielle Forderungen.[45] Der Schlichtungsspruch ist für alle Beteiligten verbindlich.

Betroffene wie Unternehmen können gegen den Schiedsspruch eine *gerichtliche Entscheidung* sowie deren Durchsetzung gemäß dem Federal Arbitration Act beantragen.[46] Sanktionsmechanismen müssten „zur Sicherstellung von Konformität hinreichend scharf“ sein.[47] Die Sanktion kann in der Veröffentlichung von Verstößen, der Löschung von Daten, die Suspendierung oder die Aberkennung der Zertifizierung, und vor Gericht auch in einem Schadenersatz (compensation for individuals for losses) bestehen.[48] Jede Seite trägt ihre Anwaltskosten. Die Anbieter von Streitschlichtungsverfahren müssen einen jährlichen Bericht über ihre Tätigkeit veröffentlichen.

2.1.6 FTC und andere

Die FTC behandelt Verweisungen aus Streitschlichtungsverfahren wegen Verletzungen der Prinzipien und Eingaben von EU-Mitgliedstaaten sowie des DOC, um gemäß dem FTC Act vorzugehen. Zur Kontaktpflege mit den EU-Mitgliedstaaten richtet die FTC standardisierte Prozesse und eine Kontaktstelle ein. Die FTC ist *nicht verpflichtet*, aber berechtigt, prüfend und sanktionierend tätig zu werden. EU-Kommissarin Jourová wies am 01.02.2016 im Innen- und Rechtsausschuss des Europaparlaments darauf hin, dass die FTC nur strategische Fälle und weniger individuelle Fälle aufgreift und bearbeitet.[49] In einem zweifellos strategischen Fall betreffend Facebook auf eine Eingabe des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) im Jahr 2012 hatte die FTC aber damals z. B. keine inhaltliche Rückmeldung gegeben.[50]

45 Annex 1 B. zu Annex 2.

46 Annex 2 III.11.d.

47 Annex 2 II.7.a.iii.

48 Annex 2 III.11.e.

49 Netzwerk Datenschutzexpertise, Privacy Shield – kein grundrechtskonformer Ersatz für Safe Harbor, S. 4.

50 Schreiben ULD an FTC 21.08.2012, https://www.datenschutzzentrum.de/facebook/kommunikation/20120821-ftc-facebook-de.pdf.

In geeigneten Fällen ist es der FTC gemäß dem U.S. SAFE WEB Act erlaubt, *ausländische Ermittlungsbehörden*, also auch europäische Datenschutzbehörden, mit eigenen Ermittlungsergebnissen zu unterstützen.[51] FTC-Ermittlungen sind nicht-öffentlich und vertraulich und werden zumeist nicht allgemein bekannt. Die FTC betont, dass sie in den 15 Jahren der Geltung von Safe Harbor 40 Sanktionsverfahren wegen Verstößen gegen Safe Harbor vorgenommen hat. Die FTC verspricht in ihrem Schreiben, die Einhaltung des Privacy Shield zu überwachen. Die Missachtung von FTC-Anordnungen kann zu *Strafen* von 16.000 $ pro Verstoß bzw. 16.000 $ pro Tag für andauernde Verstöße führen.[52]

Die FTC kann *Beanstandungen* aussprechen, Beseitigungs- und Unterlassungsverfügungen erlassen oder eine Beschwerde bei einem Bundesgericht einlegen. Möglich ist für die FTC die Verhängung von Bußgeldern bei Missachtung einer Beseitigungs- oder Unterlassungsverfügung oder die Verfolgung einer zivil- oder strafrechtlichen Missachtung von einer Bundesgerichts-Anordnung. Hierüber wird das DOC von der FTC informiert.[53] Verstößt ein Unternehmen dauernd gegen die Prinzipien, so wird es vom DOC von der Privacy-Shield-Liste gestrichen.[54]

Das *US-Wirtschaftsministerium* (DOC) verpflichtet sich, für das Privacy Shield mehr Personal einzustellen und bei einer Häufung von Beschwerden oder anderweitigen Hinweisen selbst Datenschutzverstößen nachzugehen und eine Kontaktstelle für die Kommunikation mit europäischen Datenschutzaufsichtsbehörden (DPA) einzurichten. Auf Beschwerden einer DPA verspricht das DOC innerhalb von 90 Tagen zu antworten.[55]

Ist ein Unternehmen von einem Verfahren bei der FTC oder einem US-Gericht betroffen, dann wird dies *veröffentlicht*.

Auf europäischer Ebene soll ein informelles „*DPA Panel*“ eingerichtet werden, das mit den US-Unternehmen zusammenarbeiten soll. Dieses soll, nachdem eine Beschwerde dort vorgetragen wurde, soweit möglich, innerhalb von 60 Tagen einen – rechtlich nicht verbindlichen – Rat erteilen. Reagiert das US-Unternehmen nicht innerhalb von 25 Tagen, so kann u. a. die FTC und in Spezialfällen das DOC informiert werden, um evtl. Sanktionen zu verhängen.[56]

2.2 Regeln für US-Behörden

Nachdem der EuGH Safe Harbor auch wegen des *undifferenzierten Massenzugriffs* von US-amerikanischen Behörden und Geheimdiensten auf EU-Daten für ungültig erklärte, musste die EU-

51 Annex 4 S. 6.

52 Annex 4, S. 7 f.

53 Annex 2 III 11.f.

54 Annex 2 III.11.g.

55 Annex 1 S. 7 f.

56 Annex 2 III.5.c.

Kommission in ihren Verhandlungen mit den USA versuchen, insofern grundrechtskonforme Rahmenbedingungen zu erreichen, um zu verhindern, dass eine Safe-Harbor-Folgeregelung erneut vom EuGH aufgehoben wird.

Ausgehandelt wurde ein Verfahren, mit dem Betroffenen die Möglichkeit eröffnet werden soll, bei einer *US-Ombudsperson* Beschwerden einzulegen, die ein weitgehendes Ermittlungsrecht erhält und den Betroffenen Antworten zukommen lässt. Als Ombudsperson hat US-Außenminister John F. Kerry Frau Under Secretary im Secretary of State Catherine Novelli bestimmt.[57] Der Mechanismus mit der Ombudsperson basiert auf der Presidential Policy Directive 28 (PPD-28) zur Geheimdiensttätigkeit, die Präsident Obama am 17.01.2014 verkündet hat.[58]

2.2.1 PPD-28

Die PPD-28 legt Prinzipien und Anforderungen für nachrichtendienstliche Tätigkeit fest, auch in Bezug auf personenbezogene Informationen zu Nicht-US-Bürgern. Danach ist für jede Überwachungsmaßnahme eine rechtliche Grundlage, also Gesetz, Regierungsanweisung oder sonstige Präsidentielle Richtlinie, erforderlich. Sie werde, so das „Office of the Director of National Intelligence“ (ODNI), nur zur Verfolgung legitimer und erlaubter Zwecke für die nationale Sicherheit angewendet. Das ODNI betont, dass gemäß der PPD-28 Datenschutz und Bürgerrechte „integrales Anliegen“ bei der Planung der Digitalüberwachung (signal intelligence) sei. Den USA gehe es dabei nicht um die Unterdrückung von Kritik und abweichenden Meinungen oder um die Diskriminierung von Personen wegen ethnischer Herkunft, Rasse, Geschlecht, sexueller Orientierung oder Religion, auch nicht um den Wettbewerbsvorteil von US-Firmen oder -Branchen. Die PPD-28 sehe vor, dass Digitalüberwachung so maßgeschneidert wie möglich sei und eine Massenüberwachung nur für spezifisch aufgezählte Zwecke genutzt wird. Die PPD-28 verpflichte die Geheimdienst-Community Verfahren zu wählen, die vernünftig gestaltet sind, um die Weitergabe und die Vorratsspeicherung von Personendaten aus der Digitalüberwachung zu minimieren.[59]

