ENTSCHEIDUNG DER KOMMISSION

vom 26. Juli 2000

gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA

(Bekannt gegeben unter Aktenzeichen K(2000) 2441)

(Text von Bedeutung für den EWR)

(2000/520/EG)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [1], insbesondere auf Artikel 25 Absatz 6,

in Erwägung nachstehender Gründe:

(1) Gemäß der Richtlinie 95/46/EG haben die Mitgliedstaaten vorzusehen, dass die Übermittlung personenbezogener Daten in ein Drittland nur zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet und die einzelstaatlichen Rechtsvorschriften zur Umsetzung anderer Bestimmungen der Richtlinie vor der Übermittlung beachtet werden.

(2) Die Kommission kann feststellen, dass ein Drittland ein angemessenes Schutzniveau gewährleistet. In diesem Fall können personenbezogene Daten aus den Mitgliedstaaten übermittelt werden, ohne dass zusätzliche Garantien erforderlich sind.

(3) Gemäß der Richtlinie 95/46/EG sollte die Angemessenheit des Schutzniveaus unter Berücksichtigung aller Umstände beurteilt werden, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen, und im Hinblick auf die gegebenen Bedingungen. Die durch die Richtlinie eingesetzte Datenschutzgruppe [2] hat Leitlinien für solche Bewertungen erstellt [3].

(4) Angesichts der verschiedenen Ansätze von Drittländern im Bereich Datenschutz sollte die Beurteilung der Angemessenheit und die Durchsetzung jeder Entscheidung gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG in einer Form erfolgen, die gegen Drittländer bzw. unter Drittländern, in denen gleiche Bedingungen vorherrschen, nicht willkürlich oder ungerechtfertigt diskriminierend wirkt und unter Berücksichtigung der bestehenden internationalen Verpflichtungen der Gemeinschaft kein verstecktes Handelshemmnis darstellt.

(5) Das durch diese Entscheidung anerkannte angemessene Schutzniveau für die Übermittlung von Daten aus der Gemeinschaft in die Vereinigten Staaten sollte erreicht sein, wenn die Organisationen die „Grundsätze des ‚sicheren Hafens' zum Datenschutz" für den Schutz personenbezogener Daten, die aus einem Mitgliedstaat in die Vereinigten Staaten übermittelt werden (im folgenden „die Grundsätze" genannt) sowie die „Häufig gestellten Fragen" („Frequently Asked Questions", im folgenden „FAQ" genannt) beachten, die Leitlinien für die Umsetzung der von der Regierung der Vereinigten Staaten von Amerika am 21. Juli 2000 veröffentlichten Grundsätze darstellen. Die Organisationen müssen ferner ihre Geschäftsbedingungen zum Datenschutz offen legen und der Zuständigkeit der Federal Trade Commission (FTC) gemäß Abschnitt 5 des Federal Trade Commission Act, der unlautere und irreführende Handlungen und Praktiken, die im Handel erfolgen oder die den Handel beeinträchtigen, verbietet, bzw. der Zuständigkeit anderer gesetzlicher Organe unterliegen, die die Einhaltung der entsprechend den FAQ umgesetzten Grundsätze effektiv gewährleisten.

(6) Bereiche und/oder Datenverarbeitungen, die nicht der Zuständigkeit einer der in Anhang VII dieser Entscheidung genannten staatlichen Einrichtungen innerhalb der Vereinigten Staaten unterliegen, fallen nicht in den Geltungsbereich dieser Entscheidung.

(7) Um die ordnungsgemäße Anwendung dieser Entscheidung zu gewährleisten, müssen Organisationen, die den Grundsätzen und den FAQ beitreten, von den interessierten Kreisen, wie etwa den betroffenen Personen, Datenexporteuren und Datenschutzbehörden, erkannt werden können. Das US-Handelsministerium bzw. die von ihm

---

[1] ABl. L 281 vom 23.11.1995, S. 31.

[2] Die Web-Anschrift der Datenschutzgruppe lautet: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[3] WP 12: Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU, von der Arbeitsgruppe am 24. Juli 1998 angenommen.

benannte Stelle sollte es zu diesem Zweck übernehmen, eine Liste der Organisationen zu führen und der Öffentlichkeit zugänglich zu machen, die selbst bescheinigen, dass sie den entsprechend den FAQ umgesetzten Grundsätzen beigetreten sind und in die Zuständigkeit zumindest eines der in Anhang VII dieser Entscheidung genannten staatlichen Organe fallen.

(8) Im Interesse der Transparenz und um die Fähigkeit der zuständigen Behörden in den Mitgliedstaaten zu erhalten, den Schutz von Personen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten, ist es ungeachtet der Feststellung des angemessenen Schutzniveaus notwendig, in dieser Entscheidung die besonderen Umstände zu nennen, unter denen die Aussetzung bestimmter Datenübermittlungen gerechtfertigt sein sollte.

(9) Der durch die Grundsätze und die FAQ geschaffene „sichere Hafen" wird möglicherweise im Licht der Erfahrungen mit Entwicklungen beim Datenschutz in einem Umfeld, in dem die Technik die Übermittlung und Verarbeitung personenbezogener Daten immer einfacher macht, und im Licht von Berichten der für die Durchsetzung zuständigen Behörden über die Anwendung gegebenenfalls überprüft werden müssen.

(10) Die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten hat zu dem Schutzniveau, das durch die Grundsätze über den sicheren Hafen in den Vereinigten Staaten geschaffen wird, Stellungnahmen abgegeben, die bei der Ausarbeitung der vorliegenden Entscheidung berücksichtigt wurden ([4]).

(11) Die in dieser Entscheidung geregelten Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 31 der Richtlinie 95/46/EG eingesetzten Ausschusses —

([4]) WP 15: Stellungnahme 1/99 zum Stand des Datenschutzes in den Vereinigten Staaten und zu den derzeitigen Verhandlungen zwischen der Europäischen Kommission und der amerikanischen Regierung;
WP 19: Stellungnahme 2/99 zur Angemessenheit der „Internationalen Grundsätze des sicheren Hafens", ausgegeben vom US-Handelsministerium am 19. April 1999;
WP 21: Stellungnahme 4/99 zu den „Häufig gestellten Fragen" (Frequently Asked Questions), vorgelegt vom US-Handelsministerium im Zusammenhang mit den vorgeschlagenen „Grundsätzen des sicheren Hafens";
WP 23: Arbeitsunterlage zum gegenwärtigen Stand der Diskussion zwischen der Europäischen Kommission und der Regierung der Vereinigten Staaten über die „Internationalen Grundsätze des sicheren Hafens";
WP 27: Stellungnahme 7/99 zum Datenschutzniveau, das die Grundsätze des sicheren Hafens in ihrer veröffentlichten Form, die dazu gehörigen häufig gestellten Fragen (FAQ) und andere vom US-Handelsministerium am 15./16. November 1999 veröffentlichte Dokumente gewährleisten;
WP 31: Stellungnahme 3/2000 zum Dialog EU-USA betreffend die Vereinbarung über den sicheren Hafen;
WP 32: Stellungnahme 4/2000 über das Datenschutzniveau, das die Grundsätze des sicheren Hafens bieten.

HAT FOLGENDE ENTSCHEIDUNG ERLASSEN:

Artikel 1

(1) Es wird davon ausgegangen, dass die dieser Entscheidung als Anhang I beigefügten „Grundsätze des ‚sicheren Hafens' zum Datenschutz", im Folgenden „die Grundsätze" genannt, die gemäß den in den vom US-Handelsministerium am 21. Juli 2000 herausgegebenen, dieser Entscheidung als Anhang II beigefügten, „Häufig gestellten Fragen" (FAQ) enthaltenen Leitlinien umgesetzt werden, für alle unter die Richtlinie 95/46/EG fallenden Tätigkeiten ein im Sinne des Artikels 25 Absatz 2 dieser Richtlinie angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die von der Europäischen Union an in den Vereinigten Staaten niedergelassene Organisationen übermittelt werden, unter Berücksichtigung folgender vom US-Handelsministerium veröffentlichter Dokumente:

a) die „sicherer Hafen Durchsetzungsmechanismen" (Anhang III),

b) ein Memorandum über Entschädigungen für die Verletzung der Privatsphäre und ausdrückliche Ermächtigungen gemäß dem US-Recht (Anhang IV),

c) ein Schreiben der Federal Trade Commission (Anhang V),

d) ein Schreiben des US-Verkehrsministeriums (Anhang VI).

(2) Im Hinblick auf jede Datenübermittlung müssen folgende Voraussetzungen erfüllt sein:

a) Die Organisation, die die Daten erhält, hat sich eindeutig und öffentlich verpflichtet, die Grundsätze einzuhalten, die entsprechend den FAQ umgesetzt wurden; und

b) die Organisation unterliegt den gesetzlichen Befugnissen einer in Anhang VII dieser Entscheidung aufgeführten staatlichen Einrichtung in den Vereinigten Staaten, die berechtigt ist, im Fall der Nichtbeachtung der Grundsätze, die entsprechend den FAQ umgesetzt wurden, Beschwerden zu prüfen und Abhilfe wegen unlauterer und irreführender Praktiken sowie Schadenersatz für Privatpersonen zu erwirken, und zwar ungeachtet des Landes, in dem sie ihren Wohnsitz haben, oder ihrer Nationalität.

(3) Die Voraussetzungen des Absatzes 2 gelten ab dem Zeitpunkt als erfüllt, zu dem die Organisation, die ihren Beitritt zu den entsprechend den FAQ umgesetzten Grundsätzen bescheinigt, dem Handelsministerium der USA (oder der von ihm benannten Stelle) die öffentliche Bekanntgabe ihrer Verpflichtung nach Absatz 2 Buchstabe a) und die Identität der staatlichen Einrichtung nach Absatz 2 Buchstabe b) mitteilt.

Artikel 2

Die vorliegende Entscheidung betrifft nur die Angemessenheit des Schutzes, der in den Vereinigten Staaten nach den entsprechend den FAQ umgesetzten Grundsätzen gewährt wird, um die Anforderungen des Artikels 25 Absatz 1 der Richtlinie 95/46/EG zu erfüllen. Die Anwendung anderer Bestimmungen der Richtlinie, die sich auf die Verarbeitung personenbezogener Daten in den Mitgliedstaaten beziehen, einschließlich Artikel 4, bleiben von dieser Entscheidung unberührt.

Artikel 3

(1) Ungeachtet ihrer Befugnisse, tätig zu werden, um die Einhaltung einzelstaatlicher Vorschriften, die gemäß anderen Bestimmungen als denjenigen des Artikels 25 der Richtlinie 95/46/EG erlassen wurden, zu gewährleisten, können die zuständigen Behörden in den Mitgliedstaaten ihre bestehenden Befugnisse ausüben, zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung an eine Organisation auszusetzen, die den Grundsätzen, die entsprechend den FAQ umgesetzt wurden, beigetreten ist, wenn

a) die in Anhang VII dieser Entscheidung erwähnte staatliche Einrichtung in den Vereinigten Staaten oder eine unabhängige Instanz im Sinne von Buchstabe a) des in Anhang I dieser Entscheidung erwähnten Durchsetzungsgrundsatzes feststellt, dass die betreffende Organisation die Grundsätze, die entsprechend den FAQ umgesetzt wurden, verletzt oder

b) eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden; wenn Grund zur Annahme besteht, dass die jeweilige Durchsetzungsinstanz nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den Fall zu lösen; wenn die fortgesetzte Datenübermittlung für die betroffenen Personen das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde, und wenn die zuständigen Behörden in den Mitgliedstaaten die Organisation unter den gegebenen Umständen in angemessener Weise unterrichtet und ihr Gelegenheit zu Stellungnahme gegeben haben.

Die Aussetzung ist zu beenden, sobald sichergestellt ist, dass die Grundsätze, die entsprechend den FAQ umgesetzt wurden, befolgt werden, und die zuständigen Behörden in der EU davon in Kenntnis gesetzt sind.

(2) Die Mitgliedstaaten informieren die Kommission unverzüglich, wenn Maßnahmen gemäß Absatz 1 ergriffen wurden.

(3) Die Mitgliedstaaten und die Kommission informieren einander auch über Fälle, bei denen die Maßnahmen der für die Einhaltung der entsprechend den FAQ umgesetzten Grundsätze in den Vereinigten Staaten verantwortlichen Einrichtungen nicht ausreichen, um die Einhaltung zu gewährleisten.

(4) Ergeben die Informationen nach den Absätzen 1, 2 und 3, dass eine der für die Einhaltung der entsprechend den FAQ umgesetzten Grundsätze in den Vereinigten Staaten verantwortlichen Einrichtungen ihrer Aufgabe nicht wirkungsvoll nachkommt, so informiert die Kommission das Handelsministerium der USA und schlägt, wenn nötig, gemäß dem Verfahren nach Artikel 31 der Richtlinie im Hinblick auf eine Aufhebung, Aussetzung oder Beschränkung des Geltungsbereichs dieser Entscheidung entsprechende Maßnahmen vor.

Artikel 4

(1) Diese Entscheidung kann jederzeit im Licht der Erfahrungen mit ihrer Anwendung angepasst werden und/oder dann, wenn das durch die Grundsätze und die FAQ gewährte Schutzniveau in die Rechtsvorschriften der USA übernommen wird.

