



Brüssel, den 12.7.2016
C(2016) 4176 final

ANNEXES 1 to 7

ANHÄNGE

zum

DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION

**gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die
Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes**

ANHANG I

Schreiben von US-Handelsministerin Penny Pritzker

7. Juli 2016

Frau Věra Jourová
Kommissionsmitglied für Justiz, Verbraucherschutz
und Gleichstellungsfragen
Europäische Kommission
Rue de la Loi/ Weststraat 200
1049 Brüssel
Belgien

Sehr geehrte Frau Jourová,

es ist mir eine große Freude, Ihnen im Namen der Vereinigten Staaten mit diesem Schreiben eine Materialsammlung zum EU-US-Datenschutzschild zukommen zu lassen, die das Ergebnis zweijähriger produktiver Gespräche zwischen den Teams unserer beiden Seiten ist. In Kombination mit anderen öffentlichen Quellen, die der Kommission zur Verfügung stehen, bietet diese Sammlung der Kommission eine fundierte Grundlage, um eine aktuelle Angemessenheitsfeststellung vorzunehmen.¹

Meines Erachtens können wir auf beiden Seiten stolz auf die erzielten Verbesserungen der Regelung sein. Der Datenschutzschild stützt sich auf Grundsätze, über die beiderseits des Atlantiks ein breiter Konsens besteht und denen wir zu mehr Wirksamkeit verholfen haben. Dank unserer Zusammenarbeit bietet sich uns eine wirkliche Gelegenheit, weltweit zur Stärkung des Datenschutzes beizutragen.

Die Materialsammlung zum Datenschutzschild umfasst die Datenschutzgrundsätze sowie ein in Anlage 1 beigefügtes Schreiben der für die Programmverwaltung zuständigen International Trade Administration (ITA) des US-Handelsministeriums, in dem die Verpflichtungen erläutert werden, die unser Ministerium mit Blick auf eine wirksame Umsetzung des Datenschutzschildes eingegangen ist. Die Sammlung umfasst ferner Anlage 2 mit den Zusagen des Ministeriums zum neuen Schiedssystem, das im Rahmen des Datenschutzschildes zur Verfügung steht.

¹ Unter der Voraussetzung, dass der Beschluss über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für Island, Liechtenstein und Norwegen gilt, wird die Materialsammlung zum Datenschutzschild sowohl die Europäische Union als auch diese drei Länder abdecken.

Meine Mitarbeiter sind angewiesen, alle notwendigen Ressourcen unverzüglich und vollständig auf die Realisierung des Datenschutzschildes zu konzentrieren und eine fristgemäße Umsetzung der in Anlage 1 und Anlage 2 aufgeführten Zusagen sicherzustellen.

Ferner beinhaltet die Sammlung zum Datenschutzschild weitere Dokumente anderer US-Behörden, darunter:

- ein Schreiben der Federal Trade Commission (FTC) zur internen Durchsetzung des Datenschutzschildes;
- ein Schreiben des Verkehrsministeriums zur internen Durchsetzung des Datenschutzschildes;
- zwei Schreiben des Amtes des Director of National Intelligence (ODNI) zu den für die nationalen Sicherheitsbehörden in den USA geltenden Garantien und Beschränkungen;
- ein Schreiben des Außenministeriums mit einer Absichtserklärung, in der die Zusage des Außenministeriums zur Einsetzung einer neuen Ombudsstelle für den Datenschutzschild erläutert wird, die für Anfragen zu Vorgängen im Zusammenhang mit der signalerfassenden Aufklärung in den USA zuständig ist und
- ein Schreiben des Justizministeriums zu den Garantien und Beschränkungen der Abfrage von Daten durch die US-Regierung aus Gründen der Strafverfolgung und des öffentlichen Interesses.

Seien Sie versichert, dass die USA diese Zusagen sehr ernst nimmt.

Innerhalb von 30 Tagen nach der endgültigen Annahme der Angemessenheitsfeststellung wird das vollständige Paket zum Datenschutzschild zur Veröffentlichung an das *Bundesregister* übermittelt.

Wir freuen uns auf unsere Zusammenarbeit bei der Umsetzung des Datenschutzschildes und der Einleitung der nächsten Phase in diesem Prozess.

Hochachtungsvoll

Penny Pritzker

Anlage 1: Schreiben des geschäftsführenden Staatssekretärs für internationalen Handel Ken Hyatt

Frau Věra Jourová
Kommissionsmitglied für Justiz, Verbraucherschutz und Gleichstellungsfragen
Europäische Kommission
Rue de la Loi/Westraat 200
1049 Brüssel
Belgien

Sehr geehrte Frau Jourová,

es ist mir eine große Freude, im Namen der International Trade Administration zu erläutern, welche Verbesserungen für den Schutz personenbezogener Daten mit den Rahmegrundsätzen des EU-US-Datenschutzschilds („Datenschutzschild“ oder „Regelung“) verbunden sind und welche Verpflichtungen das Handelsministerium („Ministerium“) eingegangen ist, um eine wirksame Funktionsweise des Datenschutzschilds zu gewährleisten. Mit dem Abschluss dieser historischen Regelung sind wichtige Fortschritte für den Datenschutz und für Unternehmen auf beiden Seiten des Atlantiks verknüpft. EU-Bürgern bietet sie die Gewissheit, dass ihre Daten geschützt werden und sie bei etwaigen Bedenken über Rechtsmittel verfügen. Zudem trägt die damit verbundene Sicherheit zum Wachstum der transatlantischen Wirtschaft bei, weil sie ein Garant dafür ist, dass Tausende von Unternehmen in Europa und den USA auch weiterhin grenzüberschreitend investieren und Geschäfte abschließen können. Das Datenschutzschild ist das Ergebnis unserer zweijährigen umfassenden Bemühungen und Zusammenarbeit mit Ihnen, unseren Kolleginnen und Kollegen in der Europäischen Kommission („Kommission“). Wir freuen uns, unsere Kooperation mit der Kommission im Sinne einer ordnungsgemäßen Funktionsweise des Datenschutzschildes fortzusetzen.

Gemeinsam mit der Kommission haben wir uns darum bemüht, den Datenschutzschild so zu gestalten, dass in den USA niedergelassene Organisationen die Möglichkeit haben, die Angemessenheitsanforderungen an den Datenschutz nach dem EU-Recht einzuhalten. Mit dem neuen Rahmen sind zahlreiche grundlegende Vorteile sowohl für Privatpersonen als auch für Unternehmen verbunden. Erstens beinhaltet es einen umfassenden Katalog von Schutzbestimmungen für die Daten von EU-Bürgern. US-Organisationen sind verpflichtet, an der Entwicklung einer einheitlichen Datenschutzstrategie mitzuwirken, sich öffentlich zur Einhaltung der Grundsätze des Datenschutzschildes zu verpflichten, damit diese Verpflichtung nach US-Recht durchsetzbar wird, die Einhaltung beim Ministerium jährlich neu zu zertifizieren, EU-Bürgern eine kostenfreie unabhängige Streitbeilegung zu ermöglichen und sich der Zuständigkeit der Federal Trade Commission („FTC“), des Verkehrsministeriums (Department of Transportation, „DOT“) oder einer anderen Durchsetzungsstelle zu unterstellen. Zweitens bietet der Datenschutzschild Tausenden von Unternehmen in den USA sowie Tochtergesellschaften europäischer Unternehmen in den USA die Möglichkeit, personenbezogene Daten aus der Europäischen Union zu empfangen, was den Datenfluss im Sinne des transatlantischen Handels erleichtert. Bereits heute weist der transatlantische Geschäftsverkehr weltweit den größten Umfang auf, denn auf ihn entfallen die Hälfte der weltweiten Wirtschaftsleistung und ein Handelsvolumen im Bereich Waren und Dienstleistungen

von nahezu einer Billion Dollar, was Millionen von Arbeitsplätzen diesseits und jenseits des Atlantiks sichert. Unternehmen, die den transatlantischen Datenverkehr nutzen, stammen aus allen Industriezweigen und umfassen sowohl große Vertreter aus der Gruppe der umsatzstärksten Unternehmen (Fortune Global 500) als auch viele kleine und mittlere Unternehmen (KMU). Dank des transatlantischen Datenverkehrs können US-Organisationen Daten verarbeiten, die erforderlich sind, um EU-Bürgern Waren, Dienstleistungen und Beschäftigungsmöglichkeiten anzubieten. Der Datenschutzschild orientiert sich an gemeinsamen Datenschutzgrundsätzen, mit denen die Unterschiede zwischen unseren beiden Rechtssystemen überbrückt werden, und trägt zur Förderung des Handels und der wirtschaftlichen Ziele sowohl in Europa als auch in den USA bei.

Die Entscheidung eines Unternehmens, sich mittels einer Selbstzertifizierung für diese neue Regelung zu registrieren, ist zwar freiwillig, sobald sich ein Unternehmen jedoch öffentlich zur Einhaltung des Datenschutzschildes verpflichtet hat, ist diese Zusage nach US-Recht entweder durch die Federal Trade Commission oder das Verkehrsministerium durchsetzbar, je nachdem welche Behörde die Zuständigkeit für die jeweilige Organisation übernimmt.

Positive Effekte der Grundsätze des Datenschutzschilds

Mit dem Datenschutzschild wird der Datenschutz wie folgt gestärkt:

- Bereitstellung zusätzlicher Informationen für Privatpersonen gemäß dem Grundsatz der Informationspflicht, darunter eine Erklärung über die Beteiligung einer Organisation am Datenschutzschild, ein Hinweis auf die Rechte des Einzelnen auf den Zugang zu personenbezogenen Daten und die Benennung der zuständigen unabhängigen Beschwerdestelle;
- Ausweitung des Schutzes personenbezogener Daten, die von einer dem Datenschutzschild angehörenden Organisation an für die Datenverarbeitung verantwortliche Dritte weitergegeben werden, indem die Parteien zum Abschluss eines Vertrags verpflichtet werden, der vorsieht, dass derartige Daten ausschließlich für begrenzte und genau bezeichnete Zwecke verarbeitet werden können, zu denen die Privatperson ihre Zustimmung erteilt hat, und dass der Datenempfänger dasselbe Schutzniveau gewährleistet, das auch in den Grundsätzen enthalten ist;
- Verbesserung des Schutzes personenbezogener Daten, die von einer dem Datenschutzschild angehörenden Organisation an einen Dritten weitergegeben werden, auch durch die Verpflichtung einer dem Datenschutzschild angehörenden Organisation, angemessene und geeignete Vorkehrungen zu treffen, um sicherzustellen, dass dieser Dritte die personenbezogenen Angaben tatsächlich auf eine Weise verarbeitet, die mit den Verpflichtungen der Organisation im Rahmen der Grundsätze vereinbar ist; nach Kenntnisnahme angemessene und geeignete Maßnahmen ergreift, um eine unrechtmäßige Verarbeitung zu unterbinden und zu beheben und dem Ministerium auf Anfrage eine Zusammenfassung oder eine aussagekräftige Kopie der in ihrem Vertrag mit diesem Dritten enthaltenen einschlägigen Datenschutzbestimmungen zur Verfügung zu stellen;
- Gewährleistung der Verantwortung einer dem Datenschutzschild angehörenden Organisation für die Verarbeitung der personenbezogenen Daten, die ihr auf Grundlage des Datenschutzschildes übermittelt werden und von ihr anschließend an einen Dritten

weitergegeben werden, der in ihrem Auftrag tätig ist, sowie der fortgesetzten Haftung gemäß der Grundsätze für den Fall, dass der Auftragnehmer diese personenbezogenen Informationen auf eine Art und Weise verwendet, die nicht in Einklang mit den Grundsätzen steht, es sei denn, sie kann nachweisen, dass sie für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist;

- Klarstellung, dass dem Datenschutzschild angehörende Organisationen personenbezogene Informationen auf diejenigen Daten beschränken müssen, die für den beabsichtigten Verwendungszweck erheblich sind;
- Anforderung an eine Organisation, jährlich beim Ministerium eine Zertifizierung ihrer Verpflichtung zur Einhaltung der Grundsätze für alle Informationen vorzunehmen, die während ihrer Teilnahme am Datenschutzschild bei ihr eingegangen sind, nachdem sie den Datenschutzschild verlassen hat und sich für die Speicherung dieser Daten entscheidet;
- Erfordernis der Bereitstellung von für den Einzelnen kostenfreien unabhängigen Beschwerdestellen;
- Anforderung an Organisationen und ihre jeweiligen unabhängigen Beschwerdestellen, rasch auf Anfragen und Auskunftsbegehren des Handelsministeriums zu reagieren, die mit dem Datenschutzschild im Zusammenhang stehen;
- Anforderung an Organisationen, auf Beschwerden im Zusammenhang mit der Einhaltung der Grundsätze, die von den Behörden der EU-Mitgliedstaaten an das Ministerium übermittelt wurden, mit der gebotenen Eile zu reagieren und
- Anforderung an eine dem Datenschutzschild angehörende Organisation, jene Teile eines der FTC vorgelegten Compliance- oder Sachstandsberichts, die den Datenschutzschild betreffen, öffentlich zu machen, wenn Anordnungen der FTC oder Gerichtsbeschlüsse wegen Nichteinhaltung gegen sie ergehen.

Verwaltung und Überwachung des Datenschutzschild-Programms durch das Handelsministerium

Das Ministerium bekräftigt seine Zusage, ein amtliches Verzeichnis der Organisationen, die sich gegenüber dem Ministerium selbst zertifiziert und eine Befolgung der Grundsätze zugesichert haben (die „Datenschutzschild-Liste“) zu führen und der Öffentlichkeit zugänglich zu machen. Diese Liste wird durch das Ministerium aktualisiert, indem Organisationen gestrichen werden, die ihre Verpflichtung freiwillig zurückziehen, die jährliche Zertifizierung gemäß den geltenden Verfahren des Ministeriums versäumen oder offensichtlich fortgesetzt die Grundsätze missachten. Außerdem führt es ein amtliches Verzeichnis der Organisationen, die sich zu einem früheren Zeitpunkt gegenüber dem US-Handelsministerium selbst zertifiziert haben, aber von der Datenschutzschild-Liste gestrichen wurden, auch wegen fortgesetzten Verstoßes gegen die Grundsätze, und macht es der Öffentlichkeit zugänglich. Das Ministerium muss die Gründe für den Ausschluss der einzelnen Organisationen benennen.

Darüber hinaus verpflichtet sich das Ministerium, Verbesserungen bei der Verwaltung und Überwachung des Datenschutzschildes vorzunehmen. Dies beinhaltet insbesondere:

Die Bereitstellung zusätzlicher Informationen auf der Website des Datenschutzschildes;

- die Pflege der Datenschutzschild-Liste sowie eines Verzeichnisses der Organisationen, die sich ursprünglich durch Selbstzertifizierung zu den Grundsätzen bekannten, aber keinen Anspruch mehr auf die Vorteile des Datenschutzschildes haben;
- Aufnahme einer Erläuterung an deutlich sichtbarer Stelle, in der klargestellt wird, dass alle von der Datenschutzschild-Liste gestrichenen Organisationen zwar keinen Anspruch mehr auf die Vorteile des Datenschutzschildes haben, jedoch mit Blick auf die personenbezogenen Informationen, die sie während ihrer Beteiligung am Datenschutzschild erhalten haben, weiterhin ihren Verpflichtungen nachkommen müssen, solange sie diese Informationen speichern und
- Erstellung eines Links zur Liste der FTC-Fälle, die mit dem Datenschutzschild in Verbindung stehen, auf der Website der FTC.

Prüfung der Selbstzertifizierungs-Anforderungen

- vor dem Abschluss der Selbstzertifizierung einer Organisation (oder der erneuten jährlichen Zertifizierung) und der Aufnahme einer Organisation in die Datenschutzschild-Liste ist zu prüfen, ob diese Organisation:
 - die erforderlichen Kontaktinformationen bereitgestellt hat;
 - die Tätigkeit der Organisation im Zusammenhang mit personenbezogenen Daten aus der EU beschrieben hat;
 - darauf hingewiesen hat, bei welchen personenbezogenen Informationen die Selbstzertifizierung zur Anwendung kommt;
 - bei Vorhandensein einer öffentlich zugänglichen Website der Organisation die Webadresse angegeben hat, auf der die Datenschutzbestimmungen eingesehen werden können, und die Datenschutzbestimmungen unter der genannten Webadresse zugänglich gemacht oder darauf hingewiesen hat, an welchem Ort die Datenschutzbestimmungen von der Öffentlichkeit eingesehen werden können, sofern eine Organisation keine öffentliche Website unterhält;
 - in die einschlägigen Datenschutzbestimmungen einen Hinweis aufgenommen hat, dass sie sich an die Grundsätze hält, und für den Fall, dass die Datenschutzbestimmungen online verfügbar sind, einen Hyperlink auf die Datenschutzschild-Website des Ministeriums angefügt hat;
 - die gesetzliche Aufsichtsbehörde benannt hat, die über Beschwerden gegen die Organisation wegen unlauteren oder irreführenden Geschäftsgebarens und wegen Verletzung von datenschutzrechtlichen Vorschriften entscheidungsbefugt ist (und in den Grundsätzen oder in einem künftigen Anhang zu den Grundsätzen aufgeführt ist);
 - sofern sie den Bestimmungen gemäß Absatz 1 Buchstabe a und Absatz 3 Buchstabe a des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung entsprechen will, indem sie sich zur Zusammenarbeit mit den entsprechenden Datenschutzbehörden verpflichtet, ihre Absicht erklärt hat, mit den entsprechenden Datenschutzbehörden bei der Behandlung von Beschwerden zusammenzuarbeiten, die unter Berufung auf die Grundsätze des Datenschutzschildes erhoben werden, und

- insbesondere dann Auskünfte zu erteilen, wenn betroffene Personen in der EU eine Beschwerde direkt an ihre nationale Datenschutzbehörde gerichtet haben;
- alle Datenschutzprogramme angegeben hat, an denen die Organisation teilnimmt;
 - die Art der anlassunabhängigen Kontrolle (z. B. intern oder extern) benannt hat, mit der die Einhaltung der Grundsätze gewährleistet werden soll;
 - sowohl in ihrem Antrag auf Selbstzertifizierung als auch in ihren Datenschutzbestimmungen auf die unabhängige Beschwerdestelle verwiesen hat, die für die Prüfung und Lösung von Beschwerden zuständig ist;
 - in ihre entsprechenden Datenschutzbestimmungen, sofern diese online verfügbar sind, einen Hyperlink zur Website oder zum Beschwerdeformular der unabhängigen Beschwerdestelle, die ungeklärte Beschwerden prüft, eingefügt hat und
 - gegebenenfalls auf ihren Wunsch verwiesen hat, dass ihr Personaldaten zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, ihre Bereitschaft erklärt hat, mit den Datenschutzbehörden zusammenzuarbeiten und deren Rat zu befolgen, wenn es um die Lösung von Beschwerden über ihren Umgang mit diesen Daten geht, dem Ministerium eine Kopie ihrer Bestimmungen zum Schutz von Personaldaten übermittelt und mitgeteilt hat, wo die Datenschutzbestimmungen durch die betroffenen Mitarbeiter eingesehen werden können.
- In Zusammenarbeit mit den unabhängigen Beschwerdestellen ist zu prüfen, ob sich die Organisationen tatsächlich für die jeweiligen Mechanismen registriert haben, die in ihren Anträgen auf Selbstzertifizierung angegeben sind, sofern eine solche Registrierung erforderlich ist.

Verstärkte Bemühungen um eine Weiterbehandlung der Fälle von Organisationen, die von der Datenschutzschild-Liste gestrichen wurden

- Hinweis an Organisationen, die wegen „fortgesetzter Missachtung der Grundsätze“ von der Datenschutzschild-Liste gestrichen wurden, dass sie nicht befugt sind, im Rahmen des Datenschutzschildes erhobene Daten zu speichern und
- Übermittlung von Fragebögen an Organisationen, deren Selbstzertifizierung ausläuft oder die freiwillig aus dem Datenschutzschild ausgeschieden sind, um zu prüfen, ob die Organisation die personenbezogenen Daten, die sie während der Beteiligung am Datenschutzschild empfangen hat, zurückgibt, löscht oder auf sie weiterhin die Datenschutzgrundsätze anwendet, und um festzustellen, falls die Organisation die personenbezogenen Daten behält, wer innerhalb der Organisation als ständiger Ansprechpartner für Fragen im Zusammenhang mit dem Datenschutzschild fungieren wird.

Aufdeckung und Handhabung von Fällen, in denen zu Unrecht eine Beteiligung an der Regelung geltend gemacht wird

- Prüfung der Datenschutzbestimmungen von Organisationen, die sich bereits am Datenschutzschild beteiligt haben, jedoch von der Datenschutzschild-Liste gestrichen

wurden, um mögliche Fälle zu ermitteln, in denen falsche Angaben zur Beteiligung am Datenschutzschild gemacht werden.

- Wenn eine Organisation: a) den Datenschutzschild verlassen hat, b) keinen Antrag auf erneute Zertifizierung ihres Beitritts zu den Grundsätzen stellt oder c) insbesondere aufgrund „fortgesetzter Missachtung der Grundsätze“ von der Beteiligung am Datenschutzschild ausgeschlossen wird, ist von Amts wegen kontinuierlich sicherzustellen, dass aus den relevanten veröffentlichten Datenschutzbestimmungen der Organisation alle Bezugnahmen auf den Datenschutzschild entfernt wurden, die auf eine weitere aktive Beteiligung der Organisation oder auf einen Anspruch auf die damit verbundenen Vorteile hindeuten. Stellt das Ministerium fest, dass diese Bezugnahmen nicht entfernt wurden, weist es die Organisation eindringlich darauf hin, dass sie die Angelegenheit einer anderen zuständigen Behörde zuzuleiten gedenkt, damit diese gegebenenfalls tätig wird, sofern die Angaben zur Beteiligung am Datenschutzschild nicht entfernt werden. Für den Fall, dass die Organisation die Bezugnahme weder entfernt noch ihren Beitritt zu den Grundsätzen des Datenschutzschildes erklärt, wird das Ministerium die Angelegenheit von Amts wegen an die FTC, das Verkehrsministerium oder eine andere zuständige Behörde verweisen oder gegebenenfalls Maßnahmen zur Einhaltung der Bestimmungen des Gütesiegels für den Datenschutzschild ergreifen.
- Einleitung weiterer Maßnahmen zur Ermittlung falscher Angaben über eine Beteiligung am Datenschutzschild oder einer missbräuchlichen Verwendung des entsprechenden Gütesiegels, auch im Rahmen von Internetrecherchen, um festzustellen, ob Abbildungen des Gütesiegels für den Datenschutzschild verwendet werden und Bezugnahmen auf den Datenschutzschild in den Datenschutzbestimmungen einer Organisation enthalten sind;
- unverzügliche Klärung aller Angelegenheiten, die bei einer Prüfung falscher Angaben zur Beteiligung am Datenschutzschild oder der missbräuchlichen Verwendung des entsprechenden Gütesiegels von Amts wegen ermittelt wurden, was auch eine im Vorangehenden beschriebene Warnung an Organisationen beinhaltet, die falsche Angaben zu ihrer Beteiligung am Datenschutzschild machen;
- Einleitung weiterer geeigneter Abhilfemaßnahmen, darunter die Beschreitung aller für das Ministerium zulässigen Rechtswege und Verweisung der Angelegenheit an die FTC, das Verkehrsministerium oder eine andere zuständige Durchsetzungsstelle und
- unverzügliche Prüfung und Behandlung von bei uns eingehenden Beschwerden über falsche Angaben zur Beteiligung.

Das Ministerium prüft die Datenschutzbestimmungen von Organisationen, um falsche Angaben zur Beteiligung am Datenschutzschild wirksamer aufdecken und dagegen vorgehen zu können. Diese Prüfung betrifft insbesondere die Datenschutzbestimmungen von Organisationen, deren Selbstzertifizierung ausgelaufen ist, weil sie es versäumt haben, ihren Beitritt zu den Grundsätzen erneut zertifizieren zu lassen. Mit Hilfe dieser Prüfungen will das Ministerium feststellen, ob die Organisationen aus ihren relevanten veröffentlichten Datenschutzbestimmungen alle Bezugnahmen entfernt haben, die auf ihre weitere aktive Beteiligung am Datenschutzschild hindeuten. Im Rahmen der beschriebenen Prüfverfahren sollen Organisationen ermittelt werden, die derartige Bezugnahmen nicht entfernt haben, und anschließend in einem Schreiben der Rechtsabteilung des Ministeriums über mögliche Durchsetzungsmaßnahmen für den Fall unterrichtet werden, dass sie diese Bezugnahmen nicht streichen. Anhand von Folgemaßnahmen stellt das Ministerium sicher, dass die Organisationen

die unzulässigen Bezugnahmen entweder entfernen oder ihren Beitritt zu den Grundsätzen erneut zertifizieren. Darüber hinaus ist das Ministerium auch darum bemüht, falsche Angaben zur Beteiligung am Datenschutzschild von Organisationen aufzudecken, die niemals am Datenschutzschild-Programm teilgenommen haben, und vergleichbare Abhilfemaßnahmen gegen diese Organisationen einzuleiten.

Regelmäßige Durchführung der von Amts wegen vorgenommenen Kontrollen der Einhaltung und Programmbewertungen

- kontinuierliche Überwachung der effektiven Einhaltung, auch durch die Zusendung detaillierter Fragebögen an teilnehmende Organisationen, um Problemfelder zu ermitteln, in denen es möglicherweise weiterer Folgemaßnahmen bedarf. Die genannten Einhaltungskontrollen sind insbesondere dann durchzuführen, wenn: a) dem Ministerium ernst gemeinte Beschwerden über die Einhaltung der Grundsätze durch eine Organisation zugegangen sind, b) eine Organisation keine zufriedenstellende Antwort auf eine mit dem Datenschutzschild verbundene Anfrage des Ministeriums übermittelt oder c) deutliche Anhaltspunkte darauf schließen lassen, dass eine Organisation ihren Zusagen im Zusammenhang mit dem Datenschutzschild nicht nachkommt. Das Ministerium stimmt diese Einhaltungskontrollen bei Bedarf mit den zuständigen Datenschutzbehörden ab, und
- bewertet regelmäßig die Verwaltung und Überwachung des Datenschutzschild-Programms, um sicherzustellen, dass die Kontrollbemühungen auch für neue Problemfelder geeignet sind.

Das Ministerium hat die Mittel für die Verwaltung und Überwachung des Datenschutzschild-Programms aufgestockt und darüber hinaus die Zahl der für die Verwaltung und Überwachung zuständigen Mitarbeiter verdoppelt. Wir werden auch weiterhin angemessene Mittel für derartige Maßnahmen bereitstellen, um eine effektive Überwachung und Verwaltung des Programms zu gewährleisten.

Überarbeitung der Website des Datenschutzschilds mit Blick auf ausgewählte Zielgruppen

Das Ministerium überarbeitet die Website des Datenschutzschilds, um sie auf drei Zielgruppen auszurichten: EU-Bürger, EU-Unternehmen und US-Unternehmen. Durch die Aufnahme von speziell auf EU-Bürger und EU-Unternehmen zugeschnittenen Materialien kann die Transparenz auf vielfältige Weise gesteigert werden. Für EU-Bürger werden folgende Punkte klar erläutert: 1) die Rechte, die für EU-Bürger mit dem Datenschutzschild verbunden sind, 2) die Rechtsbehelfe, die EU-Bürgern zur Verfügung stehen, wenn sie der Ansicht sind, dass eine Organisation ihrer Verpflichtung zur Einhaltung der Grundsätze nicht nachkommt und 3) die Verfügbarkeit von Informationen zur Selbstzertifizierung einer Organisation im Rahmen des Datenschutzschilds. Für EU-Unternehmen werden folgende Kontrollen erleichtert: 1) ob eine Organisation Anspruch auf die Vorteile aus dem Datenschutzschild hat, 2) welche Informationen von der Selbstzertifizierung einer Organisation im Rahmen des Datenschutzschilds abgedeckt werden, 3) welche Datenschutzbestimmungen auf diese Informationen zur Anwendung kommen und 4) anhand welcher Methoden eine Organisation die Einhaltung der Grundsätze prüft.

Ausbau der Zusammenarbeit mit den Datenschutzbehörden

Für den Ausbau der Kooperationsmöglichkeiten mit den Datenschutzbehörden richtet das Ministerium eine spezielle Kontaktstelle ein, die als Bindeglied zu den Datenschutzbehörden fungiert. Sollte eine Datenschutzbehörde, auch aufgrund einer Beschwerde durch einen EU-Bürger, den Verdacht hegen, dass eine Organisation die Grundsätze nicht einhält, kann sie sich an die spezielle Kontaktstelle im Ministerium wenden, um eine weitere Kontrolle der Organisation zu veranlassen. An die Kontaktstelle können auch Fälle überwiesen werden, in denen Organisationen falsche Angaben zu ihrer Beteiligung am Datenschutzschild machen, obgleich sie ihren Beitritt zu den Grundsätzen niemals selbst bescheinigt haben. Die Kontaktstelle unterstützt Datenschutzbehörden bei der Erfassung von Informationen zur Selbstzertifizierung oder zum bisherigen Beitritt einer Organisation zum Programm und beantwortet Anfragen der Datenschutzbehörden zur Umsetzung der spezifischen Datenschutzschild-Anforderungen. Darüber hinaus stellt das Ministerium den Datenschutzbehörden Material zum Datenschutzschild zur Verfügung, das sie auf ihre eigenen Websites stellen können, um für mehr Transparenz zugunsten von EU-Bürgern und EU-Unternehmen zu sorgen. Ein stärkeres Bewusstsein für den Datenschutzschild und die damit verbundenen Rechte und Pflichten kann die Erkennung von Problemen unmittelbar nach ihrem Auftreten begünstigen und die Einleitung geeigneter Abhilfemaßnahmen begünstigen.

Erleichterung der Lösungsfindung bei Beschwerden wegen Verletzung der Datenschutzvorschriften

An das Ministerium gerichtete Beschwerden einer Datenschutzbehörde über die Nichteinhaltung der Grundsätze durch eine dem Datenschutzschild angehörende Organisation gehen dem Ministerium über die spezielle Kontaktstelle zu. Nach Eingang ist das Ministerium nach besten Kräften um eine Klärung der Beschwerde mit der dem Datenschutzschild angehörenden Organisation bemüht. Innerhalb von 90 Tagen nach Eingang der Beschwerde unterrichtet das Ministerium die Datenschutzbehörde über den aktuellen Sachstand. Um die Einreichung derartiger Beschwerden zu erleichtern, erstellt das Ministerium ein Standardformular für Datenschutzbehörden, das bei der speziellen Kontaktstelle im Ministerium eingereicht werden kann. In der speziellen Kontaktstelle werden alle von den Datenschutzbehörden an das Ministerium übermittelten Fälle erfasst, und das Ministerium erstellt bei der jährlichen Überprüfung einen Bericht, der in aggregierter Form die im Laufe des Jahres bei ihm eingegangenen Beschwerden enthält.

Annahme von Schiedsverfahren und Auswahl von Schiedsrichtern in Abstimmung mit der Kommission

Das Ministerium kommt seinen Zusagen gemäß Anhang I nach und macht die Verfahren im Anschluss an eine Einigung bekannt.

Gemeinsame Überprüfung der Funktionsweise des Datenschutzschilds

Das Handelsministerium, die FTC und andere Stellen werden bei Bedarf jährliche Sitzungen mit der Kommission, betroffenen Datenschutzbehörden und gegebenenfalls auch Vertretern der Artikel-29-Datenschutzgruppe organisieren, auf denen das Ministerium über den aktuellen Sachstand mit Blick auf das Datenschutzschild-Programm informiert. Bei den

jährlichen Sitzungen werden aktuelle Probleme im Zusammenhang mit der Funktionsweise, Durchführung, Überwachung und Durchsetzung des Datenschutzschilds, darunter die von den Datenschutzbehörden an das Ministerium übermittelten Fälle, die Ergebnisse der von Amts wegen durchgeführten Kontrollen einer Einhaltung der Grundsätze sowie möglicherweise relevante Gesetzesänderungen, erörtert. Die erste jährliche Überprüfung und gegebenenfalls anschließende Überprüfungen werden einen Dialog zu weiteren Themen wie z. B. automatische Entscheidungsprozesse, einschließlich eines Meinungs austauschs über Gemeinsamkeiten und Unterschiede der diesbezüglichen Konzepte der EU und der USA beinhalten.

Aktualisierung von Gesetzen

Das Ministerium wird die Kommission in angemessener Weise über wesentliche Änderungen des Rechts der Vereinigten Staaten unterrichten, wenn sie für den Datenschutzschild relevant sind und den Datenschutz sowie die Beschränkungen und Schutzvorkehrungen für den Zugriff staatlicher Behörden auf personengebundene Daten und deren anschließende Verwendung betreffen.

Ausnahmen aus Gründen der nationalen Sicherheit

Der Rechtsbeauftragte im Amt des Directors of National Intelligence, Robert Litt, hat Justin Antonipillai und Ted Dean im Handelsministerium zwei Schreiben zu den Einschränkungen bei der Einhaltung der Grundsätze des Datenschutzschildes aus Gründen der nationalen Sicherheit übermittelt, die an Sie weitergeleitet wurden. In diesen Schreiben werden unter anderem die Strategien, Garantien und Beschränkungen erläutert, die für signalerfassende Aufklärung in den USA gelten. Darüber hinaus enthalten diese Schreiben Erläuterungen zur Transparenz, die von den Nachrichtendiensten in dieser Hinsicht geschaffen wurde. Die Kommission kann bei ihrer Überprüfung der Datenschutzschild-Regelung aus den in diesen Schreiben enthaltenen Informationen mit Sicherheit schließen, dass der Datenschutzschild in Übereinstimmung mit den darin aufgeführten Grundsätzen ordnungsgemäß funktioniert. Wir gehen davon aus, dass Sie bei der jährlichen Überprüfung der Datenschutzschild-Regelung künftig auf von den Nachrichtendiensten öffentlich gemachte Informationen sowie auf weitere Informationen zurückgreifen werden.

Ausgehend von den Grundsätzen des Datenschutzschilds und den Begleitschreiben und -materialien, einschließlich der Zusagen des Ministeriums zur Verwaltung und Überwachung der Grundsätze des Datenschutzschilds, rechnen wir damit, dass die Kommission die EU-US-Datenschutzschild-Regelung als ausreichend erachtet, um einen Schutz im Sinne der EU-Rechtsvorschriften zu gewährleisten, und dass Daten weiterhin an Organisationen übermittelt werden, die sich am Datenschutzschild beteiligen.

Hochachtungsvoll

Ken Hyatt

Anlage 2: Schiedsmodell

ANLAGE I

In dieser Anlage I sind die Bedingungen aufgeführt, unter denen dem Datenschutz angehörende Organisationen zur Behandlung von Ansprüchen im Schiedsverfahren nach dem Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung verpflichtet sind. Die im Folgenden beschriebene Möglichkeit des verbindlichen Schiedsverfahrens bezieht sich auf bestimmte „Restansprüche“ in Bezug auf Daten, die unter den EU-US-Datenschutzschild fallen. Damit soll Privatpersonen ein zeitnaher, unabhängiger und fairer Mechanismus bereitgestellt werden, der sich mit geltend gemachten Verstößen gegen die Grundsätze befasst, die nicht von einem der gegebenenfalls in Anspruch genommenen anderen Mechanismen des Datenschutzschildes geklärt werden konnten.

A. Anwendungsbereich

Mit dem Schiedsverfahren können Privatpersonen bei Restansprüchen feststellen lassen, ob eine dem Datenschutzschild angehörende Organisation ihre Pflichten im Rahmen der Grundsätze gegenüber der betreffenden Person verletzt hat und ob diese Verletzung vollständig oder teilweise ungeahndet bleibt. Diese Option steht nur für diese Zwecke zur Verfügung, nicht jedoch beispielsweise bei den geregelten Abweichungen von den Grundsätzen¹ oder im Hinblick auf eine Behauptung zur Angemessenheit des Datenschutzschildes.

B. Verfügbare Abhilfemaßnahmen

Im Rahmen dieses Schiedsverfahrens ist das Datenschutzschild-Panel (bestehend aus einem oder drei von den Parteien ausgewählten Schiedsrichtern) befugt, einzelfallabhängige nichtmonetäre billigkeitsrechtliche Ansprüche (wie z. B. Zugang, Korrektur, Löschung oder Rückgabe der betreffenden Daten der Person) anzuerkennen, um die Verstöße gegen die Grundsätze abzustellen. Dieses sind die einzigen Befugnisse des Schiedsforums in Bezug auf Abhilfemaßnahmen. Bei der Prüfung von Abhilfemaßnahmen muss das Schiedsforum andere bereits von anderen Mechanismen im Rahmen des Datenschutzschildes verhängte Abhilfemaßnahmen berücksichtigen. Schadenersatz, Kosten, Gebühren oder andere derartige Maßnahmen sind nicht verfügbar. Jede Partei muss selbst für die anfallenden Anwaltsgebühren aufkommen.

C. Voraussetzungen für das Schiedsverfahren

Wer das Schiedsverfahren in Anspruch nehmen möchte, muss vor der Einleitung einer Schiedsklage 1) den behaupteten Verstoß direkt bei der Organisation geltend machen und der Organisation Gelegenheit geben, die Angelegenheit innerhalb der in Abschnitt III.11 d)i) der Grundsätze aufgeführten Frist zu klären, 2) das kostenlose unabhängige Beschwerdeverfahren im Rahmen der Grundsätze in Anspruch nehmen und 3) die Angelegenheit kostenlos über seine zuständige Datenschutzbehörde dem Handelsministerium zuleiten und dem Handelsministerium

¹ Abschnitt I.5 der Grundsätze.

die Gelegenheit geben, die Angelegenheit nach Möglichkeit innerhalb der im Schreiben der International Trade Administration des Handelsministeriums gesetzten Frist zu klären.

Das Schiedsverfahren kann nicht in Anspruch genommen werden, wenn der von der Person geltend gemachte Verstoß 1) bereits Gegenstand eines verbindlichen Schiedsverfahrens war, 2) Gegenstand eines rechtskräftigen Urteils in einem Gerichtsverfahren mit der Person als Prozesspartei war oder 3) von den Parteien bereits geregelt wurde. Darüber hinaus kann das Schiedsverfahren nicht in Anspruch genommen werden, wenn eine EU-Datenschutzbehörde 1) gemäß Abschnitt III.5 oder III.9 der Grundsätze zuständig ist oder 2) befugt ist, den geltend gemachten Verstoß direkt mit der Organisation zu klären. Die Befugnis einer Datenschutzbehörde, den gleichen Anspruch gegen einen für die Verarbeitung Verantwortlichen in der EU geltend zu machen, schließt die Inanspruchnahme des Schiedsverfahrens gegen eine nicht an die Befugnis der Datenschutzbehörde gebundene andere rechtliche Einheit allein nicht aus.

D. Verbindlichkeit von Schiedssprüchen

Die Entscheidung einer Einzelperson, dieses verbindliche Schiedsverfahren in Anspruch zu nehmen, ist vollkommen freiwillig. Die Schiedssprüche sind für alle beteiligten Parteien verbindlich. Mit der Inanspruchnahme verzichtet die betreffende Person auf die Möglichkeit, ein anderes Forum mit der Klärung des geltend gemachten Verstoßes zu befassen; wenn jedoch diesem Verstoß mit der Anerkennung nichtmonetärer Ansprüche nicht vollständig abgeholfen wird, kann die betreffende Person dennoch Schadensersatzansprüche vor Gericht geltend machen.

E. Überprüfung und Durchsetzung

Privatpersonen und dem Datenschutzschild angehörende Organisationen können eine gerichtliche Überprüfung und Durchsetzung der Schiedsentscheidungen nach US-Recht gemäß Federal Arbitration Act beantragen.² Derartige Fälle müssen bei dem Bundesbezirksgericht

² In Kapitel 2 des Federal Arbitration Act („FAA“) heißt es: „Eine Schiedsvereinbarung oder ein Schiedsspruch aus einem vertraglichen oder nicht vertraglichen Rechtsverhältnis, das als kommerziell gilt, einschließlich einer Transaktion, eines Vertrages oder einer Vereinbarung nach [§ 2 des FAA], fällt unter das Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche vom 10. Juni 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 („New Yorker Übereinkommen“).“ 9 U.S.C. § 202. Weiter ist im FAA festgelegt: „Eine Schiedsvereinbarung oder ein Schiedsspruch aus einem derartigen Verhältnis, das ausschließlich zwischen Bürgern der Vereinigten Staaten besteht, fällt nur dann unter das [New Yorker] Übereinkommen, wenn dieses Verhältnis im Ausland befindliche Immobilien umfasst, eine Leistung oder Rechtsdurchsetzung im Ausland anstrebt oder in einer anderweitigen hinreichenden Beziehung zu einem oder mehreren anderen Staaten steht.“ Ebenda. Nach Kapitel 2 kann „jede Partei des Schiedsverfahrens einen Antrag bei einem nach diesem Kapitel zuständigen Gericht auf eine Anordnung zur Bestätigung des Schiedspruchs gegen eine andere Partei des Schiedsverfahrens stellen. Das Gericht bestätigt den Schiedsspruch, sofern es keinen der Gründe für eine Verweigerung oder einen Aufschub der Anerkennung oder Durchsetzung des Schiedspruchs gemäß dem besagten [New Yorker] Übereinkommen findet.“ Ebenda § 207. Weiter heißt es in Kapitel 2: „Die Bezirksgerichte der Vereinigten Staaten ... haben ungeachtet des Streitwerts die ursprüngliche Zuständigkeit für ... eine Klage oder ein Verfahren [im Rahmen des New Yorker Übereinkommens]. Ebenda § 203.

eingereicht werden, dessen territoriale Zuständigkeit sich auf den Hauptgeschäftsort der dem Datenschuttschild angehörenden Organisation erstreckt.

Mit diesem Schiedsverfahren sollen individuelle Streitigkeiten geklärt werden, und die Schiedsentscheidungen sollen nicht als zur Nachahmung empfohlener oder verbindlicher Präzedenzfall bei Angelegenheiten anderer Parteien dienen, einschließlich bei künftigen Schiedsverfahren oder an Gerichten der EU oder der USA oder in Verfahren der FTC.

F. Das Schiedsforum

Die Parteien wählen die Schiedsrichter aus dem im Folgenden erörterten Verzeichnis der Schiedsrichter aus.

Nach geltendem Recht erstellen das US-Handelsministerium und die Europäische Kommission ein Verzeichnis mit mindestens 20 Schiedsrichtern, die aufgrund ihrer Unabhängigkeit, Integrität und Sachkenntnis ausgewählt werden. Dafür gilt Folgendes:

Die Schiedsrichter

- 1) verbleiben für einen Zeitraum von 3 Jahren in dem Verzeichnis, sofern keine außergewöhnlichen Umstände oder wichtigen Gründe vorliegen; dieser Zeitraum kann um weitere drei Jahre verlängert werden;
- 2) sind gegenüber einer der Parteien oder einer dem Datenschuttschild angehörenden Organisation bzw. gegenüber den USA, der EU oder einem EU-Mitgliedstaat oder einer anderen Regierungsbehörde, öffentlichen Behörde oder Strafverfolgungsbehörde weder weisungsgebunden noch anderweitig verpflichtet;
- 3) müssen als Rechtsanwalt in den USA zugelassen und im US-Privatrecht bewandert sein und Sachkenntnis im EU-Datenschutzrecht aufweisen.

Außerdem heißt es in Kapitel 2: „Kapitel 1 gilt für Klagen und Verfahren nach diesem Kapitel, soweit jenes Kapitel nicht mit diesem Kapitel oder dem [New Yorker] Übereinkommen, wie von den Vereinigten Staaten ratifiziert, kollidiert.“ Ebenda § 208. In Kapitel 1 heißt es wiederum: „Eine schriftliche Bestimmung in einem Vertrag über eine geschäftliche Transaktion, wonach ein Streit aufgrund dieses Vertrages oder dieser Transaktion oder die Weigerung, diesen bzw. diese ganz oder teilweise zu erfüllen, im Schiedsverfahren beizulegen ist, oder eine schriftliche Vereinbarung, wonach ein bestehender Streit aufgrund dieses Vertrages, dieser Transaktion oder dieser Weigerung an ein Schiedsgericht zu verweisen ist, ist gültig, unwiderruflich und vollstreckbar, sofern nicht Gründe nach Recht oder Billigkeit für den Rücktritt von einem Vertrag vorliegen.“ Ebenda § 2. Weiter heißt es in Kapitel 1: „Jede Partei im Schiedsverfahren kann bei einem angegebenen Gericht eine Anordnung zur Bestätigung des Schiedsspruchs beantragen, woraufhin das Gericht eine derartige Anordnung erlassen muss, sofern der Schiedsspruch nicht gemäß § 10 und 11 des [FAA] aufgegeben, geändert oder korrigiert wird.“ Ebenda § 9.

G. Schiedsverfahren

Im Einklang mit dem geltenden Recht vereinbaren das Handelsministerium und die Europäische Kommission innerhalb von 6 Monaten nach Annahme des Angemessenheitsbeschlusses die Übernahme einer Reihe von bestehenden, etablierten US-Schiedsverfahren (wie z. B. AAA oder JAMS) zur Regelung des Verfahrens vor dem Datenschutzschild-Panel, wobei die folgenden Aspekte zugrunde gelegt werden:

1. Eine Person kann vorbehaltlich der vorstehend aufgeführten Voraussetzungen ein verbindliches Schiedsverfahren einleiten, indem sie der Organisation eine Mitteilung zukommen lässt. Die Mitteilung enthält eine Zusammenfassung der gemäß Abschnitt C unternommenen Schritte zur Klärung einer Beschwerde, eine Beschreibung des geltend gemachten Verstoßes und, nach eigener Wahl, Belegunterlagen und -materialien und/oder eine Rechtserörterung mit Bezug zum geltend gemachten Verstoß.
2. Es werden Verfahren entwickelt, die sicherstellen, dass für einen geltend gemachten Verstoß nicht mehrere Verfahren geführt oder mehrere Abhilfemaßnahmen getroffen werden.
3. Die FTC kann parallel zum Schiedsverfahren tätig werden.
4. An den Schiedsverfahren dürfen keine Vertreter der USA, der EU oder eines EU-Mitgliedstaats oder einer anderen Regierungsbehörde, staatlichen Behörde oder Strafverfolgungsbehörde teilnehmen, wobei auf Antrag einer Person aus der EU die EU-Datenschutzbehörden Hilfe bei der Erstellung ausschließlich der Mitteilung leisten können, jedoch keinen Zugang zu Offenlegungen und anderen Materialien in Bezug auf diese Schiedsverfahren haben dürfen.
5. Ort des Schiedsverfahrens sind die Vereinigten Staaten, und die betroffene Person kann sich für eine Teilnahme per Video oder Telefonkonferenz entscheiden, die für sie mit keinen Kosten verbunden ist. Eine persönliche Anwesenheit ist nicht erforderlich.
6. Verfahrenssprache ist Englisch, wenn von den Parteien nicht anders vereinbart. Auf einen begründeten Antrag hin und unter Berücksichtigung dessen, ob sich die Person von einem Anwalt vertreten lässt, werden Dolmetscher für die mündliche Verhandlung sowie Übersetzungen der Verfahrensunterlagen bereitgestellt, ohne dass sich daraus Kosten für die Person ergeben, es sei denn, das Panel gelangt in einem konkreten Fall zu dem Schluss, dass eine Kostenübernahme nicht gerechtfertigt oder unverhältnismäßig wäre.
7. Den Schiedsrichtern vorgelegte Unterlagen werden vertraulich behandelt und nur in Verbindung mit dem Schiedsverfahren genutzt.
8. Wenn erforderlich, kann eine die Person betreffende Offenlegung zugelassen werden, wobei diese Offenlegung von den Parteien vertraulich behandelt und nur in Verbindung mit dem Schiedsverfahren genutzt wird.
9. Schiedsverfahren sollen innerhalb von 90 Tagen nach Zustellung der Mitteilung an die betreffende Organisation abgeschlossen werden, sofern von den Parteien nicht anderweitig vereinbart.