Von US-Firmen könnten Daten nur auf einer gesetzlichen Grundlage wie z. B. dem Foreign Intelligence Surveillance Act (FISA) oder gemäß den Regeln zu National Security Letters abverlangt werden. Das ODNI betont, dass die verfassungsrechtlichen Anforderungen, insbesondere des 4. Zusatzartikels, zu beachten seien.[60] Soweit machbar, werde gezielte Überwachung einer Massenüberwachung vorgezogen. Nicht jede technisch machbare Maßnahme sei zulässig, sondern nur eine, die vernünftig (reasonable) ist. Massenüberwachung sei nur zulässig für folgende sechs „spezifische“ Zwecke: „Terrorismusabwehr, Abwehr von Nulkearwaffenverbreitung, Cybersicherheit, Feststellung und Abwehr von Gefahren für die USA oder alliierte Streitkräfte, Bekämpfung grenzüberschreitender Kriminalitätsrisiken einschließlich dem Sichentziehen von Strafen“. Die Einhaltung dieser „Verwendungsbeschränkungen“ werde durch den Director for National Intelligence (DNI) überprüft

57 Annex 3, Anschreiben.

58 Dokumentiert unter http://fas.org/irp/offdocs/ppd/ppd-28.pdf.

59 Annex 6 S. 2 f.

60 Annex 7 S. 1 f.

und von ihm, soweit möglich, offengelegt. Es sei wichtig zu betonen, dass sich die Massenüberwachung „nur auf einen kleinen Anteil des Internet“ beziehe. Nur nachrichtendienstlich wertvolle Informationen würden den Analysten vorgelegt. Dadurch werde die Beachtung von Datenschutz und Bürgerrechten gewährleistet.[61]

Im Rahmen des (klassifizierten) National Intelligence Priorities Framework (NIPF) würde Digitalüberwachung vom National Signals Intelligence Committee (SIGCOM) genehmigt, wobei hieran folgende Anforderungen gestellt würden: Ist das Überwachungsziel oder die verwendete Methode besonders sensitiv? Wenn ja, bedarf es einer Überprüfung durch einen höherrangigen Regierungsbeamten. Stellt die Datenerhebung, unabhängig von der Nationalität, ein unvertretbares Risiko für Datenschutz und Bürgerrechte dar? Sind zusätzliche Vorkehrungen bei der Weitergabe oder der Vorratsspeicherung nötig, um Datenschutz oder nationale Sicherheitsinteressen zu sichern?[62] Bei allem Respekt gegenüber dem Privacy Shield erklärt das ODNI, dass die USA nicht auf spezifische Methoden oder Operationen von vornherein verzichten könne.[63]

§ 4 der PPD-28 fordere, dass auch in Bezug auf *Nicht-US-Bürger* Grenzen der Vorratshaltung und Weitergabe bestehen. Die Aufbewahrung müsse einem der vom NIPF autorisierten Geheimdienstziele dienen, Hinweise auf eine Straftat geben oder einem der anderen Aufbewahrungsanforderungen genügen, die im Executive Order 123333, section 2.3 festgeschrieben sind. Werden diese Anforderungen nicht erfüllt, so müssten die Daten spätestens nach fünf Jahren gelöscht werden, es sei denn, der DNI stellt fest, dass eine weitergehende Speicherung im nationalen Sicherheitsinteresse der USA liegt.[64] Zusätzlich wird von allen Diensten bei der Umsetzung von PPD-28 gefordert, dass eine Weitergabe nur deshalb, weil sich die Daten auf Ausländer beziehen, nicht zulässig sei.[65]

In einem weiteren Kapitel beschreibt das ODNI die *Aufsicht und Kontrolle der geheimdienstlichen Digitalüberwachung*. Es würden hunderte von Aufsichtspersonen beschäftigt, allein von der NSA 300, die für die Regelkonformität zuständig seien.[66]

2.2.2 Ombudsperson

§ 4(d) PPD-28 sieht die Benennung eines „Senior Coordinator for International Information Technology Diplomacy“ (Senior Coordinator) vor als Kontaktstelle für andere Regierungen zur Austausch von Bedenken in Bezug auf Geheimdienstaktivitäten der USA. Frau Novelli wurde im Januar 2015 zum Senior Coordinator ernannt. Gemäß dem im Annex 3 dokumentierten „EU-U.S. Privacy Shield

61 Annex 6 S. 4.

62 Annex 6 S. 5.

63 Annex 6 S. 6.

64 Annex 6 S. 6 f.

65 Annex 6 S. 7.

66 Annex 6 S. 7.

Ombudsperson Mechanism regarding Signals Intelligence“ (künftig zitiert als Omb-Mech)[67] wird die Senior Coordinator zur Privacy Shield Ombudsperson eingesetzt. Sie arbeitet eng mit den Ministerien und den Geheimdiensten zusammen. Sie berichtet direkt dem Außenminister und sei von der Geheimdienst-Community unabhängig. Sie arbeitet auch mit Aufsichtsinstanzen zusammen. Insbesondere koordiniert sie sich eng mit dem Büro des Director of National Intelligence (ODNI), dem US-Justizministerium sowie weiteren Ministerien und Stellen, die in den USA mit nationaler Sicherheit befasst sind, Generalinspekteuren (Inspectors General), Informationsfreiheitsbeauftragten (Freedom of Information Act Officers) und Bürgerrechts- und Datenschutzbeauftragten (Civil Liberties and Privacy Officers). Sie kann Anfragen an den Civil Liberties Oversight Board zur Berücksichtigung überweisen.

Es soll eine EU-Stelle für Individualbeschwerden (EU Individual Complaint Handling Body – künftig *EU-Beschwerdestelle*) eingerichtet werden, die Beschwerden entgegennimmt, prüft und an die Ombudsperson weiterleitet. Diese prüft, ob die Anfrage den Anforderungen von § 3.b des Omb-Mech entspricht. Bei Bedarf kommuniziert sie mit dem Beschwerdeführer über die EU-Beschwerdestelle. Nach Prüfung der Beschwerde bestätigt die Ombudsperson der EU-Beschwerdestelle, dass hierzu korrekt ermittelt wurde und, entweder, dass das US-Recht und die Begrenzungen des ODNI-Briefes (Annex 6) beachtet worden sind, oder, bei Verstößen, dass dem Verstoß abgeholfen wurde. Die Ombudsperson wird weder bestreiten noch bestätigen, dass eine Person von einer Geheimdienstoperation betroffen war, noch mitteilen, welche Abhilfe erfolgt ist.[68] Außerdem können Anfragen gemäß § 5 Omb-Mech als Informationsfreiheitsanfragen gemäß den geltenden Regeln behandelt werden. Die EU-Beschwerdestelle bescheidet daraufhin den Beschwerdeführer.

2.2.3 Rechtsbehelfe?

Der *Freedom of Information Act* (FOIA) ist veröffentlicht als United States Code (U.S.C. § 552).[69] Jede Behörde hat einen FOIA-Beauftragten und informiert über das Internet, unter welchen Voraussetzungen Anfragen erfolgen können. Keine Auskunft nach dem FOIA wird erteilt bei klassifizierten Unterlagen über die nationale Sicherheit, Personeninformationen zu Dritten und Informationen über strafrechtliche Ermittlungen.[70] Beschwerden wegen Informationszugangsfragen nach dem FOIA werden zunächst verwaltungsintern beschieden und gehen dann vor ein Bundesgericht. Das Gericht entscheidet, ob Dokumente nach 5 U.S.C. § 552(a)(4)(b) rechtmäßig zurückgehalten werden. Es gab schon Fälle, in denen Gerichte gegen die Regierungsklassifikation geurteilt haben.

In § 6 Omb-Mech werden weitere Rechtsbehelfe aufgeführt: Der gesetzlich unabhängige *Generalinspekteur* kann Untersuchungen und Audits durchführen gemäß dem Inspector General Act aus dem Jahr 1978. Jede Einrichtung der Geheimdienst-Community hat ihren eigenen Generalinspekteur, der u. a. auch nachrichtendienstliche Aktivitäten im Ausland überprüfen kann. Die

67 Der Omb-Mech ist zu finden in Annex 3.

68 Annex 3 § 4.e Omb-Mech.

69 www.FOIA.gov und http://www.justice.gov/oip/foia-resources.

70 § 5.c Omb-Mech.