In jedem Fall nimmt die Kommission drei Jahre, nachdem sie die Mitgliedstaaten von dieser Entscheidung in Kenntnis gesetzt hat, anhand der verfügbaren Informationen eine Bewertung ihrer Umsetzung vor und unterrichtet den nach Artikel 31 der Richtlinie 95/46/EG eingesetzten Ausschuss über sämtliche relevanten Feststellungen, einschließlich aller Erkenntnisse, die die Beurteilung der Vereinbarung in Artikel 1 als zur Gewährleistung des Datenschutzes angemessen im Sinne von Artikel 25 der Richtlinie 95/46/EG berühren könnten, sowie etwaiger Belege dafür, dass die vorliegende Entscheidung in diskriminierender Weise angewandt wird.

(2) Die Kommission legt erforderlichenfalls gemäß dem Verfahren nach Artikel 31 der Richtlinie Vorschläge für Maßnahmen vor.

Artikel 5

Die Mitgliedstaaten ergreifen binnen 90 Tagen, nachdem sie von der Entscheidung in Kenntnis gesetzt worden sind, alle für ihre Umsetzung erforderlichen Maßnahmen.

Artikel 6

Diese Entscheidung ist an alle Mitgliedstaaten gerichtet.

Brüssel, den 26. Juli 2000

Für die Kommission

Frederik BOLKESTEIN

Mitglied der Kommission

ANHANG I

GRUNDSÄTZE DES „SICHEREN HAFENS“ ZUM DATENSCHUTZ

vorgelegt vom amerikanischen Handelsministerium am 21. Juli 2000

Die umfassende Rechtsvorschrift der Europäischen Union zum Schutz personenbezogener Daten, die Datenschutzrichtlinie (nachstehend „die Richtlinie“ genannt), trat am 25. Oktober 1998 in Kraft. Sie legt fest, dass personenbezogene Daten nur in Nicht-EU-Länder übermittelt werden können, die einen „angemessenen“ Schutz der Privatsphäre gewährleisten. Die Vereinigten Staaten und die Europäische Union haben beide das Ziel, den Datenschutz für ihre Staatsbürger zu verstärken, wobei die Vereinigten Staaten jedoch einen anderen Ansatz verfolgen als die Europäische Gemeinschaft. Die USA verwenden einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und Selbstregulierung basiert. Angesichts dieser Unterschiede fühlen sich viele US-Organisationen verunsichert bezüglich der Auswirkung des seitens der EU geforderten „Angemessenheits-Standards“ für die Übermittlung personenbezogener Daten aus der Europäischen Union in die Vereinigten Staaten.

Um diese Unsicherheit auszuräumen und einen berechenbareren Rahmen für solche Datenübermittlungen zu schaffen, legt das Handelsministerium unter seiner gesetzlichen Autorität, internationalen Handel zu pflegen, zu fördern und zu entwickeln, dieses Papier und so genannte „Häufig gestellte Fragen“ — FAQs („die Grundsätze“) vor. Die Grundsätze wurden in Absprache mit der Industrie und der breiten Öffentlichkeit entwickelt, um den Handel zwischen der Europäischen Union und den Vereinigten Staaten zu erleichtern. Sie sind ausschließlich für den Gebrauch durch US-Organisationen bestimmt, die personenbezogene Daten aus der Europäischen Union erhalten, um sich für den „sicheren Hafen“ und die daraus erwachsende Vermutung der „Angemessenheit“ des Datenschutzes zu qualifizieren. Da die Grundsätze ausschließlich für diesen spezifischen Zweck erarbeitet wurden, können sie für andere Zwecke ungeeignet sein. Die Grundsätze können nicht benutzt werden als Ersatz für nationale Rechtsvorschriften über die Verarbeitung personenbezogener Daten in den Mitgliedstaaten, mit denen die Richtlinie umgesetzt wird.

Die Entscheidung der einzelnen Organisationen, sich für den „sicheren Hafen“ zu qualifizieren, ist vollkommen freiwillig, und die Organisationen können sich für das Konzept des „sicheren Hafens“ auf verschiedene Arten qualifizieren. Organisationen, die sich dazu entschließen, den Grundsätzen beizutreten, müssen die Grundsätze einhalten, um die Vorteile des „sicheren Hafens“ erhalten und behalten zu können, und sie müssen diese Absicht öffentlich bekannt machen. Wenn sich eine Organisation beispielsweise einem vom Privatsektor entwickelten Datenschutzprogramm anschließt, das sich an diese Grundsätze hält, qualifiziert sie sich für den „sicheren Hafen“. Darüber hinaus können sich Organisationen auch qualifizieren, wenn sie eigene Maßnahmen zum Schutz personenbezogener Daten entwickeln, sofern diese den Grundsätzen entsprechen. Verstößt eine Organisation, deren Datenschutzmaßnahmen ganz oder teilweise auf Selbstregulierung beruhen, gegen diese Selbstregulierung, muss dieser Verstoß auch gemäß Abschnitt 5 des Federal Trade Commission Act zur Verhinderung unlauterer und irreführender Praktiken oder ähnlichen Rechtsvorschriften verfolgbar sein (der Anhang enthält die Liste der von der EU anerkannten staatlichen Einrichtungen in den Vereinigten Staaten). Zudem können Organisationen, die Gesetzen, Regulierungs-, Verwaltungs- oder anderen Rechtsvorschriften (oder Regeln) unterliegen, die wirksam personenbezogene Daten schützen, ebenfalls in den Genuss der Vorteile des „sicheren Hafens“ gelangen. In allen Fällen gelten die Vorteile des Konzepts des „sicheren Hafens“ ab dem Tag, an dem die Organisation, die sich für die Grundsätze des sicheren Hafens qualifizieren möchte, gegenüber dem Handelsministerium (oder einer von ihm benannten Stelle) gemäß den in den FAQ zur Selbstzertifizierung dargelegten Leitlinien erklärt, dass sie den Grundsätzen beitritt.

Die Geltung dieser Grundsätze kann begrenzt werden a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte, 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.

Organisationen können aus praktischen oder anderen Gründen die Grundsätze auf alle Datenverarbeitungsverfahren anwenden, die Verpflichtung zur Anwendung der Grundsätze entsteht jedoch erst mit dem Beitritt zum „sicheren Hafen“. Bei manuell verarbeiteten Daten ist die Einhaltung der Grundsätze zur Qualifizierung für den „sicheren Hafen“ nicht erforderlich. Organisationen, die vom „sicheren Hafen“ profitieren wollen, um manuell verarbeitete Daten aus der EU zu erhalten, müssen die Grundsätze auf alle Daten anwenden, die nach ihrem Beitritt übermittelt werden. Eine Orga-

nisation, die die Vorteile des sicheren Hafens auf Personaldaten ausdehnen will, die im Rahmen eines Beschäftigungsverhältnisses aus der EU übermittelt werden, muss darauf hinweisen, wenn sie sich dem US-Handelsministerium (oder einer von diesem benannten Stelle) gegenüber auf die Grundsätze verpflichtet, und sie muss die in der FAQ zur Selbstzertifizierung beschriebenen Anforderungen erfüllen. Organisationen können auch die in Artikel 26 der Richtlinie geforderten Garantien bieten, wenn sie in schriftlichen Vereinbarungen mit Stellen, die Daten aus der EU übermitteln, die Grundsätze für die materiellen Datenschutzvorschriften anwenden, sobald die weiteren Vorschriften für derartige Musterverträge von der Kommission und den Mitgliedstaaten genehmigt sind.

Für Fragen der Auslegung und der Einhaltung der Grundsätze des „sicheren Hafens" (einschließlich der FAQ) und der einschlägigen Geschäftsbedingungen für den Datenschutz einzelner dem „sicheren Hafen" angehöriger Organisationen gilt das US-Recht; es gilt nicht, wenn sich eine Organisation zur Zusammenarbeit mit europäischen Datenschutzbehörden verpflichtet hat. Sofern nicht anderweitig festgelegt, finden die Grundsätze des „sicheren Hafens" in sämtlichen Teilen, einschließlich der FAQ, in allen Fällen, in denen sie relevant sind, Anwendung.

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 US-Organisation übermittelt werden.

INFORMATIONSPFLICHT

Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten 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 [1].

WAHLMÖGLICHKEIT

Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen („opt out"), ob ihre personenbezogenen Daten a) an Dritte [1] weitergegeben werden sollen oder b) für einen Zweck verwendet werden sollen, der mit dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck unvereinbar ist. Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare und verständliche, leicht zugängliche und kostengünstige Verfahren ermöglicht werden.

Bei sensiblen Daten (wie z. B. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder philosophische Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung („opt in") der betroffenen Personen, wenn die Daten an Dritte weitergegeben oder für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat. In jedem Fall sollen die Organisationen alle ihnen von Dritten übermittelten Informationen als sensibel behandeln, die der Übermittler als sensibel einstuft und behandelt.

WEITERGABE

Eine Organisation darf Daten nur dann an Dritte weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Möchte eine Organisation Daten an einen Dritten weitergeben, der in ihrem Auftrag und auf ihre Anweisung tätig ist (vergleiche Fußnote), kann sie dies tun, sofern der Dritte entweder dem „sicheren Hafen" angehört oder der Richtlinie unterliegt, oder von einer anderen Feststellung angemessenen Schutzniveaus erfasst wird oder sich schriftlich in einer Vereinbarung mit der Organisation dazu verpflichtet, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den entsprechenden Grundsätzen des „sicheren Hafens" gefordert wird. Eine Organisation, die diese Forderungen erfüllt, kann nicht haftbar gemacht werden (sofern sie nichts anderes vereinbart hat), wenn ein Dritter, an den sie Daten übermittelt hat, Beschränkungen der Verarbeitung dieser Daten missachtet oder sie in einer Weise verarbeitet, die seinen Erklärungen widerspricht, es sei denn, die Organisation wusste oder konnte wissen, dass der Dritte die Daten in unzulässiger Weise verarbeiten würde, und hat keine angemessenen Schritte unternommen, um das zu unterbinden.

---

[1] Die Übermittlung solcher Daten an einen Dritten ist nicht mitteilungspflichtig bzw. unterliegt nicht dem Grundsatz der Wahlmöglichkeit, wenn dieser im Auftrag oder auf Anweisung der Organisation tätig ist. Der Grundsatz der Weitergabe gilt jedoch auch in solchen Fällen.

SICHERHEIT

Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene Sicherheitsvorkehrungen treffen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen.

DATENINTEGRITÄT

In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten für den beabsichtigten Verwendungszweck erheblich sein. 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 Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind.

AUSKUNFTSRECHT

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, 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.

DURCHSETZUNG

Für einen effektiven Schutz der Privatsphäre müssen Mechanismen geschaffen werden, die die Einhaltung der Grundsätze des sicheren Hafens 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: a) leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, behandelt werden und nach denen Schadenersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen; b) Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Unternehmen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden; c) 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.

Anlage

Liste der von der Europäischen Union anerkannten US-Behörden

Die Europäische Union erkennt an, dass die nachfolgend genannten Behörden befugt sind, Beschwerden zu prüfen und Unterlassung wegen unfairer oder betrügerischer Praktiken zu erwirken sowie Schadenersatz bei Verletzung der gemäß den FAQ umgesetzten Grundsätze:

— die Federal Trade Commission aufgrund ihrer Befugnisse nach Abschnitt 5 des Federal Trade Commission Act;

— das US-Verkehrsministerium aufgrund seiner Befugnisse nach Titel 49 des United States Code, Abschnitt 41712.

ANHANG II

HÄUFIG GESTELLTE FRAGEN (FAQ)

FAQ 1 — Sensible Daten

F: *Muss eine Organisation für die Verarbeitung sensibler Daten stets die Zustimmung der betroffenen Person einholen?*

A: Nein, die Zustimmung ist nicht erforderlich, wenn die Verarbeitung: 1. im lebenswichtigen Interesse der betroffenen Person oder einer anderen Person liegt; 2. zur Geltendmachung von Rechtsansprüchen oder für die Rechtsverteidigung notwendig ist; 3. für eine medizinische Behandlung oder Diagnose erforderlich ist; 4. durch eine politisch, philosophisch, 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; 5. zur Erfüllung der arbeitsrechtlichen Pflichten der Organisation notwendig ist; 6. sich auf Daten bezieht, die von der Person nachweislich veröffentlicht worden sind.

FAQ 2 — Ausnahmen für den journalistischen Bereich

F: *Die Pressefreiheit ist durch die amerikanische Verfassung geschützt, und die Richtlinie sieht Ausnahmen für den Fall vor, dass personenbezogene Daten zu journalistischen Zwecken verarbeitet werden. Gelten also die Grundsätze des „sicheren Hafens" auch für personenbezogene Daten, die zu journalistischen Zwecken beschafft, gepflegt oder verbreitet werden?*

A: Wenn die im Ersten Zusatz zur Verfassung der Vereinigten Staaten verankerte Pressefreiheit mit dem Recht auf Schutz der Privatsphäre kollidiert, wird, soweit es um die Tätigkeit natürlicher oder juristischer Personen in den USA geht, die Interessenabwägung vom Ersten Verfassungsgrundsatz beherrscht. Die Grundsätze vom „sicheren Hafen" 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.

FAQ 3 — Hilfsweise Haftung

F: *Sind Internetdienstanbieter (Internet service providers, ISP), Telekommunikationsunternehmen und andere Organisationen nach den Grundsätzen des „sicheren Hafens" haftbar, wenn sie im Namen einer anderen Organisation Daten, die gegen die für sie geltenden Bestimmungen verstoßen, lediglich übermitteln, weiterleiten oder zwischenspeichern?*

A: Nein. Wie auch die Richtlinie selbst begründen die Grundsätze des „sicheren Hafens" keine hilfsweise Haftung. Soweit eine Organisation personenbezogene Daten Dritter nur weiterleitet und weder Mittel noch Zweck ihrer Verarbeitung bestimmt, ist sie nicht haftbar.