H. Kosten

Die Schiedsrichter sollen angemessene Maßnahmen zur Minimierung der Kosten oder Gebühren der Schiedsverfahren ergreifen.

Nach Maßgabe des geltenden Rechts wird das Handelsministerium in Abstimmung mit der Europäischen Kommission die Einrichtung eines Fonds ermöglichen, in den die dem Datenschutzschild angehörenden Organisationen einen Jahresbeitrag einzahlen, der sich zum Teil nach der Größe der Organisation richtet und die Schiedskosten, einschließlich Schiedsrichtergebühren, bis zu einer Obergrenze deckt. Der Fonds wird von einem Dritten verwaltet, der regelmäßig über die Tätigkeit des Fonds Bericht erstattet. Bei der jährlichen Überprüfung werden das Handelsministerium und die Europäische Kommission die Tätigkeit des Fonds, einschließlich der Notwendigkeit einer Anpassung des Beitrags oder der Obergrenze, kontrollieren und unter anderem die Anzahl der Schiedsverfahren sowie deren Kosten und Dauer prüfen, und zwar im gegenseitigen Einvernehmen, dass den am Datenschutzschild teilnehmenden Organisationen keine übermäßige finanzielle Belastung auferlegt wird. Rechtsanwaltsgebühren sind von dieser Bestimmung oder einem anderen Fonds im Rahmen dieser Bestimmung nicht erfasst.

ANHANG II
GRUNDSÄTZE DES EU-US-DATENSCHUTZSCHILDS
VORGELEGT VOM AMERIKANISCHEN HANDELSMINISTERIUM

I. ÜBERBLICK

1. Die Vereinigten Staaten und die Europäische Union haben beide das Ziel, den Datenschutz zu verstärken, wobei die Vereinigten Staaten jedoch einen anderen Ansatz verfolgen als die Europäische Gemeinschaft. Die USA verfolgen einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und freiwilliger Selbstkontrolle basiert. Angesichts dieser Unterschiede und um Organisationen in den Vereinigten Staaten einen zuverlässigen Mechanismus für die Übermittlung personenbezogener Daten aus der Europäischen Union in die Vereinigten Staaten bereitzustellen und dabei gleichzeitig sicherzustellen, dass betroffene EU-Bürger weiter in den Genuss wirksamer Garantien und eines wirksamen Schutzes bei der Verarbeitung ihrer personenbezogenen Daten nach deren Übermittlung in Nicht-EU-Länder kommen, legt das Handelsministerium im Rahmen seiner gesetzlichen Befugnis, internationalen Handel zu pflegen, zu fördern und zu entwickeln (15 U.S.C. § 1512), diese Grundsätze des Datenschutzschildes, einschließlich der Zusatzgrundsätze (im Folgenden insgesamt „Grundsätze“) vor. Die Grundsätze wurden in Absprache mit der Europäischen Kommission sowie mit der Industrie und anderen Interessenträgern entwickelt, um den Handel zwischen der Europäischen Union und den Vereinigten Staaten zu erleichtern. Sie sind ausschließlich für den Gebrauch durch Organisationen in den Vereinigten Staaten bestimmt, die personenbezogene Daten aus der Europäischen Union erhalten, um sich für den Datenschutzschild zu qualifizieren und so vom Angemessenheitsbeschluss der Europäischen Kommission zu profitieren.¹ Die Grundsätze berühren nicht die Anwendung nationaler Rechtsvorschriften über die Verarbeitung personenbezogener Daten in den Mitgliedstaaten, mit denen die Richtlinie 95/46/EG (im Folgenden „Richtlinie“) umgesetzt wird. Ebenso wenig schränken die Prinzipien ansonsten nach US-Recht geltende Datenschutzverpflichtungen ein.
2. Um sich auf den Datenschutzschild zur Übermittlung personenbezogener Daten aus der EU stützen zu können, muss eine Organisation gegenüber dem Handelsministerium (oder einer von ihm benannten Stelle) (im Folgenden „Ministerium“) durch Selbstzertifizierung erklären, dass sie sich an die Grundsätze hält. Obwohl Entscheidungen von Organisationen, so dem Datenschutzschild beizutreten, vollkommen freiwillig sind, ist die wirksame Einhaltung der Grundsätze obligatorisch: Organisationen, die dem Ministerium eine Selbstzertifizierung bekanntgeben und öffentlich erklären, dass sie die

¹ Unter der Voraussetzung, dass der Beschluss über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für Island, Liechtenstein und Norwegen gilt, wird die Materialsammlung zum Datenschutzschild sowohl die Europäische Union als auch diese drei Länder abdecken. Demzufolge sind bei Bezugnahmen auf die EU und ihre Mitgliedstaaten auch Island, Liechtenstein und Norwegen eingeschlossen.

Grundsätze befolgen, müssen diese vollständig einhalten. Um dem Datenschutzschild beizutreten, muss eine Organisation a) den Untersuchungs- und Durchsetzungsbefugnissen der Federal Trade Commission (im Folgenden „FTC“), des Verkehrsministeriums oder anderer gesetzlicher Organe, die die Einhaltung der Grundsätze effektiv gewährleisten, unterliegen (*andere von der EU anerkannte Behörden der Vereinigten Staaten können künftig als Anhang beigefügt werden*), b) öffentlich seine Bereitschaft erklären, die Grundsätze einzuhalten, c) ihre Datenschutzbestimmungen im Einklang mit diesen Grundsätzen offenlegen und d) diese vollständig umsetzen. Ein Verstoß der Organisation gegen diese Grundsätze ist gemäß Abschnitt 5 des Federal Trade Commission Act zur Verhinderung unlauterer und irreführender Praktiken, die im Handel erfolgen oder den Handel beeinträchtigen (15 U.S.C. § 45(a)), oder ähnlichen Rechtsvorschriften verfolgbar.

3. Das Handelsministerium wird eine verbindliche Liste der US-Organisationen führen und der Öffentlichkeit zugänglich machen, die sich gegenüber dem Ministerium selbst zertifiziert und zugesichert haben, die Grundsätze zu befolgen (im Folgenden „Datenschutzschild-Liste“). Das Ministerium wird eine Organisation von der Datenschutzschild-Liste streichen, wenn sie freiwillig aus dem Datenschutzschild ausscheidet oder wenn sie es versäumt, ihre jährlich fällige Zertifizierung gegenüber dem Ministerium zu erneuern. Die Streichung einer Organisation von der Datenschutz-Liste bedeutet, dass sie nicht mehr in den Genuss des Angemessenheitsbeschlusses der Europäischen Kommission zum Empfang personenbezogener Daten aus der EU kommen kann. Die Organisation muss die Grundsätze für personenbezogene Daten, die sie während der Zeit ihrer Teilnahme am Datenschutzschild erhalten hat, weiter einhalten, solange sie diese Daten speichert, und gegenüber dem Ministerium jährlich die Einhaltung zusichern; ansonsten muss die Organisation die Daten zurückgeben oder löschen oder für sie einen „angemessenen“ Schutz bieten. Das Ministerium wird zudem jene Organisationen von der Datenschutzschild-Liste streichen, die die Grundsätze fortgesetzt missachten; diese Organisationen verlieren die mit dem Datenschutzschild verbundenen Vorteile und müssen die personenbezogenen Daten zurückgeben oder löschen, die sie im Rahmen des Datenschutzschilds erhalten haben.
4. Das Ministerium wird ferner ein verbindliches Verzeichnis der US-Organisationen führen und der Öffentlichkeit zugänglich machen, die ehemals eine Selbstzertifizierung gegenüber dem Ministerium abgegeben haben, aber von der Datenschutzschild-Liste gestrichen wurden. Das Ministerium wird deutlich auf Folgendes hinweisen: diese Organisationen nehmen nicht am Datenschutzschild teil; die Streichung von der Datenschutzschild-Liste bedeutet, dass diese Organisationen nicht geltend machen können, dass sie den Datenschutzschild einhalten, und sie alle Aussagen oder irreführende Praktiken vermeiden müssen, die auf eine Teilnahme am Datenschutzschild hindeuten; und diese Organisationen können nicht mehr die sich aus dem

Angemessenheitsbeschluss der Europäischen Kommission ergebenden Vorteile in Anspruch nehmen, die ihnen den Empfang personenbezogener Daten aus der EU ermöglichen. Gegen eine Organisation, die nach ihrer Streichung von der Datenschutzschild-Liste weiter eine Teilnahme am Datenschutzschild behauptet oder sonstige falsche Angaben zum Datenschutzschild macht, können von der FTC, vom Verkehrsministerium oder anderen Behörden entsprechende Durchsetzungsmaßnahmen eingeleitet werden.

5. Die Einhaltung dieser Grundsätze kann begrenzt sein: a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, aus denen sich widersprüchliche Verpflichtungen oder ausdrückliche Ermächtigungen ergeben, vorausgesetzt, die Organisation kann in Wahrnehmung einer derartigen Ermächtigung nachweisen, dass die Grundsätze nur insoweit nicht eingehalten werden, als die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung dies erfordert, oder c) wenn die Richtlinie oder das nationale Recht Ausnahmeregelungen vorsieht, sofern diese Ausnahmeregelungen unter vergleichbaren Voraussetzungen getroffen werden. Im Hinblick auf das Ziel eines wirksameren Schutzes der Privatsphäre sollen die Organisationen die Grundsätze in vollem Umfang und in transparenter Weise anwenden, unter anderem indem sie angeben, in welchen Fällen Abweichungen von den Grundsätzen, die nach b) zulässig sind, bei ihren Datenschutzmaßnahmen regelmäßig Anwendung finden werden. Aus demselben Grund wird, wenn die Wahlmöglichkeit nach den Grundsätzen und/oder nach dem US-Recht besteht, von den Organisationen erwartet, dass sie sich, sofern möglich, für das höhere Schutzniveau entscheiden.
6. Die Organisationen sind verpflichtet, die Grundsätze nach ihrem Beitritt zum Datenschutzschild auf alle personenbezogenen Daten anzuwenden, die im Vertrauen auf den Datenschutzschild übermittelt werden. Eine Organisation, die sich für eine Ausdehnung der Vorteile des Datenschutzschildes auf Personaldaten entscheidet, die im Rahmen eines Beschäftigungsverhältnisses aus der EU übermittelt werden, muss darauf hinweisen, wenn sie sich dem Ministerium gegenüber auf die Grundsätze verpflichtet, und sie muss die in den Zusatzgrundsätzen zur Selbstzertifizierung beschriebenen Anforderungen erfüllen.
7. Für Fragen der Auslegung und der Einhaltung der Grundsätze sowie der einschlägigen Datenschutzbestimmungen durch Organisationen, die dem Datenschutzschild angehören, gilt das US-Recht; es gilt nicht, wenn sich diese Organisationen zur Zusammenarbeit mit europäischen Datenschutzbehörden verpflichtet haben. Sofern nicht anderweitig festgelegt, finden sämtliche Bestimmungen der Grundsätze in allen Fällen, in denen sie relevant sind, Anwendung.
8. Begriffsbestimmungen:

- a. „Personenbezogene Daten“ sind in beliebiger Form aufgezeichnete Daten über eine identifizierte oder identifizierbare Person, die unter die Richtlinie fallen und aus der Europäischen Union an eine Organisation in den Vereinigten Staaten übermittelt werden.
 - b. „Verarbeitung“ personenbezogener Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe oder die Verbreitung sowie das Löschen oder Vernichten.
 - c. „Für die Verarbeitung Verantwortlicher“ bezeichnet eine Person oder Organisation, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
9. Der Tag des Wirksamwerdens der Grundsätze ist der Tag, an dem der Angemessenheitsbeschluss der Kommission endgültig genehmigt wird.

II. GRUNDSÄTZE

1. INFORMATIONSPFLICHT

- a. Die Organisation muss Privatpersonen über Folgendes informieren:
 - i. ihre Teilnahme am Datenschutzschild mit einem Link zur Datenschutzschild-Liste oder der Webanschrift der Liste,
 - ii. die Arten der erfassten personenbezogenen Daten und gegebenenfalls die Einrichtungen oder Tochterunternehmen der Organisation, die die Grundsätze ebenfalls einhalten,
 - iii. ihre Verpflichtung, die Grundsätze auf alle aus der EU empfangenen personenbezogenen Daten unter Zugrundelegung des Datenschutzschildes anzuwenden,
 - iv. zu welchem Zweck sie die personenbezogenen Daten über sie erhebt und verwendet,
 - v. wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, wozu auch Angaben zu einer relevanten Einrichtung in der EU gehören, die auf derartige Nachfragen oder Beschwerden eingehen kann,
 - vi. die Kategorie und Identität von Dritten, an die die Daten weitergegeben werden, sowie der Zweck der Weitergabe,
 - vii. das Recht von Privatpersonen auf Zugang zu ihren personenbezogenen Daten,
 - viii. welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe ihrer personenbezogenen Daten einzuschränken,
 - ix. das zur Bearbeitung von Beschwerden und für einen kostenlosen Rechtsschutz für die Privatperson benannte unabhängige Streitbeilegungsgremium, und ob es sich 1) um das von Datenschutzbehörden eingerichtete Gremium, 2) um einen in der EU ansässigen Anbieter für alternative Streitbeilegung oder 3) um einen in den Vereinigten Staaten ansässigen Anbieter für alternative Streitbeilegung handelt,
 - x. die für die Organisation geltenden Ermittlungs- und Durchsetzungsbefugnisse der FTC, des

- Verkehrsministeriums oder einer anderen bevollmächtigten US-Behörde,
- xi. die Möglichkeit, unter bestimmten Bedingungen ein verbindliches Schiedsverfahren anzustrengen,
 - xii. die Bestimmung, personenbezogene Daten auf rechtmäßige Anfrage von Behörden offenzulegen, um Erfordernissen der nationalen Sicherheit oder der Strafverfolgung nachzukommen, und
 - xiii. die Haftung der Organisation bei Weitergabe an Dritte.
- b. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig ersucht werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

2. WAHLMÖGLICHKEIT

- a. Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen („Opt-out“), ob ihre personenbezogenen Daten i) an Dritte weitergegeben werden sollen oder ii) für einen Zweck verwendet werden sollen, der sich von dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck wesentlich unterscheidet. Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare, verständliche und leicht zugängliche Verfahren ermöglicht werden.
- b. Abweichend vom vorstehenden Absatz unterliegt die Übermittlung solcher Daten an einen Dritten nicht dem Grundsatz der Wahlmöglichkeit, wenn dieser im Auftrag oder auf Anweisung der Organisation tätig ist. Die Organisation schließt jedoch stets einen Vertrag mit dem Beauftragten.
- c. Bei sensiblen Daten (d. h. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder weltanschauliche Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung („Opt-in“) der betroffenen Personen, wenn diese Daten i) an Dritte weitergegeben oder ii) für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat. Darüber hinaus sollen die Organisationen alle ihnen von Dritten übermittelten personenbezogenen Daten als sensibel behandeln, die der Übermittler als sensibel einstuft und behandelt.

3. VERANTWORTLICHKEIT FÜR DIE WEITERGABE

- a. Eine Organisation darf personenbezogene Daten nur dann an Dritte, die als für die Verarbeitung Verantwortliche tätig sind, weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Die Organisation muss auch einen Vertrag mit dem als für die Verarbeitung Verantwortlichen tätigen Dritten schließen, in dem festgelegt ist, dass diese Daten nur in begrenztem Rahmen für bestimmte Zwecke im Einklang mit der von der betroffenen Person erteilten Zustimmung verarbeitet werden dürfen und dass der Empfänger das gleiche Schutzniveau vorsieht wie die Grundsätze und er die Organisation entsprechend unterrichten muss, wenn er feststellt, dass er diese Verpflichtung nicht mehr erfüllen kann. Der Vertrag muss festlegen, dass im Falle einer derartigen Festlegung der als Verantwortlicher tätige Dritte die Verarbeitung einstellt oder mit anderen sinnvollen und geeigneten Maßnahmen Abhilfe schafft.
- b. Bei der Weitergabe von personenbezogenen Daten an einen Dritten, der in ihrem Auftrag und auf ihre Anweisung tätig ist, gilt für eine Organisation Folgendes: i) sie darf diese Daten nur in begrenztem Rahmen für bestimmte Zwecke weitergeben; ii) sie muss sich vergewissern, dass der Beauftragte verpflichtet ist, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den Grundsätzen gefordert wird; iii) sie muss mit angemessenen und geeigneten Schritten sicherstellen, dass der Beauftragte die weitergegebenen personenbezogenen Daten in einer den Verpflichtungen der Organisation im Rahmen der Grundsätze konformen Weise verarbeitet; iv) sie muss vom Beauftragten verlangen, dass er sie unterrichtet, wenn er feststellt, dass er seine Verpflichtung, das gleiche Schutzniveau vorzusehen wie in den Grundsätzen gefordert, nicht mehr erfüllen kann, v) sie muss auf entsprechenden Hinweis, einschließlich nach iv), sinnvolle und geeignete Schritte unternehmen, um eine unbefugte Verarbeitung zu unterbinden; vi) sie muss dem Ministerium auf Verlangen eine Zusammenfassung oder ein Exemplar der einschlägigen Datenschutzbestimmungen ihres Vertrags mit diesem Beauftragten vorlegen.

4. SICHERHEIT

- a. Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene und geeignete Maßnahmen ergreifen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen; dabei sind insbesondere die Risiken bei der Verarbeitung und die Art der personenbezogenen Daten zu berücksichtigen.

5. DATENINTEGRITÄT UND ZWECKBINDUNG

- a. In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten auf die Informationen beschränkt sein, die für den Verarbeitungszweck erheblich sind.² Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. In dem für diese Zwecke notwendigen Umfang muss die Organisation durch angemessene Maßnahmen gewährleisten, dass die personenbezogenen Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind. Die Organisation muss die Grundsätze so lange einhalten, wie sie diese Informationen aufbewahrt.
- b. Die Daten dürfen nur so lange in einer Form aufbewahrt werden, die eine Person identifiziert oder identifizierbar macht³, wie damit ein Verarbeitungszweck im Sinne von 5a erfüllt wird. Diese Verpflichtung hindert Organisationen nicht daran, personengebundene Informationen über längere Zeiträume zu verarbeiten, solange und soweit diese Verarbeitung hinreichend den Zwecken einer Archivierung im öffentlichen Interesse, des Journalismus, der Literatur und Kunst, der wissenschaftlichen oder historischen Forschung und der statistischen Analyse dient. In diesen Fällen unterliegt die Verarbeitung den anderen Grundsätzen und Bestimmungen der Regelung. Die Organisationen sollen zur Einhaltung dieser Bestimmung angemessene und geeignete Maßnahmen ergreifen.

6. AUSKUNFTSRECHT

- a. Privatpersonen müssen Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt, und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind oder unter Missachtung der Grundsätze verarbeitet wurden, es sei denn, die Belastung oder die Kosten für die Gewährung des Zugangs würden in dem jeweiligen Fall in einem Missverhältnis zu den Nachteilen für den Betroffenen stehen, oder Rechte anderer Personen als des Betroffenen würden verletzt.

7. RECHTSSCHUTZ, DURCHSETZUNG UND HAFTUNG

² Je nach Sachlage kommt als zulässiger Zweck für die Verarbeitung beispielsweise Folgendes in Frage: Pflege von Kundenbeziehungen, Compliance-Erwägungen und rechtliche Erwägungen, Wirtschaftsprüfung, Sicherheit und Betrugsprävention, Erhaltung oder Wahrung der Rechte der Organisation oder andere Zwecke, die nach vernünftigem Ermessen den Erwartungen im Zusammenhang mit der Erhebung entsprechen.

³ In diesem Zusammenhang gilt eine Person als „identifizierbar“, wenn sie in Anbetracht der mit hinreichender Wahrscheinlichkeit genutzten Mittel der Identifizierung (z. B. unter Berücksichtigung des Kosten- und Zeitaufwands für die Identifizierung und der zum Zeitpunkt der Verarbeitung verfügbaren Technik) und der Aufbewahrungsform der Daten nach vernünftigem Ermessen von der Organisation oder von einem Dritten mit Zugriff auf die Daten identifiziert werden kann.

- a. Für einen effektiven Schutz der Privatsphäre müssen belastbare Mechanismen geschaffen werden, die die Einhaltung der Grundsätze gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens Folgendes umfassen:
 - i. leicht zugängliche, von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, ohne Kosten für den Betroffenen untersucht und zügig behandelt werden und nach denen Schadenersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen;
 - ii. Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Organisationen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden, und insbesondere in Bezug auf Verstöße;
 - iii. Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Organisationen die Einhaltung der Grundsätze zwar erklärt, sich aber trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.
- b. Organisationen und die von ihnen gewählten unabhängigen Beschwerdestellen werden rasch auf Anfragen und Auskunftsbegehren des Ministeriums reagieren, die mit dem Datenschutzschild im Zusammenhang stehen. Alle Organisationen müssen zügig auf von Behörden der EU-Mitgliedstaaten über das Ministerium weitergeleitete Beschwerden bezüglich der Einhaltung der Grundsätze reagieren. Organisationen, die sich für eine Zusammenarbeit mit Datenschutzbehörden entschieden haben, einschließlich Organisationen, die Personaldaten verarbeiten, müssen im Zusammenhang mit der Untersuchung und Bearbeitung von Beschwerden unmittelbar auf diese Behörden eingehen.
- c. Organisationen sind verpflichtet, Ansprüche im Schiedsverfahren zu regeln und die in Anlage I aufgeführten Bedingungen einzuhalten, sofern eine Privatperson durch Benachrichtigung der betreffenden Organisation und entsprechend den Verfahren und Bedingungen nach Anlage I ein verbindliches Schiedsverfahren beantragt hat.
- d. Im Zusammenhang mit einer Weitergabe ist eine dem Datenschutzschild angehörende Organisation für die Verarbeitung der personenbezogenen Daten, die sie im Rahmen des Datenschutzschildes erhält und anschließend

an einen Dritten weitergibt, der in ihrem Auftrag und auf ihre Anweisung tätig ist, verantwortlich. Die dem Datenschutzschild angehörende Organisation bleibt nach den Grundsätzen haftbar, wenn ihr Beauftragter diese personenbezogenen Daten auf eine Art und Weise verarbeitet, die nicht im Einklang mit den Grundsätzen steht, es sei denn, sie weist nach, dass sie für das Ereignis, das den Schaden bewirkt hat, nicht verantwortlich ist.

- e. Ist gegen eine Organisation eine Anordnung der FTC oder ein Gerichtsbeschluss wegen eines Verstoßes ergangen, macht die Organisation jene Teile eines der FTC vorgelegten Compliance- oder Sachstandsberichts, die den Datenschutzschild betreffen, öffentlich, soweit dies mit den Verpflichtungen zur Geheimhaltung im Einklang steht. Das Ministerium hat eine spezielle Kontaktstelle eingerichtet, an die sich Datenschutzbehörden bei Compliance-Problemen von dem Datenschutzschild angehörenden Organisationen wenden können. Die FTC wird Fälle der Missachtung der Grundsätze, die ihr vom Ministerium und Behörden der EU-Mitgliedstaaten zugeleitet wurden, vorrangig behandeln und vorbehaltlich der geltenden Geheimhaltungsvorschriften zeitnah mit den vorliegenden staatlichen Behörden Informationen zu diesen Fällen austauschen.

III. ZUSATZGRUNDSÄTZE

1. Sensible Daten

- a. Eine Organisation muss keine ausdrückliche Zustimmung (Opt-in) für die Verarbeitung sensibler Daten einholen, wenn die Verarbeitung
 - i. im lebenswichtigen Interesse der betroffenen Person oder einer anderen Person liegt;
 - ii. zur Geltendmachung von Rechtsansprüchen oder für die Rechtsverteidigung notwendig ist;
 - iii. für eine medizinische Behandlung oder Diagnose erforderlich ist;
 - iv. durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Körperschaft, die keinen Erwerbszweck verfolgt, im Rahmen rechtmäßiger Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder der Organisation oder Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, beziehen und die Daten nicht ohne Einwilligung der betroffenen Person an Dritte weitergegeben werden;
 - v. zur Erfüllung der arbeitsrechtlichen Pflichten der Organisation notwendig ist;
 - vi. sich auf Daten bezieht, die von der Person nachweislich veröffentlicht worden sind.

2. Ausnahmen für den journalistischen Bereich

- a. Da die Pressefreiheit durch die amerikanische Verfassung geschützt ist und die Richtlinie Ausnahmen für den Fall vorsieht, dass personenbezogene Daten zu journalistischen Zwecken verarbeitet werden, ist für die Interessenabwägung, wenn die im ersten Zusatzartikel zur Verfassung der Vereinigten Staaten verankerte Pressefreiheit mit dem Recht auf Schutz der Privatsphäre kollidiert, der erste Zusatzartikel maßgeblich, soweit es um die Tätigkeit natürlicher oder juristischer Personen in den USA geht.
- b. Die Grundsätze des Datenschutzschildes gelten nicht für personenbezogene Daten, die zur Veröffentlichung, zur Verbreitung über Rundfunk und Fernsehen oder für andere Formen öffentlicher Kommunikation gesammelt werden, unabhängig davon, ob sie tatsächlich genutzt werden oder nicht, ebenso nicht für früher veröffentlichtes Material, das aus Medienarchiven stammt.

3. Hilfsweise Haftung

- a. Internetdiensteanbieter (Internet Service Providers, „ISP“), Telekommunikationsunternehmen und andere Organisationen sind nicht nach den Grundsätzen haftbar, wenn sie im Namen einer anderen Organisation Daten lediglich übermitteln, weiterleiten oder zwischenspeichern. Wie auch die Richtlinie selbst begründet der Datenschutzschild keine hilfsweise Haftung. Soweit eine Organisation personenbezogene Daten Dritter nur weiterleitet und weder Mittel noch Zweck ihrer Verarbeitung bestimmt, ist sie nicht haftbar.

4. Due-Diligence-Prüfung und Wirtschaftsprüfung

- a. Bei der Tätigkeit von Investmentbanken und Wirtschaftsprüfern kann es vorkommen, dass personenbezogene Daten ohne Wissen und Einwilligung des Betroffenen verarbeitet werden. Dies ist unter den nachfolgend aufgeführten Voraussetzungen mit den Grundsätzen der Informationspflicht, des Wahlrechts und des Auskunftsrechts vereinbar.
- b. Aktiengesellschaften und personenbezogene Aktiengesellschaften, einschließlich dem Datenschutzschild angehörende Organisationen, werden regelmäßig einer Wirtschaftsprüfung unterzogen. Diese Prüfungen, vor allem wenn damit ein potenzielles Fehlverhalten untersucht wird, können in Gefahr geraten, wenn sie vorzeitig bekannt werden. Eine dem Datenschutzschild angehörende Organisation, bei der eine Fusion oder Übernahme ansteht, muss zudem eine Due-Diligence-Prüfung durchführen oder ist Gegenstand einer derartigen Prüfung. Dabei werden oft personenbezogene Daten erhoben und verarbeitet, wie z. B. Informationen über Führungskräfte und andere Leistungsträger. Eine vorzeitige Bekanntgabe könnte den Abschluss behindern oder gegen geltende Wertpapiervorschriften verstoßen. Investmentbanken und Rechtsanwälte, die eine Due-Diligence-Prüfung durchführen, oder Wirtschaftsprüfer können personenbezogene Daten ohne Wissen des Betroffenen nur verarbeiten, soweit und solange das aufgrund gesetzlicher oder im öffentlichen Interesse liegender Erfordernisse notwendig ist, und können das auch in anderen Fällen, wenn die Anwendung der Grundsätze ihren legitimen Interessen zuwiderlaufen würde. Legitim sind u. a. die Kontrolle von Organisationen auf Erfüllung ihrer gesetzlichen Pflichten, die Prüfung ihrer Rechnungslegung und die Wahrung der Vertraulichkeit von Informationen betreffend mögliche Übernahmen, Fusionen und Joint Ventures sowie ähnliche Vorgänge, die von Investmentbanken oder Wirtschaftsprüfern abgewickelt werden.

5. Die Rolle der Datenschutzbehörden

- a. Die Organisationen werden ihre Verpflichtung zur Zusammenarbeit mit Datenschutzbehörden der Europäischen Union wie nachfolgend dargelegt umsetzen. Nach den Grundsätzen des Datenschutzschilds müssen in den USA ansässige Organisationen, die personenbezogene Daten aus der EU

erhalten, mit geeigneten Mitteln dafür sorgen, dass diese Grundsätze gewahrt werden. Wie im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung beschrieben, gehören zu diesen Mitteln a)i) Rechtsbehelfe für Personen, über die die Organisationen Daten besitzen, a)ii) Verfahren, mit denen sie überprüfen, ob ihre Aussagen und Zusicherungen betreffend ihre Datenschutzpraxis den Tatsachen entsprechen; a)iii) die Pflicht der Organisationen, Abhilfe zu schaffen, falls es zu Problemen kommt, weil die Grundsätze bei ihnen nicht gewahrt werden, sowie Sanktionen für Verstöße gegen diese Grundsätze. Den Punkten a)i) und a)iii) des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung können Organisationen dadurch entsprechen, dass sie die hier festgelegten Anforderungen zur Zusammenarbeit mit den Datenschutzbehörden einhalten.

b. Eine Organisation verpflichtet sich zur Zusammenarbeit mit den Datenschutzbehörden, indem sie in der Mitteilung über die Selbstzertifizierung gegenüber dem Handelsministerium (*siehe* Zusatzgrundsatz „Selbstzertifizierung“) Folgendes erklärt:

- i. dass sie den Bestimmungen der Punkte a)i) und a)iii) des Datenschutzschild-Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung entsprechen will, indem sie sich zur Zusammenarbeit mit den entsprechenden Datenschutzbehörden verpflichtet;
- ii. dass sie mit den entsprechenden Datenschutzbehörden bei der Untersuchung und Behandlung von Beschwerden zusammenarbeiten will, die unter Berufung auf die Grundsätze des Datenschutzschildes erhoben werden;
- iii. dass sie sich an die Empfehlung der entsprechenden Datenschutzbehörden hält, wenn diese der Organisation aufgeben, spezifische Maßnahmen zu treffen, um den Grundsätzen des Datenschutzschildes zu entsprechen; hierzu gehören auch Rechtsmittel und Entschädigungsleistungen zugunsten von Personen, die infolge Nichteinhaltung der Grundsätze Nachteile erlitten haben; ferner, dass sie den entsprechenden Datenschutzbehörden schriftlich die Durchführung dieser Maßnahmen bestätigt.

c. Tätigkeit von Gremien der Datenschutzbehörden

- i. Die Kooperation der Datenschutzbehörden erfolgt über Information und Beratung:
 1. Die Beratung übernimmt ein informelles Gremium, in dem europäische Datenschutzbehörden vertreten sind, so dass u. a. ein einheitlicher schlüssiger Ansatz gewährleistet wird.

2. Das Gremium berät die betreffenden US-amerikanischen Organisationen bei ungeklärten Beschwerden von Einzelpersonen über den Umgang mit personenbezogenen Daten, die aus der EU im Rahmen des Datenschutzschildes übermittelt wurden. Diese Beratung soll gewährleisten, dass die Grundsätze des Datenschutzschildes korrekt angewendet werden; sie schließt die Rechtsmittel für die betroffene(n) Einzelperson(en) ein, die die Datenschutzbehörden für angemessen erachten.
 3. Das Gremium erbringt derartige Beratungsleistungen auf Anfrage der betreffenden US-Organisationen und/oder auf direkt eingegangene Beschwerden von Einzelpersonen gegen Organisationen, die sich auf die Grundsätze des Datenschutzschildes und zur Zusammenarbeit mit den Datenschutzbehörden verpflichtet haben. Dabei ermutigt es die betroffenen Einzelpersonen zunächst, die verfügbaren internen Verfahren zur Behandlung von Beschwerden, die die Organisation bereitstellt, zu nutzen, und unterstützt sie erforderlichenfalls dabei.
 4. Das Gremium gibt erst dann eine Empfehlung ab, wenn beide Parteien hinreichend Gelegenheit zur Stellungnahme oder zum Vorlegen von Beweisen hatten. Es wird sich bemühen, die Empfehlung so rasch zur Verfügung zu stellen, wie ein ordnungsgemäßes Vorgehen dies erlaubt. Grundsätzlich wird das Gremium sich bemühen, die Beratung binnen sechzig Tagen nach Eingang einer Beschwerde oder dem Ersuchen einer Organisation anzubieten, und falls möglich noch rascher.
 5. Soweit es ihm angemessen erscheint, veröffentlicht das Gremium die Ergebnisse der Beschwerdeprüfungen.
 6. Die Beratung ist weder für das Gremium selbst noch für eine der beteiligten Datenschutzbehörden mit irgendeiner Form der Haftung verbunden.
- ii. Organisationen, die sich für diese Form der Streitbeilegung entscheiden, müssen sich verpflichten, den Empfehlungen der Datenschutzbehörden zu folgen. Kommt die Organisation den Empfehlungen des Gremiums nicht binnen 25 Tagen nach und hat sie keine befriedigende Erklärung für die Verzögerung gegeben, so teilt das Gremium seine Absicht mit, die Angelegenheit an die Federal Trade Commission, das Verkehrsministerium oder eine andere Stelle zu verweisen, die Zuständigkeit bzw. Durchsetzungsgewalt in Fällen von Irreführung oder unrichtiger Erklärung besitzt. Oder es teilt mit, dass es zu dem Schluss gelangt ist, dass eine gravierende Verletzung der Kooperations-

vereinbarung vorliegt und diese mithin null und nichtig ist. In diesem Fall unterrichtet das Gremium das Handelsministerium, so dass die Datenschutzschild-Liste entsprechend geändert werden kann. Jede Unterlassung der Zusammenarbeit und jeder Verstoß gegen die Grundsätze des Datenschutzschilds können als Irreführung gemäß § 5 des FTC Act oder anderen vergleichbaren Gesetzen rechtlich verfolgt werden.

- d. Wünscht eine Organisation, dass ihr die Vorteile des Datenschutzschilds auch bei Personaldaten zuteilwerden, die zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, muss es sich in Bezug auf diese Daten zur Zusammenarbeit mit den Datenschutzbehörden verpflichten (*siehe* Zusatzgrundsatz „Personaldaten“).
- e. Organisationen, die sich für diese Option entscheiden, zahlen eine Jahresgebühr, die dazu bestimmt ist, die laufenden Kosten des Gremiums der Datenschutzbehörden zu decken; ferner können sie zur Begleichung der Kosten für alle erforderlichen Übersetzungen herangezogen werden, die sich aus der Beratungstätigkeit des Gremiums im Zusammenhang mit Beschwerden gegenüber den Organisationen ergeben. Die Jahresgebühr beträgt höchstens 500 USD und ist für kleinere Organisationen geringer.

6. Selbstzertifizierung

- a. In den Genuss der Vorteile des Datenschutzschilds kommt eine Organisation ab dem Tag, an dem das Ministerium ihren Selbstzertifizierungsantrag nach Feststellung der Vollständigkeit in die Datenschutzschild-Liste aufgenommen hat.
- b. Um sich für den Datenschutzschild selbst zu zertifizieren, muss die Organisation dem Ministerium einen von einem leitenden Mitarbeiter im Namen der Organisation unterzeichneten Selbstzertifizierungsantrag einreichen, der mindestens folgende Angaben enthält:
 - i. Name der Organisation, Postanschrift, E-Mail-Adresse, Telefon- und Faxnummer;
 - ii. Beschreibung der Tätigkeit der Organisation im Zusammenhang mit personenbezogenen Daten aus der EU;
 - iii. Beschreibung der Datenschutzbestimmungen der Organisation, die folgende Angaben umfassen muss:
 - 1. ob die Organisation über eine öffentliche Website verfügt, die entsprechende Webadresse, unter der diese Beschreibung eingesehen kann, oder, wenn die Organisation nicht über eine öffentliche Website verfügt, der Ort, an dem diese Beschreibung von der Öffentlichkeit eingesehen werden kann;

2. Tag, an dem diese Vorkehrungen in Kraft gesetzt wurden;
 3. Kontaktstelle, die für die Bearbeitung von Beschwerden, Auskunftersuchen und anderen Angelegenheiten des Datenschutzschilds zuständig ist;
 4. die gesetzliche Aufsichtsbehörde, die über Beschwerden gegen die Organisation wegen unlauteren oder irreführenden Geschäftsgebarens und wegen Verletzung von datenschutzrechtlichen Vorschriften entscheidungsbefugt ist (und in den Grundsätzen oder in einem künftigen Anhang zu den Grundsätzen aufgeführt ist);
 5. die Bezeichnungen aller Datenschutzprogramme, an denen die Organisation teilnimmt;
 6. die Art der anlassunabhängigen Kontrolle (z. B. intern oder extern) (*siehe* Zusatzgrundsatz „Anlassunabhängige Kontrolle“);
 7. die unabhängige Beschwerdestelle zur Behandlung ungeklärter Beschwerdefälle.
- c. Wenn die Organisation wünscht, dass ihr die Vorteile des Datenschutzschilds auch bei Personaldaten zuteilwerden, die zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, so ist dies möglich, wenn eine in den Grundsätzen oder in einem künftigen Anhang zu den Grundsätzen aufgeführte gesetzliche Aufsichtsbehörde befugt ist, Beschwerden gegen die Organisation aufgrund der Verarbeitung von Personaldaten entgegenzunehmen. Darüber hinaus muss die Organisation darauf in ihrem Selbstzertifizierungsantrag hinweisen und sich bereit erklären, gemäß den Zusatzgrundsätzen „Personaldaten“ und „Rolle der Datenschutzbehörden“, soweit anwendbar, mit der (den) Datenschutzbehörde(n) in der EU zusammenzuarbeiten und den Empfehlungen dieser Behörden nachzukommen. Außerdem muss die Organisation dem Ministerium ihre Datenschutzbestimmungen für Personaldaten sowie Angaben dazu übermitteln, wo die Datenschutzbestimmungen von den betroffenen Mitarbeitern eingesehen werden können.
- d. Das Ministerium führt die Datenschutzschild-Liste der Organisationen, die Selbstzertifizierungsanträge eingereicht haben und denen damit die Vorteile des Datenschutzschilds zustehen; die Liste wird anhand der jährlich eingereichten Selbstzertifizierungsanträge und der Meldungen aktualisiert, die gemäß dem Zusatzgrundsatz „Beschwerdeverfahren und Durchsetzung“ eingehen. Diese Selbstzertifizierungsanträge sind mindestens jährlich neu vorzulegen, andernfalls wird die Organisation von der Datenschutzschild-Liste gestrichen, und die Vorteile des

Datenschutzschilder sind nicht mehr garantiert. Die Datenschutzschild-Liste und die von den Organisationen vorgelegten Selbstzertifizierungsanträge werden der Öffentlichkeit zugänglich gemacht. Alle Organisationen, die vom Ministerium auf die Datenschutzschild-Liste gesetzt werden, müssen in ihren relevanten veröffentlichten Datenschutzbestimmungen auch erklären, dass sie sich an die Grundsätze des Datenschutzschildes halten. Wenn die Datenschutzbestimmungen einer Organisation online verfügbar sind, müssen sie mit einem Hyperlink zur Website des Datenschutzschildes beim Ministerium versehen sein sowie mit einem Hyperlink zur Website oder dem Beschwerdeformular der unabhängigen Beschwerdestelle, die ungeklärte Beschwerden prüft.

- e. Die Datenschutzgrundsätze werden bei Zertifizierung unverzüglich wirksam. In Anbetracht der Tatsache, dass sich die Grundsätze auf die Geschäftsbeziehungen zu Dritten auswirken, werden Organisationen, die sich innerhalb der ersten zwei Monate nach Inkrafttreten der Datenschutzschild-Regelung dafür zertifizieren, ihre bestehenden Geschäftsbeziehungen zu Dritten so bald wie möglich, spätestens jedoch neun Monate nach ihrer Zertifizierung gegenüber dem Datenschutzschild, mit dem Grundsatz der Verantwortlichkeit für die Weitergabe in Übereinstimmung bringen. In diesem Übergangszeitraum werden die Organisationen bei der Übermittlung von Daten an einen Dritten i) die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwenden und sich ii) bei Übergabe personenbezogener Daten an einen Dritten, der in ihrem Auftrag und auf ihre Anweisung tätig ist, vergewissern, dass der Beauftragte mindestens das Schutzniveau gewährleistet, das in den Grundsätzen gefordert wird.
- f. Eine Organisation muss die Grundsätze des Datenschutzschildes auf alle unter Bezugnahme auf den Datenschutzschild aus der EU empfangenen personenbezogenen Daten anwenden. Die Verpflichtung auf die Grundsätze des Datenschutzschildes gilt ohne zeitliche Begrenzung für personenbezogene Daten, die der Organisation übermittelt wurden, während sie in den Genuss der Vorteile des Datenschutzschildes gelangte. Diese Daten unterliegen den Grundsätzen so lange, wie die Organisation sie speichert, verarbeitet oder weitergibt, und das auch dann noch, wenn sie aus welchem Grund auch immer den Datenschutzschild verlässt. Eine Organisation, die aus dem Datenschutzschild ausscheidet, diese Daten aber behalten möchte, muss sich dem Handelsministerium gegenüber jährlich dazu verpflichten, die Grundsätze weiterhin anzuwenden, oder für den „angemessenen“ Schutz der Daten durch andere zulässige Mittel sorgen (z. B. durch einen Vertrag, der den Anforderungen der von der Europäischen Kommission gebilligten einschlägigen Standardklauseln vollauf genügt); andernfalls muss die Organisation die Daten zurückgeben oder löschen. Eine Organisation, die aus dem Datenschutzschild ausscheidet, muss aus den relevanten Datenschutzbestimmungen jede

Bezugnahme auf den Datenschutzschild entfernen, die darauf hindeutet, dass sich die Organisationen weiterhin aktiv am Datenschutzschild beteiligt und Anspruch auf die damit verbundenen Vorteile hat.

- g. Eine Organisation, die aufgrund einer Fusion oder einer Übernahme ihren Status als selbstständige rechtliche Einheit verliert, muss dies dem Ministerium vorher mitteilen. In dieser Mitteilung sollte auch darauf hingewiesen werden, ob die übernehmende Einheit bzw. die Einheit, die aus der Fusion hervorgeht, i) weiterhin nach dem Gesetz, das für die Fusion oder Übernahme maßgeblich war, an die Grundsätze des Datenschutzschilds gebunden ist oder ii) entscheidet, ihren Beitritt zu den Grundsätzen des Datenschutzschildes selbst zu zertifizieren, bzw. andere Garantien, beispielsweise durch schriftliche Vereinbarungen, schafft, die die Einhaltung der Grundsätze des Datenschutzschilds gewährleisten. Ist weder i) noch ii) der Fall, müssen alle Daten, die im Rahmen des Datenschutzschilds gesammelt wurden, unverzüglich gelöscht werden.
- h. Wenn eine Organisation aus welchem Grund auch immer den Datenschutzschild verlässt, muss sie alle Erklärungen entfernen, die darauf hindeuten, dass sie sich weiter am Datenschutzschild beteiligt oder Ansprüche auf die damit verbundenen Vorteile hat. Wurde das Gütesiegel des EU-US-Datenschutzschilds verwendet, ist auch dies zu entfernen. Bei falschen Angaben über die Einhaltung der Datenschutzgrundsätze, die die Organisation gegenüber der Öffentlichkeit macht, können die FTC oder andere zuständige staatliche Stellen gegen sie vorgehen. Falsche Angaben gegenüber dem Ministerium unterliegen dem False Statements Act (18 U.S.C. § 1001).

7. Anlassunabhängige Kontrolle

- a. Organisationen müssen sich anhand von Kontrollverfahren vergewissern, dass der von ihnen zugesicherte Datenschutz im Rahmen des Datenschutzschilds tatsächlich besteht und dass ihre Datenschutzpolitik tatsächlich umgesetzt worden ist und den Grundsätzen des Datenschutzschilds entspricht.
- b. Die nach dem Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung erforderliche anlassunabhängige Kontrolle muss eine Organisation entweder selbst durchführen oder von einer externen Stelle durchführen lassen.
- c. Im Falle der Selbstkontrolle muss die Organisation in einer Erklärung feststellen, dass ihre veröffentlichten Datenschutzbestimmungen betreffend personenbezogene Daten aus der EU sachgerecht, umfassend, an auffälliger Stelle bekannt gemacht, vollständig umgesetzt und für jedermann zugänglich sind. Sie muss ferner feststellen, dass ihre Datenschutzbestimmungen den Grundsätzen des Datenschutzschilds entsprechen, dass betroffene Personen über interne Beschwerdeverfahren und Beschwerdeverfahren bei unabhängigen Schiedsstellen informiert

werden, dass sie ihre Beschäftigten systematisch in der Praxis des Datenschutzes unterweist und Verstöße gegen die Datenschutzregeln ahndet und dass es bei ihr interne Verfahren gibt, nach denen die Einhaltung der Datenschutzvorschriften regelmäßig und objektiv überprüft wird. Die Selbstkontrolle muss mindestens einmal jährlich stattfinden, eine Erklärung über ihre Durchführung ist von einem leitenden Angestellten oder einem bevollmächtigten Vertreter der Organisation zu unterzeichnen; sie ist vorzulegen auf Verlangen von Einzelpersonen, im Rahmen einer Untersuchung oder bei einer Beschwerde wegen Nichteinhaltung von Datenschutzvorschriften.