Empfehlungen eines Generalinspekteurs sind jedoch nicht verpflichtend. *Bürgerrechts- und Datenschutzbeauftragte* haben insbesondere Beratungs- und Informationsfunktionen. So gibt es z. B. einen ODNI´s Civil Liberties and Privacy Officer (ODNI CLPO). Auch die NSA kann einen CLPO vorweisen.[71] Gemäß 2 U.S.C. §2000ee et seq. gibt es ein Privacy and Civil Liberties Oversight Board, das Datenschutzbemühungen in Behörden unterstützt.[72]

Das ODNI beschreibt zudem den Kontrollmechanismus des FISA, des *Foreign Intelligence Surveillance Acts* – Section 702. Die Regelung erlaubt die zwangsweise Erhebung nachrichtendienstlicher Informationen bei Internet-Servicediensten in Bezug auf Nicht-US-Bürger. Voraussetzung sei dafür eine jährliche Zertifizierung durch das FISA-Gericht auf Antrag des vom Präsidenten benannten und vom US-Senat bestätigten US-Justizministers (Attorney General) und des ODNI, wobei spezifische Kategorien identifiziert würden. Dadurch handele es sich nicht um Massenüberwachung, sondern diese „besteht ausschließlich darin, gezielt spezifische Personen, zu denen individualisiert Merkmale festgelegt worden sind“, zu erfassen. Dies erfolgt z. B. über individuelle Selektoren, etwa E-Mail-Adressen oder Telefonnummern. Dadurch wurden 2014 gezielt ca. 90.000 Personen gemäß Section 702 erfasst, was ein winziger Anteil der über 3 Mrd. Internetnutzer weltweit sei.[73] Das FISA-Gericht, besetzt mit unabhängigen Bundesrichtern, spiele eine wichtige Rolle bei der Umsetzung von Section 702. Das Gericht überprüft jährlich die Zertifizierungen. Nicht alle Entscheidungen des FIS-Gerichts seien geheim, einige seien entklassifiziert worden. Eine Auswirkung des FOIA sei, dass das FISA-Gericht einen externen Anwalt als unabhängigen Vertreter des Datenschutzes (amicus curiae) in Fällen neuer oder bedeutender rechtlicher Fragen benennen kann. Der Grad an Beteiligung unabhängiger Gerichte in Fragen des Auslandsgeheimdienstes sei deshalb beispiellos.[74]

Der im Juni 2015 in Kraft getretene *USA FREEDOM Act* erhöhe, so das ODNI, die öffentliche Transparenz der US-Überwachung und der nationalen Sicherheitsbehörden. Das Gesetz verbiete Massenüberwachung bei Datenspeicherungen auch in Bezug auf Nicht-US-Bürger gemäß dem FISA oder über die Verwendung der National Security Letters. Das Gesetz fordere die Anwendung „spezifischer Selektionsbegriffe“, also eine Konkretisierung auf eine Person, ein Konto oder eine Adresse. Der DNI werde nach Beratung mit dem US-Justizminister befugt, FISA-Gerichtsentscheidungen zu deklassifizieren oder zu veröffentlichen. Weiterhin könnten Offenlegungen der FISA-Sammlung und von Anträgen erfolgen. Unternehmen hätten nach dem Gesetz zudem das Recht, die aggregierten statistischen Zahlen von FISA-Anordnungen und National Security Letters aus Gründen der Strafverfolgung oder der nationalen Sicherheit in Transparenzberichten zu veröffentlichen, soweit dem keine US-Gesetze entgegenstehen. So ergebe sich aus dem Bericht eines größeren Unternehmens, dass von 400 Mio. Internetkonto-Inhabern weniger als 20.000 von Herausgabeverlangen betroffen waren.[75]

71 https://www.nsa.gov/civil_liberties/.

72 § 6.b.iv Omb-Mech; Annex 6 S. 7 ff.

73 Annex 6 S. 11.

74 Annex 6 S. 12.

75 Annex 2 III.16, Annex 6 S. 14.

[Privacy Shield – Darstellung und rechtliche Bewertung

Im Hinblick auf den gerichtlichen *Rechtsschutz* verweist das ODNI darauf, dass die Möglichkeit eines Rechtsbehelfs vor dem FISA-Gericht nicht auf US-Bürger begrenzt ist. Rechtsschutzmöglichkeiten bestünden für EU-Bürger zudem nach dem Computer Fraud and Abuse Act, der vorsätzlichen unauthorisierten Zugang zu Computersystemen verbietet. Gemäß dem Electronic Communications Privacy Act können Personen unabhängig von ihrer Nationalität gerichtlich gegen Regierungsbeamte vorgehen, die unzulässig und vorsätzlich Zugriff auf gespeicherte Daten genommen haben. Nach dem Right to Financial Privacy Act könne eine Bank oder ein Kunde die US-Regierung auf Schadenersatz wegen unzulässigem Zugang zu Kundendaten verklagen. Letztlich könne auch über den FOIA Rechtsschutz erlangt werden.[76]

2.2.4 Strafverfolgung

In einem Annex 7 nimmt das US-Justizministerium zu der Frage des Datenschutzes beim Zugriff auf Unternehmensdaten für Zwecke der Strafverfolgung Stellung. Es weist darauf hin, dass mit einer Zwangsmaßnahme der Anklagebehörde (Grand Jury oder Trial Subpoena) die Herausgabe von Daten durchgesetzt werden kann. In straf- wie in zivilrechtlichen Ermittlungen kann dies auch mit einer Verwaltungs-Zwangsmaßnahme (Administrative Subpoena Authority) erreicht werden. Außerdem können Datenherausgaben über gerichtliche Anordnungen bewirkt werden. Beispiele sind in Bezug auf Verkehrsdaten Court Orders for Pen Register and Trap and Traces[77], in Bezug auf Bestands-, Verkehrs- und Inhaltsdaten auch in Echtzeit der Electronic Communications Privacy Act (ECPA) bzw. als Teil davon der Stored Communications Act[78], für Echtzeitüberwachung das Federal Wiretap Law[79] und durch die Beschlagnahme von Datenträgern die Search Warrant-Rule 41. Danach würden regelmäßig ein hinreichender Verdacht (propable cause) vorausgesetzt und begrenzende, die Betroffenen schützende Vorkehrungen vorgesehen. In Ergänzung hat das Justizministerium Richtlinien (guidelines and policies) herausgegeben, die den Ermittlungsmaßnahmen auch im Interesse des Datenschutzes und des Schutzes von Bürgerrechten weitere Grenzen setze.[80]

3 Rechtliche Anforderungen an den Datentransfer in die USA

3.1 Europäische Datenschutzrichtlinie

Die geplante Angemessenheitsentscheidung der EU-Kommission basiert auf Art. 25 der Europäischen Datenschutzrichtlinie (EG-DSRl – Richtlinie 95/46/EG):

„(1) Die Mitgliedstaaten sehen vor, dass die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen

76 Annex 6 S. 16 f.

77 18 U.S.C. §§ 3121-3127.

78 18 U.S.C. §§ 2701-2712.

79 18 U.S.C. §§ 2510-2522.

80 Annex 7 S. 3 ff.

einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt. …

(6) Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet. Die Mitgliedstaaten treffen die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.“

3.2 Safe-Harbor-Urteil des EuGH

Der EuGH hat im Safe-Harbor-Urteil[81] die Anforderungen an einen grundrechtskonformen Datentransfer in Staaten außerhalb der EU beschrieben:

„(39) Wie sich aus Art. 1 und aus den Erwägungsgründen 2 und 10 der Richtlinie 95/46 ergibt, soll diese nicht nur einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechte natürlicher Personen, insbesondere des Grundrechts auf Achtung der Privatsphäre, bei der Verarbeitung personenbezogener Daten gewährleisten, sondern auch ein hohes Niveau des Schutzes dieser Grundrechte und Grundfreiheiten. Die Bedeutung sowohl des durch Art. 7 der Charta gewährleisteten Grundrechts auf Achtung des Privatlebens als auch des durch ihren Art. 8 gewährleisteten Grundrechts auf Schutz personenbezogener Daten wird im Übrigen in der Rechtsprechung des Gerichtshofs hervorgehoben ….