FAQ 4 — Investmentbanken und Wirtschaftsprüfer

F: *Bei der Tätigkeit von Investmentbanken und Wirtschaftsprüfern kann es vorkommen, dass personenbezogene Daten ohne Wissen und Einwilligung des Betroffenen verarbeitet werden. Unter welchen Voraussetzungen ist das mit den Grundsätzen des „sicheren Hafens" — Informationspflicht, Wahlrecht und Auskunftsrecht (notice, choice and access) — vereinbar?*

A: Investmentbanken 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 Unternehmen auf Erfüllung ihrer gesetzlichen Pflichten, die Prüfung ihrer Rechnungslegung und die Wahrung der Vertraulichkeit von Information betreffend mögliche Übernahmen, Fusionen und Joint Ventures sowie ähnliche Vorgänge, die von Investmentbanken oder Wirtschaftsprüfern abgewickelt werden.

FAQ 5 [1] **— Die Rolle der Datenschutzbehörden**

F: *Wie können Organisationen, die sich zur Zusammenarbeit mit Datenschutzbehörden in der Europäischen Union verpflichten, diese Verpflichtung eingehen und wie wird sie umgesetzt?*

A: Nach den Grundsätzen des „sicheren Hafens" 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 Durchsetzungsgrundsatz beschrieben, gehören diesen Mitteln unter anderem a) Rechtsbehelfe für Personen, über die die Organisationen Daten besitzen, b) Verfahren, mit denen sie überprüfen, ob ihre Aussagen und Zusicherungen betreffend ihre Datenschutzpraxis den Tatsachen entsprechen, c) die Pflicht der Organisationen, Abhilfe zu schaffen, falls es zu Problemen kommt, weil die Grundsätze des „sicheren Hafens" bei ihnen nicht gewahrt werden, sowie Sanktionen für Verstöße gegen diese Grundsätze. Dem Durchsetzungsprinzip (Buchstaben a) und c)) des „sicheren Hafens" können Organisationen dadurch entsprechen, dass sie sich gemäß dieser FAQ zur Zusammenarbeit mit den Datenschutzbehörden in der Europäischen Union verpflichten.

Eine Organisation kann sich zur Zusammenarbeit mit den Datenschutzbehörden verpflichten, indem sie in der Mitteilung, mit der sie das US-Handelsministerium von der Übernahme des Konzepts des „sicheren Hafens" in Kenntnis setzt, Folgendes erklärt (siehe FAQ 6 — Selbstzertifizierung):

1. dass sie den Bestimmungen der Buchstaben a) und c) des Durchsetzungsprinzips entsprechen will, indem sie sich zur Zusammenarbeit mit den entsprechenden Datenschutzbehörden verpflichtet;

2. dass sie mit den entsprechenden Datenschutzbehörden bei der Behandlung von Beschwerden zusammenarbeiten will, die unter Berufung auf die Grundsätze des „sicheren Hafens" erhoben werden;

3. dass sie sich an die Empfehlung der entsprechenden Datenschutzbehörden hält, wenn diese der Organisation aufgeben, spezifische Maßnahmen zu treffen, um den Grundsätzen des „sicheren Hafens" zu entsprechen; hierzu gehören auch Rechtsmittel und Entschädigungsleistungen zu Gunsten von Personen, die infolge Nichteinhaltung der Grundsätze Nachteile erlitten haben; ferner, dass sie den entsprechenden Datenschutzbehörden schriftlich die Durchführung dieser Maßnahmen bestätigt.

Die Kooperation der Datenschutzbehörden erfolgt über Information und Beratung:

— Die Beratung übernimmt ein informelles Gremium, in dem europäische Datenschutzbehörden vertreten sind, sodass u. a. ein einheitlicher schlüssiger Ansatz gewährleistet wird.

— 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 „sicheren Hafens" übermittelt wurden. Diese Beratung soll gewährleisten, dass die Grundsätze des sicheren Hafens korrekt angewendet werden; sie schließt die Rechtsmittel für die betroffene(n) Einzelperson(en) ein, die die Datenschutzbehörden für angemessen erachten.

— 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 „sicheren Hafens" 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.

— 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.

— Soweit es ihm angemessen erscheint, veröffentlicht das Gremium die Ergebnisse der Beschwerdeprüfungen.

— Die Beratung ist weder für das Gremium selbst noch für eine der beteiligten Datenschutzbehörden mit irgendeiner Form der Haftung verbunden.

[1] Die Einbeziehung dieser FAQ in das Paket hängt von der Zustimmung der Datenschutzbehörden ab. Diese haben den vorliegenden Text in der Arbeitsgruppe nach Artikel 29 erörtert, und eine Mehrheit hat sich positiv dazu geäußert. Endgültig wollen sie sich aber erst im Rahmen einer Gesamtstellungnahme äußern, die die Arbeitsgruppe nach Artikel 29 zu dem Gesamtpaket abgeben wird.

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 keine befriedigende Erklärung für die Verzögerung gegeben, so teilt das Gremium seine Absicht mit, die Angelegenheit an die US-Federal-Trade-Commission 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 Kooperationsvereinbarung vorliegt, und diese mithin null und nichtig ist. In diesem Fall unterrichtet das Gremium das US-Handelsministerium (oder eine von ihm benannte Stelle), sodass das Verzeichnis der dem „sicheren Hafen" angehörenden Organisationen entsprechend geändert werden kann. Jede Unterlassung der Zusammenarbeit und jeder Verstoß gegen die Grundsätze des „sicheren Hafens" können als Irreführung gemäß Abschnitt 5 des US-FTC-Acts oder anderen vergleichbaren Gesetzen rechtlich verfolgt werden.

Organisationen, die sich für die Zusammenarbeit gemäß der Vereinbarung zum „sicheren Hafen" 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.

Die Option der Zusammenarbeit mit den Datenschutzbehörden steht den Organisationen, die der Vereinbarung zum „sicheren Hafen" beitreten, für drei Jahre offen. Die Datenschutzbehörden werden die Vereinbarung vor Ablauf dieses Zeitraums überprüfen, falls sich zu viele US-amerikanische Organisationen für diese Option entscheiden.

FAQ 6 — Selbstzertifizierung

F: *Wie zertifiziert eine Organisation, dass sie die Grundsätze des „sicheren Hafens" als verbindlich anerkennt?*

A: In den Genuss der Vorteile des „sicheren Hafens" kommt eine Organisation ab dem Tag, an dem sie dem US-Handelsministerium (oder einer von diesem benannten Stelle) gegenüber erklärt, dass sie entsprechend den nachstehenden Leitlinien den Grundsätzen des „sicheren Hafens" beitritt (Selbstzertifizierung).

Um sich selbst zu zertifizieren, muss die Organisation dem US-Handelsministerium (oder einer von diesem benannten Stelle) ein von einem leitenden Mitarbeiter im Namen der Organisation unterzeichnetes Schreiben vorlegen, das mindestens folgende Angaben enthält:

1. Name der Organisation, Postanschrift, E-Mail-Adresse, Telefon- und Faxnummer;

2. Beschreibung der Tätigkeit der Organisation im Zusammenhang mit personenbezogenen Daten aus der EU; und

3. Beschreibung der Geschäftsbedingungen für den Datenschutz der Organisation, die folgende Angaben umfassen muss: a) Ort, an dem diese Beschreibung von der Öffentlichkeit eingesehen werden kann; b) Tag, an dem diese Vorkehrungen in Kraft gesetzt wurden; c) Kontaktstelle, die für die Bearbeitung von Beschwerden, Auskunftsersuchen und anderen Angelegenheiten des sicheren Hafens zuständig ist; d) die gesetzliche Aufsichtsbehörde, die über Beschwerden gegen die Organisation wegen unlauteren oder irreführenden Geschäftsgebarens und wegen Verletzung von datenschutzrechtlichen Vorschriften entscheidungsbefugt ist (und im Anhang zu den Grundsätzen aufgeführt ist); e) die Bezeichnungen aller Datenschutzprogramme, an denen die Organisation teilnimmt; f) die Art der anlassunabhängigen Kontrolle (z. B. intern oder extern) [2] und g) das unabhängige Schiedsverfahren zur Behandlung ungelöster Beschwerdefälle.

Wenn die Organisation wünscht, dass ihr die Vorteile des sicheren Hafens auch bei Personaldaten zuteil werden, die zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, muss es eine gesetzliche Aufsichtsbehörde geben, die über Beschwerden gegen die Organisation hinsichtlich Arbeitnehmerdaten beschwerdebefugt ist; diese Stelle muss im Anhang zu den Grundsätzen genannt sein. Darüber hinaus muss die Organisation darauf in der Selbstzertifizierung hinweisen und sich bereit erklären, gemäß FAQ 9 und 5, soweit anwendbar, mit der (den) Datenschutzbehörde(n) in der EU zusammenzuarbeiten und den Empfehlungen dieser Behörden nachzukommen.

Das Ministerium (oder die von ihm benannte Stelle) führt eine Liste aller Organisationen, die sich selbst zertifizieren und denen damit die Vorteile des „sicheren Hafens" zustehen. Die Liste wird nach den jährlich eingehenden Selbstzertifizierungsschreiben und den nach FAQ 11 eingegangenen Mitteilungen aktualisiert. Das Selbstzertifizierungsschreiben ist mindestens jährlich neu vorzulegen, andernfalls wird die Organisation von der Liste gestrichen und

[2] Siehe FAQ 7 zum Thema anlassunabhängige Kontrolle.

verliert damit ihren Status als „sicherer Hafen". Die Liste und die von den Organisationen vorgelegten Selbstzertifizierungsschreiben werden der Öffentlichkeit zugänglich gemacht. Alle Organisationen, die sich selbst zertifizieren, müssen in ihren relevanten veröffentlichten Geschäftsbedingungen zum Datenschutz auch erklären, dass sie sich an die Grundsätze des „sicheren Hafens" halten.

Die Verpflichtung auf die Grundsätze des „sicheren Hafens" gilt ohne zeitliche Begrenzung für Daten, die der Organisation übermittelt wurden, während sie den Status eines „sicheren Hafens" hatte. Diese Daten unterliegen den Grundsätzen des „sicheren Hafens" so lange, wie die Organisation sie speichert, verarbeitet oder weitergibt, und das auch dann noch, wenn sie aus welchem Grund auch immer den „sicheren Hafen" verlässt.

Eine Organisation, die aufgrund einer Fusion oder einer Übernahme ihren Status als selbstständige rechtliche Einheit verliert, muss dies dem Handelsministerium (oder einer von ihm benannten Stelle) vorher mitteilen. In dieser Mitteilung sollte auch darauf hingewiesen werden, ob die übernehmende Einheit bzw. die Einheit, die aus der Fusion hervorgeht, 1. weiterhin nach dem Gesetz, unter dem die Fusion oder Übernahme stattfand, an die Grundsätze des „sicheren Hafens" gebunden ist oder 2. entscheidet, ihren Beitritt zu den Grundsätzen des „sicheren Hafens" selbst zu zertifizieren, bzw. andere Garantien, beispielsweise durch schriftliche Vereinbarungen, schafft, die die Einhaltung der Grundsätze des „sicheren Hafens" gewährleisten. Ist weder 1. noch 2. der Fall, müssen alle Daten, die im Rahmen des „sicheren Hafens" gesammelt wurden, unverzüglich gelöscht werden.

Eine Organisation muss die Grundsätze des „sicheren Hafens" nicht unterschiedslos auf alle personenbezogenen Daten anwenden, sie muss sie aber auf alle nach ihrer Verpflichtung auf diese Grundsätze aus der EU empfangenen personenbezogenen Daten anwenden.

Macht eine Organisation gegenüber der Öffentlichkeit unzutreffende Angaben über ihre Anwendung der Grundsätze des „sicheren Hafens", kann die Federal Trade Commission oder eine andere zuständige staatliche Stelle gegen sie vorgehen. Unzutreffende Angaben gegenüber dem US-Handelsministerium oder einer von ihm benannten Stelle können nach dem False Statements Act (18 U.S.C. § 1001) strafrechtlich verfolgt werden.

FAQ 7 — Anlassunabhängige Kontrolle

F: *Nach welchen Verfahren prüfen Organisationen, dass der von ihnen zugesicherte Datenschutz tatsächlich besteht und dass ihre Datenschutzpolitik tatsächlich umgesetzt worden ist und den Grundsätzen des „sicheren Hafens" entspricht?*

A: Die nach dem Durchsetzungsgrundsatz erforderliche anlassunabhängige Kontrolle kann eine Organisation entweder selbst durchführen oder von einer externen Stelle durchführen lassen.

Die Selbstkontrolle umfasst eine Erklärung darüber, dass die Organisation feststellt, dass ihre veröffentlichten Geschäftsbedingungen zum Datenschutz 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 Geschäftsbedingungen zum Datenschutz den Grundsätzen des „sicheren Hafens" 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 sanktioniert und dass es bei ihr interne Verfahren gibt, nach denen die Einhaltung der Datenschutzvorschriften regelmäßig und objektiv überprüft wird. Die Selbstkontrolle sollte 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.

Organisationen sollten die Umsetzung ihrer nach den Grundsätzen des „sicheren Hafens" konzipierten Geschäftsbedingungen zum Datenschutz 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 Geschäftsgebaren entscheidungsbefugt ist.

Bei externer anlassunabhängiger Kontrolle ist nachzuweisen, dass die Geschäftsbedingungen zum Datenschutz der Organisation für den Schutz personenbezogener Daten aus der EU den Grundsätzen des „sicheren Hafens" entsprechen, dass diese Regeln eingehalten werden und dass betroffene Personen über die Beschwerdewege informiert werden, die ihnen offen stehen. Dazu können ohne Einschränkung Buchprüfungen und Zufallskontrollen durchgeführt sowie „Köder" und jede Art von technischen Hilfsmitteln eingesetzt werden. Die externe Kontrolle sollte 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.