- d. Bei externer anlassunabhängiger Kontrolle ist nachzuweisen, dass die Bestimmungen der Organisation für den Schutz personenbezogener Daten aus der EU den Grundsätzen des Datenschutzschildes entsprechen, dass diese Regeln eingehalten werden und dass betroffene Personen über die Beschwerdewege informiert werden, die ihnen offenstehen. Dazu können ohne Einschränkung Buchprüfungen und Zufallskontrollen durchgeführt sowie „Köder“ und jede Art von technischen Hilfsmitteln eingesetzt werden. Die externe Kontrolle muss mindestens einmal jährlich stattfinden, eine Erklärung über ihre Durchführung ist entweder vom Prüfer oder von einem leitenden Angestellten bzw. einem bevollmächtigten Vertreter der Organisation zu unterzeichnen; sie ist vorzulegen auf Verlangen von Einzelpersonen, im Rahmen einer Untersuchung oder bei einer Beschwerde wegen Nichteinhaltung von Datenschutzvorschriften.
- e. Organisationen müssen die Umsetzung ihrer nach den Grundsätzen des Datenschutzschildes konzipierten Datenschutzbestimmungen dokumentieren und im Fall einer Untersuchung oder einer Beschwerde wegen Verletzung der Datenschutzvorschriften ihre Unterlagen der unabhängigen Schiedsstelle übergeben, die für die Prüfung von Beschwerden zuständig ist, oder der gesetzlichen Aufsichtsbehörde, die bei unlauterem und irreführendem Geschäftsgebahren entscheidungsbefugt ist. Die Organisationen müssen zudem unverzüglich auf Anfragen und andere Auskunftsbegehren des Ministeriums reagieren, die sich auf die Einhaltung der Grundsätze beziehen.

8. Auskunftsrecht

- a. Das Auskunftsrecht in der Praxis
 - i. Nach den Grundsätzen des Datenschutzschildes ist das Auskunftsrecht grundlegend für den Schutz der Privatsphäre. Es ermöglicht dem Einzelnen, die Richtigkeit von Daten zu überprüfen, die über ihn gespeichert sind. Das Auskunftsrecht bedeutet, dass Privatpersonen einen Anspruch darauf haben,

1. von einer Organisation bestätigt zu bekommen, ob diese personengebundene Daten der betroffenen Person verarbeitet oder nicht;⁴
 2. dass ihnen diese Daten übermittelt werden, damit sie deren Richtigkeit und die Rechtmäßigkeit der Verarbeitung überprüfen können;
 3. die Daten korrigieren, ändern oder löschen zu lassen, wenn sie falsch sind oder unter Verletzung der Grundsätze verarbeitet wurden.
- ii. Wer Zugang zu den ihn betreffenden Daten verlangt, muss das nicht begründen. Verlangt jemand Zugang zu den über ihn gespeicherten Daten, sollte sich die angesprochene Organisation zunächst fragen, welche Gründe die Person dazu veranlassen. Ist beispielsweise eine Anfrage vage formuliert oder betrifft sie einen sehr weiten Bereich, so kann die Organisation mit der Person in Dialog treten, um die Gründe für die Anfrage besser zu verstehen und die gewünschten Daten zu ermitteln. Die Organisation kann sich danach erkundigen, mit welchen Teilen der Organisation die Person Kontakt hatte oder um welche Art von Daten bzw. deren Nutzung es geht.
- iii. Wegen seines grundlegenden Charakters sollen Organisationen das Auskunftsrecht nie ohne Not beschränken. Müssen z. B. bestimmte Daten geschützt werden und lassen sie sich leicht von den personenbezogenen Daten trennen, zu denen Zugang verlangt wird, sollte die Organisation die geschützten Daten unkenntlich machen und die übrigen zur Verfügung stellen. Beschließt eine Organisation in einem bestimmten Fall, den Zugang einzuschränken, sollte sie der Person, die um Zugang ersucht hat, ihre Entscheidung begründen und ihr eine Kontaktstelle nennen, die weitere Auskünfte erteilt.

b. Aufwand oder Kosten für die Gewährung des Zugangs

- i. Das Recht auf Zugang zu personenbezogenen Daten darf nur in Ausnahmefällen eingeschränkt werden, wenn legitime Rechte Dritter verletzt würden oder wenn die Zugangsgewährung mit Kosten oder Aufwand verbunden ist, die im Einzelfall in keinem Verhältnis zum Nachteil für die Privatsphäre des Betroffenen stehen. Zwar sind bei der Beurteilung der Zumutbarkeit die Kosten

⁴ Die Organisation sollte Anfragen von Privatpersonen zum Zweck der Verarbeitung, zu den Datenkategorien, die verarbeitet werden, sowie zu den Empfängern oder Kategorien der Empfänger der personenbezogenen Daten beantworten.

und der Aufwand zu berücksichtigen, die die Gewährung des Zugangs erfordert, sie sind aber nicht entscheidend.

- ii. Bilden die personenbezogenen Daten etwa die Grundlage für Entscheidungen, die für die Person von großer Tragweite sind (z. B. die Gewährung oder Versagung erheblicher Vorteile wie eine Versicherung, einen Kredit oder einen Arbeitsplatz), dann ist es der Organisation im Einklang mit den anderen Bestimmungen dieser Zusatzgrundsätze zumutbar, über diese Daten Auskunft zu geben, selbst wenn das einen relativ hohen Kosten- und Arbeitsaufwand erfordert. Wenn die angeforderten personenbezogenen Daten nicht sensibel sind oder nicht für Entscheidungen verwendet werden, die für die Person von großer Tragweite sind, die Daten aber leicht zugänglich sind und kostengünstig zur Verfügung gestellt werden können, muss die Organisation Zugang zu diesen Daten gewähren.

c. Vertrauliche Geschäftsdaten

- i. Vertrauliche Geschäftsdaten sind Daten, die ihr Inhaber durch besondere Vorkehrungen vor unbefugtem Zugriff geschützt hat, weil ihre Kenntnis Konkurrenten Vorteile verschaffen würde. Eine Organisation kann den Zugang zu personenbezogenen Daten verwehren oder einschränken, wenn durch einen vollständigen Zugang eigene vertrauliche Geschäftsdaten, wie z. B. von der Organisation erarbeitete Marketingkonzepte und Klassifikationen, oder aber Geschäftsdaten anderer, die einer vertraglichen Geheimhaltungspflicht unterliegen, offenbart würden.
- ii. Können vertrauliche Geschäftsdaten leicht von den personengebundenen Daten getrennt werden, zu denen Zugang verlangt wird, sollte die Organisation die vertraulichen Daten unkenntlich machen und die nichtvertraulichen zur Verfügung stellen.

d. Datenbanken von Organisationen

- i. Es genügt, wenn Organisationen der betreffenden Person mitteilen, welche personenbezogenen Daten über sie gespeichert sind; der Person muss kein Zugang zur Datenbank der Organisation gewährt werden.
- ii. Die Organisation muss nur Auskunft über die von ihr gespeicherten personenbezogenen Daten geben. Das Auskunftsrecht begründet keine Pflicht, Dateien mit personenbezogenen Daten aufzubewahren, zu pflegen oder erforderlichenfalls umzustrukturieren.

e. Wann eine Beschränkung des Zugangs möglich ist

- i. Da Organisationen sich immer redlich bemühen müssen, Privatpersonen Zugang zu ihren personenbezogenen Daten zu verschaffen, ist eine Beschränkung des Zugangs nur in wenigen Fällen möglich und muss stets konkret begründet werden. Wie entsprechend der Richtlinie kann eine Organisation den Zugang zu personenbezogenen Daten insoweit beschränken, als ihre Bekanntgabe wesentliche öffentliche Belange gefährden würde wie die nationale Sicherheit, die Verteidigung oder die öffentliche Sicherheit. Außerdem kann der Zugang verwehrt werden, wenn personenbezogene Daten ausschließlich für wissenschaftliche oder statistische Zwecke verarbeitet werden sollen. Weitere Gründe für die Verweigerung oder Beschränkung des Zugangs sind:
 1. Beeinträchtigung des Rechtsvollzugs oder der Rechtsvollstreckung oder eines zivilrechtlichen Verfahrens, einschließlich der Abwehr, Untersuchung und Verfolgung von Straftaten, oder des Rechts auf einen fairen Prozess;
 2. die Bekanntgabe der Daten würde die legitimen Rechte oder wichtigen Interessen anderer verletzen;
 3. gesetzliche oder andere berufliche Rechte und Pflichten werden verletzt;
 4. die Sicherheitsprüfung von Arbeitnehmern oder ein Beschwerdeverfahren oder die Vertraulichkeit im Zusammenhang mit der Neubesetzung von Stellen oder der Umstrukturierung von Organisationen werden beeinträchtigt; oder
 5. die Vertraulichkeit ist gefährdet, die bei der Überwachung, bei der Prüfung und bei sonstigen gesetzlich vorgeschriebenen Ordnungsfunktionen im Zusammenhang mit der ordnungsgemäßen Wirtschaftsführung oder bei künftigen oder laufenden Verhandlungen über die Organisation erforderlich ist.
 - ii. Eine Organisation, die sich auf einen dieser Ausnahmefälle beruft, muss nachweisen, dass er tatsächlich vorliegt, und der anfragenden Person die Gründe für die Beschränkung des Zugangs sowie eine Anlaufstelle für weitere Fragen mitteilen.
- f. Recht auf Erhalt einer Bestätigung sowie Erhebung einer Gebühr zur Deckung der Kosten der Zugangserteilung
- i. Personen haben das Recht, eine Bestätigung darüber zu erhalten, ob die Organisation sie betreffende personenbezogene Daten besitzt. Ebenso haben Personen ein Recht darauf, dass ihnen die sie betreffenden personenbezogenen Daten mitgeteilt werden. Eine

- Organisation kann eine Gebühr erheben, die nicht überhöht sein darf.
- ii. Die Erhebung einer Gebühr kann beispielsweise gerechtfertigt sein, wenn das Auskunftsbegehren offenkundig überzogen ist, insbesondere bei ständiger Wiederholung.
 - iii. Der Zugang darf nicht aus Kostengründen verwehrt werden, wenn die Personen, die den Zugang verlangen, bereit sind, diese Kosten zu übernehmen.
- g. Wiederholte oder belästigende Auskunftsbegehren
- i. Eine Organisation kann die Zahl der Anfragen einer Person innerhalb eines bestimmten Zeitraums angemessen begrenzen. Bei der Festlegung dieser Grenze sind Faktoren zu berücksichtigen wie die Häufigkeit, mit der Daten aktualisiert werden, der Zweck, für den die Daten verwendet werden, und die Art der Daten.
- h. Auskunftserschleichung
- i. Eine Organisation muss nur Auskunft erteilen, wenn die anfragende Person ihre Identität zweifelsfrei nachweist.
- i. Frist für die Auskunftserteilung
- i. Eine Organisation soll innerhalb angemessener Frist auf angemessene und eine für die anfragenden Personen leicht verständliche Weise auf Auskunftsbegehren antworten. Organisationen, die betroffene Personen regelmäßig informieren, können einem einzelnen Auskunftsbegehren im Rahmen ihrer regelmäßigen Auskünfte nachkommen, wenn es dadurch nicht zu einer übermäßigen Verzögerung kommt.

9. Personaldaten

- a. Abdeckung durch den Datenschutzschild
- i. Übermittelt eine in der EU ansässige Organisation im Rahmen des Beschäftigungsverhältnisses erhobene personenbezogene Daten über ihre (früheren oder derzeitigen) Beschäftigten an eine Mutterorganisation, eine verbundene Organisation oder eine nicht verbundene Dienstleistungsorganisation in den USA, die sich auf die Grundsätze des Datenschutzschilds verpflichtet hat, so fällt diese Übermittlung in den Anwendungsbereich der Grundsätze des Datenschutzschilds. In einem solchen Fall gelten für die Erhebung der Daten und ihre Verarbeitung vor der Übermittlung die Rechtsvorschriften des EU-Mitgliedstaats, aus dem sie stammen; sämtliche nach diesen Rechtsvorschriften geltende Bedingungen und Beschränkungen der Übermittlung müssen beachtet werden.

- ii. Die Grundsätze des Datenschutzschildes gelten nur für die Übermittlung von und den Zugriff auf Daten über identifizierte oder identifizierbare Einzelpersonen. Die Verwendung von statistischen Informationen, die auf aggregierten Beschäftigungsdaten beruhen und keine personenbezogenen Daten enthalten, oder von anonymisierten Daten ist unter dem Datenschutzaspekt unbedenklich.

b. Anwendung der Grundsätze der Informationspflicht und des Wahlrechts

- i. Eine Organisation in den USA, die unter Anwendung der Grundsätze des Datenschutzschildes Personaldaten aus der EU empfangen hat, darf diese Dritten nur offenlegen oder diese nur für andere Zwecke nutzen, wenn das mit den Grundsätzen der Informationspflicht und der Wahlmöglichkeit vereinbar ist. Will beispielsweise eine Organisation in den USA Personaldaten einer Organisation in der EU für Zwecke wie Direktmarketing nutzen, muss sie zuvor den betroffenen Personen die Wahlmöglichkeit geben, es sei denn, diese haben bereits der Nutzung der Daten für die jeweiligen Zwecke zugestimmt. Diese Nutzung darf nicht mit den Zwecken unvereinbar sein, zu denen die personengebundenen Daten erhoben wurden oder denen der Betroffene nachträglich zugestimmt hat. Macht ein Beschäftigter von seinem Recht Gebrauch, die Erlaubnis zu versagen, darf das keine Minderung seiner Berufschancen und keine Sanktionen gegen ihn zur Folge haben.
- ii. Es ist darauf hinzuweisen, dass aufgrund einiger allgemeingültiger Bedingungen für die Übermittlung von Daten durch bestimmte EU-Mitgliedstaaten die Nutzung der Daten für andere Zwecke auch nach der Übermittlung in Länder außerhalb der EU ausgeschlossen werden kann; solche Bedingungen müssen eingehalten werden.
- iii. Außerdem ist den individuellen Datenschutzbedürfnissen der Arbeitnehmer angemessen Rechnung zu tragen. Auf Wunsch könnte etwa der Zugriff auf bestimmte personenbezogene Daten beschränkt werden oder Daten könnten anonymisiert oder Codes/Pseudonymen zugeordnet werden, wenn der tatsächliche Name für den vorgesehenen Zweck nicht benötigt wird.
- iv. Die Organisation ist in dem Maß und so lange von der Pflicht zur Information und zur Beachtung der Wahlmöglichkeit befreit, wie es für Beförderungen, Ernennungen und ähnliche Personalentscheidungen notwendig ist.

c. Anwendung des Auskunftsrechts

- i. Im Zusatzgrundsatz „Auskunftsrecht“ wird ausgeführt, aus welchen Gründen der Zugang zu Personaldaten beschränkt oder

verwehrt werden kann. Selbstverständlich müssen Arbeitgeber in der Europäischen Union Arbeitnehmern aus der EU nach den Rechtsvorschriften ihres Landes Zugang zu Personaldaten gewähren, unabhängig davon, wo diese Daten verarbeitet oder gespeichert werden. Nach den Grundsätzen des Datenschutzschildes muss eine Organisation, die solche Daten in den USA verarbeitet, diesen Zugang direkt oder unter Einschaltung des EU-Arbeitgebers gewährleisten.

d. Rechtsdurchsetzung

- i. Soweit personenbezogene Daten nur im Rahmen des Beschäftigungsverhältnisses verwendet werden, bleibt gegenüber dem Arbeitnehmer in erster Linie die in der EU ansässige Organisation verantwortlich. Folglich ist ein europäischer Arbeitnehmer, der gegen die Verwendung der ihn betreffenden Daten Beschwerde erhoben hat (organisationsintern, bei einer externen Stelle oder nach einem tarifvertraglich vorgesehenen Verfahren) und mit dem Ergebnis nicht zufrieden ist, an den zuständigen Datenschutzbeauftragten oder die für arbeitsrechtliche Fragen zuständige Behörde des Landes zu verweisen, in dem er beschäftigt ist. Das gilt auch, wenn für den als unzulässig betrachteten Umgang mit den personenbezogenen Daten die US-Organisation verantwortlich ist, die die Informationen von dem Arbeitgeber erhalten hat, und somit ein Verstoß gegen die Grundsätze des Datenschutzschildes vorliegt. So lässt sich am ehesten klären, wie die einander überschneidenden Bestimmungen des Arbeitsrechts, der Tarifverträge und des Datenschutzrechts miteinander in Einklang zu bringen sind.
- ii. Eine auf die Grundsätze des Datenschutzschildes verpflichtete amerikanische Organisation, die Personaldaten, die im Rahmen eines Beschäftigungsverhältnisses aus der Europäischen Union übermittelt wurden, verwendet und wünscht, dass auf solche Übermittlungen die Grundsätze des Datenschutzschildes angewandt werden, muss sich also verpflichten, gegebenenfalls bei Untersuchungen der in der EU jeweils zuständigen Behörden mitzuwirken und deren Empfehlungen zu befolgen.

e. Anwendung des Grundsatzes der Verantwortlichkeit für die Weitergabe

- i. Bei gelegentlichen beschäftigungsbezogenen operativen Erfordernissen der dem Datenschutzschild angehörenden Organisation im Hinblick auf im Rahmen des Datenschutzschildes übertragene personenbezogene Daten, wie z. B. die Buchung von Flügen, Hotelzimmern oder den Abschluss von Versicherungen, kann die Übertragung personenbezogener Daten einer geringen Zahl von Arbeitnehmern an für die Verarbeitung Verantwortliche ohne Anwendung des Auskunftsrechtgrundsatzes oder Abschluss

eines Vertrags mit dem als für die Verarbeitung Verantwortlicher tätigen Dritten erfolgen, wie es ansonsten entsprechend dem Grundsatz der Verantwortlichkeit für die Weitergabe notwendig wäre, vorausgesetzt, die dem Datenschutzschild angehörende Organisation hat die Grundsätze der Informationspflicht und der Wahlmöglichkeit eingehalten.

10. Obligatorische Verträge bei Weitergabe

a. Datenverarbeitung im Auftrag

- i. Wenn personenbezogene Daten aus der EU in den USA im Auftrag verarbeitet werden sollen, muss dafür ein Vertrag geschlossen werden unabhängig davon, ob der Auftragsverarbeiter der Vereinbarung zum Datenschutzschild beigetreten ist oder nicht.
- ii. Werden Daten lediglich zur Verarbeitung im Auftrag übermittelt, muss der in der Europäischen Union für die Verarbeitung Verantwortliche darüber stets einen Vertrag schließen, gleich ob die Verarbeitung in oder außerhalb der EU stattfindet und ob der Auftragsverarbeiter dem Datenschutzschild angehört oder nicht. Mit dem Vertrag soll sichergestellt werden, dass der Auftragsverarbeiter
 1. nur auf Weisung des für die Verarbeitung Verantwortlichen handelt;
 2. die geeigneten technischen und organisatorischen Mittel bereitstellt, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang erforderlich sind und weiß, ob eine Weitergabe zulässig ist;
 3. unter Berücksichtigung der Art der Verarbeitung den für die Verarbeitung Verantwortlichen dabei unterstützt, auf Privatpersonen einzugehen, die ihre Rechte im Rahmen der Grundsätze wahrnehmen.
- iii. Da die dem Datenschutzschild angehörenden Organisationen einen angemessenen Schutz gewähren, ist bei reinen Verarbeitungsverträgen mit diesen Organisationen keine vorherige Genehmigung erforderlich (oder die Genehmigung wird von dem jeweiligen EU-Mitgliedstaat automatisch erteilt), wie sie bei Verträgen mit Empfängern, die sich nicht auf die Grundsätze des Datenschutzschilds verpflichtet haben bzw. nicht auf andere Weise einen angemessenen Schutz bieten, erforderlich wäre.

- b. Datenübermittlung innerhalb einer kontrollierten Gruppe von Unternehmen
 - i. Werden personengebundene Daten zwischen zwei für die Verarbeitung Verantwortlichen innerhalb einer kontrollierten Gruppe von Unternehmen übermittelt, ist ein Vertrag nach dem Grundsatz der Vertraulichkeit der Weitergabe nicht immer erforderlich. Für die Verarbeitung Verantwortliche innerhalb einer kontrollierten Gruppe von Unternehmen können für diese Übermittlungen andere Instrumente zugrunde legen, wie z. B. verbindliche unternehmensinterne Vorschriften der EU oder andere konzerninterne Instrumente (z. B. Compliance- und Kontrollprogramme), um die Kontinuität des Schutzes personenbezogener Daten im Rahmen der Grundsätze zu sichern. Bei einer derartigen Übermittlung bleibt die dem Datenschutzschild angehörende Organisation für die Einhaltung der Grundsätze verantwortlich.

- c. Datenübermittlung zwischen für die Verarbeitung Verantwortlichen
 - i. Bei der Übermittlung von Daten zwischen für die Verarbeitung Verantwortlichen muss der Empfänger keine dem Datenschutzschild angehörende Organisation sein oder über eine unabhängige Beschwerdestelle verfügen. Die dem Datenschutz angehörende Organisation muss einen Vertrag mit dem empfangenden externen für die Verarbeitung Verantwortlichen schließen, der das gleiche Schutzniveau wie im Rahmen des Datenschutzschilds vorsieht, wobei es nicht erforderlich ist, dass der als für die Verarbeitung Verantwortlicher tätige Dritte eine dem Datenschutzschild angehörende Organisation ist oder über eine unabhängige Beschwerdestelle verfügen muss, vorausgesetzt, er stellt ein gleichwertiges Beschwerdeverfahren zur Verfügung.

11. Beschwerdeverfahren und Durchsetzung

- a. Im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung ist festgelegt, wie dem Datenschutzschild Geltung zu verschaffen ist. Wie Punkt a)ii) des Grundsatzes zu entsprechen ist, wird im Zusatzgrundsatz „Anlassunabhängige Kontrolle“ ausgeführt. Der vorliegende Zusatzgrundsatz befasst sich mit den Punkten a)i) und a)iii), die beide die Forderung nach unabhängigen Beschwerdestellen enthalten. Das Beschwerdeverfahren kann auf verschiedene Weise ausgestaltet werden, es muss aber die im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung genannten Anforderungen erfüllen. Organisationen erfüllen die Anforderungen wie folgt: i) indem sie von der Privatwirtschaft entwickelte Datenschutzprogramme befolgen, in deren Regeln die Grundsätze des Datenschutzschilds integriert sind und die wirksame

Durchsetzungsmechanismen vorsehen, wie sie im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung beschrieben sind; ii) indem sie sich gesetzlich oder durch Rechtsverordnung vorgesehenen Kontrollorganen unterwerfen, die Beschwerden von Einzelpersonen nachgehen und Streitigkeiten schlichten; iii) indem sie sich verpflichten, mit den Datenschutzbehörden in der Europäischen Union oder mit deren bevollmächtigten Vertretern zusammenzuarbeiten.

- b. Die hier angeführten Möglichkeiten sind Beispiele, es handelt sich nicht um eine abschließende Aufzählung. Die Privatwirtschaft kann auch andere Durchsetzungsmechanismen einführen, sie müssen nur die Forderungen erfüllen, die im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung und in den Zusatzgrundsätzen niedergelegt sind. Zu beachten ist, dass die Forderungen des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung die Forderung ergänzen, wonach auch bei freiwilliger Selbstkontrolle Verstöße gegen die Grundsätze gemäß § 5 des Federal Trade Commission Act oder einem ähnlichen Gesetz verfolgbar sein müssen.
- c. Um die Einhaltung ihrer Verpflichtungen im Rahmen des Datenschutzschildes zu gewährleisten und die Verwaltung des Programms zu unterstützen, müssen Organisationen sowie deren unabhängige Beschwerdestellen dem Ministerium auf Anfrage Informationen zum Datenschutzschild übermitteln. Darüber hinaus müssen die Organisationen umgehend auf von den Datenschutzbehörden über das Ministerium an sie weitergeleitete Beschwerden bezüglich ihrer Einhaltung der Grundsätze antworten. In der Antwort soll darauf eingegangen werden, ob die Beschwerde begründet ist, und wenn ja, wie die Organisation den Missstand zu beheben gedenkt. Das Ministerium wird die Vertraulichkeit der bei ihm eingegangenen Informationen gemäß dem US-Recht wahren.
- d. Anrufung unabhängiger Beschwerdestellen
 - i. Die Verbraucher sollen dazu angehalten werden, Beschwerden zunächst an die Organisation zu richten, die ihre Daten verarbeitet, ehe sie eine unabhängige Beschwerdestelle anrufen. Organisationen müssen dem Verbraucher innerhalb von 45 Tagen nach Eingang einer Beschwerde antworten. Die Unabhängigkeit einer Beschwerdestelle ist an verschiedenen Merkmalen erkennbar wie Unparteilichkeit, transparente Besetzung und Finanzierung oder nachweisbare einschlägige Tätigkeit. Wie im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung gefordert, müssen einem Beschwerdeführer kostenlose Rechtsbehelfe ohne Weiteres zur Verfügung stehen. Eine Beschwerdestelle muss jede von einer Einzelperson vorgetragene Beschwerde prüfen, es sei denn, sie ist offensichtlich unbegründet oder nicht ernsthaft. Der Betreiber der Beschwerdestelle kann allerdings Kriterien für die

Zulässigkeit von Beschwerden festlegen. Diese Kriterien sollen transparent und einsichtig sein (z. B. Ausschluss von Beschwerden, die nicht unter das jeweilige Datenschutzprogramm fallen oder die in die Zuständigkeit einer anderen Stelle fallen) und sollen nicht zu einer Lockerung der Pflicht führen, berechtigten Beschwerden nachzugehen. Beschwerdestellen sollen Beschwerdeführer zudem umfassend und in leicht zugänglicher Form über den Ablauf des Verfahrens informieren. Zu diesen Informationen gehören auch Angaben über die Datenschutzpraxis der Beschwerdestelle im Einklang mit den Grundsätzen des Datenschutzschildes. Ferner sind die Stellen gehalten, sich an der Erarbeitung von Hilfsmitteln, die das Verfahren vereinfachen, wie z. B. Standardformularen für Beschwerden, zu beteiligen.

- ii. Unabhängige Beschwerdestellen müssen auf ihren öffentlichen Websites Informationen zu den Grundsätzen des Datenschutzschildes und zu den von ihnen in diesem Rahmen erbrachten Dienstleistungen veröffentlichen. Diese Informationen müssen Folgendes umfassen: 1) Angaben über die Anforderungen an unabhängige Beschwerdestellen in den Grundsätzen des Datenschutzschildes oder einen Link zu diesen Anforderungen; 2) einen Link zur Datenschutzschild-Website des Ministeriums; 3) einen Hinweis, dass das Beschwerdeverfahren im Rahmen des Datenschutzschildes für Privatpersonen kostenlos ist; 4) eine Beschreibung, wie eine Beschwerde im Zusammenhang mit dem Datenschutzschild eingereicht werden kann; 5) Bearbeitungsfristen für Beschwerden im Zusammenhang mit dem Datenschutzschild; 6) eine Beschreibung der Palette möglicher Abhilfemaßnahmen.
- iii. Die unabhängigen Beschwerdestellen müssen alljährlich einen Bericht vorlegen, der zusammengefasste statistische Angaben zu ihren Dienstleistungen beinhaltet. Der Jahresbericht muss folgende Angaben enthalten: 1) die Gesamtzahl der im Berichtsjahr eingegangenen Beschwerden, die den Datenschutzschild betreffen; 2) die eingegangenen Beschwerden nach Kategorien; 3) qualitative Angaben zur Streitbeilegung, z. B. die Bearbeitungsdauer von Beschwerden; 4) die Ergebnisse der eingegangenen Beschwerden, namentlich Anzahl und Art der verfügbaren Abhilfemaßnahmen oder Sanktionen.
- iv. Wie in Anlage I ausgeführt, steht Privatpersonen ein Schiedsverfahren offen, anhand dessen bei Restansprüchen festgestellt wird, ob eine dem Datenschutzschild angehörende Organisation ihre Pflichten im Rahmen der Grundsätze gegenüber der betreffenden Person verletzt hat und ob diese Verletzung vollständig oder teilweise ungeahndet bleibt. Diese Option steht

nur für diese Zwecke zur Verfügung, nicht jedoch beispielsweise bei den geregelten Abweichungen von den Grundsätzen⁵ oder im Hinblick auf eine Behauptung zur Angemessenheit des Datenschutzschildes. Im Rahmen dieses Schiedsverfahrens ist das Datenschutzschild-Panel (bestehend aus einem oder drei von den Parteien ausgewählten Schiedsrichtern) befugt, einzelfallabhängige nichtmonetäre billigkeitsrechtliche Ansprüche (wie z. B. Zugang, Korrektur, Löschung oder Rückgabe der betreffenden Daten der Person) anzuerkennen, um die Verstöße gegen die Grundsätze abzustellen. Privatpersonen und dem Datenschutzschild angehörende Organisationen können eine gerichtliche Überprüfung und Durchsetzung der Schiedsentscheidungen nach US-Recht gemäß Federal Arbitration Act beantragen.

e. Rechtsbehelfe und Sanktionen

- i. Die Inanspruchnahme eines Rechtsbehelfs soll dazu führen, dass die Organisation, gegen die sich die Beschwerde richtet, die Folgen ihres Verstoßes gegen die Grundsätze soweit möglich abstellt oder rückgängig macht und die den Beschwerdeführer betreffenden Daten künftig entweder im Einklang mit den Grundsätzen schützt oder nicht mehr verarbeitet. Sanktionen müssen so empfindlich sein, dass sie die Einhaltung der Grundsätze gewährleisten. Den Beschwerdestellen stehen Sanktionen von abgestufter Strenge zur Verfügung, mit denen sie gegen Verstöße von unterschiedlicher Schwere angemessen vorgehen können. Als Sanktionen kommen in Frage die öffentliche Bekanntmachung des Verstoßes, in bestimmten Fällen die Anordnung der Löschung der betreffenden Daten⁶, der vorübergehende oder dauernde Entzug der Zugehörigkeit zur Zuständigkeit einer Beschwerdestelle, Entschädigungen für Personen, denen durch die Nichteinhaltung der Grundsätze ein Schaden entstanden ist, und Auflagen. Beschwerdestellen und Einrichtungen der freiwilligen Selbstkontrolle des privaten Sektors müssen bei Missachtung ihrer Entscheidungen die Gerichte anrufen oder die zuständige entscheidungsbefugte Behörde verständigen und das Ministerium unterrichten.

f. Befassung der FTC

- ii. Die FTC will Beschwerden wegen Verletzung der Grundsätze, die an sie verwiesen wurden i) von Einrichtungen der Selbstkontrolle

⁵ Abschnitt I.5 der Grundsätze.

⁶ Beschwerdestellen können Sanktionen nach eigenem Ermessen verhängen. Die Sensibilität der Daten ist ein maßgebendes Kriterium, wenn zu entscheiden ist, ob Daten zu löschen sind oder ob eine Organisation mit der Erhebung, Nutzung oder Weitergabe von Daten die Grundsätze des Datenschutzschildes in eklatanter Weise verletzt hat.

für den Datenschutz und anderen unabhängigen Beschwerdestellen, ii) von EU-Mitgliedstaaten, iii) vom Ministerium, vorrangig behandeln und feststellen, ob gegen § 5 des FTC Act verstoßen wurde, der unlautere und irreführende Geschäftspraktiken verbietet. Hat die FTC Grund zu der Annahme, dass ein solcher Verstoß vorliegt, kann sie eine behördliche Anordnung erwirken, die die beanstandete Praxis untersagt, oder sie kann vor einem Bezirksgericht klagen. Entscheidet das Gericht in ihrem Sinne, kann ein Bundesgericht eine Anordnung mit gleicher Wirkung erlassen. Dazu gehören falsche Angaben zur Einhaltung der Grundsätze des Datenschutzschildes oder zur Beteiligung am Datenschutzschild von Organisationen, die entweder nicht mehr auf der Datenschutzschild-Liste stehen oder nie eine Selbstzertifizierung gegenüber dem Ministerium abgegeben haben. Gegen die Missachtung einer behördlichen Unterlassungsanordnung kann die FTC Geldstrafen verhängen; gegen die Missachtung der Anordnung eines Bundesgerichts kann sie zivil- und strafrechtlich vorgehen. Die FTC unterrichtet das Ministerium über von ihr unternommene Schritte. Andere Behörden sind angehalten, dem Ministerium das abschließende Ergebnis in solchen Fällen und sonstige Entscheidungen über die Beachtung der Grundsätze des Datenschutzschildes mitzuteilen.

g. Fortgesetzte Missachtung der Grundsätze

- i. Missachtet eine Organisation fortgesetzt die Grundsätze, verliert sie die mit dem Datenschutzschild verbundenen Vorteile. Organisationen, die fortwährend gegen die Grundsätze verstoßen haben, werden vom Ministerium von der Datenschutzschild-Liste gestrichen und müssen die im Rahmen des Datenschutzschildes empfangenen personenbezogenen Daten zurückgeben oder löschen.
- ii. Eine fortgesetzte Missachtung liegt vor, wenn sich eine Organisation, die sich gegenüber dem Ministerium selbst zertifiziert hat, weigert, der endgültigen Entscheidung einer Einrichtung der freiwilligen Selbstkontrolle, einer unabhängigen Beschwerdestelle oder eines staatlichen Kontrollorgans zu folgen, oder wenn von einer solchen Stelle festgestellt wird, dass die Organisation so häufig gegen die Grundsätze verstößt, die es einzuhalten vorgibt, dass diese Behauptung nicht mehr glaubwürdig ist. In diesen Fällen muss die Organisation das dem Ministerium unverzüglich mitteilen. Die Unterlassung dieser Mitteilung kann nach dem False Statements Act strafrechtlich verfolgt werden (18 U.S.C § 1001). Beteiligt sich eine Organisation nicht mehr an einem Programm der freiwilligen Selbstkontrolle für den Datenschutz oder an der unabhängigen

Streitbeilegung, liegt eine fortgesetzte Missachtung der Grundsätze vor, da die Verpflichtung zur Einhaltung fortbesteht.

- iii. Bei Eingang einer Mitteilung über die fortgesetzte Missachtung der Grundsätze wird das Ministerium die betreffende Organisation von der Datenschuttschild-Liste streichen, unabhängig davon, ob die Mitteilung durch die Organisation selbst, durch eine Einrichtung der freiwilligen Selbstkontrolle für den Datenschutz bzw. eine andere unabhängige Beschwerdestelle oder durch ein staatliches Kontrollorgan erfolgt. Das geschieht jedoch erst, nachdem die 30-tägige Frist abgelaufen ist, in der die betroffene Organisation Gelegenheit hat zu reagieren. Aus der Datenschuttschild-Liste des Ministeriums lässt sich also ersehen, welche Organisationen als Beteiligte am Datenschuttschild anerkannt sind und welche diese Anerkennung verloren haben.
- iv. Eine Organisation, die sich einer Einrichtung der freiwilligen Selbstkontrolle anschließt, um sich erneut für den Datenschuttschild zu qualifizieren, muss dieser Einrichtung ihre frühere Teilnahme am Datenschuttschild vollständig offenbaren.

12. Wahlmöglichkeit – Zeitpunkt des Widerspruchs

- a. Allgemein soll der Grundsatz der Wahlmöglichkeit gewährleisten, dass personenbezogene Daten in einer Weise genutzt und weitergegeben werden, die mit den Erwartungen und Entscheidungen des Betroffenen übereinstimmt. Dementsprechend sollte der Betroffene zu jeder Zeit entscheiden können, ob seine personenbezogenen Daten für das Direktmarketing verwendet werden dürfen oder nicht; hierfür können die Organisationen aber eine angemessene Frist festlegen, die sie zur effektiven Berücksichtigung eines Widerspruchs („Opt-out“) benötigen. Daneben kann die Organisation hinreichende Informationen anfordern, die die Identität der Person bestätigen, die Widerspruch einlegt. In den Vereinigten Staaten können Betroffene von der Wahlmöglichkeit Gebrauch machen, indem sie auf ein zentrales „Widerspruchsprogramm“ zurückgreifen, wie dem Mail Preference Service der Direct Marketing Association. Organisationen, die an dem Mail Preference Service teilnehmen, sollten Verbraucher, die keine kommerziellen Informationen erhalten möchten, auf diesen Dienst hinweisen. Auf jeden Fall sollte den Betroffenen ein leicht zugänglicher und erschwinglicher Mechanismus zur Verfügung gestellt werden, um diese Möglichkeit nutzen zu können.
- b. Gleichmaßen kann eine Organisation Daten für bestimmte Zwecke des Direktmarketing verwenden, wenn es unmöglich ist, dem Betroffenen vor Nutzung der Daten eine Widerspruchsmöglichkeit einzuräumen, sofern die Organisation dem Betroffenen unmittelbar danach (und auf Verlangen jederzeit) die Möglichkeit einräumt, den Erhalt weiterer Direktwerbung

(ohne Kosten für den Verbraucher) abzulehnen, und die Organisation den Wünschen des Betroffenen nachkommt.

13. Reisedaten

- a. Flugreservierungsdaten und andere Reisedaten wie Daten über Vielflieger, über Hotelreservierungen und über spezielle Bedürfnisse wie religiös begründete besondere Speisewünsche oder die Notwendigkeit pflegerischer Betreuung dürfen in bestimmten Fällen an Organisationen außerhalb der EU weitergegeben werden. Nach Artikel 26 der Richtlinie dürfen personenbezogene Daten in ein Drittland übermittelt werden, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, wenn i) die Übermittlung für die Erfüllung eines Vertrags wie der Vielflieger-Vereinbarung notwendig ist oder ii) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat. US-Organisationen, die sich den Grundsätzen des Datenschutzschildes angeschlossen haben, gewährleisten einen angemessenen Schutz personenbezogener Daten und können deshalb solche Daten aus der EU empfangen, ohne dass diese Voraussetzungen oder die in Artikel 26 der Datenschutzrichtlinie genannten Voraussetzungen erfüllt sein müssen. Da das Konzept des Datenschutzschildes besondere Regeln für den Umgang mit sensiblen Daten vorsieht, können auch solche Daten (die etwa für die pflegerische Betreuung eines Kunden benötigt werden) an Organisationen übermittelt werden, die am Datenschutzschild teilnehmen. Allerdings ist die übermittelnde Organisation stets dem Recht des EU-Mitgliedstaats unterworfen, in dem sie tätig ist, und das kann unter anderem bedeuten, dass sie im Umgang mit sensiblen Daten besondere Vorschriften zu beachten hat.

14. Arzneimittel und Medizinprodukte

- a. Anwendung des Rechts der EU-Mitgliedstaaten oder der Grundsätze des Datenschutzschildes
 - i. Das Recht der EU-Mitgliedstaaten gilt für die Erhebung der personenbezogenen Daten und für ihre Verarbeitung vor der Übermittlung in die USA. Die Grundsätze des Datenschutzschildes gelten, nachdem die Daten in die USA übermittelt worden sind. Daten, die für die pharmazeutische Forschung oder sonstige Zwecke benutzt werden, sollten gegebenenfalls anonymisiert werden.
- b. Künftige Forschungsarbeiten
 - i. In medizinischen und pharmazeutischen Studien gewonnene personenbezogene Daten sind oft sehr wertvoll für künftige Forschungsarbeiten. Wenn für ein Forschungsvorhaben erhobene personenbezogene Daten an eine dem Datenschutzschild

beigetrete US-Organisation übermittelt werden, darf die Organisation diese Daten für ein anderes Forschungsvorhaben verwenden, wenn das dem Betroffenen schon zu Anfang ordnungsgemäß mitgeteilt und wenn ihm eine Wahlmöglichkeit eingeräumt wurde. Eine Mitteilung muss Angaben über die künftige Verwendung der Daten enthalten wie Angaben über regelmäßige Folgeuntersuchungen, ähnliche Forschungsvorhaben, für die sie verwendet werden sollen, oder ihre kommerzielle Nutzung.

- ii. Es versteht sich, dass dabei nicht jede künftige Verwendung der Daten angegeben werden kann. Die Verwendung für einen anderen Forschungszweck kann sich aus neuen Erkenntnissen über die ursprünglichen Daten, aus neuen medizinischen Entdeckungen und Fortschritten sowie aus Entwicklungen im Gesundheitswesen und in der Gesetzgebung ergeben. Gegebenenfalls ist in der Mitteilung darauf hinzuweisen, dass personenbezogene Daten für künftige medizinische und pharmazeutische Forschungsarbeiten verwendet werden können, die nicht vorauszusehen sind. Entspricht die neue Verwendung nicht dem allgemeinen Forschungszweck, für den die personenbezogenen Daten ursprünglich erhoben wurden oder in den der Betroffene später eingewilligt hat, muss erneut seine Einwilligung eingeholt werden.

c. Rückzug aus einem klinischen Versuch

- i. Ein Teilnehmer kann sich jederzeit aus einem klinischen Versuch zurückziehen oder dazu aufgefordert werden. Personenbezogene Daten, die vor seinem Rückzug erhoben wurden, können jedoch weiterhin verarbeitet werden wie die übrigen im Rahmen des Versuchs erhobenen Daten, wenn er darauf hingewiesen wurde, als er seine Bereitschaft zur Teilnahme erklärte.

d. Übermittlung von Daten an Aufsichtsbehörden zur Überprüfung

- i. Hersteller von Arzneimitteln und Medizinprodukten dürfen in klinischen Versuchen in der EU gewonnene personenbezogene Daten zur Überprüfung an Aufsichtsbehörden in den USA übermitteln. Unter Beachtung der Grundsätze der Informationspflicht und der Wahlmöglichkeit dürfen sie die Daten auch an andere Stellen wie Organisationen und Wissenschaftler übermitteln.

e. Blindversuche

- i. Zur Wahrung der Objektivität dürfen bei klinischen Versuchen die Teilnehmer und oft auch die Forscher selbst nicht erfahren, wer wie behandelt wird, denn das würde die Aussagefähigkeit der Ergebnisse in Frage stellen. Teilnehmern an solchen sogenannten Blindversuchen muss kein Zugang zu Daten über ihre Behandlung

während des Versuchs gewährt werden, wenn ihnen diese Beschränkung vor ihrer Teilnahme erklärt wurde und die Offenlegung der Daten den Nutzen der Forschungsarbeit gefährden würde.

- ii. Wer sich dennoch zur Teilnahme an dem Versuch entschließt, muss hinnehmen, dass die ihn betreffenden Daten unter Verschluss gehalten werden. Nach Abschluss des Versuchs und Auswertung der Ergebnisse müssen die Teilnehmer allerdings auf Verlangen Zugang zu ihren Daten erhalten. Dafür sollten sie sich in erster Linie an den Arzt oder an anderes medizinisches Personal wenden, von dem sie während des Versuchs behandelt wurden, hilfsweise an die Organisation, in deren Auftrag der Versuch durchgeführt wurde.

f. Überwachung der Sicherheit und Wirksamkeit von Produkten

- i. Wenn ein Hersteller von Arzneimitteln oder Medizinprodukten Maßnahmen zur Überwachung der Sicherheit und Wirksamkeit seiner Produkte trifft und u. a. über Zwischenfälle berichtet und laufend Daten über Patienten/Versuchspersonen erhebt, die bestimmte Arzneimittel oder Medizinprodukte nutzen, muss er die im Datenschutzschild verankerten Grundsätze der Informationspflicht, der Wahlmöglichkeit, der Weiterübermittlung und des Auskunftsrechts nicht beachten, soweit die Grundsätze mit gesetzlichen Pflichten kollidieren. Das gilt sowohl für Berichte von Dienstleistern des Gesundheitswesens an Arzneimittel- und Medizinprodukthersteller als auch für Berichte von Arzneimittel- und Medizinproduktherstellern an Behörden wie die amerikanische Food and Drug Administration.

g. Verschlüsselte Daten

- i. Forschungsdaten werden stets an der Quelle verschlüsselt, damit aus ihnen nicht die Identität einzelner Personen zu ersehen ist. Den Pharmaorganisationen, also den Projektträgern, wird der Schlüssel nicht ausgehändigt, er verbleibt beim Forscher, so dass er unter bestimmten Umständen (z. B. wenn eine nachträgliche Überwachung notwendig ist) einzelne Versuchspersonen identifizieren kann. Die Übermittlung derart verschlüsselter Daten von der EU in die USA ist nicht als Übermittlung personenbezogener Daten anzusehen, die den Grundsätzen des Datenschutzschildes unterliegt.

15. Daten aus öffentlichen Registern und öffentlich zugängliche Daten

- a. Eine Organisation muss die im Datenschutzschild verankerten Grundsätze der Sicherheit, Datenintegrität und Zweckbindung sowie des Rechtsschutzes, der Durchsetzung und der Haftung auf personenbezogene Daten aus öffentlich zugänglichen Quellen anwenden. Diese Grundsätze gelten auch für personenbezogene Daten, die aus öffentlichen Datenbeständen erhoben werden, d. h. aus Datenbeständen, die von Ämtern aller Ebenen geführt werden und der Öffentlichkeit zur Einsichtnahme offen stehen.
- b. Die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Verantwortlichkeit für die Weitergabe sind nicht auf Daten in öffentlichen Registern anzuwenden, wenn diese nicht mit nichtöffentlichen Daten kombiniert sind und solange die von der zuständigen Behörde festgelegten Bedingungen für ihre Abfrage beachtet werden. Im Allgemeinen gelten die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Verantwortlichkeit für die Weitergabe auch nicht für öffentlich verfügbare Daten, es sei denn, der europäische Übermittler weist darauf hin, dass diese Daten Beschränkungen unterliegen, aufgrund derer die Organisation die genannten Grundsätze im Hinblick auf die von ihr geplanten Verwendung anwenden muss. Organisationen haften nicht dafür, wie diese Daten von denen genutzt werden, die sie aus veröffentlichtem Material entnommen haben.
- c. Wird festgestellt, dass eine Organisation unter Missachtung der Grundsätze absichtlich personenbezogene Daten offengelegt hat, so dass diese Ausnahme von der Regel für die Organisation selbst oder aber für andere von Nutzen ist, verliert sie ihre Vorteile aufgrund des Datenschutzschilds.
- d. Das Auskunftsrecht gilt für Daten in öffentlichen Registern nur, wenn sie mit anderen personenbezogenen Daten kombiniert sind (außer bei kleinen Mengen, die verwendet wurden, um die öffentlichen Daten zu indexieren oder zu ordnen). Die Bestimmungen der einschlägigen Rechtsvorschriften über die Einsichtnahme in Datenbestände sind jedoch einzuhalten. Sind dagegen Daten aus öffentlichen Beständen mit anderen als den genannten Datenmengen aus nichtöffentlichen Quellen kombiniert, muss die Organisation Zugang zu allen personenbezogenen Daten gewähren, sofern nicht einer der genannten Ausnahmefälle vorliegt.
- e. Wie bei Daten, die aus öffentlichen Beständen gewonnen wurden, ist das Auskunftsrecht nicht auf Daten anzuwenden, die bereits der Öffentlichkeit zur Verfügung stehen, sofern sie mit nicht öffentlich verfügbaren Daten kombiniert sind. Organisationen, die öffentlich zugängliche Information gegen Entgelt anbieten, können ihre üblichen Gebühren erheben. Alternativ können Personen Zugang zu sie betreffenden Daten von der Organisation verlangen, die sie ursprünglich erhoben hat.