(70) Zwar enthält weder Art. 25 Abs. 2 der Richtlinie 95/46 noch eine andere Bestimmung der Richtlinie eine Definition des Begriffs des angemessenen Schutzniveaus. Insbesondere sieht Art. 25 Abs. 2 der Richtlinie lediglich vor, dass die Angemessenheit des Schutzniveaus, das ein Drittland bietet, „unter Berücksichtigung aller Umstände beurteilt [wird], die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen“, und enthält eine nicht abschließende Aufzählung der bei einer solchen Beurteilung zu berücksichtigenden Umstände.

(71) Wie schon aus dem Wortlaut von Art. 25 Abs. 6 der Richtlinie 95/46 hervorgeht, verlangt diese Bestimmung jedoch zum einen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau „gewährleistet“. Zum anderen ist nach dieser Bestimmung die Angemessenheit des Schutzniveaus, das ein Drittland gewährleistet, „hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen“ zu beurteilen.

(72) Somit setzt Art. 25 Abs. 6 der Richtlinie 95/46 die in Art. 8 Abs. 1 der Charta ausdrücklich vorgesehene Pflicht zum Schutz personenbezogener Daten um und soll, wie der Generalanwalt in Nr.

81 EuGH U. v. 06.10.2016, C-362/14 = NJW 2015, 3151 ff.

[Privacy Shield – Darstellung und rechtliche Bewertung

139 seiner Schlussanträge ausgeführt hat, den Fortbestand des hohen Niveaus dieses Schutzes im Fall der Übermittlung personenbezogener Daten in ein Drittland gewährleisten.

(73) Zwar impliziert das Wort ´angemessen` in Art. 25 Abs. 6 der Richtlinie 95/46, dass nicht verlangt werden kann, dass ein Drittland ein dem in der Unionsrechtsordnung garantiertes identisches Schutzniveau gewährleistet. Wie der Generalanwalt in Nr. 141 seiner Schlussanträge ausgeführt hat, ist der Ausdruck ´angemessenes Schutzniveau` jedoch so zu verstehen, dass verlangt wird, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet, das dem in der Union aufgrund der Richtlinie 95/46 im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist. Ohne ein solches Erfordernis würde nämlich das in der vorstehenden Randnummer erwähnte Ziel missachtet. Außerdem könnte das durch die Richtlinie 95/46 im Licht der Charta garantierte hohe Schutzniveau leicht umgangen werden, indem personenbezogene Daten aus der Union in Drittländer übermittelt würden, um dort verarbeitet zu werden.

(74) Aus dem ausdrücklichen Wortlaut von Art. 25 Abs. 6 der Richtlinie 95/46 geht hervor, dass es die Rechtsordnung des Drittlands, auf das sich die Entscheidung der Kommission bezieht, ist, die ein angemessenes Schutzniveau gewährleisten muss. Auch wenn sich die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden können, die in der Union herangezogen werden, um die Wahrung der Anforderungen, die sich aus der Richtlinie im Licht der Charta ergeben, zu gewährleisten, müssen sich diese Mittel gleichwohl in der Praxis als wirksam erweisen, um einen Schutz zu gewährleisten, der dem in der Union garantierten der Sache nach gleichwertig ist.

(75) Unter diesen Umständen ist die Kommission bei der Prüfung des von einem Drittland gebotenen Schutzniveaus verpflichtet, den Inhalt der in diesem Land geltenden, aus seinen innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen resultierenden Regeln sowie die zur Gewährleistung der Einhaltung dieser Regeln dienende Praxis zu beurteilen, wobei sie nach Art. 25 Abs. 2 der Richtlinie 95/46 alle Umstände zu berücksichtigen hat, die bei einer Übermittlung personenbezogener Daten in ein Drittland eine Rolle spielen. ...

(78) Hierzu ist festzustellen, dass angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung der Privatsphäre und der großen Zahl von Personen, deren Grundrechte im Fall der Übermittlung personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, verletzt werden können, der Wertungsspielraum der Kommission hinsichtlich der Angemessenheit des durch ein Drittland gewährleisteten Schutzniveaus eingeschränkt ist, so dass eine strikte Kontrolle der Anforderungen vorzunehmen ist, die sich aus Art. 25 der Richtlinie 95/46 im Licht der Charta ergeben. ...

(81) Auch wenn der Rückgriff eines Drittlands auf ein System der Selbstzertifizierung als solcher nicht gegen das Erfordernis in Art. 25 Abs. 6 der Richtlinie 95/46 verstößt, dass in dem betreffenden Drittland „aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen“ ein angemessenes Schutzniveau gewährleistet sein muss, beruht die Zuverlässigkeit eines solchen Systems im Hinblick auf dieses Erfordernis wesentlich auf der Schaffung wirksamer Überwachungs- und Kontrollmechanismen, die es erlauben, in der Praxis etwaige Verstöße gegen Regeln zur Gewährleistung des Schutzes der Grundrechte, insbesondere des Rechts auf Achtung der Privatsphäre sowie des Rechts auf den Schutz personenbezogener Daten, zu ermitteln und zu ahnden.“

[Privacy Shield – Darstellung und rechtliche Bewertung

In Randnummer 83 des Safe-Harbor-Urteils stellte der EuGH dann fest, dass die Kommissions-Entscheidung zu Safe-Harbor „keine hinreichenden Feststellungen zu den Maßnahmen (enthält), mit denen die Vereinigten Staaten von Amerika aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen im Sinne von Art. 25 Abs. 6 der Richtlinie ein angemessenes Schutzniveau gewährleisten“. Derartige Feststellungen hält der EuGH für erforderlich.

„(84) Hinzu kommt, dass die Geltung der genannten Grundsätze nach Abs. 4 von Annex I der Entscheidung 2000/520 begrenzt werden kann, und zwar u. a. ´insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss`, sowie ´durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte`.

(85) Hierzu wird in Abschnitt B von Annex IV der Entscheidung 2000/520 hinsichtlich der Grenzen für die Geltung der Grundsätze des ´sicheren Hafens` Folgendes hervorgehoben: ´Es steht jedoch eindeutig fest, dass, wenn aufgrund des US-amerikanischen Rechts eine den Grundsätzen des sicheren Hafens entgegenstehende Verpflichtung auferlegt wird, die US-Unternehmen die Gesetze einhalten müssen, und zwar ungeachtet dessen, ob sie auf die Grundsätze des sicheren Hafens verpflichtet sind oder nicht.`

(86) In der Entscheidung 2000/520 wird somit den ´Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen` Vorrang vor den Grundsätzen des ´sicheren Hafens` eingeräumt; aufgrund dieses Vorrangs sind die selbstzertifizierten US-Organisationen, die aus der Union personenbezogene Daten erhalten, ohne jede Einschränkung verpflichtet, die Grundsätze des ´sicheren Hafens` unangewandt zu lassen, wenn sie in Widerstreit zu den genannten Erfordernissen stehen und sich deshalb als mit ihnen unvereinbar erweisen.

(87) Angesichts ihres generellen Charakters ermöglicht die Ausnahme in Abs. 4 von Annex I der Entscheidung 2000/520 es daher, gestützt auf Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder von Rechtsvorschriften der Vereinigten Staaten in die Grundrechte der Personen einzugreifen, deren personenbezogene Daten aus der Union in die Vereinigten Staaten übermittelt werden oder werden könnten. Für die Feststellung des Vorliegens eines Eingriffs in das Grundrecht auf Achtung der Privatsphäre kommt es nicht darauf an, ob die betreffenden Informationen über die Privatsphäre sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten. ...“

In Randnummer 88 fordert der EuGH, dass es staatlicher Regelungen bedarf, „die dazu dienen, etwaige Eingriffe – zu denen die staatlichen Stellen dieses Landes in Verfolgung berechtigter Ziele wie der nationalen Sicherheit berechtigt wären – in die Grundrechte der Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden, zu begrenzen“. In Randnummer 89 wird betont, dass es „eines wirksamen Rechtsschutzes gegen derartige Eingriffe“ bedarf. Dabei genüge nicht die Feststellung der Einhaltung der Anforderungen, die Grundlage für den Angemessenheitsbeschluss waren (dort Safe Harbor). Vielmehr müsste auch „die Rechtmäßigkeit von Eingriffen in Grundrechte, die sich aus Maßnahmen staatlichen Ursprungs ergeben, zur Anwendung kommen“.