FAQ 8 — Auskunftsrecht

Auskunftsrecht

Personen müssen Zugang zu Daten haben, die eine Organisation über sie gespeichert hat, und diese Daten berichtigen, ergänzen oder löschen lassen können, wenn sie unrichtig sind. Der Zugang kann jedoch verwehrt werden, wenn seine Gewährung mit Kosten oder Arbeit verbunden ist, die im Einzelfall in keinem Verhältnis zum Nachteil für die Privatsphäre des Betroffenen stehen, oder wenn legitime Rechte Dritter verletzt würden.

F 1: *Gibt es ein absolutes Auskunftsrecht?*

A 1: Nein. Nach den Grundsätzen des „sicheren Hafens" ist das Auskunftsrecht zwar grundlegend für den Schutz der Privatsphäre und ermöglicht es dem Einzelnen, die Richtigkeit von Daten zu überprüfen, die über ihn gespeichert sind. Die Pflicht einer Organisation, Personen Zugang zu den sie betreffenden personenbezogenen Daten zu gewähren, hat jedoch Grenzen, die sich nach dem Grundsatz der Verhältnismäßigkeit und der Zumutbarkeit bestimmen, und muss in bestimmten Fällen abgemildert werden. In der Begründung zu den Datenschutzleitlinien der OECD von 1980 wird schon klar gesagt, dass das Auskunftsrecht nicht absolut ist. Die Organisation ist nicht verpflichtet, so gründlich zu recherchieren, wie es etwa im Rahmen einer gerichtlichen Untersuchung erforderlich wäre, und muss auch nicht Zugang zu allen verschiedenen Speicherformen gewähren, in denen Daten über den Betroffenen gespeichert sind.

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 und/oder um welche Art von Daten (oder deren Nutzung) es geht. Wer Zugang zu den ihn betreffenden Daten verlangt, muss das allerdings nicht begründen.

Bei der Beurteilung der Zumutbarkeit sind die Kosten und die Arbeit zu berücksichtigen, die die Gewährung des Zugangs erfordert, sie sind aber nicht entscheidend. Bilden die 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 zumutbar, über diese Daten Auskunft zu geben, selbst wenn das einen relativ hohen Kosten- und Arbeitsaufwand erfordert.

Wenn die angeforderten Daten nicht sensibel sind oder nicht für Entscheidungen verwendet werden, die für die Person von großer Tragweite sind (z. B. nichtsensible Marketingdaten, nach denen entschieden wird, ob die Person einen Katalog zugesandt bekommt), aber leicht zugänglich sind und kostengünstig zur Verfügung gestellt werden können, muss die Organisation Zugang zu den Daten gewähren, die sie über die Person speichert. Diese Daten können von der Person selbst erhoben, im Verlauf eines Geschäftsvorgangs gesammelt oder von anderen erlangt worden sein.

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 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, keinen Zugang zu gewähren, sollte sie der Person, die um Zugang ersucht hat, ihre Entscheidung begründen und ihr eine Kontaktstelle nennen, die weitere Auskünfte erteilt.

F 2: *Was sind vertrauliche Geschäftsdaten und dürfen Organisationen den Zugang zu personenbezogenen Daten verwehren, um vertrauliche Geschäftsdaten zu schützen?*

A 2: Vertrauliche Geschäftsdaten (in den Federal Rules of Civil Procedure on discovery als „confidential commercial information" bezeichnet) sind Daten, die ihr Inhaber durch besondere Vorkehrungen vor unbefugtem Zugriff geschützt hat, weil ihre Kenntnis Konkurrenten Vorteile verschaffen würde. Ein spezielles Rechnerprogramm, das eine Organisation verwendet, etwa ein Modellierungsprogramm, oder die Einzelheiten dieses Programms können vertrauliche Geschäftsdaten sein. Können vertrauliche Geschäftsdaten leicht von den Daten getrennt werden, zu

denen Zugang verlangt wird, sollte die Organisation die vertraulichen Daten unkenntlich machen und die nichtvertraulichen zur Verfügung stellen. Eine Organisation kann den Zugang zu personenbezogenen Daten verwehren oder einschränken, wenn dadurch eigene vertrauliche Geschäftsdaten, wie z. B. von der Organisation erarbeitete Marketingkonzepte und Klassifikationen, offenbart würden oder aber Geschäftsdaten anderer, die einer vertraglichen Geheimhaltungspflicht unterliegen, sofern eine Geheimhaltungsverpflichtung in solchen Fällen üblich oder vorgeschrieben ist.

F 3: *Kann eine Organisation, die personenbezogene Daten in ihren Datenbanken gespeichert hat, Personen lediglich mitteilen, welche Daten über sie gespeichert sind, oder muss sie ihnen Zugang zu den Datenbanken gewähren?*

A 3: Es genügt eine Mitteilung über die gespeicherten Daten, der Person muss kein Zugang zu den Datenbanken der Organisation gewährt werden.

F 4: *Muss eine Organisation ihre Datenbanken erforderlichenfalls umstrukturieren, um Auskunft gewähren zu können?*

A 4: 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.

F 5: *Den vorstehenden Antworten ist zu entnehmen, dass Personen der Zugang zu sie betreffenden Daten in bestimmten Fällen verwehrt werden kann. In welchen anderen Fällen ist das noch möglich?*

A 5: Das ist nur in wenigen Fällen möglich und muss in jedem Fall konkret begründet werden. Eine Organisation kann den Zugang zu personenbezogenen Daten insoweit verwehren, 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:

a) Beeinträchtigung von Rechtsvollzug oder Vollstreckung, einschließlich der Verhütung, Untersuchung oder Aufdeckung von Straftaten, oder des Rechts auf einen fairen Prozess;

b) Beeinträchtigung eines zivilrechtlichen Verfahrens, einschließlich der Abwehr, Untersuchung und Verfolgung von Rechtsansprüchen, oder des Rechts auf einen fairen Prozess;

c) die personenbezogenen Daten haben Bezüge zu anderen Personen, die nicht unkenntlich gemacht werden können;

d) gesetzliche oder andere berufliche Rechte und Pflichten werden verletzt;

e) es kommt zum Bruch der notwendigen Vertraulichkeit künftiger oder laufender Verhandlungen, z. B. über die Übernahme börsennotierter Organisationen;

f) die Sicherheitsprüfung von Arbeitnehmern oder ein Beschwerdeverfahren wird beeinträchtigt;

g) die Vertraulichkeit, die bei der Neubesetzung von Stellen oder bei der Umorganisation von Organisationen für eine gewisse Zeit gewahrt werden muss, wird gefährdet;

h) die Vertraulichkeit ist gefährdet, die bei der Überwachung, bei der Prüfung und bei sonstigen gesetzlich vorgeschriebenen Ordnungsfunktionen im Zusammenhang mit der ordnungsgemäßen Wirtschaftsführung erforderlich ist;

i) die Gewährung des Zugangs ist mit unverhältnismäßigen Kosten oder Arbeit verbunden, oder sie führt zur Beeinträchtigung der Rechte oder der berechtigten Interessen anderer.

Eine Organisation, die sich auf einen dieser Ausnahmefälle beruft, muss nachweisen, dass er tatsächlich vorliegt (was in der Regel der Fall ist). Wie bereits gesagt, sollen der anfragenden Person die Gründe für eine Zugangsverweigerung oder -beschränkung mitgeteilt werden, und es soll ihr eine Anlaufstelle für weitere Fragen genannt werden.

F 6: *Kann eine Organisation eine Gebühr erheben, um die Kosten für die Auskunftserteilung zu decken?*

A 6: Ja, die OECD-Leitlinien gestehen Organisationen das Recht zu, eine Gebühr zu erheben. Sie darf aber nicht überhöht sein. Organisationen dürfen also eine angemessene Gebühr in Rechnung stellen. Eine Gebühr kann sinnvoll sein, um wiederholten oder belästigenden Anfragen vorzubeugen.

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.

Der Zugang darf nicht aus Kostengründen verwehrt werden, wenn die Personen, die den Zugang verlangen, bereit sind, diese Kosten zu übernehmen.

F 7: *Ist eine Organisation verpflichtet, Zugang zu personenbezogenen Daten zu gewähren, die sie aus öffentlichen Datenbeständen gewonnen hat?*

A 7: Zunächst eine Begriffsklärung: öffentliche Datenbestände sind Datenbestände, die von Ämtern aller Ebenen geführt werden und der Öffentlichkeit zur Einsichtnahme offen stehen. Das Auskunftsrecht gilt für solche Daten nur, wenn sie mit anderen personenbezogenen Daten kombiniert sind. Das Auskunftsrecht gilt nicht, wenn lediglich kleine Mengen von Daten aus nichtöffentlichen Quellen verwendet wurden, um die öffentlichen Daten zu indexieren oder zu ordnen. Die Bestimmungen der einschlägigen Rechtsvorschriften über die Einsichtnahme in Datenbestände sind einzuhalten. Sind 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.

F 8: *Gilt das Auskunftsrecht für öffentlich verfügbare personenbezogene Daten?*

A 8: Wie bei Daten, die aus öffentlichen Beständen gewonnen wurden (siehe F 7), ist das Auskunftsrecht nicht auf Daten anzuwenden, die bereits der Öffentlichkeit zur Verfügung stehen, sofern sie mit nicht öffentlich verfügbaren Daten kombiniert sind.

F 9: *Wie kann sich eine Organisation vor wiederholten oder belästigenden Auskunftsbegehren schützen?*

A 9: Eine Organisation muss solchen Auskunftsbegehren nicht entsprechen. Deshalb kann sie für Auskünfte eine angemessene Gebühr erheben oder 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.

F 10: *Wie kann sich eine Organisation vor Auskunftserschleichung schützen?*

A 10: Eine Organisation muss nur Auskunft erteilen, wenn die anfragende Person ihre Identität zweifelsfrei nachweist.

F 11: *Gibt es eine Frist, innerhalb deren Auskunft erteilt werden muss?*

A 11: Ja, eine Organisation soll ohne übermäßige Verzögerung und innerhalb angemessener Frist Auskunft erteilen. Wie in der Begründung der OECD-Datenschutzleitlinien von 1980 dargelegt wird, kann diese Forderung auf verschiedene Weise erfüllt werden. So kann eine Organisation, die Daten verarbeitet, von der Pflicht zur sofortigen Auskunftserteilung befreit werden, wenn sie erfasste Personen regelmäßig informiert.

FAQ 9 — Personaldaten

F 1: *Gilt der Grundsatz des „sicheren Hafens", wenn personenbezogene Daten, die im Rahmen eines Beschäftigungsverhältnisses erhoben wurden, aus der EU in die Vereinigten Staaten übermittelt werden?*

A 1: Ja. 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 Grund-

sätze des „sicheren Hafens“ verpflichtet hat, so fällt diese Übermittlung in den Anwendungsbereich der Grundsätze des „sicheren Hafens“. 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 geltenden Bedingungen und Beschränkungen der Übermittlung müssen beachtet werden.

Die Grundsätze des „sicheren Hafens“ gelten nur für die Übermittlung von und den Zugriff auf Daten über identifizierte Einzelpersonen. Statistische Informationen, die auf aggregierten, anonymisierten oder pseudonymisierten Beschäftigungsdaten beruhen, sind unter dem Datenschutzaspekt unbedenklich.

F 2: *Wie sind die Grundsätze der Informationspflicht und des Wahlrechts auf solche Daten anzuwenden?*

A 2: Eine Organisation in den USA, die unter Anwendung der Grundsätze des „sicheren Hafens“ Personaldaten aus der EU empfangen hat, darf diese Dritten nur offen legen und 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. 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.

Es ist darauf hinzuweisen, dass auf Grund einiger allgemein gültiger Bedingungen für die Übermittlung von Daten durch bestimmte 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.

Außerdem ist den individuellen Datenschutzbedürfnissen der Arbeitnehmer angemessen Rechnung zu tragen. Auf Wunsch könnte etwa der Zugriff auf bestimmte Daten beschränkt werden oder Daten könnten anonymisiert oder Codes/Pseudonymen zugeordnet werden, wenn der tatsächliche Name für den vorgesehenen Zweck nicht benötigt wird.

Wo es um Beförderungen, Ernennungen und ähnliche Personalentscheidungen geht, ist die Organisation in dem Maß und so lange von der Pflicht zur Information und zur Beachtung der Wahlmöglichkeit befreit, wie es zur Wahrung ihrer legitimen Interessen notwendig ist.

F 3: *Wie ist der Grundsatz des Auskunftsrechts anzuwenden?*

A 3: In den Antworten auf die FAQs zum Auskunftsrecht wird ausgeführt, aus welchen Gründen der Zugang zu Personaldaten beschränkt oder verwehrt werden kann. Selbstverständlich müssen Arbeitgeber aus 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 „sicheren Hafens“ muss eine Organisation, die solche Daten in den USA verarbeitet, diesen Zugang direkt oder unter Einschaltung des EU-Arbeitgebers gewährleisten.

F 4: *Welche Möglichkeiten der Rechtsdurchsetzung hat der Arbeitnehmer nach den Grundsätzen des „sicheren Hafens“?*

A 4: Soweit Personaldaten 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 der als unzulässig betrachtete Umgang mit ihn betreffenden Daten in den Vereinigten Staaten stattgefunden hat, hierfür die US-Organisation, die die Informationen von dem Arbeitgeber erhalten hat, und nicht der Arbeitgeber verantwortlich ist und somit ein Verstoß gegen die Grundsätze des „sicheren Hafens“ vorliegt und nicht ein Verstoß gegen nationale Rechtsvorschriften, die zur Umsetzung der Datenschutzrichtlinie erlassen wurden. So lässt sich am ehesten klären, wie die einander überschneidenden Bestimmungen des Arbeitsrechts, der Tarifverträge und des Datenschutzrechts miteinander in Einklang zu bringen sind.