16. Anträge von Behörden auf Datenzugriff

- a. Um für Transparenz bei rechtmäßige Anträgen von Behörden auf Zugang zu personenbezogenen Daten zu sorgen, können dem Datenschuttschild angehörende Organisationen freiwillig in regelmäßigen Abständen Transparenzberichte über die Anzahl der Anträge von Behörden auf Datenzugriff aus Gründen der Strafverfolgung oder nationalen Sicherheit veröffentlichen, soweit diese Offenlegungen nach geltendem Recht zulässig sind.
- b. Die von den Organisationen in diesen Berichten aufgeführten Angaben können zusammen mit veröffentlichten nachrichtendienstlichen sowie mit sonstigen Informationen in die gemeinsame jährliche Überprüfung der Funktionsweise des Datenschuttschilds im Einklang mit den Grundsätzen einfließen.
- c. Auch wenn keine Information gemäß Punkt a)xii) des Grundsatzes der Informationspflicht erfolgt ist, behindert oder beeinträchtigt dies nicht die Möglichkeiten einer Organisation, rechtmäßigen Anfragen nachzukommen.

ANLAGE I: SCHIEDSMODELL

In dieser Anlage I sind die Bedingungen aufgeführt, unter denen dem Datenschutz angehörende Organisationen zur Behandlung von Ansprüchen im Schiedsverfahren nach dem Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung verpflichtet sind. Die im Folgenden beschriebene Möglichkeit des verbindlichen Schiedsverfahrens bezieht sich auf bestimmte „Restansprüche“ in Bezug auf Daten, die unter den EU-US-Datenschutzschild fallen. Damit soll Privatpersonen ein zeitnaher, unabhängiger und fairer Mechanismus bereitgestellt werden, der sich mit geltend gemachten Verstößen gegen die Grundsätze befasst, die nicht von einem der gegebenenfalls in Anspruch genommenen anderen Mechanismen des Datenschutzschilds geklärt werden könnten.

A. Anwendungsbereich

Mit dem Schiedsverfahren können Privatpersonen bei Restansprüchen feststellen lassen, ob eine dem Datenschutzschild angehörende Organisation ihre Pflichten im Rahmen der Grundsätze gegenüber der betreffenden Person verletzt hat und ob diese Verletzung vollständig oder teilweise ungeahndet bleibt. Diese Option steht nur für diese Zwecke zur Verfügung, nicht jedoch beispielsweise bei den geregelten Abweichungen von den Grundsätzen⁷ oder im Hinblick auf eine Behauptung zur Angemessenheit des Datenschutzschilds.

B. Verfügbare Abhilfemaßnahmen

Im Rahmen dieses Schiedsverfahrens ist das Datenschutzschild-Panel (bestehend aus einem oder drei von den Parteien ausgewählten Schiedsrichtern) befugt, einzelfallabhängige nichtmonetäre billigkeitsrechtliche Ansprüche (wie z. B. Zugang, Korrektur, Löschung oder Rückgabe der betreffenden Daten der Person) anzuerkennen, um die Verstöße gegen die Grundsätze abzustellen. Dieses sind die einzigen Befugnisse des Schiedsforums in Bezug auf Abhilfemaßnahmen. Bei der Prüfung von Abhilfemaßnahmen muss das Schiedsforum andere bereits von anderen Mechanismen im Rahmen des Datenschutzschilds verhängte Abhilfemaßnahmen berücksichtigen. Schadenersatz, Kosten, Gebühren oder andere derartige Maßnahmen sind nicht verfügbar. Jede Partei muss selbst für die anfallenden Anwaltsgebühren aufkommen.

C. Voraussetzungen für das Schiedsverfahren

Wer das Schiedsverfahren in Anspruch nehmen möchte, muss vor der Einleitung einer Schiedsklage 1) den behaupteten Verstoß direkt bei der Organisation geltend machen und der Organisation Gelegenheit geben, die Angelegenheit innerhalb der in Abschnitt III.11 d)i) der Grundsätze aufgeführten Frist zu klären, 2) das kostenlose unabhängige Beschwerdeverfahren im Rahmen der Grundsätze in Anspruch nehmen und 3) die Angelegenheit kostenlos über seine zuständige Datenschutzbehörde dem Handelsministerium zuleiten und dem Handelsministerium die Gelegenheit geben, die Angelegenheit nach Möglichkeit innerhalb der im Schreiben der International Trade Administration des Handelsministeriums gesetzten Frist zu klären.

⁷ Abschnitt I.5 der Grundsätze.

Das Schiedsverfahren kann nicht in Anspruch genommen werden, wenn der von der Person geltend gemachte Verstoß 1) bereits Gegenstand eines verbindlichen Schiedsverfahrens war, 2) Gegenstand eines rechtskräftigen Urteils in einem Gerichtsverfahren mit der Person als Prozesspartei war oder 3) von den Parteien bereits geregelt wurde. Darüber hinaus kann das Schiedsverfahren nicht in Anspruch genommen werden, wenn eine EU-Datenschutzbehörde 1) gemäß Abschnitt III.5 oder III.9 der Grundsätze zuständig ist oder 2) befugt ist, den geltend gemachten Verstoß direkt mit der Organisation zu klären. Die Befugnis einer Datenschutzbehörde, den gleichen Anspruch gegen einen für die Verarbeitung Verantwortlichen in der EU geltend zu machen, schließt die Inanspruchnahme des Schiedsverfahrens gegen eine nicht an die Befugnis der Datenschutzbehörde gebundene andere rechtliche Einheit allein nicht aus.

D. Verbindlichkeit von Schiedssprüchen

Die Entscheidung einer Einzelperson, dieses verbindliche Schiedsverfahren in Anspruch zu nehmen, ist vollkommen freiwillig. Die Schiedssprüche sind für alle beteiligten Parteien verbindlich. Mit der Inanspruchnahme verzichtet die betreffende Person auf die Möglichkeit, ein anderes Forum mit der Klärung des geltend gemachten Verstoßes zu befassen; wenn jedoch diesem Verstoß mit der Anerkennung nichtmonetärer Ansprüche nicht vollständig abgeholfen wird, kann die betreffende Person dennoch Schadensersatzansprüche vor Gericht geltend machen.

E. Überprüfung und Durchsetzung

Privatpersonen und dem Datenschutzschild angehörende Organisationen können eine gerichtliche Überprüfung und Durchsetzung der Schiedsentscheidungen nach US-Recht gemäß Federal Arbitration Act beantragen.⁸ Derartige Fälle müssen bei dem Bundesbezirksgericht

⁸ In Kapitel 2 des Federal Arbitration Act („FAA“) heißt es: „Eine Schiedsvereinbarung oder ein Schiedsspruch aus einem vertraglichen oder nicht vertraglichen Rechtsverhältnis, das als kommerziell gilt, einschließlich einer Transaktion, eines Vertrages oder einer Vereinbarung nach [§ 2 des FAA], fällt unter das Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche vom 10. Juni 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 („New Yorker Übereinkommen“).“ 9 U.S.C. § 202. Weiter ist im FAA festgelegt: „Eine Schiedsvereinbarung oder ein Schiedsspruch aus einem derartigen Verhältnis, das ausschließlich zwischen Bürgern der Vereinigten Staaten besteht, fällt nur dann unter das [New Yorker] Übereinkommen, wenn dieses Verhältnis im Ausland befindliche Immobilien umfasst, eine Leistung oder Rechtsdurchsetzung im Ausland anstrebt oder in einer anderweitigen hinreichenden Beziehung zu einem oder mehreren anderen Staaten steht.“ Ebenda. Nach Kapitel 2 kann „jede Partei des Schiedsverfahrens einen Antrag bei einem nach diesem Kapitel zuständigen Gericht auf eine Anordnung zur Bestätigung des Schiedsspruchs gegen eine andere Partei des Schiedsverfahrens stellen. Das Gericht bestätigt den Schiedsspruch, sofern es keinen der Gründe für eine Verweigerung oder einen Aufschub der Anerkennung oder Durchsetzung des Schiedsspruchs gemäß dem besagten [New Yorker] Übereinkommen findet.“ Ebenda § 207. Weiter heißt es in Kapitel 2: „Die Bezirksgerichte der Vereinigten Staaten ... haben ungeachtet des Streitwerts die ursprüngliche Zuständigkeit für ... eine Klage oder ein Verfahren [im Rahmen des New Yorker Übereinkommens]. Ebenda § 203.

Außerdem heißt es in Kapitel 2: „Kapitel 1 gilt für Klagen und Verfahren nach diesem Kapitel, soweit jenes Kapitel nicht mit diesem Kapitel oder dem [New Yorker] Übereinkommen, wie von den Vereinigten Staaten ratifiziert, kollidiert.“ Ebenda § 208. In Kapitel 1 heißt es wiederum: „Eine schriftliche Bestimmung in einem Vertrag über eine geschäftliche Transaktion, wonach ein Streit aufgrund dieses Vertrages oder dieser Transaktion oder die Weigerung, diesen bzw. diese ganz oder teilweise zu erfüllen, im Schiedsverfahren beizulegen ist, oder eine

eingereicht werden, dessen territoriale Zuständigkeit sich auf den Hauptgeschäftsort der dem Datenschutzschild angehörenden Organisation erstreckt.

Mit diesem Schiedsverfahren sollen individuelle Streitigkeiten geklärt werden, und die Schiedsentscheidungen sollen nicht als zur Nachahmung empfohlener oder verbindlicher Präzedenzfall bei Angelegenheiten anderer Parteien dienen, einschließlich bei künftigen Schiedsverfahren oder an Gerichten der EU oder der USA oder in Verfahren der FTC.

F. Das Schiedsforum

Die Parteien wählen die Schiedsrichter aus dem im Folgenden erörterten Verzeichnis der Schiedsrichter aus.

Nach geltendem Recht erstellen das US-Handelsministerium und die Europäische Kommission ein Verzeichnis mit mindestens 20 Schiedsrichtern, die aufgrund ihrer Unabhängigkeit, Integrität und Sachkenntnis ausgewählt werden. Dafür gilt Folgendes:

Die Schiedsrichter

- 1) verbleiben für einen Zeitraum von 3 Jahren in dem Verzeichnis, sofern keine außergewöhnlichen Umstände oder wichtigen Gründe vorliegen; dieser Zeitraum kann um weitere drei Jahre verlängert werden;
- 2) sind gegenüber einer der Parteien oder einer dem Datenschutzschild angehörigen Organisation bzw. gegenüber den USA, der EU oder einem EU-Mitgliedstaat oder einer anderen Regierungsbehörde, öffentlichen Behörde oder Strafverfolgungsbehörde weder weisungsgebunden noch anderweitig verpflichtet;
- 3) müssen als Rechtsanwalt in den USA zugelassen und im US-Privatrecht bewandert sein und Sachkenntnis im EU-Datenschutzrecht aufweisen.

G. Schiedsverfahren

Im Einklang mit dem geltenden Recht vereinbaren das Handelsministerium und die Europäische Kommission innerhalb von 6 Monaten nach Annahme des Angemessenheitsbeschlusses die Übernahme einer Reihe von bestehenden, etablierten US-Schiedsverfahren (wie z. B. AAA oder JAMS) zur Regelung des Verfahrens vor dem Datenschutzschild-Panel, wobei die folgenden Aspekte zugrunde gelegt werden:

1. Eine Person kann vorbehaltlich der vorstehend aufgeführten Voraussetzungen ein verbindliches Schiedsverfahren einleiten, indem sie der Organisation eine Mitteilung zukommen lässt. Die Mitteilung enthält eine Zusammenfassung der gemäß Abschnitt C

schriftliche Vereinbarung, wonach ein bestehender Streit aufgrund dieses Vertrages, dieser Transaktion oder dieser Weigerung an ein Schiedsgericht zu verweisen ist, ist gültig, unwiderruflich und vollstreckbar, sofern nicht Gründe nach Recht oder Billigkeit für den Rücktritt von einem Vertrag vorliegen.“ Ebenda § 2. Weiter heißt es in Kapitel 1: „Jede Partei im Schiedsverfahren kann bei einem angegebenen Gericht eine Anordnung zur Bestätigung des Schiedsspruchs beantragen, woraufhin das Gericht eine derartige Anordnung erlassen muss, sofern der Schiedsspruch nicht gemäß § 10 und 11 des [FAA] aufgegeben, geändert oder korrigiert wird.“ Ebenda § 9.

unternommenen Schritte zur Klärung einer Beschwerde, eine Beschreibung des geltend gemachten Verstoßes und, nach eigener Wahl, Belegunterlagen und -materialien und/oder eine Rechtserörterung mit Bezug zum geltend gemachten Verstoß.

2. Es werden Verfahren entwickelt, die sicherstellen, dass für einen geltend gemachten Verstoß nicht mehrere Verfahren geführt oder mehrere Abhilfemaßnahmen getroffen werden.
3. Die FTC kann parallel zum Schiedsverfahren tätig werden.
4. An den Schiedsverfahren dürfen keine Vertreter der USA, der EU oder eines EU-Mitgliedstaats oder einer anderen Regierungsbehörde, staatlichen Behörde oder Strafverfolgungsbehörde teilnehmen, wobei auf Antrag einer Person aus der EU die EU-Datenschutzbehörden Hilfe bei der Erstellung ausschließlich der Mitteilung leisten können, jedoch keinen Zugang zu Offenlegungen und anderen Materialien in Bezug auf diese Schiedsverfahren haben dürfen.
5. Ort des Schiedsverfahrens sind die Vereinigten Staaten, und die betroffene Person kann sich für eine Teilnahme per Video oder Telefonkonferenz entscheiden, die für sie mit keinen Kosten verbunden ist. Eine persönliche Anwesenheit ist nicht erforderlich.

6. Verfahrenssprache ist Englisch, wenn von den Parteien nicht anders vereinbart. Auf einen begründeten Antrag hin und unter Berücksichtigung dessen, ob sich die Person von einem Anwalt vertreten lässt, werden Dolmetscher für die mündliche Verhandlung sowie Übersetzungen der Verfahrensunterlagen bereitgestellt, ohne dass sich daraus Kosten für die Person ergeben, es sei denn, das Panel gelangt in einem konkreten Fall zu dem Schluss, dass eine Kostenübernahme nicht gerechtfertigt oder unverhältnismäßig wäre.
7. Den Schiedsrichtern vorgelegte Unterlagen werden vertraulich behandelt und nur in Verbindung mit dem Schiedsverfahren genutzt.
8. Wenn erforderlich, kann eine die Person betreffende Offenlegung zugelassen werden, wobei diese Offenlegung von den Parteien vertraulich behandelt und nur in Verbindung mit dem Schiedsverfahren genutzt wird.
9. Schiedsverfahren sollen innerhalb von 90 Tagen nach Zustellung der Mitteilung an die betreffende Organisation abgeschlossen werden, sofern von den Parteien nicht anderweitig vereinbart.

H. Kosten

Die Schiedsrichter sollen angemessene Maßnahmen zur Minimierung der Kosten oder Gebühren der Schiedsverfahren ergreifen.

Nach Maßgabe des geltenden Rechts wird das Handelsministerium in Abstimmung mit der Europäischen Kommission die Einrichtung eines Fonds ermöglichen, in den die dem Datenschutzschild angehörenden Organisationen einen Jahresbeitrag einzahlen, der sich zum Teil nach der Größe der Organisation richtet und die Schiedskosten, einschließlich Schiedsrichtergebühren, bis zu einer Obergrenze deckt. Der Fonds wird von einem Dritten verwaltet, der regelmäßig über die Tätigkeit des Fonds Bericht erstattet. Bei der jährlichen Überprüfung werden das Handelsministerium und die Europäische Kommission die Tätigkeit des Fonds, einschließlich der Notwendigkeit einer Anpassung des Beitrags oder der Obergrenze, kontrollieren und unter anderem die Anzahl der Schiedsverfahren sowie deren Kosten und Dauer prüfen, und zwar im gegenseitigen Einvernehmen, dass den am Datenschutzschild teilnehmenden Organisationen keine übermäßige finanzielle Belastung auferlegt wird. Rechtsanwaltsgebühren sind von dieser Bestimmung oder einem anderen Fonds im Rahmen dieser Bestimmung nicht erfasst.

ANHANG III
Schreiben des US-Außenministers John Kerry

7. Juli 2016

Sehr geehrte Frau Jourová,

es freut mich sehr, dass wir eine Einigung zum Datenschutzschild zwischen der Europäischen Union und den USA erzielen konnten, die auch eine Ombudsstelle beinhaltet, bei der EU-Behörden Auskunftsbegehren von EU-Bürgern im Zusammenhang mit signalerfassender Aufklärung in den USA einreichen können.

Präsident Barack Obama hat am 17. Januar 2014 in der Presidential Policy Directive 28 (PPD-28) eine grundlegende Reform der Nachrichtendienste angekündigt. Im Rahmen der PPD-28 habe ich Under-Secretary Catherine A. Novelli, die ebenfalls das Amt eines Senior Coordinator für internationale Diplomatie im Bereich der Informationstechnologie bekleidet, zur Ansprechpartnerin für ausländische Regierungen benannt, die Bedenken im Zusammenhang mit der US-Signalaufklärung vorbringen. Ausgehend von dieser Funktion habe ich in Übereinstimmung mit den in Anlage A festgelegten Bestimmungen, die seit meinem Schreiben vom 22. Februar 2016 aktualisiert wurden, eine Ombudsstelle des Datenschutzschilds ins Leben gerufen. Dieses Amt wird von Under-Secretary Novelli bekleidet, die unabhängig von den Nachrichtendiensten in den USA arbeitet und mir direkt unterstellt ist.

Meine Mitarbeiter sind angewiesen, die erforderlichen Ressourcen für die Einrichtung dieser neuen Ombudsstelle einzusetzen, und ich bin überzeugt, dass wir den Bedenken der EU-Bürger auf diese Weise wirksam begegnen können.

Hochachtungsvoll

John F. Kerry

ANLAGE A

OMBUDSSTELLE DES EU-U.S.-DATENSCHUTZSCHILDS FÜR DIE SIGNALERFASSENDE AUFKLÄRUNG

In Anerkennung der Bedeutung des EU-U.S.-Datenschutzschilds gibt die vorstehende Absichtserklärung einen Überblick über das Verfahren zur Umsetzung eines neuen Mechanismus für die signalerfassende Aufklärung, der mit der Presidential Policy Directive 28 („PPD-28“) im Einklang steht.¹

Am 17. Januar 2014 hielt Präsident Obama eine Ansprache, in der er wichtige Reformen im Bereich Nachrichtendienste in Aussicht stellte. Dabei betonte er: „Unsere Bemühungen tragen nicht nur zum Schutz unserer eigenen Nation bei, sondern auch zu dem unserer Freunde und Verbündeten. Wirksam werden unsere Bemühungen aber nur dann sein, wenn die normalen Bürger in anderen Ländern ebenfalls darauf vertrauen, dass die Vereinigten Staaten ihre Privatsphäre respektieren.“ Präsident Obama kündigte die Veröffentlichung einer neuen Presidential Directive, der „PPD-28“, an mit „klaren Vorschriften dazu, was wir unternehmen und was nicht, wenn es um unsere Auslandsaufklärung geht“.

In § 4 Buchstabe d der PPD-28 wird der Außenminister beauftragt, einen „Senior Coordinator for International Information Technology Diplomacy“ (Senior Coordinator) zu benennen, „der ... als Ansprechpartner für ausländische Regierungen fungiert, die Bedenken im Zusammenhang mit der Signalaufklärung der Vereinigten Staaten vorbringen.“ Seit Januar 2015 nimmt Under Secretary C. Novelli die Aufgaben des Senior Coordinators wahr.

In der vorliegenden Absichtserklärung wird der vom Senior Coordinator befolgte neue Mechanismus beschrieben, der bei Daten, die gemäß dem Datenschutzschild, den Standardklauseln (standard contractual clauses, SCC), den verbindlichen unternehmensinternen Datenschutzregelungen (binding corporate rules, BCR) sowie den „Ausnahmeregelungen“² oder

¹ Unter der Voraussetzung, dass der Beschluss über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für Island, Liechtenstein und Norwegen gilt, wird die Materialsammlung zum Datenschutzschild sowohl die Europäische Union als auch diese drei Länder abdecken. Demzufolge sind bei Bezugnahmen auf die EU und ihre Mitgliedstaaten auch Island, Liechtenstein und Norwegen eingeschlossen.

² „Ausnahmeregelungen“ steht in diesem Zusammenhang für einen oder mehrere kommerzielle Datenübermittlungen, die unter der Voraussetzung stattfinden, dass: (a) die betroffene Person ihre unmissverständliche Einwilligung zu der vorgeschlagenen Datenübermittlung erteilt hat oder (b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist; oder (c) die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person von dem für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wird; oder (d) die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist; oder (e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist; oder (f) die Übermittlung aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

„etwaigen künftigen Ausnahmeregelungen“³ von der EU unter Einhaltung des dafür bestehenden Weges laut geltendem Recht und bestehender Auslegungspraxis in die Vereinigten Staaten übermittelt werden, die Bearbeitung von Anfragen zum Zugriff auf Daten, die die nationale Sicherheit betreffen, und die Beantwortung solcher Anfragen erleichtern soll.

1. **Die Ombudsperson des Datenschutzschildes:** Der Senior Coordinator fungiert als Ombudsperson des Datenschutzschildes und benennt gegebenenfalls zusätzliche Beamte des Außenministeriums, die ihn bei der Wahrnehmung seiner in dieser Absichtserklärung im Einzelnen dargelegten Pflichten unterstützen (der Koordinator und etwaige weitere Beamte, die diese Aufgaben wahrnehmen, werden nachstehend als „Ombudsstelle des Datenschutzschildes“ bezeichnet). Die Einrichtung arbeitet eng mit den jeweiligen Beamten aus anderen Regierungsstellen zusammen, die dem geltendem Recht und der bestehenden Auslegungspraxis der Vereinigten Staaten entsprechend für die Bearbeitung von Anträgen zuständig sind. Die Ombudsstelle untersteht unmittelbar dem Außenminister, der dafür Sorge trägt, dass die Ombudsstelle ihre Aufgabe objektiv und frei von unzulässiger Einflussnahme erfüllt, die sich auf die zu erteilende Antwort auswirken kann.
2. **Wirksame Koordinierung:** Die Ombudsstelle setzt die nachstehend beschriebenen Kontrollstellen wirksam ein, koordiniert sie und stellt auf diese Weise sicher, dass sich die Antwort der Ombudsstelle auf Anträge der EU-Stelle für Individualbeschwerden auf die erforderlichen Informationen stützt. Bezieht sich der Antrag auf die Vereinbarkeit der Überwachung mit dem US-Recht, kann die Ombudsstelle des Datenschutzschildes mit einer der unabhängigen Kontrollstellen mit Ermittlungsbefugnissen zusammenarbeiten.
 - a. Die Ombudsstelle des Datenschutzschildes arbeitet eng mit anderen Regierungsbeamten der Vereinigten Staaten, unter anderem auch mit entsprechenden unabhängigen Aufsichtsgremien, zusammen und stellt sicher, dass die eingegangenen Anträge vollständig sind und dem geltenden Recht und der bestehenden Auslegungspraxis entsprechend bearbeitet und geklärt werden. Insbesondere sorgt die Ombudsstelle für

³ „Etwaige künftige Ausnahmeregelungen“ steht in diesem Zusammenhang für eine oder mehrere kommerzielle Datenübermittlungen, die unter einer der folgenden Voraussetzungen stattfinden, soweit die betreffende Voraussetzung rechtlich zulässige Gründe für die Übermittlung personenbezogener Daten aus der EU in die USA darstellt: (a) die betroffene Person hat ihre unmissverständliche Einwilligung zu der vorgeschlagenen Datenübermittlung erteilt, nachdem sie über die möglichen Risiken einer ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien durchgeführten Datenübermittlung informiert wurde; oder (b) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben; oder (c) bei einer Übermittlung an einen Drittstaat oder eine internationale Organisation, bei der keine andere bestehende oder künftige Ausnahmeregelung anwendbar ist, nur, wenn es sich dabei um keine Wiederholung handelt, wenn die Übermittlung sich nur auf eine begrenzte Zahl betroffener Personen bezieht, wenn ein zwingendes berechtigtes Interesse des für die Verarbeitung Verantwortlichen vorliegt, das nicht von den berechtigten Interessen oder den Rechten und Freiheiten der betroffenen Person außer Kraft gesetzt wird, und wenn der für die Verarbeitung Verantwortliche alle Umstände beurteilt hat, die bei einer Datenübermittlung eine Rolle spielen, und gegebenenfalls auf der Grundlage dieser Beurteilung geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.

eine enge Koordinierung mit dem Amt des Director of National Intelligence, dem Justizministerium und den anderen Regierungsstellen, die entsprechend mit der nationalen Sicherheit der Vereinigten Staaten befasst sind, sowie den Generalinspektoren, den Beauftragten für den Freedom of Information Act und den Bürgerrechts- und Datenschutzbeauftragten.

- b. Damit gewährleistet ist, dass die Ombudsstelle des Datenschutzschildes im Sinne von § 4 Buchstabe e auf die eingegangenen Anträge nach § 3 Buchstabe b zu reagieren vermag, vertraut die Regierung der Vereinigten Staaten auf Mechanismen zur ressortübergreifenden Koordinierung und Überwachung von Angelegenheiten der nationalen Sicherheit.
- c. Die Ombudsstelle des Datenschutzschildes kann Anträge betreffende Angelegenheiten dem Privacy and Civil Liberties Oversight Board zur Prüfung vorlegen.

3. Einreichung von Anträgen:

- a. Ein Antrag wird zunächst bei den für die Überwachung der nationalen Sicherheitsbehörden und/oder die Verarbeitung von personenbezogenen Daten durch Behörden zuständigen Aufsichtsstellen der Mitgliedstaaten eingereicht. Die Einreichung des Antrags bei der Ombudsstelle erfolgt durch eine zentrale EU-Stelle (im Folgenden zusammen „EU-Stelle für Individualbeschwerden“).
- b. Die EU-Stelle für Individualbeschwerden stellt mit den nachstehenden Maßnahmen sicher, dass ein Antrag ordnungsgemäß abgefasst ist:
 - (i) Sie überprüft die Identität der betreffenden Privatperson und die Tatsache, dass diese im eigenen Namen und nicht als Vertreter/in einer staatlichen oder zwischenstaatlichen Organisation handelt.
 - (ii) Sie stellt sicher, dass der Antrag schriftlich abgefasst ist und die folgenden grundlegenden Informationen enthält:
 - alle Informationen, die dem Antrag zugrunde liegen,
 - die Art der Information oder der angestrebten Abhilfe,
 - die Regierungsstellen der Vereinigten Staaten, die gegebenenfalls beteiligt sein sollen, und
 - sonstige Maßnahmen, die ergriffen wurden, um die erbetenen Informationen bzw. die angestrebte Abhilfe zu erlangen, und das Ergebnis dieser sonstigen Maßnahmen.
 - (iii) Sie prüft, ob der Antrag sich auf Daten bezieht, bei denen begründet davon ausgegangen werden kann, dass sie gemäß Datenschutzschild, SCC, BCR, Ausnahmeregelungen oder etwaigen künftigen Ausnahmeregelungen von der EU in die Vereinigten Staaten übermittelt wurden.

(iv) Sie trifft eine erste Feststellung, dass der Antrag nicht schikanös oder missbräuchlich ist bzw. nicht bösgläubig erfolgte.

- c. Um für die Zwecke der weiteren Bearbeitung durch die Ombudsstelle des Datenschuttschildes im Sinne dieser Absichtserklärung abgefasst zu sein, muss ein Antrag nicht den Nachweis enthalten, dass tatsächlich im Wege der Signalaufklärung ein Zugriff der US-Regierung auf die Daten des Antragstellers erfolgt ist.

4. Zusagen zur Kommunikation mit der vorlegenden EU-Stelle für Individualbeschwerden

- a. Die Ombudsstelle des Datenschuttschildes bestätigt den Eingang des Antrags gegenüber der EU-Stelle für Individualbeschwerden, durch die die Übermittlung erfolgte.
- b. Die Ombudsstelle des Datenschuttschildes nimmt eine erste Prüfung vor, um festzustellen, ob der Antrag in Übereinstimmung mit Abschnitt 3 Buchstabe b abgefasst wurde. Stellt die Ombudsstelle irgendwelche Unzulänglichkeiten fest oder hat sie Fragen zur Abfassung eines Antrags, so setzt sie sich mit der EU-Stelle für Individualbeschwerden in Verbindung und versucht, die betreffenden Fragen zu klären.
- c. Benötigt die Ombudsstelle des Datenschuttschildes zur Erleichterung der angemessenen Bearbeitung eines Antrags weitere Informationen oder müssen von der Privatperson, die den Antrag ursprünglich einreichte, besondere Maßnahmen ergriffen werden, so setzt die Ombudsstelle des Datenschuttschildes die vorlegende EU-Stelle für Individualbeschwerden hiervon in Kenntnis.
- d. Die Ombudsstelle des Datenschuttschildes überprüft den Status des Antrags und stellt für die vorlegende EU-Stelle für Individualbeschwerden entsprechende Aktualisierungen bereit.
- e. Sobald ein Antrag wie in Abschnitt 3 dieser Absichtserklärung beschrieben abgefasst wurde, sendet die Ombudsstelle des Datenschuttschildes vorbehaltlich der andauernden Informationsschutzverpflichtung nach geltendem Recht und bestehender Auslegungspraxis zeitnah eine angemessene Antwort an die vorlegende EU-Stelle für Individualbeschwerden. Die Ombudsstelle lässt der vorlegenden EU-Stelle eine Antwort zukommen, in der sie bestätigt, dass (i) die Beschwerde ordnungsgemäß geprüft wurde und dass (ii) die US-Gesetze und -Rechtsvorschriften, Executive Orders, Presidential Directives und die Auslegungspraxis der Behörden mit den im ODNI-Schreiben dargelegten Einschränkungen und Garantien eingehalten wurden bzw. dass – im Falle der Nichteinhaltung – diese Nichteinhaltung abgestellt wurde. Durch die Ombudsstelle wird weder bestätigt noch bestritten, dass die betreffende Privatperson Ziel einer Überwachungsmaßnahme war, noch bestätigt die Ombudsstelle die spezielle Abhilfe, die geleistet wurde. Wie in Abschnitt 5 weiter erläutert wird, werden Anträge im

Rahmen des Freedom of Information Acts so bearbeitet, wie in diesem Gesetz und den geltenden Bestimmungen vorgesehen.

- f. Die Ombudsstelle des Datenschutzschildes nimmt unmittelbaren Kontakt zur EU-Stelle für Individualbeschwerden auf, die ihrerseits für den Kontakt zu der Privatperson, die den Antrag einreichte, verantwortlich ist. Ist der unmittelbare Kontakt Bestandteil eines der nachstehend beschriebenen Verfahren, so erfolgt dieser Kontakt den vorhandenen Verfahren entsprechend.
 - g. Die Zusagen in dieser Absichtserklärung gelten nicht für pauschale Aussagen, wonach der EU-U.S.-Datenschutzschild den Datenschutzerfordernissen der Europäischen Union nicht entspreche. Sie wurden ausgehend von dem gemeinsamen Verständnis der Europäischen Kommission und der US-Regierung getroffen, dass es in Anbetracht der Bandbreite der im Rahmen dieses Mechanismus erteilten Zusagen möglicherweise zu ressourcenbedingten Einschränkungen kommen könnte, unter anderem bei Anträgen im Zusammenhang mit dem Freedom of Information Act (FOIA). Sollte die Wahrnehmung der Aufgaben der Ombudsstelle des Datenschutzschildes über die vertretbaren ressourcenbedingten Einschränkungen hinausgehen und die Erfüllung dieser Zusagen erschweren, so wird die US-Regierung der Europäischen Kommission gegenüber etwaige Anpassungen zur Sprache bringen, die unter diesen Umständen angebracht sind.
5. **Auskunftsbegehren:** Anträge auf Zugang zu amtlichen Unterlagen der Vereinigten Staaten können im Rahmen des Freedom of Information Act (FOIA) gestellt und bearbeitet werden.
- a. Der FOIA bietet jedermann die Möglichkeit, den Zugang zu vorhandenen Unterlagen von Regierungsstellen zu beantragen, und zwar unabhängig von der Nationalität des Antragstellers. Dieses Gesetz ist kodifiziert im United States Code unter 5 U.S.C. § 552. Das Gesetz selbst kann zusammen mit zusätzlichen Informationen zum FOIA unter www.FOIA.gov und <http://www.justice.gov/oip/foia-resources> abgerufen werden. Jede Regierungsstelle hat einen verantwortlichen FOIA-Beauftragten, und auf ihrer öffentlichen Website finden sich Angaben dazu, wie ein FOIA-Antrag bei der betreffenden Stelle einzureichen ist. Die Behörden verfügen über gegenseitige Konsultationsverfahren zu FOIA-Anträgen, für die Unterlagen erforderlich sind, die von einer anderen Stelle vorgehalten werden.
 - b. Beispiele:
 - (i) Das Amt des Director of National Intelligence (ODNI) hat für das ODNI das ODNI-FOIA-Portal eingerichtet: <http://www.dni.gov/index.php/about-this-site/foia>. Dieses Portal enthält Angaben zur Übermittlung von Anträgen, zur Überprüfung des Status laufender Anträge und zum Zugang zu Informationen, die vom ODNI im Rahmen des FOIA freigegeben und veröffentlicht wurden. Auf dem FOIA-Portal des ODNI finden sich Links zu anderen FOIA-Websites für Nachrichtendienste: <http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites>.

- (ii) Das Office of Information Policy des Justizministeriums stellt umfassende FOIA-Informationen bereit: <http://www.justice.gov/oip>. Dazu gehören nicht nur Angaben zur Weiterleitung von FOIA-Anträgen an das Justizministerium, sondern auch Hinweise für die US-Regierung zur Auslegung und Anwendung der FOIA-Anforderungen.
 - c. Gemäß FOIA gelten für den Zugang zu Regierungsunterlagen bestimmte detailliert aufgeführte Ausnahmeregelungen. Dazu zählen Einschränkungen des Zugriffs auf Informationen, die aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen, personenbezogene Informationen Dritter und Informationen, die strafrechtliche Ermittlungen betreffen, vergleichbar mit den Einschränkungen, die von den einzelnen EU-Mitgliedstaaten durch deren eigene Gesetze über den Zugang zu Informationen auferlegt werden. Diese Einschränkungen gelten für Amerikaner und für Nicht-Amerikaner gleichermaßen.
 - d. Bei Streitigkeiten im Zusammenhang mit der Freigabe von Unterlagen, die im Rahmen des FOIA angefordert werden, kann der Verwaltungsgerichtsweg eingeschlagen und anschließend ein Bundesgericht angerufen werden. Das Gericht hat de novo zu bestimmen, ob Unterlagen aus triftigen Gründen zurückgehalten werden (5 U.S.C. § 552 Buchstabe a Ziffer 4 Teil B), und kann die Behörden anweisen, Zugang zu Unterlagen zu gewähren. In einigen Fällen wurden von Gerichten die Behauptungen von Behörden zurückgewiesen, Informationen müssten zurückgehalten werden, weil sie aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen. Obwohl kein Schadensersatz geltend gemacht werden kann, können die Gerichte die Erstattung der Anwaltsgebühren zuerkennen.
6. **Anträge auf Einleitung weiterer Maßnahmen:** Ein Antrag unter Berufung auf eine Rechtsverletzung oder anderes Fehlverhalten wird den zuständigen Regierungsstellen der Vereinigten Staaten zugeleitet, darunter unabhängigen Überwachungsstellen, die befugt sind, den betreffenden Antrag zu prüfen und bei Verstößen gegen Vorschriften die nachstehend beschriebenen Maßnahmen zu ergreifen.
- a. Generalinspektoren sind rechtlich unabhängig und verfügen über weitreichende Befugnisse zur Durchführung von Untersuchungen, Audits und Überprüfungen von Programmen, darunter auch bei Missbrauchsfällen oder Rechtsverstößen, und können Abhilfemaßnahmen empfehlen.
 - (i) In der geänderten Fassung des Inspector General Act von 1978 fungieren die Generalinspektoren (IG) auf Bundesebene als unabhängige und objektive Instanzen innerhalb der meisten Behörden, deren Aufgabe es ist, Verschwendung, Betrug und Missbrauch in den Programmen und Aktivitäten der jeweiligen Behörde zu bekämpfen. Zu diesem Zweck ist jeder IG für die Durchführung von Audits und Untersuchungen im Zusammenhang mit den Programmen und Aktivitäten seiner

Behörde verantwortlich. Darüber hinaus sind die Generalinspektoren anleitend und koordinierend tätig, erteilen Empfehlungen für Maßnahmen zur Förderung von Wirtschaftlichkeit, Effizienz und Wirksamkeit, decken Betrug und Amtsmissbrauch in den Programmen und Aktivitäten ihrer Behörde auf und verhindern sie.

- (ii) Jeder Nachrichtendienst hat ein eigenes Büro des Generalinspektors, das unter anderem für die Kontrolle der Auslandsaufklärung zuständig ist. Mehrere Berichte von Generalinspektoren zu nachrichtendienstlichen Programmen wurden veröffentlicht.
- (iii) Beispiele:
- Das Büro des Generalinspektors der Intelligence Community (IC IG) wurde gemäß § 405 des [Intelligence Authorization Act of Fiscal Year 2010](#) eingerichtet. Das IC IG ist zuständig für IC-weite Audits, Untersuchungen, Inspektionen und Überprüfungen, bei denen alle nachrichtendienstliche Missionen betreffenden systemimmanenten Risiken, Schwachstellen und Unzulänglichkeiten ermittelt und aufgegriffen werden, um mit Blick auf IC-weite Einsparungen und Wirkungen Verbesserungen herbeizuführen. Das IC IG ist befugt, Beschwerden oder Informationen nachzugehen, die mutmaßliche Verstöße gegen Gesetze oder Rechtsvorschriften, Fälle von Verschwendung, Betrug und Amtsmissbrauch oder eine erhebliche oder besondere Gefahr für die öffentliche Gesundheit und Sicherheit im Zusammenhang mit nachrichtendienstlichen Programmen und Aktivitäten des ODNI und/oder der Intelligence Community betreffen. Das IC IG stellt Informationen darüber bereit, wie das IC IG unmittelbar kontaktiert werden kann, wenn ein Bericht übermittelt werden soll:
<http://www.dni.gov/index.php/about-this-site/contact-the-ig>.
 - Das Büro des Generalinspektors (OIG) im [U.S. Department of Justice](#) (DOJ, Justizministerium) ist eine auf gesetzlicher Grundlage eingesetzte unabhängige Instanz, deren Aufgabe es ist, Verschwendung, Betrug, Amtsmissbrauch und Fehlverhalten in DOJ-Programmen und durch Bedienstete des Ministeriums aufzudecken und zu unterbinden und zur Wirtschaftlichkeit und Effizienz dieser Programme beizutragen. Das OIG untersucht mutmaßliche Straf- und Zivilrechtsverletzungen durch DOJ-Bedienstete und nimmt darüber hinaus Audits und Inspektionen zu DOJ-Programmen vor. Es ist zuständig für alle Beschwerden über Fehlverhalten von Bediensteten des Justizministeriums, unter anderem auch von Bediensteten des Federal Bureau of Investigation, der Drug Enforcement Administration, des Federal Bureau of Prisons, des U.S. Marshals Service, des Bureau of Alcohol, Tobacco, Firearms, and Explosives, der United States Attorneys Offices und der Bediensteten, die in anderen Bereichen oder Büros des Justizministeriums beschäftigt sind. (Die einzige Ausnahme besteht darin, dass Missbrauchsvorwürfe gegenüber einem Department Attorney oder Mitarbeiter der

Strafverfolgungsbehörden, die sich auf die Wahrnehmung der Befugnisse des Department Attorney zur Durchführung von Ermittlungen, zur Austragung von Rechtsstreitigkeiten oder zur Rechtsberatung beziehen, in die Zuständigkeit des Office of Professional Responsibility des Ministeriums fallen.) Darüber hinaus wird der Generalinspekteur in § 1001 des USA Patriot Act, der am 26. Oktober 2001 Rechtskraft erlangte, angewiesen, Beschwerden gegen mutmaßliche Verletzungen von Bürgerrechten und bürgerlichen Freiheiten durch Bedienstete des Justizministeriums entgegenzunehmen und entsprechenden Informationen nachzugehen. Das OIG unterhält eine öffentliche Website – <https://www.oig.justice.gov> –, auf der auch eine „Hotline“ zur Einreichung von Beschwerden zu finden ist: <https://www.oig.justice.gov/hotline/index.htm>.

- b. Die Datenschutz- und Bürgerrechtsbeauftragten und -gremien innerhalb der US-Regierung sind ebenfalls mit entsprechenden Befugnissen ausgestattet. Beispiele:
- (i) In § 803 der Durchführungsempfehlungen zum 9/11 Commission Act von 2007, kodifiziert im United States Code unter 42 U.S.C. § 2000-ee1, werden für bestimmte Ministerien und Behörden (darunter das Außenministerium, das Justizministerium und das ODNI) Datenschutz- und Bürgerrechtsbeauftragte eingeführt. § 803 besagt, dass diese Datenschutz- und Bürgerrechtsbeauftragten als Hauptratgeber fungieren, die unter anderem sicherstellen sollen, dass das betreffende Ministerium, die Behörde oder der Dienst über angemessene Verfahren verfügt, um sich mit Beschwerden von Privatpersonen auseinanderzusetzen, die dem Ministerium, der Behörde oder dem Dienst vorwerfen, gegen ihre Datenschutz- oder Bürgerrechte verstoßen zu haben.
 - (ii) Das Büro des ODNI für Bürgerrechte und Datenschutz (ODNI's Civil Liberties and Privacy Office, ODNI CLPO) wird geleitet vom Bürgerrechtsbeauftragten des ODNI, eines Amtes, das durch den National Security Act von 1948 in der geänderten Fassung eingeführt wurde. Zu den Pflichten des ODNI CLPO gehört die Schaffung der notwendigen Voraussetzungen dafür, dass die Strategien und Verfahren der Nachrichtendienste einen angemessenen Schutz der Privatsphäre und der bürgerlichen Freiheiten vorsehen, sowie die Prüfung und Untersuchung von Beschwerden wegen mutmaßlichen Amtsmissbrauchs oder Verstößen gegen die Bürgerrechte und den Datenschutz in Programmen und Aktivitäten des ODNI. Das ODNI CLPO stellt auf seiner Website Informationen für die Öffentlichkeit bereit, darunter auch Hinweise dazu, wie Beschwerden einzureichen sind: www.dni.gov/clpo. Geht beim ODNI CLPO eine Beschwerde wegen eines Verstoßes gegen den Datenschutz oder die Bürgerrechte ein, bei der IC-Programme und -Aktivitäten eine Rolle spielen, so spricht es mit den anderen Nachrichtendiensten ab, wie mit dieser Beschwerde innerhalb der Intelligence Community weiter verfahren werden soll. Hierzu sei angemerkt, dass die National Security Agency (NSA) ebenfalls über ein Büro für Bürgerrechte und Datenschutz

verfügt, das auf seiner Website – https://www.nsa.gov/civil_liberties/ – Angaben zu seinen Zuständigkeiten bereitstellt. Liegen Informationen vor, dass eine Behörde gegen die Datenschutzbestimmungen verstößt (als Beispiel sei § 4 der PPD-28 genannt), dann verfügen die Behörden über Compliance-Mechanismen, mit denen ein solcher Vorfall geprüft und ausgeräumt wird. Nach PPD-28 sind die Behörden gehalten, Fälle von Nichteinhaltung der Vorschriften an das ODNI zu melden.

- (iii) Das Büro für Datenschutz und Bürgerrechte (Office of Privacy and Civil Liberties, OPCL) des Justizministeriums unterstützt den Leitenden Datenschutz- und Bürgerrechtsbeauftragten (Chief Privacy and Civil Liberties Officer, CPCLO) des Ministeriums bei der Wahrnehmung seiner Pflichten und Zuständigkeiten. Hauptaufgabe des OPCL ist der Schutz der Privatsphäre und der Bürgerrechte der amerikanischen Bürger durch Überprüfung, Kontrolle und Koordinierung der Datenschutzaktivitäten des Ministeriums. Das OPCL sorgt für die juristische Beratung und Anleitung der Struktureinheiten des Ministeriums und stellt sicher, dass das Ministerium sich an die geltenden Datenschutzbestimmungen hält, unter anderem an den Privacy Act von 1974, die Datenschutzbestimmungen des E-Government Act von 2002 und auch den Federal Information Security Management Act sowie an die verwaltungspolitischen Richtlinien, die im Nachgang zu diesen Gesetzen erlassen wurden; darüber hinaus konzipiert das Büro Datenschutzzschulungen des Ministeriums und führt diese durch, unterstützt den CPCLO bei der Weiterentwicklung der Datenschutzstrategie des Ministeriums, verfasst Datenschutzberichte für den Präsidenten und den Kongress und überprüft den praktischen Umgang des Ministeriums mit Informationen, damit sichergestellt ist, dass dabei der Datenschutz und die Bürgerrechte respektiert werden. Das OPCL informiert die Öffentlichkeit unter <http://www.justice.gov/opcl> über seine Aufgaben.
- (iv) Damit der Datenschutz und die Bürgerrechte gewährleistet sind, überprüft das Privacy and Civil Liberties Oversight Board gemäß 42 U.S.C. § 2000ee ff. kontinuierlich (i) die Strategien und Verfahren der Ministerien, der Behörden und der Exekutive im Zusammenhang mit den Bemühungen zum Schutz der Nation vor Terrorismus und deren Umsetzung sowie (ii) andere Aktivitäten der Exekutive in Verbindung mit diesen Maßnahmen, um festzustellen, ob bei diesen Aktivitäten Datenschutz und Bürgerrechte angemessen geschützt werden und mit den für diesen Bereich geltenden Gesetzen, Rechtsvorschriften und Strategien konform gehen. Es nimmt Berichte und andere Informationen von Datenschutz- und Bürgerrechtsbeauftragten entgegen, prüft diese und erteilt den Betroffenen gegebenenfalls Empfehlungen zu ihrer Tätigkeit. In § 803 der Durchführungsempfehlungen zum 9/11 Commission Act von 2007, kodifiziert unter 42 U.S.C. § 2000ee-1, werden die Datenschutz- und Bürgerrechtsbeauftragten von acht Bundesbehörden (darunter der Verteidigungsminister, der Minister für innere Sicherheit, der Director of National Intelligence und der CIA-Direktor) und etwaige zusätzliche Behörden, die vom Board benannt werden, angewiesen, dem PCLOB in regelmäßigen Abständen Berichte vorzulegen, unter anderem auch zu Anzahl, Art

und Grundstimmung der Beschwerden, die bei der jeweiligen Behörde wegen mutmaßlicher Verstöße eingegangen sind. Nach dem Gesetz, das die Befugnisse des PCLOB regelt, ist das Board gehalten, diese Berichte entgegenzunehmen und gegebenenfalls den Datenschutz- und Bürgerrechtsbeauftragten Empfehlungen zu ihrer Tätigkeit zu erteilen.