[Privacy Shield – Darstellung und rechtliche Bewertung

Problematisch sei nach Randnummer 90, wenn „amerikanischen Behörden auf die aus den Mitgliedstaaten in die Vereinigten Staaten übermittelten personenbezogenen Daten zugreifen und sie in einer Weise verarbeiten konnten, die namentlich mit den Zielsetzungen ihrer Übermittlung unvereinbar war und über das hinausging, was zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig war“. Es bedürfe für die Betroffenen administrativer oder gerichtliche Rechtsbehelfe, „die es ihnen erlaubten, Zugang zu den sie betreffenden Daten zu erhalten und gegebenenfalls deren Berichtigung oder Löschung zu erwirken“.

„(91) Zu dem innerhalb der Union garantierten Schutzniveau der Freiheiten und Grundrechte ist festzustellen, dass eine Unionsregelung, die einen Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte enthält, nach ständiger Rechtsprechung des Gerichtshofs klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen muss, so dass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht. …

(92) Darüber hinaus verlangt der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene vor allem, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken. …

(93) Nicht auf das absolut Notwendige beschränkt ist eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen. …

(94) Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens. …

(95) Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz. Nach Art. 47 Abs. 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Insoweit ist schon das Vorhandensein einer wirksamen, zur Gewährleistung der Einhaltung des Unionsrechts dienenden gerichtlichen Kontrolle dem Wesen eines Rechtsstaats inhärent. …

(96) Nach den namentlich in den Rn. 71, 73 und 74 des vorliegenden Urteils getroffenen Feststellungen erfordert der Erlass einer Entscheidung der Kommission nach Art. 25 Abs. 6 der Richtlinie 95/46 die

gebührend begründete Feststellung dieses Organs, dass das betreffende Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Grundrechte gewährleistet, das dem in der Rechtsordnung der Union garantierten Niveau, wie es sich insbesondere aus den vorstehenden Randnummern des vorliegenden Urteils ergibt, der Sache nach gleichwertig ist."

3.3 Anforderungen der künftigen EU-DSGVO

In Art. 41 Abs. 2[82] Entwurf für eine Europäische Datenschutz-Grundverordnung (EU-DSGVO), worüber am 15.12.2015 im Trilog zwischen dem Parlament, dem Rat und der Kommission der EU Einigkeit hergestellt wurde[83], werden die künftigen Anforderungen an eine Angemessenheitsentscheidung festgelegt:

„Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt die Kommission insbesondere

(a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Drittland bzw. der betreffenden internationalen Organisation geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, einschließlich solcher, die die öffentliche Sicherheit, die Verteidigung, die nationale Sicherheit, das Strafrecht sowie den Zugang von Behörden zu personenbezogenen Daten betreffen, als auch die Umsetzung dieser Rechtsvorschriften, Datenschutzbestimmungen, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weitergabe personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation sowie die Rechtsprechung, wirksame und durchsetzbare Rechte der betroffenen Person und wirksame administrative und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden;

(b) die Existenz und die Wirksamkeit einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Sanktionsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind; und

(c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtlich verbindlichen Konventionen oder Instrumenten sowie aus der Teilnahme des Drittlands an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben."

82 In der Endfassung voraussichtlich Art. 45.

83 Rat der EU, v. 28.01.2016, 5455/16, Interinstitutionelles Dossier: 2012/0011 (COD), abzurufen z. B. unter https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/EU-Datenschutzreform_tritt_in_entscheidende_Phase_-_UPDATE_neu_18_02_2016/280116GRV-politische_Einigung.pdf.

4 Bewertung

Die rechtliche Bewertung des Privacy Shields erfolgt auf der Grundlage von *Art. 25 Abs. 6 EG-DSRl*, wonach die Kommission feststellen kann, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Datenschutzniveau im Sinne des Absatzes 2 gewährleistet. Gemäß Absatz 2 sind alle Umstände zu berücksichtigen, die bei der Datenübermittlung eine Rolle spielen.

Dabei sind die in der *Grundrechtecharta* (EUGRCh) garantierten Rechte zu beachten, hier insbesondere die Art. 7, 8 und 47, die Privatsphäre, Datenschutz und Rechtsschutz gewährleisten. In den USA besteht kein diesen Artikeln entsprechender Grundrechtsschutz auf Verfassungsebene.[84] Nicht erforderlich ist, dass die Grundrechte als solche vom Drittland garantiert werden. Wohl aber müssen die geltenden Rechtsvorschriften im Ergebnis einen angemessenen Schutz geben. Insofern werden vom EuGH hohe Anforderungen gestellt, die im Folgenden geprüft werden.

4.1 Rechtsvorschriften

Art. 25 Abs. 6 EG-DSRl nimmt Bezug auf „Rechtsvorschriften“. Das Privacy Shield basiert aber auf nicht auf internationalen Abkommen oder Gesetzen, sondern auf *Briefen der US-Regierung und -Behörden*, die teilweise Bezug nehmen auf US-Gesetze sowie auf die Rechtspraxis. Im Entwurf ihres EU-Privacy-Shield-Beschlusses benennt die EU-Kommission in den Randnummern 112-116 keinen gesetzlichen Rahmen, sondern bezieht sich ausschließlich auf die in den Schreiben von US-Behörden erwähnten Maßnahmen des Privacy Shield in Bezug auf Transparenz und Umsetzung. Sie unterlässt es, die brieflichen Zusicherungen auf ihre Realitätsnähe und auf ihre effektive rechtliche Wirkung hin zu bewerten. Auch unterlässt sie es zu prüfen, welchen *Rechtscharakter* die Schreiben nach US-Recht haben und welche Bedeutung weitere Schreiben der US-Regierung haben können, die in Konflikt mit den vorliegenden Schreiben stehen. Dies überlässt sie künftigen Evaluationen. Es werden keine Angaben gemacht, welche Rechtsfolgen die Aufnahme der Briefe ins „U.S. Federal Register“ hat.[85] Damit wird auch die künftige Regelung des Art. 41 Abs. 2 c EU-DSGVO konterkariert, der eine hohe rechtliche Verbindlichkeit für Angemessenheitsentscheidungen der EU-Kommission einfordert.

Das Privacy Shield hat mit Safe Harbor gemein, dass es trotz aller Transparenzregelungen in Bezug auf Inhalte und Verfahren *für Betroffene undurchsichtig* bleibt. Dies ist u. a. dem „Regelungs“-Konzept in Form von Briefen zuzuschreiben, in denen inhaltlich überlappend zu Einzelfragen Aussagen gemacht werden, die mit ihrer Terminologie und ihren Verweisungen oft selbst für Fachleute unverständlich bleiben.

Die Privacy-Shield-Prinzipien und deren Erläuterungen zeichnen sich durch *Unklarheiten* und – aus rechtlicher Sicht – viel Prosa aus. Aussagen werden oft nur beispielhaft gemacht und lassen so weiten Raum für unterschiedliche Interpretationen.

84 Weichert, RDV 2012, 115; Arzt, Polizeiliche Überwachungsmaßnahmen in den USA, 2004, S. 20 ff.; Böhm, A comparison between US and EU data protection legislation for law enforcement purposes, 2015, S. 51.

85 EU-K-Beschluss-E Rn. 12.

Man kann bei der Lektüre der Dokumente den Eindruck haben, dass die *Strukturierung* den Leser verwirren soll. Ein geordnetes Regelungskonzept ist nicht erkennbar. Materielle und prozedurale Regelungen gehen durcheinander, ohne sich an eine vorgegebene Ordnung zu halten. Innerhalb der Anhänge erfolgen nur schwer nachvollziehbare Verweisungen aufeinander.

Art. 25 Abs. 2 EG-DSRl sieht vor, dass die Beurteilung der Angemessenheit „unter Berücksichtigung aller Umstände" erfolgen muss.[86] Das Privacy Shield ist von dem Ansatz „Quantität statt Qualität" gekennzeichnet: Es werden teils parallel und teils aufeinander aufbauend eine Vielzahl von Mechanismen etabliert und dargestellt, die administrativ äußerst aufwändig sind und oft nur eine begrenzte oder gar keine rechtliche Verbindlichkeit haben. Die Erwartung besteht anscheinend darin, dass die Zahl der erwähnten Mechanismen den Mangel an Verbindlichkeit kompensieren kann.