Eine auf die Grundsätze des „sicheren Hafens“ verpflichtete amerikanische Organisation, die Personaldaten, die im Rahmen eines Beschäftigungsverhältnisses aus der Europäischen Union übermittelt wurden, benutzt und wünscht, dass auf solche Übermittlungen die Grundsätze des „sicheren Hafens“ angewandt werden, muss sich also verpflichten, gegebenenfalls bei Untersuchungen der in der EU jeweils zuständigen Behörden mitzuwirken und deren Empfehlungen zu befolgen. Die Datenschutzbehörden, die einer Zusammenarbeit in diesem Sinne zustimmen, setzen

die Europäische Kommission und das amerikanische Handelsministerium davon in Kenntnis. In den Fällen, in denen eine auf die Grundsätze des „sicheren Hafens" verpflichtete amerikanische Organisation Personaldaten aus einem Mitgliedstaat, dessen Datenschutzbehörde einer Zusammenarbeit nicht zugestimmt hat, übermitteln will, gilt FAQ 5 ([3]).

FAQ 10 — Datenverarbeitung im Auftrag (Artikel 17 der Datenschutzrichtlinie)

F: *Wenn 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 sicheren Hafen beigetreten ist oder nicht?*

A: Ja. Werden Daten lediglich zur Verarbeitung im Auftrag übermittelt, muss der in Europa für die Verarbeitung Verantwortliche darüber stets einen Vertrag schließen, gleich ob die Verarbeitung in oder außerhalb der EU stattfindet. Der Vertrag soll die Interessen des für die Verarbeitung Verantwortlichen schützen, also der natürlichen oder juristischen Person, die Mittel und Zweck der Verarbeitung bestimmt und die gegenüber der (den) betroffenen Person(en) voll verantwortlich bleibt. Im Vertrag wird festgehalten, welche Arbeiten genau auszuführen sind und mit welchen Vorkehrungen für die Sicherheit der Daten zu sorgen ist.

Eine amerikanische Organisation, die der Vereinbarung zum „sicheren Hafen" beigetreten ist und personenbezogene Daten aus der EU zur Verarbeitung im Auftrag übermittelt bekommt, braucht bei diesen Daten die Grundsätze nicht anzuwenden, denn die Verantwortung dafür gegenüber der betroffenen Person liegt nach den geltenden EU-Rechtsvorschriften (die strenger sein können als die Grundsätze des „sicheren Hafens") weiterhin bei dem für die Verarbeitung Verantwortlichen.

Da die dem „sicheren Hafen" angehörenden Organisationen einen angemessenen Schutz gewähren, ist bei reinen Verarbeitungsverträgen mit dem „sicheren Hafen" angehörenden Organisationen keine vorherige Genehmigung erforderlich (oder die Genehmigung wird von dem jeweiligen Mitgliedstaat automatisch erteilt), wie sie bei Verträgen mit Empfängern, die sich nicht auf die Grundsätze des sicheren Hafens verpflichtet haben bzw. nicht auf andere Weise einen angemessenen Schutz bieten, erforderlich wäre.

FAQ 11 — Schiedsverfahren und Durchsetzungsprinzip

F: *Wie sind die im Durchsetzungsprinzip enthaltenen Anforderungen an die Behandlung von Beschwerden in die Praxis umzusetzen und was geschieht, wenn eine Organisation fortgesetzt gegen die Grundsätze des „sicheren Hafens" verstößt?*

A: Im Durchsetzungsprinzip ist festgelegt, wie den Grundsätzen des sicheren Hafens Geltung zu verschaffen ist. Wie Punkt b) des Durchsetzungsgrundsatzes zu entsprechen ist, wird in FAQ 7 (Kontrolle) ausgeführt. Diese FAQ 11 befasst sich mit den Punkten a) und c), die beide die Forderung nach unabhängigen Schiedsstellen enthalten. Das Beschwerdeverfahren kann auf verschiedene Weise ausgestaltet werden, es muss aber die im Durchsetzungsgrundsatz genannten Anforderungen erfüllen. Organisationen können diese Forderungen des Durchsetzungsgrundsatzes wie folgt erfüllen: 1. indem sie von der Privatwirtschaft entwickelte Datenschutzprogramme befolgen, in deren Regeln die Grundsätze des „sicheren Hafens" integriert sind und die wirksame Durchsetzungsmechanismen vorsehen, wie sie im Durchsetzungsgrundsatz beschrieben sind; 2. indem sie sich gesetzlich oder durch Rechtsverordnung vorgesehenen Kontrollorganen unterwerfen, die Beschwerden von Einzelpersonen nachgehen und Streitigkeiten schlichten; 3. indem sie sich verpflichten, mit den Datenschutzbehörden in der Europäischen Union oder mit deren bevollmächtigten Vertretern zusammenzuarbeiten. 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 Durchsetzungsgrundsatz und in den FAQ niedergelegt sind. Zu beachten ist, dass die Forderungen des Durchsetzungsgrundsatzes die Forderung ergänzen, die im dritten Absatz der Einführung zu den Grundsätzen des sicheren Hafens formuliert ist. Danach müssen auch bei Selbstregulierung Verstöße gegen die Grundsätze gemäß Abschnitt 5 des Federal Trade Commission Act oder einem ähnlichen Gesetz verfolgbar sein.

Anrufung unabhängiger Beschwerdestellen:

Die Verbraucher sollen dazu angehalten werden, Beschwerden zunächst an die Organisation zu richten, die ihre Daten verarbeitet, ehe sie eine unabhängige Beschwerdestelle anrufen. Die Unabhängigkeit einer Beschwerdestelle ist an verschiedenen Merkmalen erkennbar wie transparente Besetzung und Finanzierung oder nachweisbare einschlägige Tätigkeit. Wie im Durchsetzungsgrundsatz gefordert, müssen einem Beschwerdeführer erschwingliche

([3]) Die Vereinbarung nach FAQ 5 ist auf drei Jahre begrenzt. Die Artikel-29-Datenschutzgruppe wird aufgefordert zu erörtern, wie eine dauerhafte Lösung für Personaldaten herbeigeführt werden kann.

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 auch 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 sicheren Hafens ([4]). Ferner sind die Stellen gehalten, sich an der Erarbeitung von Hilfsmitteln, die das Verfahren vereinfachen, wie z. B. Standardformularen für Beschwerden, zu beteiligen.

Rechtsbehelfe und Sanktionen:

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 des sicheren Hafens 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 Daten ([5]), 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 Selbstregulierungsorgane des privaten Sektors müssen bei Missachtung ihrer Entscheidungen die Gerichte anrufen oder die zuständige entscheidungsbefugte Behörde verständigen und das US-Handelsministerium (oder eine von ihm beauftragte Stelle) unterrichten.

Befassung der FTC:

Die FTC will Beschwerden wegen Verletzung der Grundsätze des sicheren Hafens, die Selbstregulierungsorgane für den Datenschutz wie BBBOnline und TRUSTe und EU-Mitgliedstaaten an sie verweisen, vorrangig behandeln, und feststellen, ob gegen Abschnitt 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. 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 Handelsministerium über von ihr unternommene Schritte. Andere Behörden sind angehalten, dem Handelsministerium das abschließende Ergebnis in solchen Fällen und sonstige Entscheidungen über die Beachtung der Grundsätze des sicheren Hafens mitzuteilen.

Fortgesetzte Missachtung der Grundsätze des „sicheren Hafens“:

Missachtet eine Organisation fortgesetzt die Grundsätze, verliert sie ihren Status als „sicheren Hafen“ und die damit verbundenen Vorteile. Eine fortgesetzte Missachtung liegt vor, wenn sich eine Organisation, die sich gegenüber dem US-Handelsministerium oder einer von ihm beauftragten Stelle selbst zertifiziert hat, weigert, der endgültigen Entscheidung eines staatlichen Kontrollorgans oder eines Selbstregulierungsorgans 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 Handelsministerium oder einer von ihm beauftragte Stelle unverzüglich mitteilen. Die Unterlassung dieser Mitteilung kann nach dem False Statements Act strafrechtlich verfolgt werden (18 U.S.C § 1001).

Jede Mitteilung über die fortgesetzte Missachtung der Grundsätze des „sicheren Hafens“ wird in das öffentliche Verzeichnis der dem „sicheren Hafen“ beigetretenen Organisationen aufgenommen, das das US-Handelsministerium (oder eine von ihm beauftragte Stelle) führt, unabhängig davon, ob die Mitteilung durch die Organisation selbst, durch ein Selbstregulierungsorgan oder 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 öffentlichen Liste des US-Handelsministeriums oder einer von ihm beauftragten Stelle lässt sich also ersehen, welche Organisationen als „sicherer Hafen“ anerkannt sind und welche diese Anerkennung verloren haben.

([4]) Beschwerdestellen sind nicht verpflichtet, sich an das Durchsetzungsprinzip zu halten. Sie können auch im Fall widerstreitender Verpflichtungen oder wenn dies ausdrücklich genehmigt wird, bei der Ausübung ihrer spezifischen Aufgaben von den Grundsätzen abweichen.

([5]) 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 in eklatanter Weise verletzt hat.

Eine Organisation, die sich einer Selbstregulierungsorganisation anschließt, um sich erneut als sicherer Hafen zu qualifizieren, muss dieser Selbstregulierungsorganisation ihre frühere Teilnahme am „sicheren Hafen" vollständig offenbaren.

FAQ 12 — Wahlmöglichkeit — Zeitpunkt des Widerspruchs

F: *Hat eine Einzelperson im Rahmen des Grundsatzes der Wahlmöglichkeit lediglich zu Beginn des Kontakts eine Wahlmöglichkeit oder jederzeit?*

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 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 der 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.

Gleichermaßen 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.

FAQ 13 — Reisedaten

F: *Wann dürfen Flugreservierungsdaten und andere Reisedaten wie Daten über Vielflieger, über Hotelreservierungen und über spezielle Bedürfnisse wie religiös begründete besondere Speisewünsche oder die Notwendigkeit pflegerischer Betreuung an Organisationen außerhalb der EU weitergegeben werden?*

A: Solche Daten dürfen in bestimmten Fällen 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 1. die Übermittlung für die Erfüllung eines Vertrags wie der Vielflieger-Vereinbarung notwendig ist und 2. die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat. US-Organisationen, die sich den Grundsätzen des „sicheren Hafens" 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 „sicheren Hafens" 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 „sicheren Hafen" 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.

FAQ 14 — Arzneimittel und Medizinprodukte

F 1: *Wenn in der EU erhobene personenbezogene Daten für Zwecke der pharmazeutischen Forschung oder für andere Zwecke in die USA übermittelt werden, gilt dann das Recht der Mitgliedstaaten oder gelten die Grundsätze des sicheren Hafens?*

A 1: Das Recht der Mitgliedstaaten gilt für die Erhebung der personenbezogenen Daten und für ihre Verarbeitung vor der Übermittlung in die USA. Die Grundsätze des sicheren Hafens 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.

F 2: *In medizinischen und pharmazeutischen Studien gewonnene personenbezogene Daten sind oft sehr wertvoll für künftige Forschungsarbeiten. Darf eine dem „sicheren Hafen" beigetretene US-Organisation, die personenbezogene Daten im Rahmen eines Forschungsvorhabens erhoben hat, diese Daten für ein anderes Forschungsvorhaben verwenden?*

A 2: Ja, 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. 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 Daten ursprünglich erhoben wurden oder in den der Betroffene später eingewilligt hat, muss erneut seine Einwilligung eingeholt werden.

F 3: *Was geschieht mit den Daten eines Teilnehmers, der sich auf eigenen Wunsch oder auf Wunsch der Trägerorganisation aus einem klinischen Versuch zurückzieht?*

A 3: Ein Teilnehmer kann sich jederzeit aus einem klinischen Versuch zurückziehen oder dazu aufgefordert werden. Daten über ihn, 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.

F 4: *Hersteller von Arzneimitteln und Medizinprodukten dürfen in klinischen Versuchen in der EU gewonnene personenbezogene Daten zur Überprüfung an Aufsichtsbehörden in den USA übermitteln. Dürfen sie die Daten auch an andere Stellen übermitteln wie Organisationen und Wissenschaftler?*

A 4: Ja, unter Beachtung der Grundsätze der Informationspflicht und der Wahlmöglichkeit.

F 5: *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. Können die Teilnehmer an solchen sogenannten Blindversuchen Zugang zu Daten über ihre Behandlung während des Versuchs verlangen?*

A 5: Nein, den Teilnehmern muss kein Zugang gewährt werden, wenn ihnen diese Beschränkung vor ihrer Teilnahme erklärt wurde und die Offenlegung der Daten den Nutzen der Forschungsarbeit gefährden würde. 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 6: *Muss ein Hersteller von Arzneimitteln oder Medizinprodukten die in den Grundsätzen des „sicheren Hafens" verankerten Grundsätze der Informationspflicht, der Wahlmöglichkeit, der Weiterübermittlung und des Auskunftsrechts beachten, wenn er 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 (z. B. Herzschrittmacher) nutzen?*

A 6: Nein, soweit die Grundsätze des „sicheren Hafens" mit gesetzlichen Pflichten kollidieren. Das gilt sowohl für Berichte von Dienstleistern des Gesundheitswesens an Arzneimittel- und Medizinproduktthersteller als auch für Berichte von Arzneimittel- und Medizinproduktherstellern an Behörden wie die amerikanische Food and Drug Administration.