ANHANG IV
Schreiben der Vorsitzenden der Federal Trade Commission Edith Ramirez

7. Juli 2016

PER E-MAIL

Věra Jourová
Kommissionsmitglied für Justiz, Verbraucherschutz
und Gleichstellungsfragen
Europäische Kommission
Rue de la Loi / Wetstraat 200
1049 Brüssel
Belgien

Sehr geehrte Frau Jourová:

Die Federal Trade Commission der Vereinigten Staaten („FTC“) nimmt gern diese Gelegenheit wahr, um darzulegen, wie sie die neue EU-US-Datenschutzschild-Regelung (die „Datenschutzschild-Regelung“ oder „Regelung“) durchzusetzen gedenkt. Nach unserer Auffassung wird die Regelung maßgeblich dazu beitragen, den datenschutzfreundlichen Geschäftsverkehr in einer zunehmend vernetzten Welt zu erleichtern. Sie wird Unternehmen in die Lage versetzen, in der globalen Wirtschaft wichtige Transaktionen durchzuführen, und zugleich sicherstellen, dass die Verbraucher in der EU ein hohes Maß an Datenschutz genießen. Die FTC bekennt sich schon seit Langem zum grenzüberschreitenden Datenschutz und wird der Durchsetzung der neuen Regelung eine hohe Priorität einräumen. Im Folgenden geben wir einen allgemeinen Überblick über die bisherigen Bemühungen der FTC um die konsequente Handhabung des Datenschutzes, namentlich der ursprünglich geltenden Safe-Harbor-Regelung, und über die Vorstellungen der FTC zur Durchsetzung der neuen Regelung.

Zum ersten Mal verpflichtete sich die FTC im Jahr 2000 öffentlich dazu, die Safe-Harbor-Regelung durchzusetzen. Der damalige FTC-Vorsitzende Robert Pitofsky sandte der Europäischen Kommission ein Schreiben, in dem er die Entschlossenheit der FTC unterstrich, den Safe-Harbor-Datenschutzgrundsätzen mit Nachdruck Geltung zu verschaffen. Wie fast 40 Durchsetzungsmaßnahmen, zahlreiche zusätzliche Ermittlungen und die Zusammenarbeit mit einzelnen europäischen Datenschutzbehörden zu Fragen von gegenseitigem Interesse deutlich machen, hat die FTC ihre Zusage eingehalten.

Nachdem die Europäische Kommission im November 2013 Bedenken zur Verwaltung und Durchsetzung des Safe-Harbor-Programms anmeldete, leiteten wir und das US-Handelsministerium Konsultationen mit Vertretern der Europäischen Kommission ein, um Möglichkeiten zur Stärkung des Programms zu erkunden. Während die Konsultationen noch

im Gange waren, verkündete der Europäische Gerichtshof am 6. Oktober 2015 ein Urteil in der Rechtssache *Schrems*, das unter anderem die Entscheidung der Europäischen Kommission über die Angemessenheit des Safe-Harbor-Programms für ungültig erklärte. Danach arbeiteten wir weiter eng mit dem Handelsministerium und der Europäischen Kommission zusammen, um den Datenschutz für Einzelpersonen in der EU effektiver zu gestalten. Die Datenschuttschild-Regelung ist ein Ergebnis dieser weiter andauernden Konsultationen. Wie beim Safe-Harbor-Programm verpflichtet sich die FTC hiermit zur konsequenten Durchsetzung der neuen Regelung. Dieses Schreiben soll diese Verpflichtung dokumentieren.

Im Mittelpunkt unseres Engagements stehen vier Kernbereiche: (1) die vorrangige Behandlung von überwiesenen Fällen und Ermittlungen; (2) die Unterbindung falscher oder irreführender Angaben zur Mitgliedschaft im Datenschuttschild; (3) die Kontrolle der Befolgung von Verfügungen; und (4) verstärkte Kontakte zu Datenschutzbehörden der EU und engere Zusammenarbeit mit ihnen bei der Durchsetzung. Nachstehend machen wir zu jedem dieser Punkte detaillierte Angaben und geben Hintergrundinformationen zu dem Beitrag, den die FTC bisher zum Schutz von Verbraucherdaten und zur Durchsetzung des Safe-Harbor-Programms leistete, sowie zur Gesamtsituation des Datenschutzes in den Vereinigten Staaten.¹

I. Hintergrund

A. Durchsetzung des Datenschutzrechts durch die FTC und konzeptionelle Fragen

Die FTC genießt umfassende zivilrechtliche Befugnisse zur Förderung des Verbraucherschutzes und des Wettbewerbs im Wirtschaftsleben. Im Rahmen ihres Auftrags zum Verbraucherschutz verschafft sie einem breiten Spektrum von Rechtsvorschriften Geltung und sorgt damit für den Schutz und die Sicherheit von Verbraucherdaten. Das wichtigste von ihr durchzusetzende Gesetz, der FTC Act, untersagt „unlautere“ und „irreführende“ Handlungen oder Praktiken, die den Geschäftsverkehr betreffen oder sich darauf auswirken.² Eine Darstellung, Unterlassung oder Praxis ist irreführend, wenn sie rechtserheblich und geeignet ist, Verbraucher zu täuschen, die sich unter den gegebenen Umständen angemessen verhalten.³ Eine Handlung oder Praxis ist unlauter, wenn sie tatsächlich oder vermutlich einen erheblichen Schaden bewirkt, der von Verbrauchern unter normalen Umständen nicht zu vermeiden ist oder nicht durch ausgleichende Vorteile für die Verbraucher oder den Wettbewerb aufgewogen wird.⁴ Die FTC setzt auch Gesetze durch, die gezielt dem Schutz von Informationen über die Gesundheit, Kredite und andere finanzielle Daten dienen, sowie dem

¹ Zusätzliche Angaben über das US-Datenschutzrecht auf Bundesebene und in den Einzelstaaten finden Sie im Anhang A und einen Überblick über unsere neuesten Durchsetzungsmaßnahmen im Bereich Datenschutz und -sicherheit in Anhang B. Dieser Überblick ist auch auf der Website der FTC abrufbar unter <https://www.ftc.gov/reports/privacy-data-security-update-2015>.

² 15 U.S.C. § 45(a).

³ Siehe FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), abrufbar unter <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

⁴ Siehe 15 U.S.C § 45(n); FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), abrufbar unter <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

Schutz von Online-Informationen zu Kindern. Zu jedem dieser Gesetze hat sie Durchführungsverordnungen erlassen.

Nach dem FTC Act ist die FTC für Sachen zuständig, die „den Geschäftsverkehr betreffen oder sich darauf auswirken“. Sie ist nicht befugt, strafrechtliche Maßnahmen zu ergreifen oder in Fragen der nationalen Sicherheit zu entscheiden. Auch liegen die meisten anderen hoheitlichen Maßnahmen außerhalb ihres Zuständigkeitsbereichs. Hinzu kommen Einschränkungen ihrer Kompetenzen im wirtschaftlichen Bereich, die den Bankensektor, den Luftverkehr, das Versicherungsgewerbe und die Betreiber öffentlicher Telekommunikationsnetze betreffen. Auch ist die FTC nicht zuständig für die meisten gemeinnützigen Organisationen, wohl aber für nur scheinbar karitative oder gemeinnützige Einrichtungen, die in Wirklichkeit gewinnorientiert sind. In ihren Aufgabenbereich fallen auch gemeinnützige Organisationen, die zugunsten gewinnorientierter Mitglieder kommerzielle Zwecke verfolgen, indem sie ihnen beispielsweise erhebliche wirtschaftliche Vorteile verschaffen.⁵ In manchen Fällen überschneiden sich die Kompetenzen der FTC mit denen anderer Strafverfolgungsbehörden.

Wir haben stabile Arbeitsbeziehungen zu Behörden des Bundes und der Einzelstaaten aufgebaut und arbeiten mit ihnen eng zusammen, um die Ermittlungen zu koordinieren oder gegebenenfalls Fälle an eine andere Stelle zu verweisen.

Die Durchsetzung ist der Dreh- und Angelpunkt des Datenschutzkonzepts der FTC. Die FTC ist bisher in über 500 Fällen Verstößen gegen den Schutz und die Sicherheit von Verbraucherdaten nachgegangen. Dabei geht es sowohl um Offline- als auch um Online-Daten und um Durchsetzungsmaßnahmen gegen große wie kleine Unternehmen, denen vorgeworfen wurde, dass sie nicht richtig mit sensiblen Verbraucherdaten umgingen, personenbezogene Daten von Verbrauchern nicht schützten, das Verhalten von Verbrauchern unter Vorspiegelung falscher Tatsachen online verfolgten, unerbetene Werbung an Verbraucher versendeten, Spyware oder andere Schadsoftware auf den PCs von Verbrauchern installierten, gegen das Anrufverbot und andere Regeln des Telemarketing verstießen und missbräuchlich Verbraucherdaten zu Mobilgeräten erfassten und weitergaben. Die Durchsetzungsmaßnahmen der FTC betrafen sowohl realwirtschaftliche als auch digitale Vorgänge und waren eine klare Ansage an die Unternehmen, dass sie die Privatsphäre von Verbrauchern zu respektieren haben.

Die FTC hat auch zahlreiche politische Initiativen zur wirksameren Gestaltung des Verbraucherschutzes verfolgt, die das Ziel all seiner Durchsetzungsmaßnahmen ist. Sie hat Workshops veranstaltet und Berichte mit Empfehlungen zu bewährten Verfahren herausgegeben, die auf folgende Ziele gerichtet sind: besserer Schutz der Privatsphäre im Mobile-Ökosystem; größere Transparenz in der Datenmaklerbranche; Ausschöpfung des Potenzials von Big Data bei gleichzeitiger Minderung der Risiken, insbesondere für Geringverdiener und unterversorgte Verbraucher; und Verdeutlichung der datenschutzrechtlichen und

⁵ Siehe *California Dental Ass'n v. FTC*, 526 U.S. 756 (1999).

sicherheitstechnischen Probleme, die sich aus der Gesichtserkennung, dem „Internet der Dinge“ und anderen Entwicklungen ergeben.

Die FTC bemüht sich auch um die Aufklärung von Verbrauchern und Unternehmen, damit ihre Initiativen zur Durchsetzung der Regeln und zur Politikgestaltung stärker zum Tragen kommen. Sie nutzte ein breites Instrumentarium – Veröffentlichungen, Online-Ressourcen, Workshops und soziale Medien –, um Informationsmaterial zu einem breiten Spektrum von Themen, darunter mobile Apps, Schutz der Privatsphäre von Kindern und Datensicherheit, zur Verfügung zu stellen. Unlängst brachte die Kommission ihre Initiative „Start With Security“ mit neuen Leitlinien für Unternehmen auf den Weg, die auf den Erfahrungen mit Datenschutzfällen der Behörde sowie einer Reihe von Workshops in verschiedenen Teilen des Landes aufbauen. Überdies spielt die FTC seit Langem eine führende Rolle bei der Aufklärung der Verbraucher über Grundfragen der Computersicherheit. Im letzten Jahr verzeichneten unsere Website OnGuard Online und ihr spanischsprachiges Pendant Alerta en Línea über fünf Millionen Aufrufe.

B. US-Rechtsschutz kommt EU-Verbrauchern zugute

Die Regelung ist im Gesamtzusammenhang des US-Datenschutzes zu sehen, der EU-Verbraucher auf verschiedene Weise schützt.

Das im FTC Act verankerte Verbot unlauterer oder irreführender Handlungen oder Praktiken ist nicht darauf beschränkt, US-Verbraucher vor US-Unternehmen zu schützen, da es Praktiken einschließt, die (1) tatsächlich oder wahrscheinlich einen nach vernünftigem Ermessen vorhersehbaren Schaden in den Vereinigten Staaten bewirken oder (2) entscheidungserhebliches Verhalten in den Vereinigten Staaten dabei eine Rolle spielt. Zudem kann die FTC beim Schutz ausländischer Verbraucher alle Rechtsbehelfe in Anspruch nehmen, darunter eine Wiederherstellungsklage, die zum Schutz inländischer Verbraucher zur Verfügung stehen.

Die Durchsetzungsmaßnahmen der FTC zählen sich sowohl für amerikanische als auch für ausländische Verbraucher deutlich aus. Beispielsweise galten die Klagen zur Durchsetzung von § 5 des FTC Act dem Schutz der Privatsphäre sowohl amerikanischer als auch ausländischer Verbraucher. In einem Fall, der den Informationsbroker Accusearch betraf, vertrat die FTC den Standpunkt, dass der Verkauf vertraulicher Telefondaten an Dritte ohne Wissen oder Zustimmung des Verbrauchers unlauteres Handeln darstellte und gegen § 5 des FTC verstieß. Accusearch verkaufte Daten, die sowohl US-Bürger als auch ausländische Verbraucher betrafen.⁶ Das Gericht erließ eine einstweilige Verfügung, die Accusearch unter anderem die Vermarktung oder den Verkauf personenbezogener Daten von Verbrauchern ohne schriftliche Einwilligung untersagte, sofern sie nicht rechtmäßig aus

⁶ Siehe Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Das Büro des kanadischen Datenschutzbeauftragten legte im Rechtsmittelverfahren gegen die FTC-Maßnahme einen Amicus-curiae-Schriftsatz vor und führte eigene Ermittlungen durch, die zu dem Schluss führten, dass die Praktiken von Accusearch auch gegen kanadisches Recht verstießen.

öffentlich zugänglichen Informationen beschafft wurden, und verhängte eine Geldbuße von fast 200.000 USD.⁷

Ein weiteres Beispiel ist der Vergleich, den die FTC mit TRUSTe geschlossen hat. Er stellt sicher, dass sich Verbraucher – auch in der Europäischen Union – auf Erklärungen verlassen können, die eine zur Selbstkontrolle verpflichtete globale Organisation zur Überprüfung und Zertifizierung von inländischen und ausländischen Online-Diensten abgibt.⁸ Hervorzuheben ist dabei, dass unser Vorgehen gegen TRUSTe auch das Selbstkontrollsystem im Bereich des Datenschutzes insgesamt stärkt, denn es gewährleistet die Rechenschaftspflicht von Einrichtungen, die in Systemen der freiwilligen Selbstkontrolle eine wichtige Rolle spielen, wozu auch grenzüberschreitende Datenschutzregelungen gehören.

Die FTC setzt darüber hinaus weitere zielgerichtete Rechtsvorschriften durch, deren Schutzwirkung sich auch auf Nicht-US-Verbraucher erstreckt, beispielsweise den Children's Online Privacy Protection Act („COPPA“). Dieses Gesetz schreibt vor, dass Betreiber von Websites und Online-Diensten, die für Kinder bestimmt sind, sowie von allgemeinen Websites, die wissentlich personenbezogene Daten von Kinder unter 13 Jahren erfassen, die Eltern davon in Kenntnis setzen und deren nachprüfbare Zustimmung einholen müssen. In den USA beheimatete Websites und Dienste, die dem COPPA unterliegen und personenbezogene Daten ausländischer Kinder erfassen, müssen das Gesetz einhalten. Es gilt auch für ausländische Websites und Online-Dienste, wenn sie für Kinder in den Vereinigten Staaten bestimmt sind oder wenn wissentlich personenbezogene Daten von Kindern in den USA erfasst werden. Neben den von der FTC durchgesetzten Bundesgesetzen können sich noch weitere Verbraucherschutz- und Datenschutzregelungen des Bundes und der Einzelstaaten als vorteilhaft für EU-Verbraucher erweisen.

C. Durchsetzung der Safe-Harbor-Regelung

Im Rahmen ihres Programms zur Durchsetzung des Datenschutzes und der Datensicherheit bemühte sich die FTC zudem um den Schutz der EU-Verbraucher, indem sie bei Verstößen gegen die Safe-Harbor-Regelung Durchsetzungsmaßnahmen einleitete. Die FTC hat im Rahmen von Safe Harbor 39 Durchsetzungsmaßnahmen eingeleitet: In 36 Fällen ging es um falsche Angaben zur Zertifizierung und in drei Fällen – Google, Facebook und Myspace – um mutmaßliche Verstöße gegen Datenschutzgrundsätze von Safe Harbor.⁹

⁷ Siehe *FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

⁸ Siehe *In the Matter of True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. Mar. 12, 2015) (Entscheidung und Verfügung), abrufbar unter <https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf>.

⁹ Siehe *In the Matter of Google, Inc.*, No. C-4336 (F.T.C. Oct. 13 2011) (Entscheidung und Verfügung), abrufbar unter <https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz>; *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (Entscheidung und Verfügung), abrufbar unter <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (Entscheidung und Verfügung), abrufbar unter <https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace>.

Diese Verfahren belegen, dass korrekte Angaben zur Zertifizierung durchgesetzt werden können und welche Folgen Verstöße nach sich ziehen. Mit Zustimmung der Gegenseite erlassene „Consent orders“ mit einer Geltungsdauer von zwanzig Jahren verpflichten Google, Facebook und Myspace dazu, umfassende Datenschutzprogramme zu erstellen, die nach menschlichem Ermessen so konzipiert sind, dass sie Datenschutzrisiken abdecken, die sich aus der Entwicklung bzw. Verwaltung neuer und bestehender Produkte und Dienstleistungen ergeben, und die Privatsphäre und die Vertraulichkeit personenbezogener Daten schützen. Die aufgrund dieser Verfügungen erstellten umfassenden Datenschutzprogramme müssen wesentliche vorhersehbare Risiken benennen und Kontrollen zur Ausräumung dieser Risiken vorsehen. Zudem müssen sich die Unternehmen kontinuierlichen unabhängigen Einschätzungen ihrer Datenschutzprogramme unterziehen, die der FTC vorzulegen sind. In den Verfügungen wird diesen Unternehmen auch untersagt, falsche Angaben zu ihrer Datenschutzpraxis und zur Beteiligung an einem Datenschutz- oder Sicherheitsprogramm zu machen. Dieses Verbot würde auch für die Handlungen und Praktiken von Unternehmen im Rahmen der neuen Datenschuttschild-Regelung gelten. Die FTC kann diese Verfügungen durch zivilrechtliche Klagen durchsetzen. So hat Google 2012 ein Bußgeld in Rekordhöhe, nämlich 22,5 Mio. USD, gezahlt, weil ihm Verstöße gegen die Verfügung vorgeworfen wurden. Die Maßnahmen der FTC tragen also zum Schutz von über einer Milliarde Verbraucher in der Welt bei, von denen Hunderte von Millionen in Europa beheimatet sind.

Einen weiteren Schwerpunkt der FTC bildeten falsche oder irreführende Behauptungen über eine Beteiligung an der Safe-Harbor-Regelung. Die FTC nimmt derartige falsche Angaben sehr ernst. Beispielsweise erhob die FTC 2011 in der Rechtssache *FTC/Karnani* Klage gegen einen Internet-Anbieter in den Vereinigten Staaten, dem vorgeworfen wurde, dass er und sein Unternehmen britischen Verbrauchern vortäuschte, der Sitz der Firma befände sich im Vereinigten Königreich, indem er unter anderem Webadressen mit der Endung .uk verwendete und auf die britische Währung und das britische Postsystem Bezug nahm.¹⁰ Als aber die Ware eintraf, stellten die Käufer fest, dass darauf wider Erwarten Einfuhrzölle erhoben wurden, die Garantiezusagen im Vereinigten Königreich nichts galten und Kosten für die Erstattung der Zollgebühren anfielen. Die FTC machte zudem geltend, dass die Beklagten die Verbraucher über ihre Beteiligung am Safe-Harbor-Programm getäuscht hatten. Im Übrigen waren alle Opfer des Betrugs Briten.

Bei vielen anderen Verfahren zur Durchsetzung der Safe-Harbor-Regelung ging es um Organisationen, die dem Programm beitraten, ohne ihre Zertifizierung jährlich zu erneuern, sich aber weiterhin als aktuelle Mitglieder ausgaben. Wie weiter unten dargelegt, verpflichtet sich die FTC auch dazu, gegen falsche Angaben über die Beteiligung an der Datenschuttschild-Regelung vorzugehen. Diese strategischen Durchsetzungsmaßnahmen ergänzen die verstärkten Bemühungen des Handelsministeriums, die Einhaltung der Anforderungen an die Zertifizierung und Rezertifizierung zu überprüfen, die tatsächliche Einhaltung zu überwachen, unter anderem durch Fragebogenaktionen bei den Teilnehmern,

¹⁰ Siehe *FTC v. Karnani*, No. 2:09-cv-05276 (C.D. Cal. May 20, 2011) (abschließende Verfügung), abrufbar unter <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf>; siehe auch Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, <http://www.business.ftc.gov/blog/2011/06/around-world-shady-ways> (9. Juni 2011).

und falsche Angaben zur Mitgliedschaft im Datenschutzschild und Fälle des Missbrauchs von Zertifizierungsmarken aufzudecken.¹¹

II. Die vorrangige Behandlung von überwiesenen Fällen und Ermittlungen

Wie schon beim Safe-Harbor-Programm verpflichtet sich die FTC, die ihr von EU-Mitgliedstaaten im Rahmen des Datenschutzschilds zugeleiteten Fälle vorrangig zu behandeln. Priorität haben auch Fälle, die Verstöße gegen die für den Datenschutzschild geltenden Leitlinien der freiwilligen Selbstkontrolle betreffen und mit denen wir von Einrichtungen der Selbstkontrolle und anderen unabhängigen Beschwerdestellen befasst werden.

Um im Rahmen der Regelung die Zuleitung von Fällen aus den EU-Mitgliedstaaten zu erleichtern, richtet die FTC ein standardisiertes Verweisungsverfahren ein und gibt den EU-Mitgliedstaaten eine Anleitung dazu, welche Art von Informationen für die FTC bei den Ermittlungen zu einem ihr zugeleiteten Fall besonders hilfreich ist. Zu diesem Zweck benennt die FTC innerhalb der Behörde eine Kontaktstelle für aus den EU-Mitgliedstaaten weitergeleitete Fälle. Es ist zweifellos von Vorteil, wenn die vorliegende Behörde bereits eine Voruntersuchung des mutmaßlichen Verstoßes eingeleitet hat und bei den Ermittlungen mit der FTC zusammenarbeiten kann.

Wenn ein EU-Mitgliedstaat oder eine der Selbstkontrolle unterliegende Organisation die FTC mit einer Sache befasst, kann diese eine Reihe von Maßnahmen ergreifen, um die aufgeworfenen Fragen zu klären. Beispielsweise können wir die Datenschutzpolitik des Unternehmens überprüfen; zusätzliche Informationen direkt beim Unternehmen oder bei Dritten einholen; die vorliegende Stelle dazu befragen; untersuchen, ob die Verstöße systematisch erfolgen oder eine größere Anzahl von Verbrauchern betreffen; in Erfahrung bringen, ob der uns zugeleitete Fall Fragen berührt, die in den Zuständigkeitsbereich des Handelsministeriums fallen; prüfen, ob Aufklärungsmaßnahmen für Verbraucher und Unternehmen hilfreich wären; und gegebenenfalls ein Verfahren einleiten.

Die FTC verpflichtet sich auch dazu, mit den vorlegenden Durchsetzungsinstanzen Informationen über die ihr zugeleiteten Sachen auszutauschen, unter anderem zu deren Status im Hinblick auf Geheimhaltungsvorschriften und Einschränkungen. In dem Maße, wie es Anzahl und Art der überwiesenen Fälle erlauben, enthalten die Informationen eine Beurteilung der Fälle, einschließlich einer Beschreibung der aufgeworfenen Kernfragen und der Maßnahmen, die gegen Verstöße im Zuständigkeitsbereich der FTC ergriffen wurden. Die FTC unterrichtet die vorliegende Behörde auch über die Art der ihr zugeleiteten Fälle, um die Wirksamkeit der Bemühungen um die Ahndung gesetzwidrigen Verhaltens zu erhöhen. Wenn eine vorliegende Durchsetzungsinstanz um Informationen zum Status eines bestimmten Falles ersucht, um eigene Durchsetzungsmaßnahmen zu verfolgen, wird die FTC diesem Wunsch

¹¹ Schreiben von Ken Hyatt, geschäftsführender Staatssekretär für internationalen Handel im Handelsministerium, Leiter der International Trade Administration, an Věra Jourová, Kommissionsmitglied für Justiz, Verbraucherschutz und Gleichstellungsfragen.

nachkommen, wobei sie die Anzahl der jeweils zu prüfenden Sachen ebenso berücksichtigt wie Geheimhaltungsvorschriften sowie andere rechtliche Vorgaben.

Die FTC wird auch eng mit den Datenschutzbehörden der EU zusammenarbeiten, um die Durchsetzung der Regelung zu unterstützen. In bestimmten Fällen könnten ein Informationsaustausch und Amtshilfe bei Ermittlungen gemäß U.S. SAFE WEB Act dazugehören, denn dieses Gesetz gestattet der FTC, ausländischen Strafverfolgungsbehörden Amtshilfe zu leisten, wenn die betreffende ausländische Behörde Vorschriften zur Unterbindung von Praktiken durchsetzt, die im Wesentlichen denen entsprechen, die auch nach den von der FTC durchgesetzten Vorschriften strafbar sind.¹² Im Rahmen dieser Amtshilfe kann die FTC Informationen weitergeben, die sie im Zusammenhang mit eigenen Ermittlungen erlangt hat, Zwangsmaßnahmen zur Beweissicherung im Auftrag von Datenschutzbehörden der EU anordnen, die eigene Ermittlungen durchführen, und Zeugen oder Beschuldigte im Zusammenhang mit Durchsetzungsmaßnahmen der Datenschutzbehörden anhören, wobei die Bestimmungen des U.S. SAFE WEB Act einzuhalten sind. Die FTC macht regelmäßig von diesem Recht Gebrauch, um anderen Behörden weltweit bei Daten- und Verbraucherschutzsachen zur Seite zu stehen.¹³

Die FTC räumt nicht nur im Rahmen des Datenschutzschildes den Fällen, die ihr von EU-Mitgliedstaaten und der Selbstkontrolle unterliegenden Organisationen zugeleitet werden, Priorität ein¹⁴, sondern verpflichtet sich auch dazu, mögliche Verstöße gegen die Regelung gegebenenfalls aus eigener Initiative zu untersuchen und dazu verschiedene Instrumente einzusetzen.

Seit gut einem Jahrzehnt verfolgt die FTC ein tragfähiges Programm zur Untersuchung von Datenschutz- und Sicherheitsproblemen, die in Unternehmen auftreten. Im Rahmen dieser Ermittlungen prüfte die FTC routinemäßig, ob sich die Unternehmen öffentlich zu den Safe-Harbor-Grundsätzen bekannten. Wenn dies der Fall war, die Ermittlungen aber offensichtliche

¹² Zur Beantwortung der Frage, ob sie ihre Befugnisse nach dem U.S. SAFE WEB Act ausüben sollte, prüft die FTC unter anderem, „(A) ob die vorliegende Behörde sich dazu bereit erklärt hat, ihrerseits der Kommission Amtshilfe zu leisten; (B) ob die Befürwortung des Antrags dem öffentlichen Interesse der Vereinigten Staaten zuwiderlaufen würde; und (C) ob die Ermittlungen oder Durchsetzungsmaßnahmen der vorliegenden Behörde Handlungen oder Praktiken zum Gegenstand haben, die einer größeren Zahl von Personen tatsächlich oder voraussichtlich zum Schaden gereichen.“ 15 U.S.C. § 46(j)(3). Die Befugnisse erstrecken sich nicht auf die Durchsetzung von Wettbewerbsvorschriften.

¹³ In den Haushaltsjahren 2012-2015 beispielsweise machte die FTC Gebrauch von ihren Befugnissen gemäß U.S. SAFE WEB Act, um auf fast 60 Anträge ausländischer Behörden hin Informationen weiterzugeben, und erließ fast 60 „civil investigative demands“ (Auskunftsersuchen zur Beweissicherung) und leistete damit Amtshilfe in 25 ausländischen Ermittlungsverfahren.

¹⁴ Auch wenn die FTC keinen Beschwerden einzelner Verbraucher nachgeht oder dabei vermittelt, wird sie Fälle, die ihr von Datenschutzbehörden der EU im Rahmen des Datenschutzschildes zugeleitet werden, vorrangig behandeln. Zudem wertet die FTC Beschwerden für ihre Datenbank Consumer Sentinel aus, die vielen Strafverfolgungsbehörden zugänglich ist, um Trends zu erkennen, Schwerpunkte der Durchsetzung festzulegen und mögliche Ziele von Ermittlungen auszumachen. EU-Bürger können dasselbe Beschwerdesystem, das US-Bürgern zur Verfügung steht, für eine Beschwerde an die FTC unter www.ftc.gov/complaint nutzen. Bei Individualbeschwerden, die den Datenschutzschild betreffen, ist es aber für EU-Bürger am zweckmäßigsten, wenn sie ihre Beschwerde bei einer Datenschutzbehörde ihres Mitgliedstaats oder einer Schiedsstelle einreichen.

Verstöße gegen diese Grundsätze erkennen ließen, berücksichtigte die FTC das mutmaßliche Fehlverhalten bei ihren Durchsetzungsmaßnahmen. Wir werden bei der neuen Regelung an diesem offensiven Vorgehen festhalten. Anzumerken ist, dass die Zahl der Untersuchungen, die von der FTC eingeleitet werden, wesentlich höher ist als die Zahl der Untersuchungen, die letztendlich zu öffentlichen Durchsetzungsmaßnahmen führen. Vielfach werden Ermittlungen der FTC eingestellt, weil keine offensichtlichen Rechtsverstöße erkennbar sind. Da die Untersuchungen vertraulich und nicht öffentlich zugänglich sind, wird häufig auch die Einstellung nicht publik gemacht.

Die fast 40 Durchsetzungsmaßnahmen, die von der FTC im Zusammenhang mit dem Safe-Harbor-Programm ergriffen wurden, belegen den Einsatz der Behörde für eine offensive Durchsetzung grenzüberschreitender Datenschutzregelungen. Die FTC wird bei ihren regelmäßigen Untersuchungen im Bereich des Datenschutzes und der Sicherheit auf mögliche Verstöße gegen die neue Regelung achten.

III. Unterbindung falscher oder irreführender Angaben zur Mitgliedschaft im Datenschutzschild

Wie bereits ausgeführt, wird die FTC gegen Unternehmen vorgehen, die falsche Angaben zu ihrer Beteiligung an der Regelung machen. Priorität erhalten dabei die Fälle, die ihr vom Handelsministerium zugeleitet werden und Organisationen betreffen, die wahrheitswidrig behaupten, aktuelle Mitglieder der Regelung zu sein, oder unbefugt Zertifizierungsmarken der Regelung verwenden.

Wenn im Übrigen eine Organisation in ihren Datenschutzbestimmungen zusichert, dass sie sich an die Grundsätze des Datenschutzschild hält, reicht die bloße Tatsache, dass sie sich beim Handelsministerium nicht registrieren lässt oder ihre Registrierung nicht verlängert, nicht aus, um sich der Durchsetzung dieser Zusicherungen durch die FTC zu entziehen.

IV. Kontrolle der Befolgung von Verfügungen

Die FTC bekräftigt zudem die von ihr eingegangene Verpflichtung, die Befolgung von Verfügungen zu überwachen, um die Einhaltung der Datenschutzschild-Regelung zu gewährleisten.

Wir werden bei künftigen die Regelung betreffenden FTC-Verfügungen durch eine Vielzahl geeigneter vorläufiger Anordnungen auf die Einhaltung der Grundsätze hinwirken. Dazu gehört die Untersagung von falschen Angaben zur neuen Regelung oder anderen Datenschutzprogrammen, wenn diese die Grundlage für das Vorgehen der FTC bilden.

Die bisherigen Verfahren der FTC zur Durchsetzung des Safe-Harbor-Programms sind sehr aufschlussreich. In den 36 Fällen, die falsche oder irreführende Angaben zur Safe-Harbor-Zertifizierung betrafen, untersagt die jeweilige Verfügung den Beklagten, falsche Angaben zur Beteiligung an Safe Harbor oder anderen Datenschutz- bzw. Sicherheitsprogrammen zu machen, und verpflichtet das Unternehmen dazu, der FTC Compliance-Berichte vorzulegen. Wenn es in den Verfahren um Verstöße gegen die Datenschutzgrundsätze von Safe Harbor ging, wurde es den Unternehmen zur Auflage

gemacht, umfassende Datenschutzprogramme einzurichten und zwanzig Jahre lang alle zwei Jahre für unabhängige externe Einschätzungen dieser Programme zu sorgen, die der FTC vorzulegen sind.

Die Nichtbefolgung von Verfügungen der FTC kann zur Folge haben, dass je Verstoß ein Bußgeld von bis zu 16.000 USD und bei anhaltenden Verstößen von 16.000 USD je Tag verhängt wird.¹⁵ Wenn sich die Praktiken auf zahlreiche Verbraucher auswirken, kann sich die Summe schnell auf Millionen von Dollar belaufen. Jeder „Consent order“ ist auch mit Berichts- und Einhaltungspflichten verbunden. Die betroffenen Unternehmen müssen über einen festgelegten Zeitraum die Belege für regelkonformes Verhalten aufbewahren. Auch sind sie gehalten, die Verfügungen an die Mitarbeiter weiterzuleiten, die für die Befolgung zuständig sind.

Wie bei all ihren Verfügungen kontrolliert die FTC auch bei Safe Harbor systematisch die Einhaltung der Auflagen. Sie nimmt die Durchsetzung ihrer Verfügungen in den Bereichen Datenschutz und -sicherheit sehr ernst und leitet erforderlichenfalls dazu juristische Schritte ein. Wie schon erwähnt, zahlte Google aufgrund der Anschuldigung, es habe gegen eine FTC-Verfügung verstoßen, ein Bußgeld von 22,5 Millionen USD. Die Verfügungen der FTC werden auch künftig alle Verbraucher weltweit schützen, die Kunden eines Unternehmens sind, und nicht nur jene unter ihnen, die Beschwerden eingereicht haben.

Abschließend dazu sei betont, dass die FTC weiterhin eine Online-Liste von Unternehmen führen wird, die Auflagen im Zusammenhang mit der Durchsetzung des Safe-Harbor-Programms und der neuen Datenschuttschild-Regelung unterliegen.¹⁶ Überdies sind nach den Grundsätzen des Datenschuttschilds alle Unternehmen, die aufgrund von Verstößen gegen die Grundsätze Auflagen der FTC oder eines Gerichts erfüllen müssen, jetzt dazu verpflichtet, sämtliche die Regelung betreffenden Abschnitte eines der FTC vorgelegten Compliance- oder Prüfberichts publik zu machen, soweit die Geheimhaltungsvorschriften und -regeln dies gestatten.

V. Verstärkte Kontakte zu Datenschutzbehörden der EU und engere Zusammenarbeit mit ihnen bei der Durchsetzung

Die FTC erkennt die wichtige Rolle an, die Datenschutzbehörden der EU bei der Einhaltung der Regelung spielen, und befürwortet verstärkte Konsultationen und eine engere Zusammenarbeit bei der Durchsetzung. Über Rücksprachen mit vorlegenden Datenschutzbehörden zu fallspezifischen Fragen hinaus verpflichtet sich die FTC, an regelmäßigen Zusammenkünften mit dazu benannten Vertretern der Artikel-29-Datenschutzgruppe teilzunehmen, um in allgemeiner Form darüber zu diskutieren, wie sich die Zusammenarbeit bei der Durchsetzung der Regelung verbessern lässt. Die FTC wird sich zudem gemeinsam mit dem Handelsministerium, der Europäischen Kommission und

¹⁵ 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

¹⁶ Siehe FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=251.

Vertretern der Artikel-20-Datenschutzgruppe an der jährlichen Überprüfung der Regelung beteiligen, um die praktische Umsetzung zu erörtern.

Die FTC wirkt auch auf die Entwicklung von Instrumenten hin, die eine verstärkte Zusammenarbeit mit Datenschutzbehörden der EU sowie ähnlichen Einrichtungen in der ganzen Welt bei Durchsetzungsmaßnahmen ermöglichen. Vor allem hat die FTC zusammen mit Partnern in der Europäischen Union und der übrigen Welt im letzten Jahr ein Warnsystem innerhalb des Global Privacy Enforcement Network („GPEN“) ins Leben gerufen, um Informationen über Ermittlungen auszutauschen und die Koordinierung der Durchsetzungsmaßnahmen zu fördern. Dieses als „GPEN Alert“ bezeichnete Instrument könnte sich bei der Datenschutzschild-Regelung als besonders nützlich erweisen. Die FTC und die Datenschutzbehörden der EU könnten es für diesbezügliche und andere datenschutzrechtliche Ermittlungen nutzen, auch als Ausgangspunkt für den Informationsaustausch, um für einen besser koordinierten und effektiveren Verbraucherschutz zu sorgen. Wir sehen erwartungsvoll der weiteren Zusammenarbeit mit den beteiligten EU-Behörden entgegen, damit wir das GPEN-Alert-System auf noch breiterer Grundlage einsetzen und weitere Instrumente entwickeln können, die zur Verbesserung der Zusammenarbeit bei der Durchsetzung des Datenschutzes, auch im Rahmen der neuen Regelung, beitragen.

Die FTC bekennt sich hiermit zu ihrer Verpflichtung, der neuen Datenschutzschild-Regelung zum Erfolg zu verhelfen. Wir freuen uns darauf, weiterhin im Zusammenwirken mit unseren Kollegen in der EU den Verbraucherschutz beiderseits des Atlantiks zu befördern.

Hochachtungsvoll

Edith Ramirez
Vorsitzende

ANLAGE A

Der EU-US-Datenschutzschild in der Praxis: Ein Überblick über das Datenschutz- und -sicherheitsumfeld in den USA

Das durch die Regelung zum EU-US-Datenschutzschild („die Regelung“) gebotene Sicherheitsniveau ist in die umfassenderen Datenschutzvorschriften des US-Rechtssystems eingebettet. Erstens wacht die Federal Trade Commission („FTC“) der USA mithilfe eines wirksamen Datenschutz- und -sicherheitsprogramms für US-Geschäftspraktiken über den weltweiten Verbraucherschutz. Zweitens hat sich das Umfeld für Verbraucherdatenschutz und -sicherheit in den USA seit dem Jahre 2000, als die ursprüngliche Safe-Harbor-Regelung zwischen den USA und der EU angenommen wurde, merklich gewandelt. In der Zwischenzeit wurden auf Bundesebene und in den Einzelstaaten zahlreiche Gesetze zum Datenschutz und zur Datensicherheit erlassen, und es war ein deutlicher Anstieg bei der Zahl der Verwaltungs- und Zivilprozesse zur Durchsetzung der Datenschutzrechte zu vermelden. Ergänzt wird der für Einzelpersonen in der EU mit der neuen Regelung verbundene Rechtsschutz durch ein breites Spektrum an US-Rechtsvorschriften für den Schutz und die Sicherheit von Verbraucherdaten, die für den Umgang mit Geschäftsdaten gelten.

I. Das allgemeine Programm des FTC zur Durchsetzung des Datenschutzes und der Datensicherheit

Die FTC ist die führende Verbraucherschutzbehörde in den USA und vorrangig im Bereich des Datenschutzes im Geschäftsverkehr aktiv. Sie ist befugt, unlautere und irreführende Handlungen oder Praktiken, die gegen den Verbraucherdatenschutz verstoßen, zu verfolgen und zielgenauere Datenschutzregelungen durchzusetzen, um bestimmte Finanz- und Gesundheitsdaten, Daten von Kindern sowie Daten, auf deren Grundlage bestimmte Entscheidungen über Anspruchsberechtigungen von Verbrauchern getroffen werden, zu schützen.

Die FTC verfügt über einzigartige Erfahrungen im Bereich der Durchsetzung des Verbraucherdatenschutzes. Die bisherigen Durchsetzungsmaßnahmen der FTC betrafen gesetzwidrige Praktiken im Offline- und Online-Umfeld. So hat die FTC beispielsweise Durchsetzungsmaßnahmen gegen bekannte Unternehmen wie Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC und Snapchat sowie gegen weniger bekannte Unternehmen eingeleitet. Sie hat Unternehmen verklagt, denen vorgeworfen wurde, unerbetene Werbung an Verbraucher zu senden, Spyware auf PCs zu installieren, personenbezogene Daten von Verbrauchern nicht zu schützen, das Verhalten von Verbrauchern unter Vorspiegelung falscher Tatsachen online zu verfolgen, die Privatsphäre von Kindern zu verletzen, missbräuchlich Verbraucherdaten über Mobilgeräte zu erfassen und Endgeräte mit Internet-Zugang, die zur Speicherung personenbezogener Daten genutzt werden, nicht zu sichern. In der Regel wurde in diesen Fällen für einen Zeitraum von zwanzig Jahren eine kontinuierliche Überwachung durch die FTC angeordnet, weitere

Gesetzesverstöße wurden untersagt und hohe Geldstrafen für den Fall angekündigt, dass die Unternehmen gegen diese Verfügungen verstoßen.¹ Die Verfügungen der FTC schützen nicht nur jene Verbraucher, die Beschwerde eingereicht haben, sondern alle Verbraucher, die Kunde eines Unternehmens sind. Auf grenzüberschreitender Ebene ist die FTC für den weltweiten Verbraucherschutz im Zusammenhang mit allen in den USA stattfindenden Praktiken zuständig.²

Bisher ist die FTC Verstößen in mehr als 130 Spam- und Spyware-Fällen nachgegangen, hat über 120 Anrufsverbote im Telemarketing verhängt, mehr als 100 Maßnahmen im Bereich des Fair Credit Reporting Act (Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten) ergriffen, ist in nahezu 60 Datensicherheitsfällen und mehr als 50 allgemeinen Datenschutzfällen sowie in etwa 30 Fällen einer Verletzung des Gramm-Leach-Bliley Act tätig geworden und hat mehr als 20 Maßnahmen zur Durchsetzung des Children's Online Privacy Protection Act („COPPA“) eingeleitet.³ Neben den genannten Fällen hat die FTC auch Warnschreiben verfasst und herausgegeben.⁴

Darüber hinaus hat die FTC im Rahmen ihrer bisherigen Bemühungen um eine konsequente Handhabung des Datenschutzes kontinuierlich über mögliche Verstöße gegen die Safe-Harbor-Regelung gewacht. Seit Annahme der Safe-Harbor-Regelung hat die FTC auf eigene Initiative zahlreiche Ermittlungen im Zusammenhang mit der Einhaltung der Safe-Harbor-Verfahren geführt und 39 Verfahren gegen US-Unternehmen wegen Verstößen gegen die Safe-Harbor-Regelung eingeleitet. Diese proaktive Herangehensweise will die FTC auch weiterhin fortsetzen und dabei der Durchsetzung der neuen Regelung eine hohe Priorität einräumen.

II. Verbraucherdatenschutz auf Bundesebene und in den Einzelstaaten

Der Überblick über die Möglichkeiten der Durchsetzung der Grundsätze des sicheren Hafens im Anhang zur Entscheidung der Kommission über die Angemessenheit des von den Grundsätzen des sicheren Hafens gewährleisteten Schutzes enthält eine Zusammenfassung

¹ Gegen ein Unternehmen, das gegen eine Verfügung der FTC verstößt, kann ein Bußgeld von bis zu 16 000 USD und bei anhaltenden Verstößen von 16 000 USD je Tag verhängt werden. Siehe 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

² Der Kongress hat ausdrücklich die Befugnis der FTC bekräftigt, Rechtsbehelfe, darunter auch eine Wiederherstellungsklage, in Anspruch zu nehmen bei allen für den Außenhandel bedeutenden Handlungen oder Praktiken, die 1. tatsächlich oder wahrscheinlich einen nach vernünftigem Ermessen vorhersehbaren Schaden in den Vereinigten Staaten bewirken oder (2) bei denen entscheidungserhebliches Verhalten in den Vereinigten Staaten eine Rolle spielt. Siehe 15 U.S.C. § 45(a)(4).

³ In einigen der von ihr behandelten Datenschutz- und -sicherheitsfälle geht die FTC davon aus, dass ein Unternehmen, das sich sowohl irreführender als auch unlauterer Praktiken bedient hat, bisweilen auch gegen mehrere Gesetze verstoßen hat, darunter gegen den Fair Credit Reporting Act, den Gramm-Leach-Bliley Act und den COPPA.

⁴ Siehe beispielsweise Pressemitteilung, FTC, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations (22. Dez. 2014), <https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa>; Pressemitteilung, FTC, FTC Warns Data Broker Operations of Possible Privacy Violations (7. Mai 2013), <https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations>; Pressemitteilung, FTC, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (3. Apr. 2013), <https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may>.

vieler der zum Zeitpunkt der Annahme der Safe-Harbor-Regelung im Jahre 2000 auf Bundesebene und in den Einzelstaaten geltenden Datenschutzgesetze.⁵ Zu diesem Zeitpunkt wurde die gewerbliche Erfassung und Verwendung personenbezogener Daten durch zahlreiche Bundesgesetze – neben §5 des FTC Act – geregelt, darunter der Cable Communications Policy Act, der Driver's Privacy Protection Act, der Electronic Communications Privacy Act, der Electronic Funds Transfer Act, der Fair Credit Reporting Act, der Gramm-Leach-Bliley Act, der Right to Financial Privacy Act, der Telephone Consumer Protection Act und der Video Privacy Protection Act. Viele Bundesstaaten hatten in diesen Bereichen eine analoge Rechtsprechung.