Die Privacy-Shield-Prinzipien für US-Privatunternehmen wie auch die Regelungen zu den US-behördlichen Zugriffsmöglichkeiten werden von der EU-Kommission nicht, wie man hätte erwarten können, mit den grundrechtlichen Garantien oder den bestehenden Datenschutzregelungen der EU abgeglichen, sondern lediglich dargestellt.[87] Der Wertungsspielraum der Kommission hinsichtlich der Angemessenheit ist aber eingeschränkt; sie müsste eine strikte Kontrolle der Anforderungen anhand eines Rechtsvergleichs und eine nachvollziehbare Abwägung vornehmen.[88] Wegen dieses *fehlenden Rechtsvergleichs* lässt die EU-Kommission nicht erkennen, ob sie geprüft hat, wo die US-Zusagen hinter dem europäischen Recht zurückbleiben und durch welche möglicherweise kompensierenden Maßnahmen die Gleichwertigkeit des Datenschutzniveaus erreicht wird bzw. werden soll.[89] Damit ist der Kommissionsbeschluss schon wegen der Verletzung der an ihn zu stellenden formellen Begründungsanforderungen rechtswidrig.

4.2 Regeln für US-Unternehmen

In einer Bewertung des Privacy Shield kommt die EU-Kommission zu dem *Ergebnis*, dass die dort vorgesehenen Rechtsbehelfe es ermöglichen, Verstöße gegen die dargelegten Prinzipien festzustellen, in der Praxis zu sanktionieren und Rechtsschutzmöglichkeiten für die Betroffenen zu eröffnen.[90] Die Kommission stellt aber an keiner Stelle fest, dass die Privacy-Shield-Prinzipien mit den europäischen Datenschutzstandards gleichwertig sind und dass nicht nur die Möglichkeit eines Rechtsschutzes in bestimmten Fällen besteht, sondern dass die Gewähr hierfür in allen wesentlichen Fällen gegeben wird.

Ein grundlegender *Mangel der Prinzipien* des Privacy Shield liegt darin, dass diese keine verbindlichen Normierungen enthalten, wie wir sie in der EG-DSRl und künftig in der EU-DSGVO finden, sondern

86 Vgl. EuGH (Fn. 6) Rn. 75.

87 Beschlussempfehlung Rn. 16-23, 52 ff.

88 EuGH (Fn. 6) Rn. 78.

89 EuGH (Fn. 6) Rn. 73, 74.

90 EU-K-Beschluss-E Rn. 115.

vielmehr vage Prinzipien, die einen breiten Auslegungsspielraum lassen, der von verarbeitenden Stellen natürlich extensiv in Anspruch genommen werden wird. Dadurch wird das europäische Datenschutzniveau stark unterschritten. Dies kann an einer Vielzahl von Beispielen dargestellt werden. Exemplarisch wird dies hier dargelegt für die „Zweckbindung“ und den Grundsatz der „Erforderlichkeit“:

Gemäß Art. 8 Abs. 2 EUGRCh dürfen personenbezogene Daten nur für festgelegte Zwecke oder auf einer gesetzlich geregelten legitimen Grundlage verarbeitet werden. Dieser europäische Standard wird durch die Privacy-Shield-Prinzipien nicht erreicht. Bei diesen handelt es sich nicht um gesetzliche Regeln, sondern im Ergebnis um eine Selbstverpflichtung. Mit dieser wird die verfassungsrechtlich geforderte strenge *Zweckbindung* unterlaufen. Die Zweckbindung wird im Prinzip Nr. 5 angesprochen, jedoch sofort wieder weitgehend aufgehoben, indem Zweckänderungen nur ausgeschlossen werden, wenn der Nutzungszweck „mit dem Zweck, für den die Daten erhoben wurden, unvereinbar ist“.[91] Eine Abwägungsklausel, wie sie z. B. in Art. 6 EG-DSRl angedeutet und im Entwurf von Art. 6 Abs. 1 EG-DSGVO explizit vorgesehen ist und die dem europäischen Standard entspricht, enthalten die Prinzipien nicht.

Ein grundlegender europäischer Datenschutzstandard ist die Beschränkung der Datenverarbeitung auf die *Erforderlichkeit*. Begründet wurde dieser Grundsatz 1983 durch das Urteil des deutschen Bundesverfassungsgerichts zur Volkszählung.[92] Inzwischen werden die Anforderungen an die Erforderlichkeit durch den Grundsatz der „Datenminimierung“ verstärkt, der als fundamentales Verarbeitungsprinzip in Art. 5 Abs. 1 lit. c EU-DSGVO vorgesehen ist.[93] Entsprechende Anforderungen sind in den Prinzipien des Privacy Shield nicht enthalten.

Der *Auskunftsanspruch* ist in Art. 8 Abs. 2 S. 2 EUGRCh zugesichert. In den Zusatzprinzipien des Privacy Shield wird dieses Recht der Betroffenen in einem Maße eingeschränkt, das weit über das des europäischen Rechts hinausgeht.[94]

Das Privacy Shield sieht, wie Safe Harbor, eine *Selbstzertifizierung* vor. Eine solche ist nach Art. 25 Abs. 6 EG-DSRl nicht generell ausgeschlossen. In jedem Fall bedarf es aber wesentlicher wirksamer Überwachungs- und Kontrollmechanismen, die es ermöglichen, Datenschutzverstöße zu ermitteln und zu ahnden.[95] Die geplanten Regeln zur Selbstzertifizierung sind aber äußerst löchrig. So enthalten sie z. B. keine Aussage, was bei einer Selbst-Zertifizierung passiert, die nicht bei der FTC oder des DOT, sondern bei einer anderen Behörde erfolgt. Die brieflichen Zusagen des DOT sind erheblich unverbindlicher als die schon wenig konkreten Zusagen der FTC.

Das *Beschwerdeverfahren* des Privacy Shield ist zwar etwas konkreter als das bisherige von Safe Harbor, aber für die Betroffenen äußerst beschwerlich und ein Hindernislauf, bei dem die Betroffenen, wenn

91 Annex 2 II.5.

92 BVerfG NJW 1984, 419 ff.

93 Vgl. auch Art. 23 Abs. 2a, 30 Abs. 1 lit. a, 38 Abs. 1a lit. bb EU-DSGVO-E.

94 Anhang 2 III.8.e.

95 EuGH (Fn. 6) Rn. 81.

sie nicht über viel zeitliche, fachliche und finanzielle Ressourcen verfügen, schnell straucheln und scheitern.

Ohne dass dies explizit zum Ausdruck gebracht wird, scheint eine Prüfung durch eine US-Behörde und insbesondere ein US-Gericht nur effektiv möglich sein, wenn zuvor oder parallel ein Streitschlichtungsverfahren durchlaufen wird. So wird auf die Klagemöglichkeit nur in diesem Bezug hingewiesen, wobei die Thematisierung von Fragen der nationalen Sicherheit oder von anderen öffentlichen Interessen ausgeschlossen ist.[96] Die Streitschlichtung ist privat organisiert und gibt dem Betroffenen keine faire Chance, da eine Vertretung durch eine Datenschutzaufsichtsbehörde ausgeschlossen ist, eine anwaltliche Vertretung selbst bezahlt werden muss, das Verfahren in englischer Sprache und in jedem Fall räumlich in den USA durchgeführt wird nach US-Rechtsregeln, die dem Betroffenen wenig transparent sind. Durch die Beschränkung auf den konkreten Einzelfall sind grundsätzliche Klärungen des Geschäftsgebarens von US-Unternehmen nicht möglich.

Private Streitschlichtungsverfahren sind in Europa im Verbraucherbereich nicht üblich und auch ungeeignet. Sie eignen sich eher für Konfliktlösungen zwischen Staaten und großen Unternehmen; sie werden praktiziert für die Auslegung von Freihandelsabkommen. Die Betroffenen können i. d. R. die Schlichter weder bewerten, die ihnen zur (gemeinsamen) Auswahl angeboten werden, noch können sie die (nicht öffentlichen) Verhandlungen aus der Ferne und ohne Kenntnis der eigenen Rechte wirksam beeinflussen.