F 7: *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. Ist die Übermittlung derart verschlüsselter Daten von der EU in die USA als Übermittlung personenbezogener Daten anzusehen, die den Grundsätzen des sicheren Hafens unterliegt?*

A 7: Nein, das gilt nicht als Übermittlung personenbezogener Daten, die den Grundsätzen des „sicheren Hafens" unterliegt.

FAQ 15 — Daten aus öffentlichen Registern und öffentlich zugängliche Daten

F: *Gelten die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Weiterübermittlung für Daten aus öffentlichen Registern beziehungsweise öffentlich verfügbaren Daten?*

A: Die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Weiterübermittlung 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 Weiterübermittlung auch nicht für öffentlich verfügbare Daten, es sei denn, der europäische Übermittler weist darauf hin, dass diese Daten Beschränkungen unterliegen, aufgrund deren 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.

Wird festgestellt, dass eine Organisation unter Missachtung der obigen Grundsätze absichtlich personenbezogene Daten offengelegt hat, sodass diese Ausnahme von der Regel für die Organisation selbst oder aber für andere von Nutzen ist, verliert sie ihren Status als „sicherer Hafen“ und die damit verbundenen Vorteile.

ANHANG III

Grundsätze des sicheren Hafens: Überblick über die Möglichkeiten der Durchsetzung

Befugnisse des Bundes und der Bundesstaaten im Zusammenhang mit unfairen und irreführenden Praktiken und Datenschutz

Im Folgenden werden die Befugnisse der Federal Trade Commission (FTC) gemäß Abschnitt 5 des Federal Trade Commission Act (U.S.C., Band 15, §§ 41—58) beschrieben, aufgrund deren die FTC berechtigt ist, gegen Personen und Einrichtungen vorzugehen, die ihren Behauptungen und/oder Verpflichtungen, personenbezogene Daten zu schützen, zuwiderhandeln. Ferner werden die Bereiche genannt, in denen die Befugnisse nicht gelten, und die Möglichkeiten anderer Bundes- oder einzelstaatlicher Stellen beschrieben, in den Fällen tätig zu werden, in denen die FTC keine Befugnisse hat [1].

Die Befugnisse der FTC gegen unfaire und irreführende Praktiken

Nach Abschnitt 5 des Federal Trade Commission Act sind unfaire und irreführende Handlungen oder Praktiken im Handel oder mit Bezug auf den Handel rechtswidrig, vergleiche U.S.C., Band 15, § 45(a)(1). Gemäß Abschnitt 5 erhält die FTC die unbeschränkte Zuständigkeit, solche Handlungen und Praktiken zu verhindern, vergleiche U.S.C., Band 15, § 45(a)(2). Dementsprechend kann die FTC nach einer formalen Anhörung eine Unterlassungsanordnung aussprechen, um dem rechtswidrigen Verhalten Einhalt zu gebieten, vergleiche U.S.C., Band 15, § 45(b). Wenn das öffentliche Interesse es erfordert, kann die FTC vor einem Bezirksgericht der Vereinigten Staaten auf einstweilige Unterlassung klagen oder eine einstweilige oder endgültige gerichtliche Verfügung erwirken, vergleiche U.S.C., Band 15, § 53(b). Handelt es sich um weit verbreitete unfaire oder irreführende Handlungen oder Praktiken, oder hat die FTC bereits eine Unterlassungsanordnung ausgesprochen, kann sie eine Verwaltungsvorschrift bezüglich dieser Handlungen oder Praktiken veröffentlichen, vergleiche U.S.C., Band 15, § 57a.

Jeder Verstoß gegen eine Anordnung der FTC wird mit einer Strafe von bis zu 11 000 USD geahndet [2], wobei jeder Tag eines fortgesetzten Verstoßes einen weiteren Verstoß darstellt, vergleiche U.S.C., Band 15, § 45 (1). Gleichermaßen wird jeder wissentliche Verstoß gegen eine FTC-Vorschrift mit einer Strafe von jeweils 11 000 USD geahndet, U.S.C., Band 15 § 45(m). Durchsetzungsmaßnahmen können entweder vom Justizministerium oder, wenn dieses es ablehnt, von der FTC ergriffen werden, U.S.C., Band 15, § 56.

Befugnisse der FTC und Datenschutz

In Ausübung der Befugnisse, die der FTC gemäß Abschnitt 5 gewährt werden, liegt nach Ansicht der FTC eine irreführende Praxis vor, wenn den Verbrauchern falsche Angaben über den Grund der Datenerhebung und über den Verwendungszweck der Informationen gemacht werden [3]. So klagte die FTC im Jahr 1998 gegen das Unternehmen GeoCities, das — entgegen seiner Darstellung und ohne vorherige Genehmigung — Daten, die es auf seiner Website gesammelt hatte, für Werbezwecke an Dritte weitergegeben hat [4]. Die FTC hat ferner erklärt, dass die Erhebung personenbezogener Daten von Kindern sowie der Verkauf und die Weitergabe dieser Daten ohne Genehmigung der Eltern wahrscheinlich als unfaire Praxis angesehen werden kann [5].

---

[1] Es werden hier weder alle Bundesgesetze zum Datenschutz in bestimmten Fällen noch alle einzelstaatlichen Gesetze noch das gesamte Common Law, die unter Umständen relevant sind, beschrieben. Zu den Bundesgesetzen, die die gewerbliche Erhebung und Verwendung personenbezogener Daten regeln, gehören unter anderem: der Cable Communications Policy Act (U. S.C., Band 47, § 551), der Driver's Privacy Protection Act (U.S.C., Band 18, § 2721), der Electronic Communications Privacy Act (U.S.C., Band 18, § 2701 et seq.), der Eletronic Funds Transfer Act (U.S.C., Band 15, §§ 1693, 1693m), der Fair Credit Reporting Act (U.S.C., Band 15, § 1681 et seq.), der Right to Financial Privacy Act (U.S.C., Band 12, § 3401 et seq.), der Telephone Consumer Protection Act (U.S.C., Band 47, § 227) und der Video Privacy Protection Act (U.S.C., Band 18, § 2710). Viele Bundesstaaten haben in diesen Bereichen eine analoge Rechtsprechung. Vergleiche z. B. Mass. Gen. Laws ch. 167B, § 16 (untersagt Finanzinstituten die Weitergabe von Finanzdaten ihrer Kunden an Dritte ohne das Einverständnis der Kunden oder gerichtliche Verfügung), N.Y. Pub. Health Law § 17 (beschränkt die Verwendung und Weitergabe von Daten über die körperliche und geistige Gesundheit und gewährt den Patienten das Recht auf Einsicht in diese Daten).

[2] In diesem Fall kann das Bezirksgericht eine Unterlassungsanordnung aussprechen, um die Anordnung der FTC durchzusetzen, vergleiche U.S.C., Band 15, § 45(1).

[3] Eine „irreführende Praxis" ist definiert als Darstellung, Unterlassung oder Handlung, die Verbraucher in erheblicher Weise täuschen können.

[4] Vergleiche www.ftc.gov/opa/1998/9808/geocitie.htm.

[5] Vergleiche Schreiben an das Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. Ferner verleiht der Children's Online Privacy Protection Act von 1998 der FTC besondere rechtliche Befugnisse, um die Erhebung personenbezogener Daten von Kindern über Websites und durch Betreiber von Online-Diensten zu regulieren, vergleiche U.S.C., Band 15, §§ 6501—6506. Das Gesetz verpflichtet die Betreiber von Online-Diensten, eine entsprechende Mitteilung zu machen und eine nachprüfbare Einverständniserklärung der Eltern anzufordern, bevor sie personenbezogene Daten von Kindern erheben, verwenden oder weitergeben, a.a.O. § 6502(b). Daneben verleiht das Gesetz den Eltern ein Zugangsrecht sowie das Recht, die fortgesetzte Verwendung der Daten zu untersagen, a.a.O.

In einem Schreiben an Herrn John Mogg, Generaldirektor bei der Europäischen Kommission, hat der Vorsitzende der FTC, Herr Pitofsky, darauf hingewiesen, dass die Datenschutzbefugnisse der FTC nicht greifen, wenn keine falsche Erklärung (bzw. überhaupt keine Erklärung) über den Verwendungszweck der Daten abgegeben wurde, vergleiche Schreiben des FTC-Vorsitzenden Pitofsky an John Mogg vom 23. September 1998. Unternehmen, die jedoch von den vorgeschlagenen Grundsätzen des sicheren Hafens Gebrauch machen wollen, müssen zertifizieren, dass sie die Daten, die sie erheben, gemäß den vorgegebenen Leitlinien schützen. Zertifiziert ein Unternehmen, dass es personenbezogene Daten schützt, und tut dies in der Folge nicht, wäre dies eine falsche Erklärung und eine irreführende Praxis im Sinne von Abschnitt 5.

Da die Rechtsbefugnisse der FTC für unfaire und irreführende Handlungen und Praktiken im oder mit Bezug auf den Handel gelten, hat die FTC keinerlei Befugnisse im Hinblick auf die Erhebung und Verwendung personenbezogener Daten für nichtgewerbliche Zwecke, wie zum Beispiel bei der Mittelbeschaffung für wohltätige Zwecke, vergleiche Pitofsky-Schreiben, Seite 3. Die Verwendung personenbezogener Daten in jeder wie auch immer gearteten geschäftlichen Transaktion rechtfertigt jedoch ein Tätigwerden der FTC. Verkauft beispielsweise ein Arbeitgeber personenbezogene Daten seiner Mitarbeiter an einen Direktvermarkter, so fällt diese Handlung in den Geltungsbereich von Abschnitt 5 FTCA.

Ausnahmeregelungen des Abschnitts 5

Gemäß Abschnitt 5 fallen folgende Unternehmen nicht unter die Befugnisse der FTC im Hinblick auf unfaire oder irreführende Handlungen und Praktiken:

— Finanzinstitute, einschließlich Banken, Spar- und Darlehenskassen, sowie Kreditgenossenschaften,

— Betreiber öffentlicher Telekommunikationsnetze und zwischenstaatlich tätige Transportunternehmen,

— Luftverkehrsunternehmen und

— Vieh- und Fleischhändler bzw. Fleischwarenproduzenten.

Vergleiche U.S.C., Band 15, § 45(a)(2). Die einzelnen Ausnahmefälle sowie die Stelle, die die entsprechenden rechtlichen Befugnisse ausübt, werden im Folgenden näher beschrieben.

Finanzinstitute ([6])

Die erste Ausnahme betrifft Banken sowie Spar- und Darlehenskassen gemäß Abschnitt 18(f)(3)[U.S.C., Band 15, § 57a(f)(3)] und Bundeskreditgenossenschaften gemäß Abschnitt 18(f)(4) [U.S.C., Band 15, § 57a(f)(4)] ([7]). Für diese Finanzinstitute gelten stattdessen die Vorschriften des Federal Reserve Board, des Office of Thrift Supervision ([8]) und des National Credit Union Administration Board, vergleiche U.S.C., Band 15, § 57a(f). Diese Regulierungsbehörden sind angehalten, Verordnungen zu erlassen, die notwendig sind, um unfaire und irreführende Praktiken dieser Finanzinstitute zu verhindern ([9]) und eine Anlaufstelle einzurichten, die sich mit Verbraucherbeschwerden befasst, vergleiche U.S.C. Band 15, § 57a(f)(1). Die Durchsetzungsbefugnisse gegenüber Banken und Spar- und Darlehenskassen sind in Abschnitt 8 des Federal Deposit Insurance Act (U.S.C., Band 12, § 1818) festgeschrieben und gegenüber Bundeskreditgenossenschaften in den Abschnitten 120 und 206 des Federal Credit Union Act (U.S.C., Band 15, §§ 57a(f)(2)-(4)).

Auch wenn die Versicherungswirtschaft nicht ausdrücklich in den Ausnahmeregelungen des Abschnitts 5 genannt ist, obliegt die Regulierung des Versicherungsgeschäfts gemäß dem McCarran-Ferguson Act (U.S.C., Band 15, § 1011 et

([6]) Am 12. November 1999 unterzeichnete Präsident Clinton den Gramm-Leach-Bliley Act (Pub. L. 106—102, kodifiziert in U.S.C. Band 15, § 6801 et seq.). Das Gesetz beschränkt Finanzinstitute in der Weitergabe personenbezogener Daten ihrer Kunden. Es verpflichtet die Finanzinstitute u. a., ihre Kunden über ihre Datenschutzpraktiken im Zusammenhang mit der gemeinsamen Nutzung personenbezogener Daten mit angegliederten und nicht angegliederten Unternehmen zu informieren. Das Gesetz ermächtigt die FTC, die Bundesbehörden im Bankwesen und weitere Behörden, Verordnungen zu erlassen, um die gesetzlich vorgeschriebenen Datenschutzbestimmungen umzusetzen. Die Behörden haben diesbezügliche Verordnungsvorschläge vorgelegt.

([7]) Definitionsgemäß gilt diese Ausnahmeregelung nicht für den Wertpapiersektor. Makler, Händler und andere im Wertpapiergeschäft Tätige unterliegen bei unfairen und irreführenden Handlungen und Praktiken der konkurrierenden Rechtsprechung der Securities and Exchange Commission und der FTC.

([8]) Die Ausnahmeregelung in Abschnitt 5 bezog sich ursprünglich auf den Federal Home Loan Bank Board, der im August 1989 durch den Financial Institutions Reform, Recovery and Enforcement Act abgeschafft wurde. Seine Aufgaben wurden dem Office of Thrift Supervision, der Resolution Trust Corporation, der Federal Deposit Insurance Corporation und dem Housing Finance Board übertragen.