Seit dem Jahr 2000 hat es auf Bundesebene und in den Einzelstaaten grundlegende Veränderungen gegeben, die zu einem zusätzlichen Verbraucherdatenschutz beitragen.⁶ So hat die FTC im Jahre 2013 auf Bundesebene beispielsweise den COPPA überarbeitet, um einige zusätzliche Schutzmechanismen für die personenbezogenen Angaben von Kindern einzuführen. Darüber hinaus hat sie mit der Datenschutz- und der Garantiebestimmung zwei Bestimmungen zur Umsetzung des Gramm- Leach-Bliley Act eingeführt, die Finanzinstitutionen dazu verpflichten⁷ ihre Praktiken beim Austausch von Informationen offenzulegen und ein umfassendes Informationssicherheitsprogramm zum Schutz von Verbraucherdaten zu erarbeiten.⁸ Der im Jahre 2003 eingeführte Fair and Accurate Credit Transactions Act („FACTA“) dient ebenfalls der Ergänzung altbewährter US-Kreditgesetze und enthält Bestimmungen zur Unkenntlichmachung, gemeinsamen Nutzung und Vernichtung sensibler Finanzdaten. Im Rahmen des FACTA hat die FTC eine Reihe von Regeln eingeführt, die sich unter anderem auf das Recht der Verbraucher auf einen kostenfreien jährlichen Kreditbericht, auf Bestimmungen zur sicheren Vernichtung von gemeldeten Verbraucherdaten, auf das Recht der Verbraucher, den Erhalt bestimmter Informationen zu Krediten und Versicherungen abzubestellen, auf das Recht der Verbraucher, der Verwendung von durch ein Tochterunternehmen bereitgestellten Angaben für die Vermarktung seiner Produkte und Dienstleistungen zu widersprechen sowie auf Anforderungen an Institutionen und Kreditgeber zur Durchführung von Programmen zur Ermittlung und Prävention von Identitätsdiebstahl beziehen.⁹ Darüber hinaus wurden die im

⁵ Siehe U.S.-Handelministerium, Safe Harbor Enforcement Overview (Überblick über die Möglichkeiten der Durchsetzung der Grundsätze des sicheren Hafens), https://build.export.gov/main/safeharbor/eu/eg_main_018481.

⁶ Für einen umfassenderen Überblick über den Rechtsschutz in den USA siehe Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5th ed. 2015).

⁷ Gemäß dem Gramm-Leach-Bliley Act sind Finanzinstitutionen alle Unternehmen, die vornehmlich mit der Bereitstellung von Finanzprodukten und –dienstleistungen befasst sind. Dazu gehören beispielsweise Scheckeinlösestellen, Kurzzeitkreditgeber, Hypothekemakler, nichtinstitutionelle Kreditgeber, Sachverständige für persönliche Vermögens- und Immobilienbewertung und professionelle Steuerberater.

⁸ Im Rahmen des Consumer Financial Protection Act von 2010 („CFPA“), Titel X der Pub. L. 111-203, 124 Stat. 1955 (21. Juli 2010) (auch bekannt unter der Bezeichnung „Dodd-Frank Wall Street Reform and Consumer Protection Act“) wurde der Großteil der Gesetzgebungsbefugnisse der FTC gemäß dem Gramm-Leach-Bliley Act an das Consumer Financial Protection Bureau („CFPB“) übertragen. Die FTC behält ihre Durchsetzungsbefugnisse im Rahmen des Gramm-Leach-Bliley Act sowie die Regelungsbefugnisse in Bezug auf Garantieregeln sowie eingeschränkte Regulierungsbefugnisse gemäß den Datenschutzregeln in Bezug auf Kraftfahrzeughändler.

⁹ Im Rahmen des CFPA verfügt die FTC über eine gemeinsame Zuständigkeit mit der CFPB bei der Durchsetzung des FCRA, während die Regulierungsbefugnis größtenteils auf die CFPB übertragen wurde (mit Ausnahme der „Roten Flaggen“ und der Vorschriften zur Datenvernichtung).

Rahmen des Health Insurance Portability and Accountability Act eingeführten Regeln im Jahre 2013 überarbeitet und um zusätzliche Garantien für den Schutz und die Sicherheit personenbezogener Gesundheitsdaten ergänzt.¹⁰ Dank neuer Vorschriften werden Verbraucher zudem vor unerbetener Telefonwerbung, computergesteuerten Werbeanrufen und Spam geschützt. Der Kongress hat ferner Gesetze erlassen, die Gesundheitsinformationen erfassende Unternehmen dazu verpflichten, Verbraucher über einen möglichen Verstoß zu unterrichten.¹¹

Auch in den Bundestaaten wurden zahlreiche Gesetze im Bereich Datenschutz und -sicherheit erlassen. Seit dem Jahre 2000 haben 47 Bundesstaaten, der District of Columbia, Guam, Puerto Rico und die Virgin Islands Gesetze eingeführt, die Unternehmen dazu verpflichten, Einzelpersonen über Verstöße gegen die Sicherheit personenbezogener Angaben zu unterrichten.¹² In mindestens 32 Staaten sowie in Puerto Rico gibt es Gesetze zur Datenvernichtung mit Vorschriften zur Zerstörung oder Vernichtung personenbezogener Daten.¹³ In einer Reihe von Bundesstaaten wurden zudem allgemeine Datensicherheitsgesetze erlassen. Darüber hinaus wurden in Kalifornien unterschiedliche Datenschutzgesetze eingeführt, darunter ein Gesetz, das Unternehmen zur Festlegung von Datenschutzbestimmungen und zur Offenlegung ihrer „do-not-track“-Verfahren verpflichtet¹⁴ sowie ein „Shine the Light“-Gesetz mit höheren Transparenzanforderungen an Datenvermittler¹⁵ und ein Gesetz, das die Einführung einer Schaltfläche vorsieht, mit der Minderjährige die Löschung bestimmter Daten in sozialen Medien auslösen können.¹⁶ Mit Hilfe dieser Gesetze sowie weiterer Befugnisse konnten die Regierungen auf Bundesebene und in den Einzelstaaten hohe Geldbußen gegen Unternehmen verhängen, die den Schutz und die Sicherheit der personenbezogenen Daten von Verbrauchern nicht gewährleistet haben.¹⁷

Auch zivilrechtliche Verfahren hatten erfolgreiche gerichtliche Entscheidungen und Vergleiche zum Ergebnis, die zu mehr Datenschutz und -sicherheit für Verbraucher beitragen. So hat beispielsweise Target im Jahre 2015 zugestimmt, im Rahmen eines Vergleichs 10 Mio. USD an Kunden zu zahlen, die Klage wegen Missbrauchs ihrer personenbezogenen Finanzdaten im Zuge einer umfassenden Datenschutzverletzung eingereicht hatten. AOL hat sich 2013 bereit erklärt, im Rahmen eines Vergleichs 5 Mio. USD zu zahlen, um eine Sammelklage wegen unzureichender Anonymisierung im Zusammenhang mit der

¹⁰ Siehe 45 C.F.R. pts. 160, 162, 164.

¹¹ Siehe beispielsweise American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) sowie einschlägige Regelungen, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

¹² Siehe beispielsweise National Conference of State Legislatures (“NCSL”), *State Security Breach Notification Laws* (Jan. 4, 2016), einzusehen unter <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

¹³ NCSL, *Data Disposal Laws* (12. Januar 2016), einzusehen unter <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx>.

¹⁴ Cal. Bus. & Professional Code §§ 22575-22579.

¹⁵ Cal. Civ. Code §§ 1798.80-1798.84.

¹⁶ Cal. Bus. & Professional Code § 22580-22582.

¹⁷ Siehe Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (17 Feb. 2014), einzusehen unter http://www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=17&pageNumber=1.

Veröffentlichung von Suchanfragen von Hunderttausenden AOL-Nutzern abzuwehren. Darüber hinaus hat ein Bundesgericht einer Zahlung in Höhe von 9 Mio. USD durch Netflix zugestimmt. Gegen das Unternehmen war Beschwerde eingereicht worden, weil es entgegen den Bestimmungen aus dem Video Privacy Protection Act von 1988 die Verleihhistorien seiner Nutzer gespeichert hatte. Bundesgerichte in Kalifornien haben zwei separate Vergleiche mit Facebook über 20 bzw. 9,5 Mio. USD genehmigt, in denen es um die Erfassung, die Verwendung und den Austausch personenbezogener Daten der Nutzer durch das Unternehmen ging. Ferner hat ein Gericht des Bundesstaats Kalifornien im Jahre 2008 einem Vergleich in Höhe von 20 Mio. USD in einem Verfahren gegen LensCrafters wegen unrechtmäßige Offenlegung medizinischer Verbraucherinformationen zugestimmt.

Alles in allem zeigt dieser Überblick, dass in den USA ein umfassender Rechtsschutz im Bereich Verbraucherdatenschutz und -sicherheit besteht. Auf dieser soliden Rechtsgrundlage, die Verbraucherdatenschutz und -sicherheit nach wie vor oberste Priorität einräumt, kann die neue Datenschutzschild-Regelung zur Anwendung kommen, mit der wirksame Garantien für Einzelpersonen in der EU verbunden sind.

ANHANG V:
Schreiben von US-Verkehrsminister Anthony Foxx

19. Februar 2016

Kommissionsmitglied Vera Jourová
Europäische Kommission
Rue de la Loi / Wetstraat 200
1049 Brüssel
Belgien

Re: EU-US-Datenschutzschild

Sehr geehrte Frau Jourová,

das US-Verkehrsministerium („Ministerium“ oder „DOT“) freut sich über diese Gelegenheit, näher auf seine Rolle bei der Umsetzung des EU-US-Datenschutzschilds eingehen zu können. Der Datenschutzschild leistet einen wesentlichen Beitrag zum Schutz personenbezogener Daten, die im Geschäftsverkehr in einer zunehmend vernetzten Welt zur Verfügung gestellt werden. Er ermöglicht Unternehmen die Durchführung wichtiger Transaktionen in der Weltwirtschaft und stellt gleichzeitig sicher, dass EU-Verbraucher weiterhin durch grundlegende Datenschutzbestimmungen geschützt werden.

Bereits vor mehr als 15 Jahren hat das Verkehrsministerium in einem an die Europäische Kommission gerichteten Schreiben erstmals sein Engagement für die Durchsetzung der Safe-Harbor-Regelung zum Ausdruck gebracht. In diesem Schreiben hat sich das Ministerium dazu verpflichtet, die Grundsätze der Safe-Harbor-Regelung mit Nachdruck geltend zu machen. An dieser Verpflichtung hält das Ministerium unverändert fest, woran mit dem vorliegenden Schreiben erinnert werden soll.

Das erneuerte Engagement des Ministeriums bezieht sich insbesondere auf die folgenden Schlüsselbereiche: 1) vorrangige Ermittlung bei mutmaßlichen Verstößen gegen die Grundsätze des Datenschutzschilds, 2) angemessene Durchsetzungsmaßnahmen gegen Organisationen, die falsche oder irreführende Angaben zur Beteiligung am Datenschutzschild machen und 3) Kontrolltätigkeit und Unterrichtung der Öffentlichkeit über behördliche Durchsetzungsmaßnahmen. Auf jede dieser Verpflichtungen wollen wir im Folgenden näher eingehen und relevante Hintergrundinformationen zur Rolle des Ministeriums beim Schutz

von Verbraucherdaten und bei der Durchsetzung der Datenschutzschild-Regelung liefern, um den notwendigen Kontext herzustellen.

I. Hintergrund

A. Die Datenschutzabteilung im Ministerium

Das Ministerium setzt sich konsequent dafür ein, die Geheimhaltung personenbezogener Daten, die Verbraucher den Luftverkehrsgesellschaften oder den Inhabern von Kartenverkaufsstellen überlassen werden, zu gewährleisten. Die Handlungsbefugnisse des Ministeriums auf diesem Gebiet ergeben sich aus 49 U.S.C. 41712. Diese Vorschrift verbietet Luftverkehrsgesellschaften oder Inhabern von Kartenverkaufsstellen, unlautere und irreführende Praktiken beim Verkauf von Flugtickets anzuwenden, die den Verbraucher schädigen bzw. schädigen könnten. § 41712 ist nach dem Vorbild von § 5 des Federal Trade Commission Act (15 U.S.C. 45) aufgebaut. Nach unserer Auslegung ist es einer Luftverkehrsgesellschaft oder einem Inhaber einer Kartenverkaufsstelle gemäß dem Gesetz über unlautere und irreführende Praktiken untersagt: 1) gegen die eigenen Datenschutzbestimmungen zu verstoßen oder 2) personenbezogene Daten in einer Art und Weise zu erfassen oder offenzulegen, die der öffentlichen Ordnung zuwiderläuft, gegen moralische Grundsätze verstößt oder dem Verbraucher einen erheblichen Schaden zufügt, der nicht durch geldwerte Vorteile aufgehoben wird. Gemäß § 41712 ist es Luftverkehrsgesellschaften oder Inhabern einer Kartenverkaufsstelle nach unserer Auslegung ebenfalls verboten: 1) gegen eine vom Ministerium verabschiedete Regel zu verstoßen, wonach bestimmte Datenschutzpraktiken als unlauter oder irreführend eingestuft werden oder 2) den Children's Online Privacy Protection Act (COPPA) oder FTC-Bestimmungen zu seiner Umsetzung zu verletzen. Gemäß Bundesgesetz verfügt das Ministerium über die alleinige Befugnis, die Datenschutzpraxis von Luftverkehrsgesellschaften zu regulieren, und mit der FTC über die gemeinsame Befugnis, die Datenschutzpraxis der Inhaber von Verkaufsstellen für Flugtickets zu regeln.

Sobald sich eine Luftverkehrsgesellschaft oder der Inhaber einer Verkaufsstelle für Flugtickets öffentlich zu den Rahmengrundsätzen des Datenschutzschildes bekennt, kann das Ministerium daher von den rechtlichen Befugnissen gemäß § 41712 Gebrauch machen und die Einhaltung dieser Grundsätze sicherstellen. Gibt also ein Passagier Informationen an eine Luftverkehrsgesellschaft oder den Inhaber einer Verkaufsstelle, die sich zur Einhaltung der Rahmengrundsätze des Datenschutzschildes verpflichtet haben, dann würde ein Verstoß gegen diese Grundsätze eine Verletzung der Bestimmungen des § 41712 darstellen.

B. Durchsetzungsmaßnahmen

Die Dienststelle des Ministeriums für Rechtsdurchsetzung und Verfahren im Luftverkehr (Office of Aviation Enforcement and Proceedings/Aviation Enforcement Office) untersucht und verfolgt Fälle, die 49 U.S.C. 41712 betreffen. Sie setzt das gesetzliche Verbot unlauterer und irreführender Praktiken gemäß § 41712 durch, insbesondere auf dem Verhandlungswege sowie durch den Erlass von Unterlassungsanordnungen und Anordnungen zur Festsetzung

zivilrechtlicher Sanktionen. Die Dienststelle wird auf mögliche Verstöße insbesondere durch Beschwerden von Privatpersonen, Reisebüros, Luftverkehrsgesellschaften sowie US-amerikanischen und ausländischen staatlichen Stellen aufmerksam. Verbraucher haben die Möglichkeit, über die Website des Ministeriums Beschwerden wegen Verletzung der Datenschutzbestimmungen durch Luftverkehrsgesellschaften und Inhaber von Kartenverkaufsstellen einzureichen.¹

Sollte in einem Fall keine angemessene und geeignete Vereinbarung erzielt werden können, ist die Dienststelle befugt, zur Rechtsdurchsetzung ein Verfahren einzuleiten, das eine Beweisverhandlung vor einem Verwaltungsrichter des Ministeriums vorsieht. Der Verwaltungsrichter ist befugt, Unterlassungsanordnungen sowie zivilrechtliche Sanktionen festzulegen. Eine Verletzung der Bestimmungen des § 41712 kann Unterlassungsanordnungen nach sich ziehen; der Verstoß gegen diese Anordnungen kann zivilrechtliche Sanktionen in Höhe von bis zu 27 500 USD für jeden Verstoß gegen § 41712 zur Folge haben.

Das Ministerium hat nicht das Recht, beschwerdeführenden Privatpersonen Schadenersatz oder finanzielle Entschädigungen zuzuerkennen. Es kann allerdings Vereinbarungen genehmigen, die sich aus von seiner Dienststelle eingebrachten Untersuchungen ergeben und dem Verbraucher als Ausgleich für andernfalls an die US-Regierung zu entrichtende Geldbußen einen unmittelbaren Vorteil (z. B. in Form von Bargeld, Gutscheinen) verschaffen. Dies wurde in der Vergangenheit so gehandhabt und kann auch im Zusammenhang mit den Rahmengrundsätzen des Datenschutzschildes weiterhin so gehandhabt werden, falls die Umstände dies erfordern. Sollte eine Luftverkehrsgesellschaft die Bestimmungen des § 41712 wiederholt verletzen, würden Zweifel an der Bereitschaft der Gesellschaft zur Einhaltung der Grundsätze aufkommen, was in gravierenden Fällen dazu führen könnte, dass die Gesellschaft als nicht mehr betriebstauglich angesehen und ihr somit die wirtschaftliche Betriebsgenehmigung entzogen würde.

Bisher sind beim Ministerium relativ wenige Beschwerden wegen mutmaßlicher Verstöße gegen die Datenschutzbestimmungen durch Inhaber von Kartenverkaufsstellen und Luftverkehrsgesellschaften eingegangen. Bei Vorliegen einer Beschwerde wird diese gemäß den im Vorangehenden ausgeführten Grundsätzen geprüft.

C. Der durch das Ministerium gewährte Rechtsschutz kommt EU-Verbrauchern zugute

Gemäß § 41712 gilt das Verbot unlauterer und irreführender Praktiken im Luftverkehr oder beim Verkauf von Flugtickets für amerikanische oder ausländische Luftverkehrsunternehmen oder Inhaber von Kartenverkaufsstellen. Das Ministerium geht häufig gegen amerikanische und ausländische Luftverkehrsunternehmen wegen Praktiken vor, die sich sowohl auf ausländische als auch auf amerikanische Verbraucher nachteilig

¹ <http://www.transportation.gov/airconsumer/privacy-complaints>.

auswirken, sofern diese bei der Erbringung von Verkehrsdienstleistungen mit Ziel oder Ausgangspunkt in den USA stattgefunden haben. Das Ministerium nutzt alle ihm zur Verfügung stehenden Rechtsbehelfe und wird dies auch weiterhin tun, um ausländische wie amerikanische Verbraucher vor unlauteren und irreführenden Praktiken im Luftverkehr vonseiten beaufsichtigter Unternehmen zu schützen.

Im Zusammenhang mit Luftverkehrsunternehmen setzt das Ministerium darüber hinaus weitere zielgerichtete Gesetze durch, die Bestimmungen zum Schutz von Verbrauchern außerhalb der USA beinhalten, darunter das COPPA. Dieses Gesetz verlangt unter anderem von Betreibern von Websites und Online-Diensten, die an Kinder gerichtet sind, sowie von für die Allgemeinheit bestimmten Websites, die wissentlich personenbezogene Daten von Kindern unter 13 erheben, dass sie die Eltern darüber in Kenntnis setzen und die nachweisliche Zustimmung der Eltern einholen. In den USA betriebene Websites und Dienste, die dem COPPA unterliegen und personenbezogene Daten von ausländischen Kindern erheben, sind an die Bestimmungen des COPPA gebunden. Im Ausland betriebene Websites und Dienste müssen sich ebenfalls daran halten, wenn sie sich an Kinder in den USA richten oder wissentlich personenbezogene Daten von Kindern in den USA erheben. Für den Fall, dass amerikanische oder ausländische Luftverkehrsunternehmen, die in den USA geschäftlich tätig sind, gegen das COPPA verstoßen, ist das Ministerium zur Einleitung von Durchsetzungsmaßnahmen befugt.

II. Durchsetzung des Datenschutzschilds

Sobald sich eine Luftverkehrsgesellschaft oder der Inhaber einer Kartenverkaufsstelle für eine Beteiligung am Datenschutzschild entscheidet und beim Ministerium eine Beschwerde eingeht, wonach diese Luftverkehrsgesellschaft bzw. dieser Inhaber einer Kartenverkaufsstelle gegen die Grundsätze verstoßen hat, kann das Ministerium folgende Schritte einleiten, um dem Datenschutzschild mit Nachdruck Geltung zu verschaffen.

A. Vorrangige Ermittlung bei mutmaßlichen Verstößen

Die Dienststelle des Ministeriums für Rechtsdurchsetzung und Verfahren im Luftverkehr prüft alle Beschwerden wegen mutmaßlicher Verstöße gegen den Datenschutzschild (dazu gehören auch Beschwerden von EU-Datenschutzbehörden) und leitet Durchsetzungsmaßnahmen ein, sofern es Anzeichen für einen Verstoß gibt. Darüber hinaus arbeitet die Dienststelle mit der FTC und dem Handelsministerium zusammen und befasst sich vorrangig mit Beschwerden über den Verstoß beaufsichtigter Unternehmen gegen im Rahmen des Datenschutzschilds eingegangene Datenschutzverpflichtungen.

Nach Eingang einer Beschwerde über einen mutmaßlichen Verstoß gegen den Datenschutzschild kann die Dienststelle im Rahmen ihrer Ermittlungen eine Reihe von Maßnahmen ergreifen. So kann sie beispielsweise die Datenschutzbestimmungen des Inhabers einer Kartenverkaufsstelle oder der Luftverkehrsgesellschaft überprüfen, beim Inhaber der Kartenverkaufsstelle, bei der Luftverkehrsgesellschaft oder bei Dritten

zusätzliche Informationen einholen, die vorlegende Stelle dazu befragen und untersuchen, ob die Verstöße systematisch erfolgen oder eine größere Anzahl von Verbrauchern betreffen. Darüber hinaus stellt die Dienststelle fest, ob in dem vorliegenden Fall Sachverhalte berührt werden, die in den Zuständigkeitsbereich des Handelsministeriums oder der FTC fallen, sie prüft, ob Aufklärungsmaßnahmen für Verbraucher und Unternehmen hilfreich wären und leitet gegebenenfalls ein Verfahren ein.

Sollte das Ministerium Kenntnis von möglichen Verstößen gegen den Datenschutzschild durch die Inhaber von Kartenverkaufsstellen erhalten, stimmt es sein weiteres Vorgehen mit der FTC ab. Darüber hinaus unterrichten wir die FTC und das Handelsministerium über die Ergebnisse von Durchsetzungsmaßnahmen im Rahmen des Datenschutzschilds.

B. Vorgehen bei falschen oder irreführenden Angaben zur Beteiligung

Das Ministerium bekräftigt seine Zusage, im Falle von Verstößen gegen den Datenschutzschild, die auch falsche oder irreführende Angaben zur Beteiligung am Datenschutzschild-Programm einschließen, Ermittlungen einzuleiten. Wir behandeln vorrangig Fälle, die uns durch das Handelsministerium übermittelt werden und Organisationen betreffen, die sich seinen Nachforschungen zufolge unrechtmäßig als Mitglied des Datenschutzschilds bezeichnen oder das Gütesiegel des Datenschutzschilds ohne Genehmigung verwenden.

Wenn im Übrigen eine Organisation in ihren Datenschutzbestimmungen zusichert, dass sie sich an die Grundsätze des Datenschutzschilds hält, reicht die bloße Tatsache, dass sie sich beim Handelsministerium nicht registrieren lässt oder ihre Registrierung nicht verlängert, nicht aus, um sich der Durchsetzung dieser Zusicherungen durch das Handelsministerium zu entziehen.

C. Überwachung von Durchsetzungsmaßnahmen bei Verstößen gegen den Datenschutzschild und Unterrichtung der Öffentlichkeit darüber

Darüber hinaus bekräftigt die Dienststelle des Ministeriums ihr Engagement für die Überwachung möglicher Durchsetzungsmaßnahmen, die zur Gewährleistung der Einhaltung der Grundsätze des Datenschutzschilds erforderlich sein können. Insbesondere wenn die Dienststelle eine Anordnung an eine Luftverkehrsgesellschaft oder einen Inhaber einer Kartenverkaufsstelle erlässt, in der künftige Verstöße gegen den Datenschutzschild und gegen § 41712 untersagt werden, überwacht sie in der Folge die Einhaltung der Vorgaben in der Unterlassungsanordnung durch die jeweilige Organisation. Die Dienststelle stellt zudem sicher, dass Anordnungen im Zusammenhang mit den Datenschutzschild betreffenden Fällen auf ihrer Website eingesehen werden können.

Einer weiteren Zusammenarbeit mit unseren Partnern in den USA und mit den verantwortlichen Akteuren in der EU in allen den Datenschutzschild betreffenden Angelegenheiten sehen wir erwartungsvoll entgegen.

Ich hoffe, dass Ihnen diese Ausführungen weiterhelfen. Falls Sie noch Fragen haben oder weitere Auskünfte benötigen, wenden Sie sich bitte vertrauensvoll an mich.

Hochachtungsvoll

Anthony R. Foxx
Verkehrsminister

ANHANG VI

Schreiben von General Counsel Robert Litt Amt des Director of National Intelligence

22. Februar 2016

Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Sehr geehrter Herr Antonipillai,
sehr geehrter Herr Dean,

im Verlaufe der letzten zweieinhalb Jahre stellten die Vereinigten Staaten im Zusammenhang mit den Verhandlungen zum EU-US-Datenschutzschild umfangreiche Informationen über die Erhebungstätigkeit der US Intelligence Community im Wege der signalerfassenden Aufklärung bereit. Dazu gehören Auskünfte zum geltenden rechtlichen Rahmen, zu der auf verschiedenen Ebenen durchgeführten Überwachung dieser Tätigkeiten, zu deren weitreichender Transparenz und zu den allgemeinen Maßnahmen für den Schutz der Privatsphäre und der bürgerlichen Freiheiten, die der Europäischen Kommission die Entscheidung über die Angemessenheit dieser Schutzmaßnahmen erleichtern sollten, soweit sie sich auf die aus Gründen der nationalen Sicherheit gewährten Ausnahmen von den Grundsätzen des Datenschutzschildes beziehen. Dieses Dokument enthält eine Zusammenfassung der übermittelten Informationen.

I. Die PPD-28 und die Durchführung der signalerfassenden Aufklärung in den USA

Die Vorgehensweise der Intelligence Community der USA bei der Beschaffung ihrer Auslandsaufklärungsdaten unterliegt einer sorgfältigen Kontrolle, steht voll und ganz im Einklang mit den Rechtsvorschriften der USA und wird auf verschiedenen Ebenen überwacht, wobei das Hauptaugenmerk auf wichtigen Daten der Auslandsaufklärung und Schwerpunkten der nationalen Sicherheit liegt. Ein Mosaik aus Gesetzen und Maßnahmen regelt die Signalaufklärung in den USA, darunter die Verfassung der USA, der Foreign Intelligence Surveillance Act (50 U.S.C., § 1801 ff.) (FISA), Executive Order 12333 und damit zusammenhängende Durchführungsverfahren, Direktiven des Präsidenten sowie zahlreiche durch das FISA-Gericht und den Justizminister gebilligte Verfahren und Leitlinien, mit denen

zusätzliche Regeln zur Einschränkung der Erhebung, Speicherung, Nutzung und Weitergabe von Auslandsaufklärungsdaten festgelegt werden.¹

a. Die PPD-28 im Überblick

Im Januar 2014 erläuterte Präsident Obama in einer Rede verschiedene Reformen in der signalerfassenden Aufklärung der USA und unterzeichnete hierzu die Presidential Policy Directive 28 (PPD-28).² Der Präsident betonte, dass die US-Signalaufklärung nicht nur dazu dient, unser Land und unsere Freiheiten zu schützen, sondern auch zum Schutz der Sicherheit und der Freiheiten anderer Länder beiträgt, einschließlich der EU-Mitgliedstaaten, die zum Schutz ihrer eigenen Bürger auf Erkenntnisse von US-Nachrichtendiensten zugreifen.

Die PPD-28 enthält eine Reihe von Grundsätzen und Anforderungen, die für sämtliche Aktivitäten der US-Signalaufklärung und für alle Personen unabhängig von Nationalität oder Standort gelten. Insbesondere werden Anforderungen an Verfahren im Zusammenhang mit der Erhebung, Speicherung und Weitergabe von personenbezogenen Daten zu Nicht-US-Bürgern festgelegt, die im Rahmen der US-Signalaufklärung gesammelt wurden. Diese Anforderungen werden nachstehend detaillierter, aber dennoch zusammenfassend, dargelegt:

- In der PPD wird bekräftigt, dass die Vereinigten Staaten Signalaufklärungsdaten nur in dem Umfang erheben, wie dies per Gesetz, Executive Order oder Presidential Directive zulässig ist.
- In der PPD sind Verfahren festgelegt, mit denen sichergestellt wird, dass signalerfassende Aufklärung nur zur Förderung von legitimen und autorisierten Zielsetzungen der nationalen Sicherheit erfolgt.
- In der PPD wird zudem gefordert, dass bei der Planung der signalerfassenden Aufklärung die Privatsphäre und die bürgerlichen Freiheiten integraler Bestandteil aller Überlegungen sind. Insbesondere sammeln die Vereinigten Staaten keine Geheimdienstinformationen, um Kritik oder abweichende Meinungen zu unterdrücken oder zu belasten, um Menschen aufgrund ihrer ethnischen Zugehörigkeit, ihrer Rasse, ihres Geschlechts, ihrer sexuellen Orientierung oder ihres Glaubens zu diskriminieren oder um amerikanischen Firmen oder bestimmten amerikanischen Branchen einen Wettbewerbsvorteil zu verschaffen.
- In der PPD ist festgelegt, dass die Datenerhebung im Rahmen der signalerfassenden Aufklärung immer so „passgerecht wie möglich“ erfolgen muss und dass Daten als Ergebnis von Sammelerhebungen nur für bestimmte, explizit aufgeführte Zwecke genutzt werden dürfen.
- In der PPD ist festgelegt, dass die Intelligence Community Verfahren anwendet, die so sinnvoll konzipiert sind, dass sie die Weitergabe und Speicherung von personenbezogenen Daten aus der signalerfassenden Aufklärung auf ein Mindestmaß

¹ Weitere Informationen zur US-Auslandsaufklärung werden online veröffentlicht und sind über „IC on the Record“ (www.icontherecord.tumblr.com) abrufbar, der öffentlichen Website des ODNI, mit der die nachrichtendienstlichen Aktivitäten der Regierung für die Öffentlichkeit transparenter gemacht werden sollen.

² *Abrufbar unter* <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

beschränken und vor allem bestimmte Schutzmaßnahmen, die für personenbezogene Daten von US-Bürgern gelten, auch auf Daten von Nicht-US-Bürger erweitern.

- Es wurden behördliche Verfahren zur Umsetzung der PPD-28 festgelegt und publik gemacht.

Die Anwendbarkeit der darin festgelegten Verfahren und Schutzmaßnahmen auf den Datenschutzschild steht außer Frage. Nach der Übermittlung von Daten an Unternehmen in den Vereinigten Staaten im Rahmen des Datenschutzschilds – oder auch auf jede andere Art und Weise – dürfen die amerikanischen Nachrichtendienste diese Daten von den Unternehmen nur abfragen, wenn ihr Antrag mit dem FISA im Einklang steht oder über einen National Security Letter erfolgt, die an anderer Stelle erläutert werden.³ Ohne dass Medienberichte bestätigt oder dementiert werden, wonach die US Intelligence Community Daten aus transatlantischen Kabeln sammelt, während sie in die Vereinigten Staaten übertragen werden, würde eine solche Datensammlung vorbehaltlich der hierin dargelegten Beschränkungen und Garantien erfolgen, einschließlich der Anforderungen der PPD-28.

b. Beschränkungen der Datenerhebung

Die PPD-28 legt eine Reihe wichtiger allgemeiner Grundsätze für die Erhebung von Signalaufklärungsdaten fest:

- Die signalerfassende Aufklärung muss gesetzlich zulässig oder vom Präsidenten autorisiert sein und muss im Einklang mit der Verfassung der USA und dem amerikanischen Recht stehen.
- Die Privatsphäre und die bürgerlichen Freiheiten sind integraler Bestandteil aller Überlegungen bei der Planung der signalerfassenden Aufklärung.
- Die signalerfassende Aufklärung kommt ausschließlich dann zum Einsatz, wenn dies der Auslandsaufklärung oder der Spionageabwehr dient.
- Die Vereinigten Staaten sammeln keine Signalaufklärungsdaten, um Kritik oder abweichende Meinungen zu unterdrücken oder zu belasten.
- Die Vereinigten Staaten sammeln keine Signalaufklärungsdaten, um Menschen aufgrund ihrer ethnischen Zugehörigkeit, ihrer Rasse, ihres Geschlechts, ihrer sexuellen Orientierung oder ihres Glaubens zu diskriminieren.
- Die Vereinigten Staaten sammeln keine Signalaufklärungsdaten, um amerikanischen Firmen oder bestimmten amerikanischen Branchen einen Wettbewerbsvorteil zu verschaffen.
- Die signalerfassende Aufklärung der USA muss *immer* so „passgerecht wie möglich“ erfolgen und dabei die Verfügbarkeit anderer Informationsquellen berücksichtigen. Das bedeutet unter anderem, dass – wann immer dies machbar ist – eine gezielte Datenerhebung und keine Sammelerhebung erfolgt.

Die Anforderung, dass die signalerfassende Aufklärung so „passgerecht wie möglich“ erfolgen sollte, gilt sowohl für die Art und Weise, in der Signalaufklärungsdaten erhoben

³ Strafverfolgungs- oder Aufsichtsbehörden können von Unternehmen die Herausgabe von Daten für Ermittlungszwecke in den USA nach Maßgabe anderer Justiz- und Aufsichtsbehörden verlangen, die nicht in den Anwendungsbereich dieses Dokuments fallen, der auf die nationalen Sicherheitsbehörden beschränkt ist.

werden, als auch für die Daten selbst. Bei der Entscheidung darüber, ob Daten dieser Art erhoben werden sollen, muss die Intelligence Community die Verfügbarkeit anderer Informationen prüfen, einschließlich diplomatische oder öffentliche Quellen, und bei der Erhebung vorrangig auf diese Alternativen zurückgreifen, sofern diese geeignet und machbar sind. Darüber hinaus sollten die Nachrichtendienste, wann immer dies praktikabel erscheint, die Erhebung auf spezifische Aufklärungsziele oder -themen im Ausland konzentrieren, indem sie Selektoren (z. B. konkrete Objekte, Suchkriterien und Identifikatoren) heranziehen.

Die der Kommission bereitgestellten Informationen müssen unbedingt in ihrer Gesamtheit gesehen werden. Die Entscheidungen darüber, was „machbar“ oder „praktikabel“ ist, bleiben nicht dem Ermessen Einzelner überlassen, sondern sind Gegenstand der Strategien, die die Nachrichtendienste zur Umsetzung der PPD-28 erlassen haben – und die öffentlich zugänglich gemacht wurden – sowie der anderen darin beschriebenen Verfahren.⁴ Wie es in der PPD-28 heißt, erfolgt bei einer Sammelerhebung von Signalaufklärungsdaten die Erhebung „aufgrund technischer oder operativer Erwägungen“ ohne die Heranziehung von Selektoren (z. B. konkrete Objekte, Suchkriterien und Identifikatoren)“. In diesem Zusammenhang wird in der PPD-28 anerkannt, dass Nachrichtendienste unter bestimmten Umständen auf die Sammelerhebung zurückgreifen müssen, um neue oder sich abzeichnende Bedrohungen zu erkennen oder andere für die nationale Sicherheit hochwichtige Informationen zu erlangen, die oftmals innerhalb des großen und komplexen Systems der modernen globalen Kommunikation verborgen sind. Auch die im Zusammenhang mit der Sammelerhebung vorgebrachten Bedenken, was den Schutz der Privatsphäre und der bürgerlichen Freiheiten betrifft, werden in der PPD-28 nicht von der Hand gewiesen. Folglich orientiert sie die Intelligence Community dahingehend, Alternativen den Vorzug zu geben, die eine gezielte Signalaufklärung ermöglichen. Nachrichtendienste sollten – wann immer dies möglich ist – die Sammelerhebung durch gezielte Informationsgewinnung ersetzen.⁵ Diese Grundsätze gewährleisten, dass ungeachtet der Ausnahme der Sammelerhebung die allgemeine Regel bestehen bleibt.

Was das Konzept der Verhältnismäßigkeit betrifft, so handelt es sich um einen fundamentalen Grundsatz des US-Rechts. Die Nachrichtendienste sollen demnach nicht theoretisch mögliche Maßnahmen ergreifen, sondern müssen ihre Bemühungen um den Schutz der legitimen Interessen auf dem Gebiet des Datenschutzes und der bürgerlichen Freiheiten mit den praktischen Erfordernissen der signalerfassenden Aufklärung in Einklang bringen. Auch in diesem Zusammenhang haben die Nachrichtendienste ihre Strategien vorgelegt, mit denen gesichert werden kann, dass die allgemeine Regel nicht untergraben wird, wenn Maßnahmen „so sinnvoll konzipiert sind, dass sie die Weitergabe und Speicherung von personenbezogenen Daten auf ein Mindestmaß beschränken“.

⁴ *Abrufbar unter* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Mit diesen Verfahren werden die in diesem Schreiben erörterten Konzepte der Zielgenauigkeit und Passgerechtigkeit in einer für die einzelnen Nachrichtendienste spezifischen Form umgesetzt.

⁵ In den Durchführungsbestimmungen der NSA zur PPD-28 – um nur ein Beispiel zu nennen – heißt es, dass nach Möglichkeit bei der Erhebung ein Selektor oder mehrere Selektoren angewandt werden, um die Erhebung auf spezifische Aufklärungsziele (z. B. einen konkreten, bekannten internationalen Terroristen oder eine Terroristengruppe) oder Aufklärungsthemen (z. B. die Verbreitung von Massenvernichtungswaffen durch eine ausländische Macht oder deren Vertreter) im Ausland zu konzentrieren.

Die PPD-28 beschränkt außerdem die Nutzung der durch Sammelerhebung gewonnenen Signalaufklärungsdaten auf eine Liste von sechs spezifischen Zielsetzungen, und zwar die Ermittlung und Abwehr bestimmter Aktivitäten ausländischer Mächte, Terrorismusbekämpfung, Nichtverbreitung von Massenvernichtungswaffen, Cybersecurity, Aufdeckung und Abwehr von Bedrohungen für die amerikanischen oder mit ihnen verbündeten Streitkräfte und Abwehr länderübergreifender krimineller Bedrohungen, einschließlich Umgehung von Sanktionen. Der Nationale Sicherheitsberater des Präsidenten wird in Absprache mit dem Director for National Intelligence (DNI) jährlich Überprüfungen zu diesen zulässigen Nutzungszwecken durchführen und feststellen, ob Änderungen erforderlich sind. Der DNI macht diese Liste unter Berücksichtigung der Interessen der nationalen Sicherheit in größtmöglichem Umfang publik. Dadurch wird die Nutzung von Signalaufklärungsdaten aus Sammelerhebungen ganz wesentlich und gleichzeitig auf transparente Art und Weise eingeschränkt.

Abgesehen davon haben die mit der Umsetzung der PPD-28 befassten Nachrichtendienste vorhandene Analysemethoden und -standards für die Abfrage ungeprüfter Signalaufklärungsdaten verschärft.⁶ Die Analysten müssen ihre Anfragen oder Suchbegriffe und -methoden so strukturieren, dass sie mit Sicherheit Aufklärungsdaten bezeichnen können, die für einen begründeten Zweck der Auslandsaufklärung oder Strafverfolgung von Belang sind. Zu diesem Zweck müssen die Nachrichtendienste bei Anfragen zu Personen die Kategorien der Signalaufklärungsdaten in den Mittelpunkt stellen, die den Erfordernissen der Auslandsaufklärung oder Strafverfolgung entsprechen, um so die Verwendung von personenbezogenen Informationen zu verhindern, die für den Zweck der Auslandsaufklärung oder Strafverfolgung nicht relevant sind.

Es ist wichtig zu betonen, dass die Sammelerhebung von Internetdaten, die von der Intelligence Community der USA im Wege der signalerfassenden Aufklärung durchgeführt wird, nur einen kleinen Teil des Internets berührt. Gezielte Abfragen, wie sie an anderer Stelle beschrieben wurden, stellen zudem sicher, dass den Analysten nur Objekte vorgelegt werden, die einen potenziellen Erkenntniswert aufweisen. Ziel dieser Einschränkungen ist es, die Privatsphäre und die bürgerlichen Freiheiten aller Personen unabhängig von ihrer Nationalität und ihrem Wohnort zu schützen.

Die Vereinigten Staaten bedienen sich aufwändiger Verfahren, um zu gewährleisten, dass signalerfassende Aufklärung nur zur Förderung von angemessenen Zielsetzungen der nationalen Sicherheit erfolgt. Jedes Jahr legt der Präsident nach einem umfassenden formellen Verfahren unter Einbeziehung aller Nachrichtendienste die höchsten Prioritäten des Landes in der Auslandsaufklärung fest. Der DNI ist für die Umsetzung dieser nachrichtendienstlichen Schwerpunkte im „National Intelligence Priorities Framework“, oder NIPF, zuständig. Durch die PPD-28 wurde das behördenübergreifende Verfahren gestärkt und weiter ausgestaltet, damit gesichert ist, dass alle Schwerpunkte der nachrichtendienstlichen Tätigkeit auf hoher politischer Ebene überprüft und bestätigt werden. Die Intelligence Community Directive (ICD) 204 gibt weiterführende Orientierung zum NIPF und wurde im Januar 2015 zur Aufnahme der

⁶ *Abrufbar unter* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Anforderungen der PPD-28 aktualisiert.⁷ Der NIPF selbst unterliegt der Geheimhaltung, jedoch finden Informationen zu den spezifischen Schwerpunkten der Auslandsaufklärung der USA jährlich Eingang in die nicht geheime „*Worldwide Threat Assessment*“ des DNI, die auf der ODNI-Website leicht zugänglich ist.

Die Schwerpunkte im NIPF tragen in recht hohem Maße allgemeinen Charakter. Sie beinhalten Themen wie die Bestrebungen feindlicher ausländischer Akteure im Bereich nuklearer und ballistischer Raketen, die Auswirkungen von Drogenkartellen und Korruption sowie Menschenrechtsverletzungen in bestimmten Ländern. Und sie gelten nicht nur für die signalerfassende Aufklärung, sondern für alle nachrichtendienstlichen Tätigkeiten. Zuständig für die Umsetzung der NIPF-Schwerpunkte bei der tatsächlichen Erhebung von Signalaufklärungsdaten ist das National Signals Intelligence Committee, oder SIGCOM. Es agiert unter der Leitung des Direktors der National Security Agency (NSA), der gemäß Executive Order 12333 die Aufgaben eines „operativen Leiters der signalerfassenden Aufklärung“ wahrnimmt und für die Überwachung und Koordinierung der Signalaufklärung der gesamten Intelligence Community zuständig ist und dabei sowohl vom Verteidigungsminister als auch vom DNI beaufsichtigt wird. Im SIGCOM sind alle Nachrichtendienste vertreten, und da die USA die PPD-28 vollständig umsetzen, werden auch andere Regierungsstellen, die ein politisches Interesse an der signalerfassenden Aufklärung haben, umfassend repräsentiert sein.

Alle Ministerien und Regierungsstellen der USA, die die Auslandsaufklärung für sich in Anspruch nehmen, richten ihre Auskunftsersuchen an das SIGCOM. Dieses prüft die Ersuchen, stellt sicher, dass sie mit dem NIPF in Einklang stehen und versieht sie mit Schwerpunkten, wobei unter anderem folgende Kriterien zur Anwendung kommen:

- Kann die signalerfassende Aufklärung in diesem Fall nützliche Informationen liefern oder gibt es bessere oder kostengünstigere Informationsquellen zur Erfüllung der Anfrage, wie etwa Bildmaterial oder öffentliche Informationsquellen?
- Wie wichtig ist dieser Informationsbedarf? Wenn er im NIPF mit hoher Priorität eingestuft ist, kommt ihm größtenteils bei der Signalaufklärung hohe Priorität zu.
- Welche Art der signalerfassenden Aufklärung könnte eingesetzt werden?
- Ist die Erhebung so passgerecht wie möglich? Sollte es zeitliche, geografische oder sonstige Beschränkungen geben?

Beim amerikanischen Verfahren zur Prüfung der Erfordernisse einer Signalaufklärung sind ausdrücklich auch andere Faktoren zu berücksichtigen, nämlich:

- Ist das Ziel der Erhebung oder die verwendete Erhebungsmethode besonders sensibel? Wenn ja, ist eine Überprüfung durch ranghohe Entscheidungsträger erforderlich.
- Ist mit der Erhebung ein ungerechtfertigtes Risiko für den Schutz der Privatsphäre und die bürgerlichen Freiheiten unabhängig von der Nationalität verbunden?

⁷ Abrufbar unter

<http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf>.

- Sind zusätzliche Garantien bezüglich Weitergabe und Speicherung erforderlich, um die Privatsphäre oder nationale Sicherheitsinteressen zu schützen?

Zum Abschluss des Verfahrens schließlich untersuchen und benennen ausgebildete NSA-Mitarbeiter auf der Grundlage der vom SIGCOM validierten Schwerpunkte konkrete Suchkriterien wie etwa Telefonnummern oder E-Mail-Adressen, anhand derer Erkenntnisse aus dem Ausland gewonnen werden können, die den Schwerpunkten entsprechen. Jeder Selektor muss überprüft und bestätigt werden, bevor er in die Erhebungssysteme der NSA aufgenommen wird. Aber selbst dann werden zum Teil noch zusätzliche Kriterien wie die Verfügbarkeit von geeigneten Erhebungsressourcen herangezogen, um zu entscheiden, ob und wann die tatsächliche Erhebung stattfindet. Durch dieses Verfahren wird gewährleistet, dass die Ziele der US-Signalaufklärung einen begründeten und wichtigen Bedarf an Auslandsaufklärungsdaten widerspiegeln. Und natürlich müssen die NSA und andere Nachrichtendienste bei Durchführung der Erhebung gemäß FISA weitere Einschränkungen nach Maßgabe des Foreign Intelligence Surveillance Court beachten. Kurz gesagt, weder die NSA noch ein anderer amerikanischer Nachrichtendienst entscheidet selbst darüber, was erhoben wird.

Generell ist dieses Verfahren Gewähr dafür, dass die Schwerpunkte der nachrichtendienstlichen Tätigkeit der USA allesamt von ranghohen politischen Entscheidungsträgern festgelegt werden, die die Erfordernisse im Bereich der Auslandsaufklärung am besten bestimmen können, und dass diese Entscheidungsträger nicht nur den potenziellen Wert der geheimdienstlichen Datenerhebung im Auge haben, sondern auch die damit verbundenen Risiken, einschließlich der Gefahren für den Datenschutz, die nationalen wirtschaftlichen Interessen und die Außenbeziehungen.