Die Aufsichtsverfahren bei den (Verbraucher-) Behörden gewähren den EU-Betroffenen nicht mehr Rechte als US-Bürgern. Da anerkannt ist, dass diese nicht ansatzweise den europäischen Datenschutzstandards entsprechen, ändert sich durch die Einbeziehung des Privacy Shields insofern nichts. Insbesondere wird nicht einmal gewährleistet, dass in jedem Fall eine aufsichtliche Prüfung zumindest durch die FTC stattfindet.

Die aufsichtliche Prüfung ist nicht ansatzweise *unabhängig*. Die gilt für die FTC, erst recht aber für die Aufsicht durch das DOC oder das DOT als Ministerien. Die Erfahrung ist, dass diese Behörden administrative Interessen verfolgen, was nicht immer die Interessen des Datenschutzes sind. In Art. 8 Abs. 3 EUGRCh ist festgelegt, dass die administrative Einhaltung der Datenschutzregelungen von einer unabhängigen Stelle überwacht wird. Dieser Rechtsgedanke wird in Art. 41 Abs. 2 des Entwurfs für eine EU-DSGVO aufgegriffen, wonach „die Existenz und die Wirksamkeit einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland“ als zentrale Bedingung für eine Angemessenheitsentscheidung genannt werden. Hierzu ist im Privacy Shield nichts vorgesehen, auch kein gleichwertiger Ersatz.

Das Datenschutzniveau des Privacy Shield müsste nicht nur gleichwertig, sondern auch „wirksam“ sein.[97] Zur *Wirksamkeit* enthält die geplante Kommissionsentscheidung keine rechtlichen oder faktisch belastbaren Ausführungen, sondern nur Willensbekundungen.

Im Entwurf für die Kommissionsentscheidung wird darauf hingewiesen, dass ein von einer unzulässigen Datenübermittlung in die USA Betroffener letztlich sich an die zuständige europäische

96 Annex 2 III.11.d, Annex 1 E. zu Annex 2.

97 EuGH (Fn. 6) Rn. 74.

Datenschutzbehörde wenden könne, der es letztlich zustehe, den Datentransfer in die USA zu unterbinden. Werde dem nicht angemessen durch die Datenschutzbehörde entsprochen, so habe der Betroffene das Recht, deshalb die Datenschutzbehörde nach vor einem *nationalen Gericht eines EU-Mitgliedsstaates* zu verklagen.[98] Diese auf dem Safe-Harbor-Urteil[99] beruhende Aussage hat derzeit keine explizite Grundlage im deutschen Recht. Unabhängig hiervon ist diese generelle Ausführung nicht in der Lage, die Defizite der Rechtsschutzmöglichkeiten des Privacy Shield zu beheben.

4.3 Beschränkung des staatlichen Datenzugriffs

Hinsichtlich des staatlichen Zugriffs auf europäische Daten durch US-Behörden stellt die EU-Kommission fest, dass dieser „darauf beschränkt ist, was streng erforderlich ist zur Erreichung der in Frage stehenden legitimen Ziele und dass es wirksamen Rechtsschutz gegen solche Eingriffe gibt“.[100] Wie sie auf der Basis der dargestellten Erkenntnisse zu diesem *Ergebnis* kommt, ist nicht nachvollziehbar.

4.3.1 Materielle Regelungen

Der EuGH hat festgestellt, dass Pauschalausnahmen hinsichtlich des Datenschutzes in Bezug auf die Erfordernisse „der *nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen*“ unzulässig sind, es sei denn, „die Organisation kann in Wahrnehmung dieser Rechte nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte“.[101] Zwar sind die erwähnten Bereiche nicht mehr, wie bei Safe Harbor, insgesamt ausgenommen, doch sehen die zentralen Einzelregelungen des Privacy Shield genau solche Pauschalausnahmen vor, ohne dass gerichtlich überprüfbare Abwägungsklauseln aufgenommen werden. Dies ist der Fall für die Anwendung der Prinzipien,[102] insbesondere auch für das grundlegende Auskunftsrecht der Betroffenen[103], bei der Streitschlichtung[104] und auch hinsichtlich der Zulassung undifferenzierter Massenüberwachung.[105]

Hinsichtlich des Behördenzugriffs zeigt sich besonders klar, dass die US-Seite bisher nicht bereit ist zu akzeptieren, dass Datenschutz ein *individuell einklagbares Grundrecht* ist und nicht nur eine

98 EU-K-Beschluss-E Rn. 44, 45.

99 EuGH (Fn. 6) Rn. 64.

100 EU-K-Beschluss-E Rn. 116..

101 EuGH (Fn. 6) Rn. 84.

102 Annex 2 I.5.

103 Annex 2 III.8.e.

104 Annex 2 III.11.d.iv. mit Verweis auf I.5 in der Fußnote.

105 Annex 6 S. 4.

administrative, im Einzelfall rechtlich unverbindliche Erwägung. Sämtliche Ausführungen zum Datenschutz in Bezug auf den behördlichen Zugriff sind allgemeiner Art und enthalten keine rechtlich verbindlichen, geschweige denn einklagbaren Ansprüche.

Die Regelungen erfassen nicht sämtliche *Verarbeitungsschritte*, wie sie vom Grundrecht nach Art. 8 EUGRCh erfasst werden, sondern lediglich die Speicherung und die Übermittlung. Nicht erfasst werden die Erhebung, die Veränderung sowie sämtliche Formen der Nutzung etwa unter Heranziehung der Methoden des Profiling oder anderer Big-Data-Analysen.

In Art. 8 Abs. 2 EUGRCh wird der *Zweckbindungsgrundsatz* grundrechtlich normiert. Dieser Grundsatz gilt auch im öffentlichen Bereich und bei der Wahrnehmung von Aufgaben der öffentlichen und der nationalen Sicherheit. Er zwingt bei staatlichen Zugriffen auf von privaten Stellen gespeicherte Daten – was zu einer Zweckänderung führt – zu Abwägungen. Derartige Abwägungen sind im Privacy Shield nicht vorgesehen.

Entgegen dem Safe-Harbor-Urteil sind keine *Rechtsbehelfe* vorgesehen, „die es ihnen erlaubten, Zugang zu den sie betreffenden Daten zu erhalten und gegebenenfalls deren Berichtigung oder Löschung zu erwirken“.[106]

Ein Rückgriff auf das *Verfassungsrecht* ist weder materiell-rechtlich noch prozessual möglich. Der nach dem 4. Zusatzartikel geforderte „Reasonable“-Test entspricht nicht ansatzweise den Anforderungen an eine Verhältnismäßigkeitsprüfung bei Grundrechtseingriffen nach europäischem Verständnis. Es sind auch keine prozessualen Vorkehrungen getroffen, über die Betroffene verfassungsrechtliche Erwägungen wirksam vortragen und damit zu einer gerichtlichen Entscheidungsgrundlage machen könnten, da die US-Verfassung Nicht-US-Bürgern insofern keine Rechte einräumt.

4.3.2 Prozedurale Regelungen

Das Datenschutzniveau des Privacy Shield müsste gleichwertig und „wirksam“ sein.[107] Zur *Wirksamkeit* enthält die geplante Kommissionsentscheidung keine Ausführungen. Dafür, dass diese besteht, gibt es keine Indizien.

In einem Schreiben vom 22.02.2016 wies die Europäische Ombudsfrau Emily O´Reilly EU-Kommissarin Jourová zu Recht darauf hin, dass der Begriff „ombudsman“ gemäß dem International Ombudsman Institut voraussetzt, dass eine „unabhängige und objektive Bewertung von Beschwerden angeboten“ wird. Eine Ombudsperson „darf keine Weisungen von irgendeiner staatlichen Stelle erhalten, die ihre Unabhängigkeit beeinträchtigen würde“. Zudem habe die Ombudsman Association im Hinblick auf die Unabhängigkeit spezifiziert, dass eine „*Ombudsperson* erkenn- und nachweisbar von denjenigen unabhängig sein muss, die sie zu kontrollieren die Befugnis hat“. Europäische Bürger hätten die berechtigte Erwartung, dass eine Ombudsperson unparteiisch und unabhängig ist.[108] Dem wird weder personell mit der von US-Außenminister Kerry vorgenommenen Benennung noch strukturell-

106 EuGH (Fn. 6) Rn. 90.

107 EuGH (Fn. 6) Rn. 74.

108 Schreiben dokumentiert unter http://www.ombudsman.europa.eu/en/resources/otherdocument.faces/en/64157/html.bookmark.

organisatorisch entsprochen.