([9]) Abschnitt 5 nimmt zwar die Finanzinstitute von der Rechtsprechung der FTC aus, fordert aber gleichzeitig, dass, wenn die FTC eine Bestimmung über unfaire oder irreführende Handlungen und Praktiken erlässt, die Regulierungsstellen im Finanzwesen innerhalb von 60 Tagen analoge Vorschriften erlassen müssen, vergleiche U.S.C., Band 15, § 57a(f)(1).

seq.) im Allgemeinen den einzelnen Bundesstaaten ([10]). Gemäß Abschnitt 2(b) des McCarran-Ferguson Act darf kein Bundesgesetz eine einzelstaatliche Regelung aufheben, beeinträchtigen oder ersetzen, es sei denn, ein solches Gesetz bezieht sich ausdrücklich auf das Versicherungsgeschäft, vergleiche U.S.C., Band 15, § 1012(b). Die Bestimmungen des FTCA gelten allerdings für die Versicherungswirtschaft in dem Umfang, in dem das Geschäft nicht durch einzelstaatliche Gesetze geregelt ist, vergleiche a.a.O. Es sei außerdem darauf hingewiesen, dass der McCarran-Ferguson Act nur im Hinblick auf die Versicherungswirtschaft den einzelstaatlichen Regelungen nachgeht. Die FTC hat also noch Restbefugnisse, wenn sich Versicherungsgesellschaften bei versicherungsfremden Geschäften in unfairer oder irreführender Weise verhalten. Dies wäre beispielsweise der Fall, wenn Versicherer persönliche Daten ihrer Versicherten an Direktvermarkter versicherungsfremder Produkte verkaufen ([11]).

T'ransportunternehmen

Die zweite Ausnahmeregelung des Abschnitts 5 betrifft die Transportunternehmen, die den Gesetzen zur Regulierung des Handels unterliegen, vergleiche U.S.C., Band 15, § 45(a)(2). In diesem Fall beziehen sich die Gesetze zur Regulierung des Handels auf Untertitel IV des Titels 49 des United States Code und auf den Communications Act von 1934 (U.S.C., Band 47, § 151 et seq.), vergleiche U.S.C. Band 15, § 44.

U.S.C., Band 49 Untertitel IV (zwischenstaatlicher Verkehr) umfasst Schienenverkehrsunternehmen, Straßenverkehrsunternehmen, Schifffahrtsunternehmen, Makler, Spediteure und Unternehmen im Leitungsverkehr, U.S.C., Band 49, § 10101 et seq. Diese Transportunternehmen unterliegen der Regulierung durch den Surface Transportation Board, einer unabhängigen Behörde innerhalb des Verkehrsministeriums, vergleiche U.S.C., Band 49, §§ 10501, 13501 und 15301. Jedem Transportunternehmen ist es untersagt, Daten über die Art, Bestimmung und sonstige Aspekte der Ladung, die zum Nachteil des Versenders benutzt werden können, weiterzugeben, vergleiche U.S.C., Band 49, §§ 11904, 14908 und 16103. Es sei darauf hingewiesen, dass diese Bestimmungen für Daten über die Ladung des Versenders gelten und daher augenscheinlich nicht für Daten zur Person des Versenders, die in keinerlei Bezug zur Ladung stehen.

Der Communications Act sieht die Regulierung des inländischen und ausländischen Nachrichtenverkehrs über Kabel und Funk durch die Federal Communications Commission (FCC) vor, vergleiche U.S.C., Band 47, §§ 151 und 152. Außer den Betreibern öffentlicher Telekommunikationsnetze unterliegen auch Fernseh- und Radiosender sowie Kabelnetzbetreiber, die nicht zu den Betreibern öffentlicher Telekommunikationsnetze gehören, dem Communications Act. An sich fallen letztere nicht unter die Ausnahmeregelung des Abschnitts 5 FTCA. Daher hat die FTC rechtliche Befugnisse, gegen diese Unternehmen wegen unfairer und irreführender Praktiken vorzugehen, während die FCC eine konkurrierende Zuständigkeit hat, ihre unabhängigen Befugnisse in diesem Bereich wie nachfolgend beschrieben durchzusetzen.

Nach dem Communications Act ist jeder Betreiber eines öffentlichen Telekommunikationsnetzes einschließlich Ortsvermittlungsstellen verpflichtet, netzwerkbezogene Daten der Kunden vertraulich zu behandeln ([12]), vergleiche U.S.C., Band 47, § 222(a). Zusätzlich zu dieser generellen Datenschutzbefugnis wurde der Communications Act durch den Cable Communications Policy Act von 1984 (der sogenannte Cable Act) geändert (U.S.C., Band 47, § 521 et seq.), um insbesondere Betreibern von Kabelnetzen aufzuerlegen, die persönlich identifizierbaren Daten der Kabelnetzkunden zu schützen, vergleiche U.S.C., Band 47, § 551 ([13]). Der Cable Act beschränkt die Erhebung personenbezogener Daten durch die Betreiber der Netzwerke und verpflichtet sie, ihre Kunden über die Art der erhobenen Daten sowie über deren Verwendungszweck zu unterrichten. Der Cable Act gibt den Kunden das Recht, auf die Daten, die sie betreffen, zuzugreifen und verpflichtet die Betreiber der Kabelnetze, die Daten zu vernichten, sobald sie nicht mehr benötigt werden.

Der Communications Act ermächtigt die FCC, diese beiden Datenschutzbestimmungen durchzusetzen, und zwar entweder auf eigene Initiative oder als Reaktion auf eine Beschwerde von außen ([14]), vergleiche U.S.C., Band 47, §§ 205, 403; a.a.O., § 208. Stellt die FCC fest, dass der Betreiber eines öffentlichen Telekommunikationsnetzes (auch der Betreiber

([10]) Nach U.S.C., Band 15, § 1012(a) unterliegen das Versicherungsgeschäft und alle daran beteiligten Personen den Gesetzen der einzelnen Bundesstaaten, in denen solche Geschäfte bzw. ihre Besteuerung geregelt sind.

([11]) Die FTC hat ihre Rechtsbefugnisse gegenüber Versicherungsgesellschaften in unterschiedlichen Fällen wahrgenommen. In einem Fall hat die FTC ein Unternehmen verklagt, das irreführende Werbung in einem Staat betrieb, in dem es keine Geschäfte tätigen durfte. Die Zuständigkeit der FTC ist begründet durch das Fehlen einer wirksamen einzelstaatlichen Regelung, da das Unternehmen sich außerhalb der Rechtshoheit des betroffenen Staates befand, vergleiche FTC v. Travelers Health Association, 362 U.S. 293 (1960).
17 Bundesstaaten haben den Entwurf für einen Insurance Information and Privacy Protection Act befürwortet, der von der National Association of Insurance Commissioners (NAIC) vorgelegt wurde. Das Gesetz enthält Bestimmungen bezüglich Meldung, Verwendung und Weitergabe sowie Zugang. Fast alle Bundesstaaten haben auch dem NAIC-Entwurf für einen Unfair Insurance Practices Act zugestimmt, der sich besonders gegen unfaire Handelspraktiken in der Versicherungswirtschaft richtet.

([12]) Mit dem Begriff der netzwerkbezogenen Kundeninformationen (customer proprietary network information) sind Daten gemeint, die die Quantität, die technische Konfiguration, die Art, den Zweck und die Häufigkeit der Nutzung eines Telekommunikationsdienstes durch einen Kunden betreffen sowie alle aus der Telefonabrechnung ersichtlichen Daten, vergleiche U.S.C., Band 47, § 222(f)(1). Der Begriff umfasst jedoch nicht Informationen der Abonnentenliste, vergleiche a.a.O.

([13]) In dem Gesetz wird nicht im Einzelnen definiert, was persönlich identifizierbare Informationen (personally identifiable information) sind.

([14]) Diese Befugnis umfasst auch das Recht, unter Abschnitt 222 des Communications Act und für Kabelnetzkunden unter Abschnitt 551 des Cable Act, mit dem der Communications Act geändert wurde, bei Datenschutzverletzungen Entschädigungen zu verlangen, vergleiche auch U.S.C., Band 47, § 551(f)(3) (Zivilklagen vor einem Bundesbezirksgericht sind nichtausschließliche Rechtsmittel, die Kabelnetzkunden neben anderen gesetzlichen Rechtsmitteln zur Verfügung stehen).

eines Kabelnetzes) die Datenschutzbestimmungen der Abschnitte 222 bzw. 551 verletzt hat, hat sie drei Handlungsmöglichkeiten: Nach einer Anhörung und der Feststellung des Verstoßes kann die FCC den Betreiber anweisen, finanzielle Entschädigungen zu zahlen ([15]), vergleiche U.S.C., Band 47, § 209. Als Alternative kann die FCC gegen den Betreiber eine Unterlassungsanordnung bezüglich der rechtswidrigen Praxis bzw. Unterlassung aussprechen, vergleiche U.S.C., Band 47, § 205(a). Schließlich kann die FCC den Betreiber auffordern, die gegebenenfalls von der FCC erlassenen Vorschriften und vorgeschriebenen Praktiken einzuhalten bzw. zu befolgen, vergleiche a.a.O.

Privatpersonen, die der Ansicht sind, dass der Betreiber eines öffentlichen Telekommunikationsnetzes oder eines Kabelnetzes gegen die Bestimmungen des Communications Act oder des Cable Act verstoßen hat, können entweder bei der FCC Beschwerde einlegen oder ihr Anliegen bei einem Bundesbezirksgericht vorbringen, vergleiche U.S.C., Band 47, § 207. Ein Beschwerdeführer, der vor einem Bundesbezirksgericht ein Verfahren gegen den Betreiber eines öffentlichen Telekommunikationsnetzes gewonnen hat, der im Sinne von Abschnitt 222 des Communications Act gegen Datenschutzbestimmungen verstoßen hat, hat ein Anrecht auf den Ersatz des tatsächlichen Schadens und der Anwaltsgebühren, vergleiche U.S.C., Band 47, § 206. Ein Beschwerdeführer, der unter Abschnitt 551 des Cable Act wegen Verletzung des Datenschutzes klagt, kann neben dem Ersatz des tatsächlichen Schadens und der Erstattung der Anwaltsgebühren auch poenalen Schadenersatz und eine angemessene Prozesskostenerstattung erhalten, vergleiche U.S.C., Band 47 § 551(f).

Die FCC hat ausführliche Vorschriften zur Umsetzung von Abschnitt 222 erlassen, vergleiche CFR Band 47, 64.2001—2009. Die Vorschriften beinhalten bestimmte Garantien um netzwerkbezogene Daten der Kunden vor nichtautorisiertem Zugriff zu schützen. Die Regelungen verpflichten die Betreiber öffentlicher Telekommunikationsnetze,

— Softwareprogramme zu entwickeln und anzuwenden, die kennzeichnen, ob der Kunde über die Verarbeitung seiner Daten informiert wurde bzw. seine Zustimmung gegeben hat, wenn die Datei des Kunden zum ersten Mal auf dem Bildschirm erscheint;

— ein elektronisches Aufzeichnungssystem zu führen, mit dem Zugriffe auf das Konto des Kunden zurückverfolgt werden können, um u. a. feststellen zu können, wer, wann und zu welchem Zweck die Datei geöffnet hat;

— ihre Mitarbeiter anzuhalten, nur mit Genehmigung die netzwerkbezogenen Daten der Kunden zu verwenden, und entsprechende Disziplinarmaßnahmen einzuführen;

— ein Überwachungs- und Kontrollverfahren einzuführen, um auch bei Werbung im Ausland die Einhaltung der Vorschriften zu gewährleisten, und

— der FCC jährlich mitzuteilen, wie sie diese Vorschriften einhalten.

Luftverkehrsunternehmen

US-amerikanische und ausländische Luftverkehrsunternehmen, die dem Federal Aviation Act von 1958 unterliegen, fallen nicht unter Abschnitt 5 FTCA, vergleiche U.S.C., Band 15, § 45(a)(2). Dies gilt für jeden, der innerhalb und außerhalb des Landes Waren, Personen oder Postsendungen auf dem Luftweg transportiert, vergleiche U.S.C., Band 49, § 40102. Luftverkehrsunternehmen fallen in die Zuständigkeit des Verkehrsministeriums. Daher ist der Verkehrsminister berechtigt, Maßnahmen zu ergreifen, um unfaire, irreführende oder wettbewerbsfeindliche Praktiken sowie Verdrängungswettbewerb im Luftverkehr zu verhindern, vergleiche U.S.C., Band 49, § 40101(a)(9). Der Verkehrsminister kann im öffentlichen Interesse gegen ein amerikanisches oder ausländisches Luftverkehrsunternehmen oder den Inhaber einer Kartenverkaufsstelle wegen unfairer oder irreführender Praktiken ermitteln, vergleiche U.S.C., Band 49, § 41712. Nach einer Anhörung kann der Verkehrsminister eine Verfügung zur Unterlassung der rechtswidrigen Praxis erlassen, vergleiche a.a.O. Soweit uns bekannt ist, hat der Verkehrsminister diese Befugnisse im Zusammenhang mit dem Schutz personenbezogener Daten von Kunden von Luftverkehrsunternehmen noch nie wahrgenommen ([16]).