Wenngleich die Vereinigten Staaten konkrete nachrichtendienstliche Methoden oder Operationen nicht bestätigen oder dementieren können, so gelten doch in Bezug auf die im Rahmen des Datenschutzschildes in die Vereinigten Staaten übermittelten Daten die Anforderungen der PPD-28 für alle von den Vereinigten Staaten durchgeführten Operationen der signalerfassenden Aufklärung, unabhängig von Art oder Quelle der erhobenen Daten. Zudem gelten die auf die signalerfassende Aufklärung anzuwendenden Einschränkungen und Garantien für alle Signalaufklärungsdaten, die für einen autorisierten Zweck erhoben wurden, was sowohl die Außenbeziehungen als auch die Belange der nationalen Sicherheit einschließt.

Die hier erörterten Verfahren lassen das deutliche Bemühen erkennen, die willkürliche und anlassunabhängige Erhebung signalerfassender Aufklärungsdaten zu verhindern und – ausgehend von den höchsten Ebenen staatlicher Verwaltung – dem Grundsatz der Verhältnismäßigkeit Geltung zu verschaffen. Mit der PPD-28 und den Durchführungsverfahren der Nachrichtendienste werden neue und bestehende Einschränkungen bei der Signalaufklärung eindeutig geregelt, und es wird konkreter festgelegt, für welchen Zweck die Vereinigten Staaten Signalaufklärungsdaten erheben und verwenden. Dadurch sollte gesichert sein, dass Aktivitäten der signalerfassenden Aufklärung jetzt und in Zukunft nur zur Verfolgung berechtigter Ziele der Auslandsaufklärung durchgeführt werden.

c. Einschränkungen der Speicherung und Weitergabe

§ 4 der PPD-28 schreibt für die gesamte Intelligence Community Grenzen für die Speicherung und Weitergabe von personenbezogenen Daten betreffend Nicht-US-Bürger vor, die im Wege der signalerfassenden Aufklärung erhoben wurden, und diese Grenzen sind mit den für US-Bürger geltenden Grenzen vergleichbar. Diese Regelungen sind Bestandteil der für die einzelnen Nachrichtendienste geltenden Verfahren, die im Februar 2015 herausgegeben wurden und öffentlich zugänglich sind. Um für eine Speicherung oder Weitergabe als Auslandsaufklärungsdaten in Frage zu kommen, müssen sich die personenbezogenen Daten auf einen autorisierten Zweck der nachrichtendienstlichen Tätigkeit beziehen, wie er entsprechend dem weiter oben beschriebenen NIPF-Verfahren bestimmt wurde, müssen mit hinreichender Bestimmtheit Anhaltspunkte für eine Straftat liefern oder einem der anderen Standards für die Speicherung von Daten zu US-Bürgern gemäß Executive Order 12333, Abschnitt 2.3., entsprechen.

Daten, für die keine derartigen Festlegungen gelten, dürfen nicht länger als fünf Jahre gespeichert werden, sofern nicht der DNI ausdrücklich bestimmt, dass eine weitere Speicherung im Interesse der nationalen Sicherheit der Vereinigten Staaten liegt. Die Nachrichtendienste müssen daher Informationen zu Nicht-US-Bürgern, die per Signalaufklärung erhoben wurden, fünf Jahre nach der Erhebung löschen, wenn nicht beispielsweise festgestellt wurde, dass die Daten für ein autorisiertes Ziel der Auslandsaufklärung von Belang sind oder der DNI unter Berücksichtigung der Auffassung des ODNI Civil Liberties Protection Officer sowie der Datenschutz- und Bürgerrechtsbeauftragten der Behörde zu der Entscheidung gelangt, dass eine weitere Speicherung dem nationalen Sicherheitsinteresse entspricht.

Darüber hinaus ist mittlerweile bei allen nachrichtendienstlichen Maßnahmen zur Umsetzung der PPD-28 ausdrücklich vorgeschrieben, dass personenbezogene Daten nicht einfach weitergegeben werden dürfen, weil die betreffende Person kein US-Bürger ist, und das ODNI hat im Sinne dieser Anforderung eine Direktive an alle Nachrichtendienste gerichtet⁸. Geheimdienstmitarbeiter sind ausdrücklich aufgefordert, bei der Erarbeitung und Weitergabe von Aufklärungsberichten den Schutz der Privatsphäre von Nicht-US-Bürgern zu berücksichtigen. Insbesondere wird signalerfassende Aufklärung über die alltäglichen Aktivitäten eines ausländischen Staatsangehörigen nicht als Auslandsaufklärung angesehen, die man allein aus diesem Grund weitergeben oder dauerhaft speichern darf, ohne dass sie einem autorisiertem Zweck der Auslandsaufklärung dient. Damit wird eine wichtige Einschränkung anerkannt und den Bedenken der Europäischen Kommission bezüglich der Breite der Definition der Auslandsaufklärung gemäß Executive Order 12333 Rechnung getragen.

d. Compliance und Überwachung

Das US-System zur Überwachung der Auslandsaufklärung sieht eine gründliche und mehrstufige Kontrolle vor, um die Einhaltung der geltenden Gesetze und Verfahren zu gewährleisten, auch was die Erhebung, Speicherung und Weitergabe von Daten zu Nicht-US-Bürgern betrifft, die per Signalaufklärung gemäß PPD-28 erhoben wurden. Das beinhaltet Folgendes:

⁸ Intelligence Community Directive (ICD) 203, abrufbar unter <http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf>.

- Die Intelligence Community beschäftigt Hunderte von Mitarbeitern für die Überwachung. Bei der NSA allein befassen sich 300 Mitarbeiter mit der Compliance, und andere Nachrichtendienste haben ebenfalls Überwachungsbüros. Darüber hinaus werden die nachrichtendienstlichen Tätigkeiten vom Justizministerium umfassend beaufsichtigt, und ebenso nimmt das Verteidigungsministerium eine Aufsichtsfunktion wahr.
- Jeder Nachrichtendienst verfügt über ein eigenes Büro des Generalinspektors, das unter anderem für die Überwachung der Auslandsaufklärung zuständig ist. Generalinspektoren sind rechtlich unabhängig, haben umfassende Befugnisse zur Durchführung von Untersuchungen, Audits und Überprüfungen im Zusammenhang mit den Programmen, darunter auch in Bezug auf Betrug sowie Missbrauchsfälle oder Rechtsverstöße, und können Korrekturmaßnahmen empfehlen. Zwar sind derartige Empfehlungen nicht bindend, doch werden die Berichte der Generalinspektoren oftmals publik gemacht und in jedem Fall dem Kongress übermittelt, was Folgeberichte einschließt, wenn in vorangegangenen Berichten empfohlene Korrekturmaßnahmen noch nicht abgeschlossen sind. Der Kongress wird daher über jede Nichteinhaltung informiert und kann durch entsprechenden Druck, nicht zuletzt über die Haushaltsmittel, auf die Durchsetzung der Korrekturmaßnahme hinarbeiten. Mehrere Berichte von Generalinspektoren zu Aufklärungsprogrammen wurden veröffentlicht.⁹
- Das ODNI Civil Liberties and Privacy Office (CLPO) hat die Aufgabe sicherzustellen, dass die Nachrichtendienste durch die Art ihrer Vorgehensweise dem Schutz der nationalen Sicherheit dienen und gleichzeitig die bürgerlichen Freiheiten und das Recht auf Privatsphäre geschützt werden.¹⁰ Andere Nachrichtendienste haben ihre eigenen Datenschutzbeauftragten.
- Dem Privacy and Civil Liberties Oversight Board (PCLOB), einem unabhängigen, gesetzlich festgelegten Gremium, obliegt die Analyse und Überprüfung von Programmen und Maßnahmen zur Terrorismusbekämpfung, einschließlich des Einsatzes signalerfassender Aufklärung, um in diesem Zusammenhang den Schutz der Privatsphäre und der bürgerlichen Freiheiten zu gewährleisten. Er hat mehrere öffentliche Berichte zu nachrichtendienstlichen Aktivitäten herausgegeben.
- Wie an anderer Stelle noch ausführlicher dargelegt wird, ist das FISA-Gericht (Foreign Intelligence Surveillance Court), das aus einem Gremium unabhängiger Bundesrichter besteht, für die Überwachung aller Signalaufklärungsaktivitäten gemäß FISA und die damit zusammenhängenden Compliance-Fragen zuständig.
- Und schließlich nimmt auch der Kongress der USA, vor allem über die Ausschüsse des Repräsentantenhauses und des Senats für Nachrichtendienste und Justiz, wichtige Kontrollaufgaben wahr, die alle Formen der Auslandsaufklärung, darunter die US-Signalaufklärung, betreffen.

⁹ *Siehe z. B.* U.S. Department of Justice, Inspector General Report „A Review of the Federal Bureau of Investigation’s Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008“ (September 2012), *abrufbar unter* <https://oig.justice.gov/reports/2016/o1601a.pdf>.

¹⁰ *Siehe* www.dni.gov/clpo.

Abgesehen von diesen formellen Überwachungsmechanismen verfügen auch die Nachrichtendienste selbst über verschiedene Mechanismen, um die Einhaltung der bereits beschriebenen Einschränkungen bei der Erhebung zu sichern. Hier einige Beispiele:

- Von Kabinettsbeamten wird gefordert, dass sie ihre Anforderungen an die Signalaufklärung jährlich validieren.
- Die NSA kontrolliert die Ziele der Signalaufklärung während der gesamten Erhebung, um festzustellen, ob damit tatsächlich wertvolle Erkenntnisse aus dem Ausland gewonnen werden, die den Schwerpunkten entsprechen. Für Ziele, bei denen dies nicht der Fall ist, wird die Erhebung eingestellt. Durch zusätzliche Verfahren ist eine regelmäßige Überprüfung der Suchkriterien gewährleistet.
- Ausgehend von der Empfehlung einer von Präsident Obama benannten unabhängigen Review Group hat der DNI einen neuen Mechanismus zur Überwachung der Erhebung und Weitergabe von Signalaufklärungsdaten eingerichtet, der bedingt durch die Art des Zieles bzw. das Mittel der Erhebung besonders sensibel ist, um auf diese Weise eine vollständige Übereinstimmung mit den auf politischer Ebene getroffenen Festlegungen sicherzustellen.
- Schließlich prüft das ODNI jährlich die von den Nachrichtendiensten vorgenommene Ressourcenverteilung nach Schwerpunkten und die nachrichtendienstliche Tätigkeit insgesamt. Im Rahmen dieser Prüfung erfolgt eine Beurteilung des Nutzens aller Arten der geheimdienstlichen Datenerhebung, einschließlich der signalerfassenden Aufklärung, und es wird sowohl ein Resümee gezogen – wie erfolgreich hat die Intelligence Community ihre Ziele umgesetzt? – als auch nach vorn geschaut – wie sieht der künftige Bedarf der Intelligence Community aus? So wird sichergestellt, dass die Ressourcen der Signalaufklärung für die wichtigsten nationalen Schwerpunkte zum Einsatz kommen.

Aus diesen umfassenden Darlegungen geht hervor, dass die Intelligence Community nicht allein entscheidet, welche Gespräche abgehört werden, dass sie keine lückenlose Erfassung anstrebt und nicht frei von Kontrolle operiert. Sie richtet ihre Aktivitäten auf die von den politischen Entscheidungsträgern festgelegten Schwerpunkt aus, was insgesamt mit einem Prozess verbunden ist, in den sich die verschiedensten staatlichen Stellen einbringen und der sowohl innerhalb der NSA als auch durch das ODNI, das Justizministerium und das Verteidigungsministerium überwacht wird.

Die PPD-28 enthält zahlreiche weitere Bestimmungen zur Sicherung des Schutzes von personenbezogenen Signalaufklärungsdaten, unabhängig von der Nationalität. Beispielsweise trifft sie mit Blick auf den Schutz dieser Daten Regelungen zur Datensicherheit, zum Zugang und zu Qualitätsverfahren und sieht obligatorische Schulungen vor, damit sich die Mitarbeiter jederzeit der Verantwortung für den Schutz personenbezogener Daten unabhängig von der Nationalität bewusst sind. Die PPD orientiert zudem auf zusätzliche Überwachungs- und Compliance-Mechanismen. Dazu gehört, dass die Verfahren zum Schutz der personenbezogenen Informationen, die bei der Signalaufklärung anfallen, regelmäßig von kompetenten Überwachungs- und Compliance-Mitarbeitern überprüft und begutachtet werden. Bei den Prüfungen muss zudem die Einhaltung der Verfahren zum Schutz solcher Daten seitens der Nachrichtendienste untersucht werden.

Darüber hinaus wird in der PPD-28 geregelt, dass wichtige Compliance-Probleme in Bezug auf Nicht-US-Bürger an höhere Regierungsebenen weitergeleitet werden. Im Falle eines wichtigen Compliance-Problems, bei dem es um personenbezogene Daten geht, die per Signalaufklärung erhoben wurden, muss das Problem ungeachtet sonstiger bestehender Berichtspflichten unverzüglich dem DNI gemeldet werden. Sind hierbei die personenbezogenen Daten einer Nicht-US-Person betroffen, entscheidet der DNI in Abstimmung mit dem Außenminister und dem Leiter des betreffenden Nachrichtendienstes darüber, ob Schritte einzuleiten sind, um die betreffende ausländische Regierung in einer Weise davon in Kenntnis zu setzen, die mit dem Schutz der Quellen und Methoden und der US-Mitarbeiter vereinbar ist. Darüber hinaus hat der Außenminister gemäß PPD-28 als Ansprechpartner für ausländische Regierungen, die Bedenken im Zusammenhang mit der US-Signalaufklärung vorbringen, eine hochrangige Beamtin eingesetzt, Under Secretary Catherine Novelli. Dieses Bekenntnis zu einem Engagement auf höchster Ebene ist beispielhaft für die Bemühungen der US-Regierung in den letzten Jahren, Vertrauen in die zahlreichen bestehenden und sich überschneidenden Bestimmungen zum Schutz der Daten von US-Bürgern und Nicht-US-Bürgern zu schaffen.

e. Zusammenfassung

Die Verfahren der Vereinigten Staaten für die Erhebung, Speicherung und Weitergabe von Daten aus der Auslandsaufklärung schließen wichtige Vorkehrungen zum Schutz der personenbezogenen Daten aller Personen unabhängig von der Nationalität ein. Insbesondere wird durch diese Verfahren sichergestellt, dass sich unsere Intelligence Community in der nach Gesetz, Executive Order oder Presidential Directive zulässigen Form auf den Schutz der nationalen Sicherheit konzentriert, dass sie die Daten vor unbefugtem Zugriff, unbefugter Nutzung und Weitergabe schützt und dass ihre Aktivitäten einer mehrstufigen Kontrolle und Überwachung unterliegen, einschließlich durch Kontrollausschüsse des Kongresses. Die PPD-28 und die Verfahren zu ihrer Durchführung machen unsere Bemühungen deutlich, bestimmte Minimierungsverfahren und andere wesentliche Grundsätze des Datenschutzes auf die personenbezogenen Daten aller Personen unabhängig der Nationalität auszuweiten. Personenbezogene Informationen, die durch die signalerfassende Aufklärung der USA erhoben wurden, unterliegen den Grundsätzen und Anforderungen des amerikanischen Rechts und den Anweisungen des Präsidenten, einschließlich der in der PPD-28 festgelegten Schutzbestimmungen. Diese Grundsätze und Anforderungen sind die Gewähr dafür, dass alle Personen unabhängig von ihrer Nationalität oder ihrem Wohnort würde- und respektvoll behandelt werden, und sie erkennen an, dass alle Personen berechnigte Datenschutzinteressen beim Umgang mit ihren personenbezogenen Informationen haben.

II. Foreign Intelligence Surveillance Act – § 702

Die Erhebung gemäß § 702 des Foreign Intelligence Surveillance Act¹¹ erfolgt nicht „massenhaft und anlassunabhängig“, sondern ist strikt auf die Erhebung ausländischer Aufklärungsdaten einzeln benannter legitimer Ziele gerichtet; ist eindeutig durch ausdrückliche gesetzliche Ermächtigung autorisiert und unterliegt sowohl der unabhängigen richterlichen Aufsicht als auch einer umfassenden Überprüfung und Überwachung innerhalb der Exekutive

¹¹ 50 U.S.C., § 1881a.

und im Kongress. Die Erhebung gemäß § 702 gilt als signalerfassende Aufklärung nach Maßgabe der Anforderungen der PPD-28.¹²

Die Erhebung gemäß § 702 stellt eine der wertvollsten Quellen für Aufklärungsdaten dar, da sowohl die Vereinigten Staaten als auch unsere europäischen Partner geschützt werden. Umfassende Informationen zur Funktionsweise und Überwachung von § 702 sind öffentlich zugänglich. Zahlreiche Gerichtsunterlagen, richterliche Entscheidungen und Überwachungsberichte im Zusammenhang mit dem Programm wurden freigegeben und auf der Website des ODNI öffentlich bekannt gemacht (www.icontherecord.tumblr.com). Außerdem führte das PCLOB eine umfassende Analyse zu § 702 durch; der entsprechende Bericht ist abrufbar unter <https://www.pclob.gov/library/702-Report.pdf>.¹³

Der § 702 wurde nach einer breiten öffentlichen Debatte als Teil des FISA Amendments Act von 2008¹⁴ im Kongress verabschiedet. Er genehmigt die Sammlung von Auslandsaufklärungsdaten durch die gezielte Überwachung von Nicht-US-Bürgern, die sich außerhalb der Vereinigten Staaten aufhalten, wobei amerikanische Anbieter elektronischer Kommunikationsdienste zur Unterstützung verpflichtet sind. § 702 autorisiert den Justizminister und den DNI – zwei vom Präsidenten ernannte und vom Senat bestätigte Beamte auf Kabinettsebene –, dem FISA Court jährliche Zertifizierungen vorzulegen.¹⁵ Diese beziehen sich auf spezifische Kategorien von zu erhebenden Auslandsaufklärungsdaten, wie etwa Erkenntnisse in Bezug auf Terrorismusbekämpfung oder Massenvernichtungswaffen, die unter die im FISA-Gesetz festgelegten Kategorien von Auslandsaufklärungsdaten fallen müssen.¹⁶ Wie das PCLOB feststellte, „ist aufgrund dieser Einschränkungen eine unbeschränkte Erhebung von Daten über Ausländer *nicht* möglich.“¹⁷

Zudem müssen die Zertifizierungen Verfahren zur „zielgenauen Erfassung“ und „Minimierung“ vorsehen, die vom FISA-Gericht zu überprüfen und zu bestätigen sind.¹⁸ Die

¹² Die Vereinigten Staaten können aufgrund anderer Bestimmungen des FISA auch gerichtliche Anordnungen erwirken, um Daten zu erlangen, wozu auch im Rahmen des Datenschutzschildes übermittelte Daten gehören. *Siehe* 50 U.S.C., § 1801 ff.. Nach Titel I und III des FISA, durch die elektronische Überwachung und Durchsuchung genehmigt werden, ist (außer in Notfällen) eine gerichtliche Anordnung erforderlich und muss in jedem Falle hinreichend Anlass zu der Vermutung bestehen, dass das Ziel eine ausländische Macht oder ein Vertreter einer ausländischen Macht ist. Titel IV des FISA genehmigt die Verwendung von Geräten zur Rufnummernerfassung von ausgehenden und eingehenden Anrufen gemäß gerichtlicher Anordnung (außer in Notfällen) bei autorisierten Untersuchungen in den Bereichen Auslandsaufklärung, Spionageabwehr oder Terrorismusbekämpfung. Titel V des FISA gestattet dem FBI, gemäß gerichtlicher Anordnung (außer in Notfällen) Geschäftsunterlagen einzuholen, die für autorisierte Untersuchungen in den Bereichen Auslandsaufklärung, Spionageabwehr oder Terrorismusbekämpfung von Belang sind. Wie weiter unten erörtert wird, untersagt der USA FREEDOM Act ausdrücklich die Verwendung von Rufnummernerfassung oder abgeforderten Geschäftsunterlagen auf der Grundlage von FISA für die Sammelerhebung und schreibt einen „konkreten Suchbegriff“ vor, um eine zielgerichtete Autorisierung zu gewährleisten.

¹³ Privacy and Civil Liberties Board, „Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act“ (2. Juli 2014) („PCLOB Report“).

¹⁴ *Siehe* Pub. L. No. 110-261, 122 Stat. 2436 (2008).

¹⁵ *Siehe* 50 U.S.C., § 1881a(a) und (b).

¹⁶ *Siehe ebenda* § 1801(e).

¹⁷ *Siehe* PCLOB Report unter 99.

¹⁸ *Siehe* 50 U.S.C., § 1881a(d) und (e).

Verfahren für eine zielgenaue Erfassung sollen sicherstellen, dass die Erhebung nur in der gesetzlich zulässigen Form stattfindet und der Anwendungsbereich der Zertifizierungen eingehalten wird; durch die Verfahren zur Minimierung sollen die Gewinnung, Weitergabe und Speicherung von Informationen über US-Bürger eingeschränkt werden, sie sehen jedoch auch einen umfassenden Schutz für Informationen über Nicht-US-Bürger vor, wie an anderer Stelle noch erläutert wird. Zudem hat der Präsident, wie bereits dargelegt, in der PPD-28 angewiesen, dass die Intelligence Community zusätzliche Schutzvorkehrungen für personenbezogene Daten von Nicht-US-Bürgern treffen, und diese Vorkehrungen gelten für Daten, die gemäß § 702 erhoben werden.

Bestätigt das Gericht die Verfahren zur zielgenauen Erfassung und Minimierung, erfolgt die Erhebung gemäß § 702 nicht als Sammelerhebung oder anlassunabhängig, sondern es geht ausschließlich um konkrete Zielpersonen, zu denen individualisierte Merkmale festgelegt worden sind, wie das PCLOB anmerkt.¹⁹ Zur zielgenauen Ausrichtung der Erhebung werden individuelle Selektoren verwendet, wie etwa E-Mail-Adressen oder Telefonnummern, die nach Erkenntnissen der Mitarbeiter der US-Nachrichtendienste vermutlich dazu verwendet werden, um Auslandsaufklärungsdaten der Art zu übermitteln, die unter die dem Gericht vorgelegte Zertifizierung fällt.²⁰ Die Grundlage für die Auswahl des Ziels muss dokumentiert werden, und die Dokumentation für die einzelnen Selektoren wird nachfolgend vom Justizministerium überprüft.²¹ Nach Informationen der Regierung der USA wurden 2014 zu etwa 90 000 Personen gezielte Erhebungen nach § 702 durchgeführt, was einem winzigen Bruchteil der weltweit mehr als drei Milliarden Internetnutzer entspricht.²²

Nach § 702 erhobene Daten sind Gegenstand der vom Gericht bestätigten Minimierungsverfahren, die Schutzmaßnahmen für Nicht-US-Bürger wie auch für US-Bürger vorsehen und die der Öffentlichkeit bekanntgegeben wurden.²³ Beispielsweise werden nach § 702 gesammelte Kommunikationsinhalte – sei es von US-Bürgern oder von Nicht-US-Bürgern – in Datenbanken mit strengen Zugangskontrollen gespeichert. Sie dürfen nur von nachrichtendienstlichem Personal überprüft werden, die in den auf den Datenschutz abgestellten Minimierungsverfahren geschult und für diesen Zugang speziell bestätigt wurden, damit sie ihre autorisierten Aufgaben wahrnehmen können.²⁴ Verwendet werden dürfen die Daten nur für die Ermittlung von Auslandsaufklärungsdaten oder den Nachweis einer Straftat.²⁵ Die Weitergabe darf gemäß PPD-28 nur dann erfolgen, wenn dies einem begründeten Ziel der Auslandsaufklärung oder der Strafverfolgung dient; die alleinige Tatsache, dass es sich bei einer

¹⁹ Siehe PCLOB Report unter 111.

²⁰ Ebenda.

²¹ Ebenda, unter 8; 50 U.S.C. § 1881a(1); siehe auch Bericht des NSA Director of Civil Liberties and Privacy „NSA’s Implementation of Foreign Intelligence Surveillance Act Section 702“ (im Folgenden „NSA-Bericht“) unter 4, abrufbar unter <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

²² Director of National Intelligence 2014 Transparency Report, abrufbar unter http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

²³ Minimierungsverfahren abrufbar unter: <http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf> („NSA-Minimierungsverfahren“); <http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf>; and <http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf>.

²⁴ Siehe NSA-Bericht unter 4.

²⁵ Siehe z. B. NSA-Minimierungsverfahren unter 6.

der Kommunikationsparteien nicht um eine US-Person handelt, ist nicht ausreichend.²⁶ Außerdem wird durch die Minimierungsverfahren und die PPD-28 die mögliche Speicherdauer der nach § 702 gewonnenen Daten begrenzt.²⁷

Der § 702 unterliegt einer umfassenden Überwachung, an der alle drei Gewalten des Staates beteiligt sind. Bei den Nachrichtendiensten, die das Gesetz umsetzen, erfolgen interne Überprüfungen auf mehreren Ebenen, einschließlich durch unabhängige Generalinspektoren, sowie technische Kontrollen des Datenzugriffs. Seitens des Justizministeriums und des ODNI wird die Anwendung von § 702 genau überprüft und untersucht, um die Einhaltung der rechtlichen Bestimmungen zu verifizieren. Unabhängig davon sind auch die Nachrichtendienste verpflichtet, potenzielle Verstöße zu melden. Hierzu erfolgt eine Untersuchung, und über alle Verstöße wird dem Foreign Intelligence Surveillance Court, dem Intelligence Oversight Board des Präsidenten und dem Kongress Bericht erstattet, und es wird gegebenenfalls Abhilfe geschaffen.²⁸ Bislang gibt es keine Fälle, in denen vorsätzlich versucht wurde, gegen das Gesetz zu verstoßen oder rechtliche Vorgaben zu umgehen.²⁹

Das FISA-Gericht spielt bei der Umsetzung von § 702 eine wichtige Rolle. Es besteht aus einem Gremium unabhängiger Bundesrichter, die ihm sieben Jahre angehören, jedoch wie alle Bundesrichter auf Lebenszeit als Richter ernannt werden. Wie bereits an anderer Stelle ausgeführt, ist es Aufgabe des Gerichts, die jährlichen Zertifizierungen und die Verfahren zur zielgenauen Erfassung und Minimierung auf die Einhaltung der Rechtsvorschriften zu überprüfen. Darüber hinaus muss die Regierung, wie ebenfalls schon festgestellt, das Gericht bei Compliance-Problemen unverzüglich in Kenntnis setzen,³⁰ und es wurden mehrere Stellungnahmen des Gerichts freigegeben und veröffentlicht, um deutlich zu machen, mit welcher außerordentlich hohem Maße an richterlicher Kontrolle und Unabhängigkeit derartige Fälle überprüft werden.

Die anspruchsvollen Prozesse des Gerichts wurden von dessen ehemaligem vorsitzenden Richter in einem Schreiben an den Kongress erläutert, das öffentlich zur Verfügung gestellt wurde.³¹ Als eine Auswirkung des USA FREEDOM Act, auf den weiter unten genauer eingegangen wird, ist das Gericht nunmehr ausdrücklich autorisiert, in Fällen neuer oder bedeutender rechtlicher Fragen einen externen Anwalt als unabhängigen Vertreter des Datenschutzes zu benennen.³² Dieser Grad der Beteiligung der unabhängigen Gerichte an Aktivitäten der Auslandsaufklärung in Bezug auf Personen, die weder Bürger dieses Landes sind

²⁶ Nachrichtendienstliche PPD-28-Verfahren abrufbar unter <http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties>.

²⁷ Siehe NSA-Minimierungsverfahren; PPD-28 Section 4.

²⁸ Siehe 50 U.S.C. § 1881(l); siehe auch PCLOB Report unter 66-76.

²⁹ Siehe Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, vorgelegt vom Justizminister und dem Director of National Intelligence unter 2-3, abrufbar unter <http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf>.

³⁰ Rule 13 der Rules of Procedures des Foreign Intelligence Surveillance Court, abrufbar unter <http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

³¹ 29. Juli 2013, Letter from The Honorable Reggie B. Walton to The Honorable Patrick J. Leahy, abrufbar unter <http://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

³² Siehe § 401 des USA FREEDOM Act, P.L. 114-23.

noch sich in diesem Land aufhalten, ist ungewöhnlich, wenn nicht sogar beispiellos, und trägt dazu bei, dass bei Erhebungen gemäß § 702 die entsprechenden rechtlichen Beschränkungen eingehalten werden.

Die Überwachung durch den Kongress erfolgt mittels gesetzlich vorgeschriebener Berichte an die Ausschüsse für Nachrichtendienste und Justiz sowie häufiger Informationsgespräche und Anhörungen. Dazu gehören ein halbjährlicher Bericht des Justizministers über die Anwendung von § 702 und alle aufgetretenen Verstöße;³³ eine gesonderte halbjährliche Einschätzung des Justizministers und des DNI, der die Einhaltung der Verfahren zur zielgenauen Erfassung und Minimierung dokumentiert, darunter auch die Einhaltung der Verfahren, die sicherstellen sollen, dass die Erhebung einem begründeten Ziel der Auslandsaufklärung dient;³⁴ und ein jährlicher Bericht der Leiter der Nachrichtendienste einschließlich einer Bestätigung, dass mit der Erhebung gemäß § 702 auch weiterhin Auslandsaufklärungsdaten erlangt werden.³⁵

Zusammenfassend ist festzustellen, dass die Erhebung gemäß § 702 gesetzlich zulässig ist, Überprüfungen auf mehreren Ebenen sowie richterlicher Aufsicht und Überwachung unterliegt und, wie das FISA-Gericht in einer jüngst freigegebenen Stellungnahme feststellte, „nicht als Sammelerhebung oder anlassunabhängig durchgeführt wird“, sondern „durch separate Entscheidungen über eine zielgenaue Erfassung für einzelne [kommunikationstechnische] Möglichkeiten.“³⁶

III. USA FREEDOM Act

Der USA FREEDOM Act, der im Juni 2015 unterzeichnet und in Kraft gesetzt wurde, brachte erhebliche Veränderungen für die Überwachungsbehörden der USA und andere nationale Sicherheitsbehörden und stellte in Bezug auf den Einsatz dieser Behörden und die Entscheidungen des FISA-Gerichts mehr Transparenz für die Öffentlichkeit her, wie weiter unten dargelegt wird.³⁷ Der Act gewährleistet, dass die in den Bereichen der Nachrichtendienste und der Strafverfolgung tätigen Berufsgruppen über die für den Schutz der Nation notwendigen Befugnisse verfügen, während ein angemessener Schutz der Privatsphäre bei Wahrnehmung dieser Befugnisse auch weiterhin gewahrt bleibt. Er bedeutet folglich eine Verstärkung des Datenschutzes und des Schutzes der bürgerlichen Freiheiten und eine Erhöhung der Transparenz.

Der Act verbietet die Sammelerhebung von Aufzeichnungen, sowohl von US- als auch von Nicht-US-Bürgern, unter Berufung auf verschiedene Bestimmungen des FISA oder durch den Einsatz von National Security Letters, einer Form von gesetzlich zulässigen behördlichen Anordnungen.³⁸ Dieses Verbot bezieht sich speziell auf Telefon-Metadaten zu Gesprächen

³³ Siehe 50 U.S.C. § 1881f.

³⁴ Siehe *ebenda*, § 1881a(1)(1).

³⁵ Siehe *ebenda*, § 1881a(1)(3). Einige dieser Berichte unterliegen der Geheimhaltung.

³⁶ Mem. Opinion and Order unter 26 (FISC 2014), abrufbar unter <http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>.

³⁷ Siehe USA FREEDOM Act von 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.

³⁸ Siehe *ebenda*, §§ 103, 201, 501. National Security Letters sind durch verschiedene Gesetze zugelassen und ermöglichen dem FBI die Einholung von Informationen aus Kreditauskünften, von Finanzdaten sowie von Daten

zwischen Personen innerhalb der USA und Personen außerhalb der USA und würde auch die Erhebung von Informationen im Rahmen des Datenschutzschildes gemäß dieser Rechtsgrundlagen einschließen. Der Act fordert, dass die Behörden bei allen dementsprechend geregelten Anforderungen von Aufzeichnungen einen „konkreten Suchbegriff“ verwenden, d. h. einen Begriff, der eine Person, ein Konto, eine Adresse oder ein persönliches Gerät so präzise bezeichnet, dass der Suchbereich in einem nach vernünftigen Ermessen möglichen Maße eingeschränkt wird.³⁹ Damit wird einmal mehr gewährleistet, dass die Erhebung von Informationen für nachrichtendienstliche Zwecke eng gefasst und zielgenau ausgerichtet ist.

Der Act bewirkte auch erhebliche Änderungen bei den Verfahren vor dem FISA-Gericht, was sowohl mit einer Erhöhung der Transparenz als auch mit einer zusätzlichen Gewähr für den Datenschutz verbunden ist. Wie bereits festgestellt, ermöglicht er die Einsetzung einer ständigen Gruppe von sicherheitsüberprüften Anwälten mit Fachkenntnissen in solchen Bereichen wie Datenschutz und bürgerliche Freiheiten, nachrichtendienstliche Datenerhebung und Kommunikationstechnologie, die benannt werden können, um in Fällen mit bedeutenden oder neuen Rechtsauffassungen vor dem Gericht als „Amicus curiae“ aufzutreten. Diese Anwälte sind ermächtigt, juristische Argumente zur Wahrung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten vorzubringen, und sie haben Zugang zu allen Informationen, einschließlich der Geheimhaltung unterliegenden Informationen, die sie nach Feststellung des Gerichts für die Erfüllung ihrer Aufgaben benötigen.⁴⁰

Aufbauend auf der bisher einmaligen Transparenz der US-Regierung in Bezug auf nachrichtendienstliche Tätigkeiten wird der DNI durch den Act verpflichtet, in Abstimmung mit dem Justizminister jegliche Entscheidung, Anordnung oder Stellungnahme des Foreign Intelligence Surveillance Court bzw. des Foreign Intelligence Surveillance Court of Review, die eine bedeutsame Auslegung oder Interpretation einer gesetzlichen Bestimmung enthält, entweder freizugeben oder eine nicht der Geheimhaltung unterliegende Zusammenfassung davon zu veröffentlichen.

Darüber hinaus sieht der Act umfangreiche Offenlegungen vor, was Erhebungen gemäß FISA und Anfragen auf der Grundlage von National Security Letters betrifft. So müssen die Vereinigten Staaten alljährlich gegenüber dem Kongress und der Öffentlichkeit unter anderem die Anzahl der beantragten und genehmigten FISA-Anordnungen und -Zertifizierungen, die geschätzte Anzahl der von Überwachungsmaßnahmen betroffenen US-Bürger und Nicht-US-Bürger und die Anzahl der Zulassungen als „Amicus curiae“ offenlegen.⁴¹ Das Gesetz verlangt

aus elektronischen Nutzer- und Transaktionsaufzeichnungen ausschließlich zum Zweck des Schutzes vor internationalem Terrorismus und verdeckten nachrichtendienstlichen Aktivitäten. *Siehe* 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. National Security Letters werden normalerweise vom FBI verwendet, um in den frühen Phasen von Ermittlungen zur Terrorismusbekämpfung und Spionageabwehr wichtige nichtinhaltliche Informationen zu sammeln – wie etwa die Identität eines Kontonutzers, der möglicherweise mit Agenten einer Terroristengruppe wie ISIL kommuniziert. Empfänger eines National Security Letter haben das Recht, diesen vor Gericht anzufechten. *Siehe* 18 U.S.C. § 3511.

³⁹ *Siehe ebenda.*

⁴⁰ *Siehe ebenda*, § 401.

⁴¹ *Siehe ebenda*, § 602.

zudem, die Öffentlichkeit zusätzlich über die Anzahl der Anfragen auf der Grundlage von National Security Letters sowohl zu US- als auch zu Nicht-US-Bürgern zu unterrichten.⁴²

In Bezug auf die Unternehmenstransparenz bietet der Act den Unternehmen eine Reihe von Optionen, wie sie die Gesamtzahl der FISA-Anordnungen und -Direktiven oder der von Behörden übermittelten National Security Letters sowie die Anzahl der von diesen Anordnungen betroffenen Kundenkonten öffentlich bekanntmachen können.⁴³ Einige Unternehmen haben diese Zahlen bereits offengelegt, wobei deutlich wurde, dass nur von wenigen Kunden Daten angefordert wurden.

Diese Berichte zur Unternehmenstransparenz zeigen auf, dass von den Anfragen der US-Nachrichtendienste nur ein winziger Bruchteil der Daten betroffen ist. In einem kürzlich erschienenen Transparenzbericht eines großen Unternehmens beispielsweise heißt es, dass die bei ihm eingegangenen Anfragen zur nationalen Sicherheit (gemäß FISA oder durch National Security Letters) weniger als 20 000 seiner Konten betreffen, und zwar zu einer Zeit, da er mindestens 400 Millionen Nutzer verzeichnete. Mit anderen Worten, alle von diesem Unternehmen gemeldeten Anfragen zur nationalen Sicherheit betrafen weniger als 0,005 % seiner Nutzer. Selbst wenn sich jede dieser Anfragen auf Daten im Rahmen der Safe-Harbor-Regelung bezogen hätten, was natürlich nicht der Fall ist, lässt sich doch zweifelsohne erkennen, dass die Anfragen zielgenau sind und einen angemessenen Umfang haben und die Erhebung weder massenhaft noch anlassunabhängig erfolgt.

Die Umstände, unter denen Empfängern von National Security Letters deren Offenlegung untersagt werden kann, wurden bereits in den Rechtsvorschriften zu deren Genehmigung entsprechend eingeschränkt. Der Act sieht darüber hinaus vor, dass solche Verpflichtungen zur Geheimhaltung regelmäßig überprüft werden müssen und Empfänger von National Security Letters darüber zu unterrichten sind, wenn die Faktenlage die Verpflichtung zur Geheimhaltung nicht länger rechtfertigt, und er kodifiziert Verfahren, mit denen Empfänger Verpflichtungen zur Geheimhaltung anfechten können.⁴⁴

Zusammenfassend lässt sich feststellen, dass die wichtigen Änderungen bei den Nachrichtendiensten der USA als Folge des USA FREEDOM Act ein deutlicher Beleg dafür sind, dass sich die Vereinigten Staaten umfassend darum bemühen, bei allen nachrichtendienstlichen Praktiken dem Schutz von personenbezogenen Daten, Privatsphäre und bürgerlichen Freiheiten sowie der Transparenz einen vorrangigen Stellenwert einzuräumen.

IV. Transparenz

Abgesehen von den Transparenzverpflichtungen gemäß dem USA FREEDOM Act stellt die Intelligence Community der USA der Öffentlichkeit umfangreiche zusätzliche Informationen bereit und setzt damit ein deutliches Zeichen, was die Transparenz in ihrer Aufklärungsarbeit

⁴² *Siehe ebenda.*

⁴³ *Siehe ebenda*, § 603.

⁴⁴ *Siehe ebenda*, §§ 502(f)–503.

betrifft. Die Intelligence Community hat zahlreiche ihrer Strategien und Verfahren, viele Entscheidungen des Foreign Intelligence Surveillance Court und andere freigegebene Materialien publik gemacht und damit ein außerordentlich hohes Maß an Transparenz bewiesen. Zudem veröffentlicht sie in viel größerem Umfang als zuvor statistische Angaben zur Einbeziehung der für Erhebungen zuständigen nationalen Sicherheitsbehörden seitens der Regierung. In ihrem am 22. April 2015 herausgegebenen zweiten Jahresbericht präsentiert sie Statistiken dazu, wie oft diese wichtigen Behörden an der Arbeit der Regierung beteiligt wurden. Das ODNI hat ebenfalls auf seiner Website und auf *IC On the Record* eine Anzahl konkreter Transparenzgrundsätze⁴⁵ und einen Plan zur Umsetzung dieser Grundsätze in konkrete messbare Initiativen veröffentlicht.⁴⁶ Im Oktober 2015 hat der Director of National Intelligence verfügt, dass im Interesse der Förderung der Transparenz und der Durchführung von Transparenzinitiativen jeder Nachrichtendienst in den Reihen seiner Führungskräfte einen Intelligence Transparency Officer benennt.⁴⁷ Dieser wird eng mit dem jeweiligen Privacy and Civil Liberties Officer zusammenarbeiten, damit Transparenz, Privatsphäre und bürgerliche Freiheiten auch weiterhin oberste Priorität genießen.

Beispielhaft für diese Bemühungen ist die Veröffentlichung von mehreren nicht der Geheimhaltung unterliegenden Berichten durch den Chief Privacy and Civil Liberties Officer der NSA während der letzten Jahre, namentlich von Berichten zu den Aktivitäten gemäß § 702, Executive Order 12333 und dem USA FREEDOM Act.⁴⁸ Darüber hinaus besteht eine enge Zusammenarbeit der Intelligence Community mit dem PCLOB, dem Kongress und den Datenschutzorganisationen in den USA (U.S. privacy advocacy community), um die Tätigkeit der US-Nachrichtendienste noch transparenter zu gestalten, wann immer dies machbar und mit dem Schutz sensibler nachrichtendienstlicher Quellen und Methoden vereinbar ist. Insgesamt gesehen ist die nachrichtendienstliche Tätigkeit der USA mindestens genauso transparent wie die eines jeden anderen Staates in der Welt und weist den höchstmöglichen Grad an Transparenz auf, bei dem der Notwendigkeit des Schutzes von sensiblen Quellen und Methoden noch entsprochen werden kann

Zusammenfassende Angaben zur umfassenden Transparenz nachrichtendienstlicher Aktivitäten der USA:

- Die Intelligence Community hat Tausende von Seiten mit gerichtlichen Stellungnahmen und behördlichen Verfahren herausgegeben und online gestellt, in denen die spezifischen Verfahren und Anforderungen unserer nachrichtendienstlichen Tätigkeit dargelegt werden. Außerdem haben wir Berichte über die Einhaltung der geltenden Beschränkungen durch die Nachrichtendienste veröffentlicht.

⁴⁵ *Abrufbar unter* <http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles>.

⁴⁶ *Abrufbar unter* <http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf>.

⁴⁷ *Siehe ebenda.*

⁴⁸ *Abrufbar unter* <https://www.nsa.gov/civil-liberties/files/nsa-report-on-section-702-program.pdf>;
<https://www.nsa.gov/civil-liberties/files/UFA-Civil-Liberties-and-Privacy-Report.pdf>;
<https://www.nsa.gov/civil-liberties/files/UFA-Civil-Liberties-and-Privacy-Report.pdf>.

- Hochrangige Beamte des Nachrichtendienstes äußern sich regelmäßig öffentlich über die Aufgaben und Aktivitäten ihrer Organisationen, wobei sie auch die für ihre Arbeit maßgeblichen Compliance-Regelungen und -Sicherungsmaßnahmen erläutern.
- Die Intelligence Community veröffentlichte zahlreiche zusätzliche Dokumente zu den nachrichtendienstlichen Aktivitäten gemäß unserem Freedom of Information Act.
- Der Präsident erließ die PPD-28 und legte damit öffentlich zusätzliche Einschränkungen für unsere nachrichtendienstliche Tätigkeit fest, und das ODNI gab zwei öffentlich zugängliche Berichte über die Umsetzung dieser Einschränkungen heraus.
- Die Intelligence Community ist nunmehr gesetzlich verpflichtet, wichtige Rechtsgutachten des FISA-Gerichts oder Zusammenfassungen dieser Gutachten zu veröffentlichen.
- Die staatlichen Behörden sind verpflichtet, jährlich darüber Bericht zu erstatten, in welchem Umfang sie bestimmte nationale Sicherheitsbehörden einbeziehen, und für Unternehmen ist dies ebenfalls möglich.
- Das PCLOB hat mehrere ausführliche öffentliche Berichte zu nachrichtendienstlichen Aktivitäten herausgegeben und wird künftig auch weiterhin so verfahren.
- Die Intelligence Community stellt Kontrollausschüssen des Kongresses umfangreiche Informationen zur Verfügung, die der Geheimhaltung unterliegen.
- Der DNI hat Transparenzgrundsätze herausgegeben, die für die Tätigkeit der Intelligence Community maßgebend sind.

Dieses hohe Maß an Transparenz wird künftig noch weiter ausgebaut. Alle für die Öffentlichkeit zugänglich gemachten Informationen werden selbstverständlich sowohl dem Handelsministerium als auch der Europäischen Kommission zur Verfügung stehen. Die jährliche Überprüfung der Umsetzung des Datenschutzschildes durch diese beiden Seiten wird der Europäischen Kommission Gelegenheit geben, alle Fragen im Zusammenhang mit neu herausgegebenen Informationen wie auch andere Aspekte bezüglich des Datenschutzschildes und seiner Handhabung anzusprechen und zu erörtern, und wir gehen davon aus, dass das Ministerium möglicherweise nach eigenem Ermessen Vertreter anderer Stellen, einschließlich der Intelligence Community, zur Teilnahme an dieser Überprüfung einlädt. Das geht natürlich über den in der PPD-28 vorgesehenen Mechanismus hinaus, mit dem geregelt wird, in welcher Form EU-Mitgliedstaaten Bedenken im Zusammenhang mit der Überwachung an einen speziell benannten Beamten im Außenministerium herantragen können.

V. Rechtsbehelfe

Das amerikanische Recht sieht eine Reihe von Rechtsschutzinstrumenten für Personen vor, die aus Gründen der nationalen Sicherheit rechtswidrig elektronisch überwacht wurden. Gemäß FISA ist das Recht, ein amerikanisches Gericht um Unterstützung anzurufen, nicht auf US-Bürger beschränkt. Jeder Person, die über eine entsprechende Klagebefugnis verfügt, würden Rechtsbehelfe zur Verfügung stehen, um auf der Grundlage des FISA gegen rechtswidrige elektronische Überwachung vorzugehen. So haben Personen, die von rechtswidriger elektronischer Überwachung betroffen sind, gemäß FISA die Möglichkeit, US-Regierungsbeamte in persönlicher Eigenschaft auf Schadenersatz zu verklagen, was pönalen Schadenersatz und Anwaltsgebühren einschließt. *Siehe* 50 U.S.C. § 1810. Klagebefugte Personen haben auch die Möglichkeit, eine Zivilklage auf Schadenersatz einschließlich Prozesskostenerstattung gegen die Vereinigten Staaten anzustrengen, wenn die durch

elektronische Überwachung im Rahmen des FISA erlangten Informationen, die sie betreffen, gesetzwidrig und vorsätzlich genutzt oder offengelegt wurden. *Siehe* 18 U.S.C. § 2712. Sofern die US-Regierung beabsichtigt, Erkenntnisse über einen Geschädigten, die direkt oder mittelbar aus der elektronischen Überwachung gemäß FISA gewonnen wurden, in einem Gerichts- oder Verwaltungsverfahren in den Vereinigten Staaten gegen die betroffene Person zu verwenden oder offenzulegen, muss sie dem Gericht und der betroffenen Person ihre Absicht mitteilen, die daraufhin die Rechtmäßigkeit der Überwachung anfechten und auf die Unterdrückung der Informationen hinwirken kann. *Siehe* 50 U.S.C. § 1806. Das FISA sieht letztlich auch Strafen für Personen vor, die vorsätzlich und unter Vortäuschung rechtlicher Kompetenz eine gesetzwidrige elektronische Überwachung vornehmen oder vorsätzlich Informationen nutzen oder offenlegen, die durch gesetzwidrige Überwachung gewonnen wurden. *Siehe* 50 U.S.C. § 1809.