Die Ombudsperson des Privacy Shield erfüllt aber auch, unabhängig von der verwendeten Begrifflichkeit, nicht die Anforderungen an eine *unabhängige Datenschutzkontrollinstanz* gemäß Art. 8 Abs. 3 EUGRCh. Sie ist als direkte Untergebene und Weisungsabhängige des US-Außenministers das diametrale Gegenteil. Sie ist der US-Regierungspolitik verpflichtet einschließlich der Außenpolitik allgemein und der nachrichtendienstlichen Aufklärung im Interesse der „nationalen Sicherheit" im Speziellen.

Das *Verfahren bei der Ombudsperson* entspricht nicht ansatzweise den rechtsstaatlichen Grundsätzen der Transparenz und Kontrollierbarkeit. Betroffene haben einen Anspruch auf Antwort, die sich nicht darauf beschränken darf, ob ein Verstoß vorliegt oder nicht. Antworten, die dem Betroffenen nicht von der Ombudsperson, sondern von der EU-Beschwerdestelle mitgeteilt werden, sollen gemäß dem Privacy Shield nicht hinterfrag- und überprüfbar sein. Dies gilt selbst für den Fall, dass ein Verstoß festgestellt wurde und eine Abhilfe nötig wäre, worüber auch keine Transparenz hergestellt wird.[109]

4.3.3 Rechtsschutzes

Die dargestellten Rechtsschutzmöglichkeiten garantieren keine umfassende Rechtsprüfung, sondern sind jeweils nur auf spezifische Fälle anwendbar. Eine datenschutzrechtliche Einzelfallprüfung wird in den meisten Fällen nicht gewährleistet. Insbesondere die von der US-Seite hervorgehobenen Verfahren vor dem FISA-Gericht sehen eine Pauschalprüfung vor. Betroffenenbeteiligung und -transparenz stehen unter dem pauschalen Vorbehalt der Nationalen Sicherheit, der vom EuGH verworfen wurde. Die vom EuGH eingeforderten individuellen Grundrechtsgarantien, die klare und präzise Regeln für die Anwendung einer Maßnahme vorsehen und materielle und prozessuale Mindestanforderungen enthalten[110], sind nicht erkennbar.

Der EuGH hat darauf hingewiesen, dass Grundrechtsbeschränkungen sich auf das „absolut Notwendige" zu beschränken haben und Speicherungen nur erlaubt sein können, wenn differenziert, unter Beachtung von Einschränkungen und Ausnahmen, vorgegangen wird.[111] Diesem Erfordernis genügen die aufgeführten Einschränkungen nicht. Schon für den Nachweis der Erforderlichkeit werden keinerlei Ausführungen gemacht, geschweige denn überprüfbare Prozeduren oder sonstige Garantien benannt.

Der EuGH hat darauf hingewiesen, dass das undifferenzierte Erfassen, Speichern und Auswerten von Daten ohne wirksame Rechtsschutzmöglichkeit nicht nur einen Grundrechtsverstoß darstellt, sondern vielmehr den *Wesensgehalt* des durch Art. 7 EUGRCh garantierten Grundrechts auf Achtung des Privatlebens und des in Art. 47 EUGRCh garantierten Grundrechts auf wirksamen gerichtlichen Rechtsschutz verletzt und dass deshalb in einer EU-Kommissionsentscheidung verbindliche und belastbare Feststellungen gemacht werden müssen.[112] Beeinträchtigt werden also nicht nur Randbereiche dieser Grundrechte, sondern jeweils deren Kern. Im Privacy Shield und im Entwurf der

109 Annex 3 § 4.e Omb-Mech.

110 EuGH (Fn. 6) Rn. 90 f.

111 EuGH (Fn. 6) Rn. 93.

112 EuGH (Fn. 6) Rn. 94-96.

Kommissionsentscheidung sind keine Vorkehrungen getroffen, diese Kernbereiche individuell oder auch nur kollektiv zu schützen.

5 Ergebnis und Schlussbemerkung

Der geplante Beschluss der EU-Kommission verstößt gegen europäische Grundrechte und entspricht nicht den Anforderungen der EG-DSRl. Er darf bzw. sollte *nicht gefasst werden*; anderenfalls würde er mit größter Wahrscheinlichkeit vom EuGH aufgehoben werden.

Safe Harbor war im Vergleich zu den anderen Angemessenheitsentscheidungen der EU-Kommission nach Art. 25 Abs. 6 EG-DSRL eine – unzulässige – *Privilegierung des transatlantischen Datenhandels*. Dies wäre auch eine Privacy-Shield-Entscheidung. Unter Berufung auf die das US-Vorbild könnten weitere Drittstaaten eine Anerkennung auf gleichem Niveau fordern, was zu einer massiven Schutzniveauabsenkung beim die EU-Außengrenzen überschreitenden Datenverkehr führen würde. Dies wiederum hätte eine Diskriminierung von Unternehmen im EU-Binnenmarkt zur Folge, deren Datenverarbeitung künftig an der EU-DSGVO gemessen wird. Diese Konsequenz kann nicht im Interesse der EU-Kommission sein.

Aber selbst den *US-Unternehmen* als Datenempfängern wird mit dem Privacy Shield kein Gefallen getan: Angesichts der offensichtlichen Rechtswidrigkeit des Privacy Shields müssten sie zunächst aufwändige Verfahren etablieren, die wegen der absehbaren Aufhebung durch den EuGH nur eine kurze Lebensdauer hätten.

Abkürzungen und Erklärungen

Annex 2 EU-U.S. Privacy Shield Framework Principles issued by the U.S. Department of Commerce

Abs. Absatz

Art. Artikel

DANA DatenschutzNachrichten (Zeitschrift)

DNI Director of National Intelligence (Nationaler Geheimdienstdirektors der USA)

DOC Department of Commerce (US-Wirtschaftsministerium)

DOT Department of Transport (US-Verkehrsministerium)

DPA Data Protection Authority (Datenschutzaufsichtsbehörde)

DVD Deutsche Vereinigung für Datenschutz

EG-DSRl Europäische Datenschutzrichtlinie

EU Europäische Union

EU-DSGVO Europäische Datenschutz-Grundverordnung

EuGH Europäischer Gerichtshof (European Court of Justice)

EUGRCh Europäische Grundrechte-Charta

EU-K-Beschluss-E Beschlussentwurf der EU-Kommission zum EU-US-Datenschutzschild (Commission Implementing Decision)

FBI Federal Bureau of Investigation (US-Bundeskriminalamt)

f/f. (fort)folgende

FISA Foreign Intelligence Surveillance Act (US-Gesetz zur geheimdienstlichen Auslandsüberwachung)

FOIA Freedom of Information Act (US-Gesetz zur Informationsfreiheit)

FTC Federal Trade Commission (US-Verbraucherbehörde)

lit. Buchstabe

Mio. Millionen

NIPF National Intelligence Priorities Framework (Nationale Rahmen für Geheimdienstprioritäten in den USA)

NJW Neue Juristische Wochenschrift (Zeitschrift)

NSA National Security Agency (US-Geheimdienst für Nachrichtenaufklärung)

ODNI Office of the Director of National Intelligence (Büro des Nationalen Geheimdienstdirektors der

USA)

Omb-Mech EU-U.S. Privacy Shield Ombudsperson Mechanism regarding Signals Intelligence (Ombudsperson-Mechanismus)

PPD Presidential Policy Directive (Richtlinie des US-Präsidenten)

RDV Recht der Datenverarbeitung (Zeitschrift)

Rn. Randnummer

S. Seite

U.S. (USA) United States of America

U.S.C. United States Code (US-Gesetz)

vgl. vergleiche