EU-Bürgern stehen andere Möglichkeiten zur Verfügung, um gegen US-Regierungsbeamte wegen der rechtswidrigen Verarbeitung oder Abfrage von Daten rechtlich vorzugehen, d. h. auch gegen Regierungsbeamte, die im Zusammenhang mit der rechtswidrigen Abfrage oder Verarbeitung von Informationen für vorgebliche Ziele der nationalen Sicherheit gegen das Gesetz verstoßen. Der Computer Fraud and Abuse Act verbietet vorsätzlichen nicht autorisierten Zugang (oder eine Ausweitung des autorisierten Zugangs) zur Einholung von Daten von einem Finanzinstitut, einem Computersystem der US-Regierung oder einem Computer, auf den über das Internet zugegriffen wird, wie auch zum Zweck der Erpressung oder des Betrugs vorgebrachte Drohungen, geschützten Computern Schaden zuzufügen. *Siehe* 18 U.S.C. § 1030. Jede Person, ganz gleich welcher Nationalität, die infolge einer Verletzung dieses Gesetzes einen Schaden oder einen Verlust erleidet, kann die Person, die gegen das Gesetz verstoßen hat (einschließlich Regierungsbeamte), nach § 1030(g) auf kompensatorischen Schadenersatz und Unterlassung verklagen oder einen anderen billigkeitsrechtlichen Rechtsbehelf erwirken, was von der Durchführung eines Strafverfahrens unabhängig ist, allerdings das Vorhandensein von mindestens einer der im Gesetz festgelegten Bedingungen voraussetzt. Der Electronic Communications Privacy Act (ECPA) regelt den Zugang der staatlichen Behörden zu gespeicherter elektronischer Kommunikation und Transaktionsaufzeichnungen sowie zu Nutzerdaten, die sich im Besitz von Drittanbietern im Bereich Kommunikation befinden. *Siehe* 18 U.S.C. §§ 2701-2712. Gemäß ECPA ist ein Geschädigter berechtigt, Regierungsbeamte wegen vorsätzlichen gesetzwidrigen Zugriffs auf gespeicherte Daten zu verklagen. Der ECPA gilt für alle Personen unabhängig von der Staatsbürgerschaft, und Geschädigte haben Anrecht auf Schadenersatz und die Anwaltsgebühren. Der Right to Financial Privacy Act (RFPA) beschränkt den Zugriff der US-Regierung auf Bank- und Brokerunterlagen einzelner Kunden. *Siehe* 12 U.S.C. §§ 3401-3422. Gemäß RFPA kann ein Bank- oder Brokerekunde die US-Regierung wegen unrechtmäßigen Zugangs zu Kundenunterlagen auf gesetzlichen, eigentlichen und pönalen Schadenersatz verklagen, und wenn sich zeigt, dass ein solcher unrechtmäßiger Zugang vorsätzlich erfolgte, wird automatisch eine Untersuchung über mögliche disziplinarische Maßnahmen gegen die betreffenden Regierungsmitarbeiter eingeleitet. *Siehe* 12 U.S.C. § 3417.

Der Freedom of Information Act (FOIA) schließlich ist ein Mittel, mit dem alle Personen zu jedem beliebigen Thema Zugang zu vorhandenen Unterlagen von Bundesbehörden erlangen können, vorbehaltlich einiger Kategorien von Ausnahmen. *Siehe* 5 U.S.C. § 552(b). Dazu gehören Zugangsbegrenzungen bei Informationen, die aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen, bei personenbezogenen Daten anderer Personen sowie bei Informationen, die strafrechtliche Ermittlungen betreffen. Diese Einschränkungen sind mit denen

vergleichbar, die andere Länder in ihren Datenzugangsgesetzen festgelegt haben, und gelten gleichermaßen für Amerikaner und Nicht-Amerikaner. Bei Streitigkeiten über die Freigabe von Unterlagen, die gemäß FOIA angefordert wurden, können auf dem Verwaltungsweg Rechtsbehelfe eingelegt werden, danach ist das Bundesgericht anzurufen. Das Gericht muss eine De-novo-Entscheidung dazu treffen, ob die Unterlagen ordnungsgemäß zurückgehalten werden, 5 U.S.C. § 552(a)(4)(B), und kann die Regierung zwingen, Zugang zu den Unterlagen zu gewähren. In einigen Fällen haben die Gerichte die Behauptungen der Regierung zurückgewiesen, dass die Information als der Geheimhaltung unterliegend zurückgehalten werden sollte.⁴⁹ Obwohl kein Schadensersatz geleistet wird, können die Gerichte die Anwaltskosten erstatten.

VI. Fazit

Die Vereinigten Staaten erkennen an, dass bei ihrer signalerfassenden Aufklärung und anderen nachrichtendienstlichen Tätigkeiten zu berücksichtigen ist, dass alle Personen unabhängig von ihrer Nationalität oder ihrem Wohnort würde- und respektvoll zu behandeln sind und dass alle Personen berechnete Datenschutzinteressen beim Umgang mit ihren personenbezogenen Daten haben. Die Vereinigten Staaten nutzen die signalerfassende Aufklärung ausschließlich zur Gewährleistung ihrer nationalen Sicherheit und ihrer außenpolitischen Interessen sowie zum Schutz ihrer Bürger und der Bürger von mit ihnen verbündeten oder befreundeten Staaten. Die Intelligence Community der USA betreibt keine systematische anlassunabhängige Überwachung von Personen, was normale europäische Bürger einschließt. Die Erhebung von Signalaufklärungsdaten erfolgt nur bei ordnungsgemäßer Ermächtigung und unter strenger Einhaltung der geltenden Einschränkungen; sie erfolgt erst nach Prüfung der Verfügbarkeit alternativer Quellen, einschließlich diplomatischer und öffentlicher Quellen, und in einer Weise, bei der vorrangig auf geeignete und machbare Alternativen zurückgegriffen wird. Und wann immer es praktikabel erscheint, wird die Erhebung unter Verwendung von Selektoren auf spezifische Aufklärungsziele oder -themen im Ausland konzentriert.

Die Politik der USA in diesem Bereich wurde in der PPD-28 bekräftigt. Innerhalb dieser Rahmenbedingungen verfügen die US-Nachrichtendienste nicht über die rechtliche Befugnis, die Ressourcen, die technischen Voraussetzungen oder den Wunsch, weltweit die gesamte Kommunikation zu überwachen. Die Nachrichtendienste lesen nicht die E-Mails einer jeden Person in den Vereinigten Staaten oder alle weltweit verschickten E-Mails. Entsprechend der PPD-28 gibt es in den Vereinigten Staaten wirksame Schutzvorkehrungen für die personenbezogenen Daten von Nicht-US-Bürgern, die per Signalaufklärung erhoben wurden. Dazu gehören Regeln und Verfahren, um – vergleichbar mit den Schutzmaßnahmen für US-Bürger – die Speicherung und Weitergabe von sie betreffenden personenbezogenen Daten auf ein Mindestmaß zu beschränken, soweit es die Gewährleistung der nationalen Sicherheit zulässt. Zudem besteht, wie oben dargelegt, ein umfassendes Überwachungsregime für die zielgenaue Autorisierung nach § 702 FISA, das seinesgleichen sucht. Und schließlich bewirken die wesentlichen Änderungen an den rechtlichen Grundlagen für die nachrichtendienstliche

⁴⁹ Siehe z. B. *New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

Tätigkeit, wie sie im USA FREEDOM Act festgelegt wurden, und auch die vom ODNI geleiteten Initiativen zur Förderung der Transparenz innerhalb der Intelligence Community eine deutliche Verbesserung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten für alle Personen unabhängig von ihrer Nationalität.

Hochachtungsvoll

Robert S. Litt

21. Juni 2016

Herrn Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

Herrn Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Avenue, N.W.
Washington, DC 20230

Sehr geehrter Herr Antonipillai, sehr geehrter Herr Dean,

ich möchte Ihnen weitere Informationen über die Art und Weise übermitteln, in der die Vereinigten Staaten die Sammelerhebung von Signalaufklärungsdaten durchführen. Wie in der Fußnote 5 der Presidential Policy Directive 28 (PPD-28) erläutert, bezieht sich der Begriff „Sammelerhebung“ auf den Erwerb einer relativ großen Menge von signalerfassenden Aufklärungsdaten unter Bedingungen, in denen die Intelligence Community keinen mit einer bestimmten Zielperson verbundenen Identifikator (wie z. B. die E-Mail-Adresse oder Telefonnummer) für eine zielgerichtete Erhebung verwenden kann. Das bedeutet jedoch nicht, dass diese Art der Erhebung „massenhaft“ oder „anlassunabhängig“ erfolgt. So wird in der PPD-28 auch gefordert, dass die signalerfassende Aufklärung „so passgerecht wie möglich“ sein sollte. Gemäß diesem Auftrag stellt die Intelligence Community mit entsprechenden Maßnahmen sicher, dass auch in Fällen, in denen keine konkreten Suchkriterien für eine gezielte Erhebung verfügbar sind, die zu erhebenden Daten wahrscheinlich Informationen der Auslandsaufklärung enthalten, die den Anforderungen entsprechen, wie sie anhand des in meinem früheren Schreiben erläuterten Prozesses formuliert wurden, und so die Menge erhobener nicht relevanter Daten minimiert wird.

Zum Beispiel kann die Intelligence Community den Auftrag erhalten, Signalaufklärungsdaten zu den Aktivitäten einer Terroristengruppe zu erlangen, die in einer Region eines Nahoststaates operiert und von der vermutet wird, dass sie Anschläge gegen westeuropäische Länder plant. Dabei sind möglicherweise die Namen, Telefonnummern, E-Mail-Adressen oder andere konkrete Identifikatoren von mit dieser Terroristengruppe in Verbindung gebrachten Personen nicht bekannt. Wir könnten uns dafür entscheiden, diese Gruppe ins Visier zu nehmen, indem wir Kommunikationsvorgänge aus dieser und in diese Region überwachen und dann weitere Auswertungen und Analysen vornehmen, um jene Vorgänge zu ermitteln, die sich auf die Gruppe beziehen. Dabei würden sich die Nachrichtendienste bemühen, die Erhebung so weit wie möglich einzugrenzen. Es würde sich also um eine „Sammelerhebung“ handeln, da eine Verwendung von Selektoren nicht möglich ist. Sie ist weder „massenhaft“ noch „anlassunabhängig“, sondern erfolgt so zielgerichtet wie möglich.

Somit erheben die Vereinigten Staaten auch dann, wenn eine zielgenaue Ausrichtung der Erhebung durch Verwendung konkreter Selektoren nicht möglich ist, nicht sämtliche

Kommunikationsdaten sämtlicher Kommunikationseinrichtungen der ganzen Welt, sondern konzentrieren ihre Erhebung mithilfe von Filtern und anderen technischen Hilfsmitteln auf jene Einrichtungen, die wahrscheinlich für die Auslandsaufklärung wertvolle Kommunikationsdaten enthalten. Somit erstreckt sich die signalerfassende Aufklärung der Vereinigten Staaten nur auf einen Bruchteil des Datenverkehrs im Internet.

Da, wie in meinem früheren Schreiben angeführt, bei einer „Sammelerhebung“ eher die Gefahr besteht, dass nicht relevante Kommunikationsdaten erhoben werden, beschränkt die PPD-28 die zulässige Verwendung von durch Sammelerhebung gewonnenen Signalaufklärungsdaten auf sechs konkrete Zielsetzungen. In der PPD-28 und bei nachrichtendienstlichen Maßnahmen zur Umsetzung der PPD-28 sind zudem Grenzen für die Speicherung und Weitergabe durch Signalaufklärung erlangter personenbezogener Daten festgelegt, und zwar ungeachtet dessen, ob die Daten durch Sammelerhebung oder gezielte Erhebung gewonnen wurden, und unabhängig von der Staatsangehörigkeit der betreffenden Person.

Daher handelt es sich bei der „Sammelerhebung“ der Intelligence Community nicht um eine „massenhafte“ oder „anlassunabhängige“ Erhebung, sondern sie umfasst vielmehr die Anwendung von Verfahren und Hilfsmitteln zum Filtern, um die Erhebung auf Material zu konzentrieren, das die Anforderungen der von den Entscheidungsträgern formulierten Anforderungen an die Auslandsaufklärung erfüllt, und zugleich die Erhebung nicht relevanter Daten zu minimieren; dabei kommen strenge Regeln für den Schutz möglicherweise erhobener nicht relevanter Informationen zur Anwendung. Die in diesem Schreiben geschilderten Strategien und Verfahren gelten für die gesamte Sammelerhebung von Signalaufklärungsdaten, einschließlich der Sammelerhebung des Datenverkehrs von und nach Europa, ohne dass hier bestätigt oder dementiert wird, ob eine derartige Erhebung erfolgt.

Sie haben zudem weitere Informationen über das Privacy and Civil Liberties Oversight Board (PCLOB) und die Generalinspektoren sowie über deren Rechtsgrundlagen angefragt. Das PCLOB ist ein unabhängiges Gremium in der Exekutive.¹ Die fünf Mitglieder dieses parteienübergreifenden Gremiums werden vom Präsidenten ernannt und vom Senat bestätigt; ihre Amtszeit beträgt sechs Jahre. Die Mitglieder des PCLOB und deren Mitarbeiter erhalten entsprechende Zugangsberechtigungen, damit sie ihren gesetzlichen Pflichten und Aufgaben uneingeschränkt nachkommen können.²

Der Auftrag des PCLOB besteht darin zu gewährleisten, dass die Anstrengungen der Bundesregierung zur Terrorismusprävention mit dem notwendigen Schutz der Privatsphäre und der bürgerlichen Freiheiten in Einklang gebracht werden. Das Gremium hat zwei grundlegende Aufgaben – Überwachung und Beratung. Dabei steckt das PCLOB sein Arbeitsgebiet selbst ab und legt fest, welche Tätigkeiten der Überwachung und Beratung es durchzuführen wünscht.

In seiner Rolle als *Überwachungsgremium* überprüft und analysiert das PCLOB die Maßnahmen der Exekutive zum Schutz der Nation vor Terrorismus, die mit dem notwendigen Schutz der

¹ 42 U.S.C. 2000ee(a), (h).

² 42 U.S.C. 2000ee(k).

Privatsphäre und der bürgerlichen Freiheiten in Einklang gebracht werden müssen.³ Die jüngste abgeschlossene Kontrollarbeit des PCLOB konzentrierte sich auf Überwachungsprogramme nach § 702 des FISA.⁴ Zurzeit überprüft das Gremium die nachrichtendienstlichen Tätigkeiten gemäß Executive Order 12333.⁵

In seiner Rolle als *Beratungsgremium* sorgt das PCLOB dafür, dass bei der Entwicklung und Umsetzung von Gesetzen, Regelungen und Maßnahmen zum Schutz der Nation vor Terrorismus die individuellen Freiheitsrechte hinreichend berücksichtigt werden.⁶

Zur Erfüllung seines Auftrags hat das Gremium per Gesetz Zugriff auf alle einschlägigen Unterlagen von Behörden wie Berichte, Audits, Überprüfungen, Dokumente, Schriftstücke, Empfehlungen und sonstige einschlägige Materialien, einschließlich gesetzlich der Geheimhaltung unterliegender Informationen.⁷ Darüber hinaus kann das PCLOB alle Beamten oder Mitarbeiter der Exekutive befragen sowie Aussagen und Zeugenaussagen einholen.⁸ Außerdem kann das Gremium schriftlich beantragen, dass der Justizminister im Namen des PCLOB Anordnungen ausstellt, mit der Parteien außerhalb der Exekutive gezwungen werden, entsprechende Informationen bereitzustellen.⁹

Nicht zuletzt muss das PCLOB gesetzlichen Anforderungen zur Transparenz gegenüber der Öffentlichkeit nachkommen. Dazu gehört, dass es die Öffentlichkeit über seine Tätigkeit auf dem Laufenden hält, indem es Anhörungen öffentlich durchführt und seine Berichte, soweit es der notwendige Schutz der Geheimhaltung unterliegender Informationen zulässt, in größtmöglichem Umfang publik macht.¹⁰ Zudem muss das PCLOB melden, wenn eine Regierungsstelle sich weigert, seinem Rat zu folgen.

Die Generalinspektoren in der Intelligence Community führen Audits, Inspektionen und Überprüfungen der Programme und Tätigkeiten der Nachrichtendienste durch, um systemimmanente Risiken, Schwachstellen und Unzulänglichkeiten zu ermitteln und anzusprechen. Darüber hinaus gehen die Generalinspektoren Beschwerden oder Informationen nach, die mutmaßliche Verstöße gegen Gesetze oder Rechtsvorschriften bzw. Misswirtschaft, die grobe Verschwendung von Mitteln, Amtsmissbrauch oder eine erhebliche oder besondere Gefahr für die öffentliche Gesundheit und Sicherheit im Zusammenhang mit nachrichtendienstlichen Programmen und Aktivitäten betreffen. Die Unabhängigkeit der Generalinspektoren ist ein maßgeblicher Faktor für die Objektivität und Integrität aller von ihnen vorgelegten Berichte, Erkenntnisse und Empfehlungen. Zu den wichtigsten Aspekten der Aufrechterhaltung der Unabhängigkeit der Generalinspektoren gehören das Verfahren der Ernennung und Abberufung von Inspektoren, gesonderte Stellen für die operative Tätigkeit, Haushalt und Personalfragen

³ 42 U.S.C. 2000ee(d)(2).

⁴ Siehe allgemein <https://www.pclob.gov/library.html#oversightreports>.

⁵ Siehe allgemein <https://www.pclob.gov/events/2015/may13.html>.

⁶ 42 U.S.C. 2000ee(d)(1); siehe auch PCLOB Advisory Function Policy and Procedure, Policy 2015-004, abrufbar unter https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.

⁷ 42 U.S.C. 2000ee(g)(1)(A).

⁸ 42 U.S.C. 2000ee(g)(1)(B).

⁹ 42 U.S.C. 2000ee(g)(1)(D).

¹⁰ 42 U.S.C. 2000eee(f).

sowie doppelte Rechenschaftspflichten gegenüber den Leitern von Regierungsbehörden sowie gegenüber dem Kongress.

Vom Kongress wurde in jeder Regierungsbehörde, darunter bei allen Nachrichtendiensten, ein unabhängiges Büro des Generalinspektors eingerichtet.¹¹ Im Zuge der Annahme des Intelligence Authorization Act for Fiscal Year 2015 werden nahezu alle Generalinspektoren mit Überwachungsaufgaben für eine Stelle der Intelligence Community vom Präsidenten ernannt und vom Senat bestätigt, einschließlich Justizministerium, Central Intelligence Agency (CIA), National Security Agency (NSA) und Intelligence Community.¹² Bei diesen Generalinspektoren handelt es sich zudem um parteiunabhängige Beamte, die nur vom Präsidenten abberufen werden können. Obgleich die Befugnis des Präsidenten zur Abberufung der Inspektoren in der US-Verfassung verankert ist, wird sie kaum wahrgenommen und erfordert, dass der Präsident dem Kongress 30 Tage vor der Abberufung eines Generalinspektors eine schriftliche Begründung zukommen lässt.¹³ Mit diesem Ernennungsverfahren wird gewährleistet, dass Beamte der Exekutive keinen ungebührlichen Einfluss auf die Auswahl, Ernennung oder Abberufung eines Generalinspektors ausüben.

Zweitens verfügen die Generalinspektoren über erhebliche gesetzliche Befugnisse zur Durchführung von Audits, Untersuchungen und Überprüfungen von Programmen und Maßnahmen der Exekutive. Neben den gesetzlich vorgeschriebenen Kontrolluntersuchungen und -überprüfungen haben die Generalinspektoren weitreichende Ermessensfreiheit zur Ausübung von Kontrollbefugnissen bei der Überprüfung der von ihnen selbst ausgewählten Programme und Aktivitäten.¹⁴ Dabei stellt das Gesetz sicher, dass den Inspektoren bei der Wahrnehmung dieser Befugnisse unabhängige Mittel zur Erfüllung ihrer Aufgaben zur Verfügung stehen, einschließlich der Möglichkeit, eigene Mitarbeiter einzustellen und ihre Haushaltsanträge an den Kongress gesondert zu dokumentieren.¹⁵ Es ist gesetzlich sichergestellt, dass die Generalinspektoren Zugang zu den für die Erfüllung ihrer Aufgaben benötigten Informationen erhalten. Dazu gehört der direkte Zugriff auf sämtliche behördlichen Unterlagen und Informationen mit ausführlichen Angaben zu den Programmen und Aktivitäten der Behörde ungeachtet der Geheimhaltungsstufe; die Befugnis zur Einholung von Informationen und Dokumenten per Anordnung sowie die Befugnis zur Vereidigung.¹⁶ In wenigen Fällen kann der Leiter einer Regierungsbehörde die Tätigkeit eines Generalinspektors untersagen, wenn z. B.

¹¹ § 2 und 4 des Inspector General Act von 1978 in der geltenden Fassung (im Folgenden „IG Act“); § 103H(b) und (e) des National Security Act von 1947 in der geltenden Fassung; § 17(a) des Central Intelligence Act (im Folgenden „CIA Act“).

¹² *Siehe* Pub. L. No. 113-293, 128 Stat. 3990, (19. Dezember 2014). Nur die Generalinspektoren der Defense Intelligence Agency und der National Geospatial-Intelligence Agency werden nicht vom Präsidenten ernannt; allerdings haben der Generalinspektor des Verteidigungsministeriums und der Generalinspektor der Intelligence Community konkurrierende Zuständigkeit für diese Behörden.

¹³ § 3 des IG Act von 1978 in der geltenden Fassung; § 103H(c) des National Security Act; und § 17(b) des CIA Act.

¹⁴ *Siehe* §§ 4(a) und 6(a)(2) des IG Act von 1947; § 103H(e) und (g)(2)(A) des National Security Act; § 17(a) und (c) des CIA Act.

¹⁵ §§ 3(d), 6(a)(7) und 6(f) des IG Act; § 103H(d), (i), (j) und (m) des National Security Act; § 17(e)(7) und (f) des CIA Act.

¹⁶ § 6(a)(1), (3), (4), (5), und (6) des IG Act; § 103H(g)(2) des National Security Act; § 17(e)(1), (2), (4), und (5) des CIA Act.

ein Audit oder eine Untersuchung des Inspektors die nationalen Sicherheitsinteressen der Vereinigten Staaten erheblich beeinträchtigen würde. Auch die Wahrnehmung dieser Befugnis ist äußerst ungewöhnlich und macht es erforderlich, dass der Leiter der Behörde den Kongress binnen 30 Tagen über die Gründe in Kenntnis setzt.¹⁷ Der Director of National Intelligence hat diese Amtsbefugnis zur Einschränkung der Tätigkeiten von Generalinspektoren noch nie eingesetzt.

Drittens haben die Generalinspektoren die Aufgabe, sowohl die Leiter der Regierungsbehörden als auch den Kongress mithilfe von Berichten umfassend und zeitnah über Betrugsfälle und andere schwerwiegende Probleme, Missstände und Mängel bei Programmen und Aktivitäten der Exekutive zu informieren.¹⁸ Die doppelte Berichterstattung stützt die Unabhängigkeit der Inspektoren, indem die Überwachung durch sie transparent wird und die Behördenleiter Gelegenheit erhalten, Empfehlungen der Inspektoren umzusetzen, bevor der Kongress gesetzgeberische Maßnahmen einleiten kann. Beispielsweise sind die Generalinspektoren gesetzlich verpflichtet, diese Probleme sowie bislang eingeleitete Abhilfemaßnahmen in halbjährlichen Berichten darzulegen.¹⁹ Die Regierungsbehörden nehmen die Feststellungen und Empfehlungen der Inspektoren ernst, und Letztere können oftmals die Akzeptanz und Umsetzung ihrer Empfehlungen in diese und andere Berichte an den Kongress und mitunter an die Öffentlichkeit aufnehmen.²⁰ Neben der doppelten Berichterstattung sind die Generalinspektoren auch dafür verantwortlich, Whistleblowern der Exekutive den Weg zu den zuständigen Kontrollgremien des Kongresses zu weisen, wo sie mutmaßliche Betrugsfälle, Verschwendung oder Missstände bei Programmen und Aktivitäten der Exekutive melden können. Die Identität der Hinweisgeber ist vor einer Preisgabe gegenüber der Exekutive geschützt, so dass sie vor möglichen unzulässigen Disziplinarmaßnahmen oder Sicherheitsüberprüfungen als Vergeltung dafür, dass sie sich an den Inspektor gewandt haben, bewahrt bleiben.²¹ Da Whistleblower oftmals die Informationsquelle für Untersuchungen der Generalinspektoren darstellen, erhöht die Möglichkeit, dass sie ihr Anliegen ohne Einflussnahme der Exekutive dem Kongress vortragen können, die Wirksamkeit der Überwachung durch die Inspektoren. Aufgrund dieser Unabhängigkeit können die Generalinspektoren Wirtschaftlichkeit, Effizienz und Rechenschaftspflicht in den Regierungsbehörden mit Objektivität und Integrität fördern.

Abschließend sei erwähnt, dass der Kongress den Rat der Generalinspektoren für Integrität und Effizienz eingerichtet hat. Dieser Rat entwickelt u. a. Standards der Generalinspektoren für

¹⁷ *Siehe z. B.* § 8(b) und 8E(a) des IG Act; § 103H(f) des National Security Act; § 17(b) des CIA Act.

¹⁸ § 4(a)(5) des IG Act; § 103H(a)(b)(3) und (4) des National Security Act; § 17(a)(2) und (4) des CIA Act.

¹⁹ § 2(3), 4(a), und 5 des IG Act; § 103H(k) des National Security Act; § 17(d) des CIA Act. Der Generalinspektor des Justizministeriums stellt seine für die Öffentlichkeit bestimmten Berichte im Internet unter folgendem Link bereit: <http://oig.justice.gov/reports/all.htm>. Ebenso veröffentlicht der Generalinspektor für die Intelligence Community seine halbjährlichen Berichte unter <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

²⁰ §§ 2(3), 4(a), und 5 des IG Act; § 103H(k) des National Security Act; § 17(d) des CIA Act. Der Generalinspektor des Justizministeriums stellt seine für die Öffentlichkeit bestimmten Berichte im Internet unter folgendem Link bereit: <http://oig.justice.gov/reports/all.htm>. Ebenso veröffentlicht der Generalinspektor für die Intelligence Community seine halbjährlichen Berichte unter <https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig>.

²¹ § 7 des IG Act; § 103H(g)(3) des National Security Act; § 17(e)(3) des CIA Act.

Audits, Untersuchungen und Überprüfungen, fördert Schulungen und ist befugt, ein angebliches Fehlverhalten von Generalinspektoren zu überprüfen; somit dient er als kritisches Auge gegenüber den Generalinspektoren, die damit betraut sind, alle anderen zu überwachen.²²

Ich hoffe, dass Ihnen diese Ausführungen weiterhelfen.

Mit freundlichen Grüßen,

Robert S. Litt
General Counsel

²² § 11 des IG Act.

ANHANG VII
Schreiben von Bruce Swartz, stellvertretender Generalstaatsanwalt des
Justizministeriums und Berater für internationale Angelegenheiten, US-
Justizministerium

19. Februar 2016

Herrn Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Herrn Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Sehr geehrter Herr Antonipillai, sehr geehrter Herr Dean,

dieses Schreiben gibt einen kurzen Überblick über die wichtigsten Ermittlungsinstrumente, mit denen aus Gründen der Strafverfolgung oder des öffentlichen (zivil- und aufsichtsrechtlichen) Interesses Geschäfts- und andere Daten von amerikanischen Unternehmen eingeholt werden können, und über die in diesen Behörden bestehenden Zugriffsbeschränkungen.¹ Die erlassenen Anordnungen sind insofern nicht diskriminierend, als sie dazu dienen, sowohl Informationen von US-amerikanischen Unternehmen einzuholen als auch solche von Unternehmen, die eine Selbstzertifizierung unter dem US-EU-Datenschutzschild vornehmen, unabhängig von der Staatsangehörigkeit der betroffenen Person. Darüber hinaus können Unternehmen, gegen die in den Vereinigten Staaten rechtliche Schritte eingeleitet werden, dieses Einholen von Informationen wie im Folgenden dargestellt anfechten.²

¹ In diesem Überblick geht es nicht um die Instrumente, die die Strafverfolgungsbehörden beispielsweise bei Ermittlungen im Zusammenhang mit dem Terrorismus oder Fragen der nationalen Sicherheit nutzen, z. B. National Security Letters (NSLs) für bestimmte Aufzeichnungen zu Kreditdaten, Finanzdaten und elektronischen Teilnehmer- und Transaktionsdaten, siehe 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, und nicht um die elektronische Überwachung, Durchsuchungsbefehle, Geschäftsunterlagen und die anderweitige Erfassung von Kommunikation gemäß dem Foreign Intelligence Surveillance Act, siehe 50 U.S.C. § 1801 ff.

² Hier geht es um die Strafverfolgungs- und Aufsichtsbehörden des Bundes; Verstöße gegen das Recht der Bundesstaaten werden von diesen selbst untersucht und vor deren Gerichten verhandelt. Die Strafverfolgungsbehörden der Bundesstaaten wenden die gemäß ihrem Recht erteilten Befehle und Anordnungen an, wie sie hier dargestellt sind, wobei die Möglichkeit besteht, dass die Verfassungen der Bundesstaaten ein Rechtsschutzniveau vorsehen, das über jenes der Verfassung der USA hinausgeht. Der von

Von besonderer Bedeutung in Bezug auf die Beschlagnahme von Daten durch öffentliche Behörden ist der vierte Zusatzartikel zur Verfassung der Vereinigten Staaten, der folgendermaßen lautet: „Das Recht des Volkes auf Sicherheit der Person und der Wohnung, der Urkunden und des Eigentums vor willkürlicher Durchsuchung, Festnahme und Beschlagnahme darf nicht verletzt werden, und Haussuchungs- und Haftbefehle dürfen nur bei Vorliegen eines eidlich oder eidesstattlich erhärteten Rechtsgrundes ausgestellt werden und müssen die zu durchsuchende Örtlichkeit und die in Gewahrsam zu nehmenden Personen oder Gegenstände genau bezeichnen.“ Wie das Oberste Gericht der Vereinigten Staaten in der Rechtssache *Berger v. State of New York* urteilte „besteht der Hauptzweck dieses Zusatzartikels, wie in zahlreichen Urteilen dieses Gerichts bestätigt wird, im Schutz der Privatsphäre und der Sicherheit von Einzelpersonen vor willkürlichem Eingriffen durch Regierungsbeamte“, siehe 388 U.S. 41, 53 (1967) (unter Berufung auf die Rechtssache *Camara vs. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). Für strafrechtliche Ermittlungen im Inland ist im vierten Zusatzartikel generell vorgeschrieben, dass den Strafverfolgungsbeamten vor der Durchführung einer Haussuchung ein gerichtlicher Hausdurchsuchungsbefehl vorliegen muss. Siehe Rechtssache *Katz v. United States*, 389 U.S. 347, 357 (1967). In Fällen, in denen diese Vorschrift nicht gilt, unterliegt das Eingreifen des Staates einer Prüfung der „Zumutbarkeit“. Somit gewährleistet also die Verfassung selbst, dass die Regierung der Vereinigten Staaten nicht uneingeschränkt oder willkürlich private Informationen beschlagnahmen darf.

Strafverfolgungsbehörden

Bundesanwälte, die Beamte des Justizministeriums sind, und Ermittler des Bundes einschließlich Ermittler des Federal Bureau of Investigation (FBI), einer Strafverfolgungsbehörde innerhalb des Justizministeriums, können von Unternehmen in den USA die Herausgabe von Unterlagen und anderen Aufzeichnungen zu strafrechtlichen Ermittlungszwecken mithilfe mehrerer Arten von Zwangsmaßnahmen – wie Anordnungen einer Grand Jury oder Behörde und Durchsuchungsbefehlen – erzwingen und auch sonstige Kommunikation gemäß den für das Abhören und für die Rufnummern Erfassung zuständigen Bundesbehörden einholen.

Anordnungen einer Grand Jury oder eines Gerichts: Mit strafrechtlichen Anordnungen sollen konkrete strafrechtliche Ermittlungen unterstützt werden. Bei einer Anordnung einer Grand Jury handelt es sich um einen offiziellen Antrag einer Grand Jury (üblicherweise auf Verlangen eines Bundesanwalts), Ermittlungen zu einem konkreten mutmaßlichen Verdacht auf einen Verstoß gegen das Strafrecht durchzuführen. Grand Juries sind eine Anklagekammer eines Gerichts, deren Mitglieder von einem Richter oder Magistrate ausgewählt werden. Bei einer Anordnung kann von der betroffenen Person verlangt werden, in einem Gerichtsverfahren auszusagen oder Geschäftsunterlagen, elektronisch gespeicherte Informationen oder sonstige materielle Beweismittel vorzulegen bzw. zur Verfügung zu stellen. Hierbei muss es sich um für die Ermittlungen relevante Informationen handeln, und die Anordnung darf nicht unverhältnismäßig sein, weil sie überzogen, repressiv oder belastend ist – denn aus diesen Gründen kann ein Empfänger die Anfechtung der Anordnung beantragen. Siehe dazu die Federal Rules of Criminal Procedure

den Bundesstaaten gewährte Rechtsschutz muss mindestens dem der US-Verfassung – insbesondere Zusatzartikel 4, aber nicht darauf beschränkt – entsprechen.

[Strafprozessordnung], S. 17. In einigen wenigen Fällen kann ein Gericht nach Anklage durch die Grand Jury die Vorlage von Unterlagen anordnen.

Behördliche Anordnungen: Bei straf- oder zivilrechtlichen Ermittlungen können behördliche Anordnungen ergehen. Im Zuge der Strafverfolgung ist es in mehreren Bundesstaaten gesetzlich zulässig, behördliche Anordnungen zu erlassen, um Geschäftsunterlagen, elektronisch gespeicherte Informationen oder sonstige materielle Beweismittel, die für Ermittlungen zu Betrug im Gesundheitswesen, zum Kindesmissbrauch, zum Schutz durch den Geheimdienst, zu Verstößen gegen das Betäubungsmittelgesetz und Ermittlungen eines Generalinspektors, die sich auf Regierungsbehörden auswirken, relevant sind, vorzulegen bzw. zur Verfügung zu stellen. Möchte die Regierung eine behördliche Anordnung gerichtlich durchsetzen, kann der Empfänger der behördlichen Anordnung – wie der Empfänger einer Anordnung einer Grand Jury – die Unverhältnismäßigkeit der Anordnung geltend machen, weil sie überzogen, repressiv oder belastend ist.

Gerichtlich angeordnete Rufnummernerfassung: Gemäß den strafrechtlichen Vorschriften zur Rufnummernerfassung können die Strafverfolgungsbehörden eine gerichtliche Anordnung erlangen, um in Echtzeit nichtinhaltliche Wähl-, Routing-, Anschluss- und Signalinformationen zu einer Telefonnummer oder E-Mail-Adresse zu erfassen, sofern bestätigt wird, dass die gelieferten Informationen für laufende strafrechtliche Ermittlungen relevant sind. Siehe 18 U.S.C. §§ 3121-3127. Dem Bundesgesetz zufolge ist die gesetzwidrige Nutzung bzw. der gesetzwidrige Einbau eines einschlägigen Geräts strafbar.

Electronic Communications Privacy Act (ECPA): Gemäß Titel II des ECPA (Gesetz zum Datenschutz in der elektronischen Kommunikation), das auch als Stored Communications Act (SCA, Gesetz zur Speicherung von Kommunikation) bezeichnet wird (18 U.S.C. §§ 2701–2712), regeln zusätzliche Vorschriften den Zugriff des Staates auf Teilnehmerdaten, Verkehrsdaten und bei Internetdiensteanbietern von Telefongesellschaften und anderen dritten Diensteanbietern gespeicherte Kommunikationsinhalte. Im SCA ist ein System gesetzlich vorgeschriebener Datenschutzrechte festgelegt, die den Datenzugriff zu Zwecken der Strafverfolgung einschränken und ihn nur in dem Maße gestatten, wie es verfassungsrechtlich für die Kunden und Abonnenten von Internetdiensteanbietern erforderlich ist. Durch das SCA wird die Privatsphäre in Abhängigkeit vom Ausmaß der Datenerfassung stärker geschützt. Um Informationen über die registrierten Abonnenten, IP-Adressen und dazugehörigen Zeitstempel und Rechnungsinformationen einholen zu können, müssen die Strafverfolgungsbehörden eine entsprechende Anordnung erhalten. Für die meisten anderen gespeicherten, nichtinhaltlichen Informationen wie E-Mail-Header ohne Betreffzeile müssen die Strafverfolgungsbehörden einem Richter konkrete Fakten vorlegen, aus denen hervorgeht, dass die beantragten Informationen für laufende strafrechtliche Ermittlungen relevant sind. Um an die gespeicherten Inhalte elektronischer Kommunikation zu gelangen, benötigen die Strafverfolgungsbehörden generell eine entsprechende richterliche Anordnung, die auf dem hinreichenden Verdacht basiert, dass das betreffende Konto Nachweise für eine Straftat enthält. Im SCA sind darüber hinaus auch die Privathaftpflicht und die strafrechtlichen Sanktionen geregelt.

Gerichtlich angeordnete Überwachung nach dem Federal Wiretap Law (Bundesabhörsgesetz): Nach dem Bundesabhörsgesetz kann die Strafverfolgung darüber hinaus zu strafrechtlichen Ermittlungszwecken in Echtzeit drahtgebundene, mündliche oder elektronische Kommunikation abhören bzw. abfangen. Siehe 18 U.S.C. §§ 2510-2522. Dies kann nur auf gerichtliche Anordnung geschehen, wenn durch einen Richter unter anderem

festgestellt wird, dass das Abhören oder elektronische Abfangen vermutlich Beweise für einen Verstoß gegen das Bundesgesetz erbringen oder Hinweise auf den Aufenthaltsort einer sich der Strafverfolgung entziehenden Person liefern wird. In diesem Gesetz sind darüber hinaus auch die Privathaftpflicht und die strafrechtlichen Sanktionen bei Verstoß gegen die Abhörvorschriften geregelt.

Durchsuchungsbefehl – Artikel 41: Nach richterlicher Anordnung können Gebäude in den USA von den Strafverfolgungsbehörden durchsucht werden. Letztere müssen dem Richter anhand eines „hinreichenden Verdachts“ glaubhaft darlegen, dass eine Straftat begangen wurde bzw. begangen werden soll und dass an dem im Durchsuchungsbefehl genannten Ort vermutlich mit der Straftat zusammenhängende Gegenstände gefunden werden. Von dieser Befugnis wird häufig Gebrauch gemacht, wenn eine polizeiliche Durchsuchung eines Gebäudes erforderlich wird, weil die Gefahr besteht, dass möglicherweise Beweismittel vernichtet werden, wenn eine Anordnung zur Herausgabe gegen das betreffende Unternehmen ergeht. *Siehe* vierter Zusatzartikel zur Verfassung der Vereinigten Staaten (auf den oben bereits eingegangen wurde), Federal Rules of Criminal Procedure, S. 41. Die Person, gegen die der Durchsuchungsbefehl ergeht, kann gegen diesen vorgehen, weil er überzogen und schikanös ist oder auf unberechtigte Weise erlangt wurde, und Geschädigte mit Klageberechtigung können bei rechtswidrigen Durchsuchungen erlangte Beweise unterdrücken. *Siehe* Rechtssache *Mapp v. Ohio*, 367 U.S. 643 (1961).

Leitlinien und Strategien des Justizministeriums: Neben diesen verfassungsrechtlichen, gesetzlich vorgeschriebenen und auf Regelungen beruhenden Einschränkungen des staatlichen Zugriffs auf Daten hat der Justizminister Leitlinien veröffentlicht, die den Datenzugriff zu Zwecken der Strafverfolgung weiter einschränken und auch die Privatsphäre und die Bürgerrechte schützen. So wird beispielsweise in den Leitlinien des Justizministers für Inlandseinsätze des FBI von September 2008 (im Folgenden FBI-Leitlinien des Justizministers), abrufbar unter <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, die Anwendung von Ermittlungstechniken zur Einholung von Informationen für Ermittlungen im Rahmen von Verstößen gegen das Bundesgesetz eingeschränkt. Diese Leitlinien verpflichten das FBI, die mit den geringsten Eingriffen verbundenen Ermittlungsmethoden anzuwenden und die Auswirkungen auf die Privatsphäre und die Bürgerrechte und die potenzielle Rufschädigung zu berücksichtigen. Darüber hinaus wird darauf hingewiesen, dass „das FBI seine Ermittlungen und sonstigen Aktivitäten selbstverständlich rechtmäßig und angemessen unter Einhaltung von Bürgerrechten und Privatsphäre so durchführen muss, dass ein unnötiges Eindringen in das Privatleben gesetzestreuer Personen vermieden wird.“ *Siehe* FBI-Leitlinien des Justizministers, Seite 5. Umgesetzt hat das FBI diese Leitlinien mithilfe des FBI Domestic Investigations and Operations Guide (abrufbar unter [https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20\(DIOG\)](https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG))), eines umfassenden Handbuchs mit detaillierten Erläuterungen zu den Grenzen der Anwendung von Ermittlungsinstrumenten und entsprechenden Hilfestellungen zur Gewährleistung des Schutzes von Bürgerrechten und Privatsphäre bei sämtlichen Ermittlungen. Weitere Vorschriften und Strategien, die die Ermittlungstätigkeit der Bundesanwälte einschränken, sind im **United States Attorneys' Manual** (USAM, Anwaltshandbuch der Vereinigten Staaten), aufgeführt, das ebenfalls online abrufbar ist unter <http://www.justice.gov/usam/united-states-attorneys-manual>.

Zivil- und Aufsichtsbehörden (öffentliches Interesse):

Auch die Zivil- oder Aufsichtsbehörden (die im öffentlichen Interesse handeln) erhalten nur sehr eingeschränkt Zugriff auf Daten von Unternehmen in den Vereinigten Staaten. Behörden mit zivilen und aufsichtsrechtlichen Aufgaben können von Unternehmen die Herausgabe von Geschäftsunterlagen, elektronisch gespeicherten Informationen oder sonstigen materiellen Beweismitteln verlangen. Diese Behörden unterliegen in der Ausübung ihrer administrativen oder zivilen Anordnungsbefugnis Einschränkungen, und zwar nicht nur durch ihre jeweiligen Gründungsgesetze, sondern auch, weil die Anordnungen vor ihrer potenziellen gerichtlichen Umsetzung einer unabhängigen gerichtlichen Überprüfung unterzogen werden. Siehe z. B. die Federal Rules of Civil Procedure [Zivilprozessordnung], S. 45. Die Behörden können nur den Zugriff auf Daten beantragen, die für Sachen innerhalb ihres Verantwortungsbereichs von Belang sind. Darüber hinaus kann ein Empfänger einer behördlichen Anordnung deren Umsetzung vor Gericht anfechten, indem er nachweist, dass die Behörde den Grundsatz der Zumutbarkeit missachtet hat, wie bereits oben dargelegt wurde.

Unternehmen, die sich Datenabfragen von Verwaltungsbehörden widersetzen möchten, können sich je nach Branche und Datenart auf weitere Rechtsgrundlagen stützen. So können Finanzinstitute beispielsweise behördliche Anordnungen anfechten, bei denen bestimmte Arten von Informationen abgerufen werden sollen, wodurch gegen das Bank Secrecy Act (Gesetz über das Bankgeheimnis) und dessen Durchführungsbestimmungen verstoßen wird. Siehe 31 U.S.C. § 5318, 31 C.F.R. Part X. Andere Unternehmen wiederum können sich auf das Fair Credit Reporting Act (Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten), siehe 15 U.S.C. § 1681b, oder andere branchenspezifische Gesetze berufen. Der Missbrauch einer Anordnungsbefugnis einer Behörde kann deren Haftung bzw. eine persönliche Haftung ihrer Beamten nach sich ziehen. Siehe z. B. das Right to Financial Privacy Act (Gesetz zum Schutz von Finanzdaten), 12 U.S.C. §§ 3401–3422. Somit schützen die Gerichte in den Vereinigten Staaten vor unangemessenen Anträgen der Regulierungsbehörden und vermitteln einen unabhängigen Überblick über die Maßnahmen der Bundesbehörden.

Jegliche gesetzliche Befugnis der Verwaltungsbehörden, Unterlagen eines Unternehmens in den Vereinigten Staaten nach einer behördlichen Durchsuchung zu beschlagnahmen, muss die Anforderungen des vierten Zusatzartikels erfüllen. *Siehe See v. City of Seattle*, 387 U.S. 541 (1967).

Fazit

Sämtliche Strafverfolgungsmaßnahmen und Aufsichtstätigkeiten in den Vereinigten Staaten müssen nach geltendem Recht erfolgen und im Einklang mit der Verfassung der USA sowie den Gesetzen, Regelungen und Vorschriften stehen. Außerdem müssen einschlägige Strategien wie die Leitlinien des Justizministers zur Regelung der Strafverfolgung auf Bundesebene befolgt werden. Mit dem oben beschriebenen Rechtsrahmen wird die Möglichkeit der amerikanischen Strafverfolgungs- und Aufsichtsbehörden eingeschränkt, Informationen von Unternehmen in den USA einzuholen – unabhängig davon, ob es sich dabei um Informationen über US-Bürger oder Drittstaatsangehörige handelt –, und die gerichtliche Überprüfung jeglicher Datenanfragen, die über diese Behörden erfolgen, ermöglicht.

Hochachtungsvoll

Bruce C. Swartz
Stellvertretender Generalstaatsanwalt des
Justizministeriums und Berater für
internationale Angelegenheiten