Es gibt zwei Bestimmungen zum Schutz personenbezogener Daten, die für Luftverkehrsunternehmen in besonderen Fällen gelten: Der Federal Aviation Act schützt die Daten von Bewerbern für Pilotenstellen, vergleiche U.S.C., Band 49, § 44936(f). Die Luftverkehrsunternehmen dürfen zwar beschäftigungsbezogene Daten der Bewerber anfordern, das Gesetz gibt dem Bewerber jedoch das Recht zu erfahren, dass die Daten angefragt wurden, der Anfrage zuzustimmen, Fehler zu korrigieren und zu verlangen, dass die Daten nur an die Personen weitergegeben werden, die über die Einstellung entscheiden. Die Vorschriften des Verkehrsministeriums sehen vor, dass Daten der Passagierlisten, die für administrative Zwecke erhoben werden, im Fall einer Flugzeugkatastrophe vertraulich behandelt und nur an das amerikanische Außenministerium, das National Transportation Board (auf dessen Anfrage) und das amerikanische Verkehrsministerium weitergegeben werden, 14 CFR part 243, § 243.9(c) (ergänzt durch 63 FR 8258).

([15]) Auch wenn dem Beschwerdeführer kein direkter Schaden entstanden ist, ist dies kein Grund, die Beschwerde abzuweisen, vergleiche U.S.C., Band 47, § 208(a).

([16]) Unseres Wissens gibt es innerhalb dieses Wirtschaftszweigs Bemühungen, das Thema Datenschutz zu behandeln. Wirtschaftsvertreter haben die vorgeschlagenen Grundsätze des sicheren Hafens und ihre möglichen Auswirkungen auf die Luftverkehrsunternehmen erörtert. Diskutiert wurde auch ein Vorschlag, Datenschutzmaßnahmen für diesen Wirtschaftszweig einzuführen, in deren Rahmen sich die teilnehmenden Unternehmen ausdrücklich dem Verkehrsministerium unterstellen.

Vieh- und Fleischhändler, Fleischwarenproduzenten

Nach dem Packers and Stockyards Act von 1921 (U.S.C., Band 7, § 181 et seq.) ist es für jeden Fleischwarenproduzenten im Zusammenhang mit Vieh, Fleisch, Fleischprodukten oder Viehprodukten in unverarbeiteter Form und für jeden, der mit Lebendgeflügel handelt im Zusammenhang mit lebendem Geflügel, rechtswidrig, wenn er an unfairen, in ungerechtfertigter Weise diskriminierenden oder irreführenden Praktiken beteiligt ist bzw. derartige Mittel einsetzt, U.S.C., Band 7, § 192(a); vergleiche auch U.S.C., Band 7, § 213(a) (verbietet alle unfairen, in ungerechtfertigter Weise diskriminierenden Praktiken oder solche Mittel im Zusammenhang mit Vieh). Für die Durchsetzung dieser Bestimmungen ist in erster Linie der Landwirtschaftsminister zuständig, während die FTC die rechtlichen Befugnisse in Bezug auf Transaktionen im Einzelhandel und Geschäfte in der Geflügelindustrie hat, vergleiche U.S.C., Band 7, § 227(b)(2).

Es ist unklar, ob der Landwirtschaftsminister, wenn ein Vieh- oder Fleischhändler entgegen seiner angekündigten Politik den Datenschutz verletzt, dies als irreführende Praxis im Sinne des Packers and Stockyards Act interpretieren würde. Die Ausnahmeregelung des Abschnitts 5 gilt jedoch für Personen, Personengesellschaften oder Kapitalgesellschaften nur insoweit, als diese dem Packers and Stockyards Act unterliegen. Fällt der Schutz personenbezogener Daten nicht in den Geltungsbereich des Packers and Stockyards Act, kommt die Ausnahmeregelung des Abschnitts 5 nicht zur Anwendung, und Fleischwarenproduzenten und Vieh- oder Fleischhändler unterliegen in dieser Hinsicht doch den Befugnissen der FTC.

Die Befugnisse der Bundesstaaten bei unfairen und irreführenden Praktiken

Nach einer Untersuchung der FTC haben alle 50 Bundesstaaten, der District of Columbia, Guam, Puerto Rico und die Virgin Islands Gesetze zur Verhinderung unfairer oder irreführender Handelspraktiken erlassen, die mehr oder weniger dem Federal Trade Commission Act (FTCA) ähneln, vergleiche Fact Sheet der FTC, erschienen in Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation, 59 Thul. L. Rev. 427 (1984). In allen Fällen hat eine Durchsetzungsstelle die Befugnis, Untersuchungen auch im Wege von Vorladungen unter Strafandrohung oder einer Aufforderung zur Abgabe von Auskünften oder Herausgabe von Unterlagen durchzuführen. Ferner kann sie Absichtserklärungen bezüglich der freiwilligen Einhaltung der Vorschriften verlangen, Unterlassungsanordnungen aussprechen oder bei Gericht einstweilige Verfügungen beantragen, um unfaire, sittenwidrige oder irreführende Handelspraktiken zu verhindern, a.a.O. 46 Bundesstaaten ermöglichen in ihrer Rechtsprechung Zivilklagen auf tatsächlichen, doppelten, dreifachen oder poenalen Schadenersatz sowie in einigen Fällen auf die Erstattung sonstiger Kosten und der Anwaltsgebühren, a.a.O.

Floridas Deceptive and Unfair Trade Practices Act beispielsweise ermächtigt den Justizminister dieses Bundesstaates, Ermittlungen durchzuführen und Zivilklage zu erheben wegen unlauteren Wettbewerbs und wegen unfairer, sittenwidriger oder irreführender Handelspraktiken, einschließlich falscher oder irreführender Werbung, irreführender Vorrechte oder Geschäftschancen, betrügerischen Telemarketings und Schneeballsystemen, vergleiche auch N.Y. General Business Law § 349 (zur Verhinderung unfairer Handlungen und irreführender Praktiken im Geschäftsleben).

Eine Befragung, die die National Association of Attorneys General (NAAG) in diesem Jahr durchgeführt hat, bestätigt dies. Alle 43 Staaten, die auf die Befragung geantwortet haben, haben so genannte Mini-FTC-Gesetze oder andere Gesetze, die einen vergleichbaren Schutz bieten. In der Befragung des NAAG gaben 39 Staaten an, dass sie die Befugnis hätten, Beschwerden von Personen entgegenzunehmen, die nicht in dem betreffenden Bundesstaat ansässig sind. Im Hinblick auf den Datenschutz von Verbrauchern haben 37 von 41 Staaten geantwortet, dass sie Beschwerden über Unternehmen entgegennähmen, die unter ihre Rechtshoheit fallen und angeblich gegen ihre selbsterklärte Datenschutzpolitik verstoßen.

ANHANG IV

Datenschutz und Schadenersatz, rechtliche Ermächtigungen, Fusionen und Übernahmen im Rahmen des US-amerikanischen Rechts

Diese Stellung nimmt Bezug auf das Ersuchen der Europäischen Kommission um Klärung des US-amerikanischen Rechts in Bezug auf a) Schadenersatzansprüche wegen Verletzung der Privatsphäre, b) „ausdrückliche Ermächtigungen" im Rahmen des US-amerikanischen Rechts für die Verwendung personenbezogener Informationen auf eine Art und Weise, die nicht in Einklang mit den US-Grundsätzen des sicheren Hafens steht, sowie c) die Auswirkungen von Fusionen und Übernahmen auf nach Maßgabe der Grundsätze des sicheren Hafens übernommene Verpflichtungen.

A. **Schadenersatz für Verletzungen der Privatsphäre**

Die Nichteinhaltung der Grundsätze des sicheren Hafens könnte je nach den rechtserheblichen Umständen zu einer Reihe von Privatklagen führen. Insbesondere könnten auf die Grundsätze des sicheren Hafens verpflichtete Unternehmen aufgrund des Umstands, dass sie ihre erklärten Datenschutzrichtlinien nicht befolgen, für Falschdarstellungen haftbar gemacht werden. Im Rahmen des Common Law haben Privatpersonen ebenso das Recht, auf Schadenersatz wegen Verletzung der Privatsphäre zu klagen. Des Weiteren sehen zahlreiche Bundes- und einzelstaatliche Datenschutzgesetze die Möglichkeit vor, dass Privatpersonen bei Verletzungen Schadenersatz erhalten.

Das Recht, im Fall eines Eingriffs in die Privatsphäre Schadenersatz zu erhalten, ist im US-amerikanischen Common Law fest verankert.

Die Verwendung personenbezogener Informationen auf eine nicht mit den Grundsätzen des sicheren Hafens in Einklang stehende Art und Weise kann im Rahmen einer Reihe von verschiedenen Rechtstheorien zu einer gesetzlichen Haftung führen. So können beispielsweise sowohl der für die Übermittlung der Daten Verantwortliche als auch die betroffenen Einzelpersonen das Safe-Harbor-Unternehmen, das seinen Verpflichtungen nach Maßgabe der Grundsätze des sicheren Hafens nicht nachkommt, wegen Falschdarstellung verklagen. Nach Maßgabe des Restatement of the Law, Second, Torts [1] gilt Folgendes:

> Wer wissentlich falsche Angaben in Bezug auf Sachverhalte, Meinungen, Absichten oder das Recht macht, um somit eine andere Person dazu zu verleiten, im Vertrauen hierauf eine Handlung vorzunehmen bzw. zu unterlassen, macht sich dieser Person gegenüber wegen arglistiger Täuschung haftbar für den finanziellen Verlust, der dieser Person entstanden ist, da sie sich begründeterweise auf die falschen Angaben verlassen hat.

Restatement, § 525. Bei einer Täuschung handelt es sich um eine „arglistige" Täuschung, wenn sie im Wissen bzw. im Glauben daran, dass diese Angabe falsch ist, erfolgt. Ibid. § 526. Im Allgemeinen gilt, dass eine Person, die arglistig falsche Angaben macht, potentiell gegenüber jedweder Person, in Bezug auf die sie beabsichtigt bzw. erwartet, dass diese auf die falschen Angaben vertraut, haftbar gemacht wird für jeweden finanziellen Verlust, den diese hierdurch erleidet. Ibid. § 531. Des Weiteren könnte eine Partei, die einer anderen gegenüber arglistig falsche Angaben macht, einem Dritten gegenüber haftbar sein, falls der Begeher der unerlaubten Handlung beabsichtigt bzw. erwartet, dass seine falschen Angaben auch diesen Dritten erreichen und dieser daraufhin entsprechend handelt. Ibid. § 533.

Im Rahmen der Grundsätze des sicheren Hafens ist die rechtserhebliche Zusicherung die öffentliche Erklärung des Unternehmens, die Grundsätze des sicheren Hafens zu befolgen. Nachdem eine solche Zusicherung abgegeben wurde, könnte eine bewusste Nichteinhaltung der Grundsätze eine Klage auf Täuschung derjenigen begründen, die auf die falschen Angaben vertrauten. Da die Zusicherung, die Grundsätze zu befolgen, der Öffentlichkeit im Allgemeinen gegenüber abgegeben wird, könnten sowohl die Einzelpersonen, die Gegenstand dieser Informationen sind, als auch der für die Übermittlung der personenbezogenen Angaben an das US-amerikanische Unternehmen Verantwortliche in Europa einen Klageanspruch gegen das US-Unternehmen wegen Täuschung haben [2]. Darüber hinaus haftet das US-Unternehmen diesen Personen gegenüber weiterhin für die „fortdauernde Täuschung", und zwar so lange sich diese zu ihrem Nachteil auf die falschen Angaben verlassen. Restatement, § 535.

---

[1] Second Restatement of the Law — Torts; American Law Institute (1997) (2. Bearbeitung der Rechtsgrundsätze, Sachgebiet unerlaubte Handlungen, Amerikanisches Rechtsinstitut).

[2] Dies könnte beispielsweise der Fall sein, wenn die Einzelpersonen auf die Zusicherungen des US-Unternehmens nach Maßgabe der Grundsätze des sicheren Hafens vertrauten, als die dem für die Datenübermittlung Verantwortlichen ihre Zustimmung erteilten, ihre personenbezogenen Informationen den Vereinigten Staaten zu übermitteln.

Diejenigen, die sich auf arglistig erteilte falsche Angaben verlassen, sind berechtigt, Schadenersatz zu erhalten. Nach Maßgabe des Restatement gilt folgende Regelung:

> Der Empfänger von arglistig erteilten falschen Angaben ist berechtigt, im Rahmen einer Täuschungsklage gegen die Person, die die falschen Angaben erteilt hat, für den ihm entstandenen finanziellen Verlust, hinsichtlich dessen ein hinreichend enger Zusammenhang (legal cause) mit der Täuschung besteht, Schadenersatz zu erhalten.

Restatement, § 549. Der zulässige Schadenersatz beinhaltet sowohl die tatsächlichen Mehraufwendungen als auch den Verlust des „geschäftlichen Nutzens" einer geschäftlichen Transaktion. Ibid.; siehe z. B. Boling v. Tennessee State Bank, 890 S.W.2d 32 (1994) (kompensatorischer Schadenersatz der Bank gegenüber den Kreditnehmern in Höhe von 14 825 USD aufgrund der Offenlegung personenbezogener Informationen sowie der Geschäftspläne der Kreditnehmer gegenüber dem Bankdirektor, hinsichtlich dessen ein Interessenkonflikt bestand).

Während es im Fall einer arglistigen Täuschung entweder des tatsächlichen Wissens oder zumindest des Glaubens bedarf, dass die Zusicherung falsch ist, kann ein Haftungsanspruch ebenso im Fall einer fahrlässigen Täuschung entstehen. Nach Maßgabe des Restatements kann jedwede Person, die im Rahmen ihrer Geschäftstätigkeit, ihrer beruflichen Tätigkeit, ihres Anstellungsverhältnisses oder einer finanziellen Transaktion falsche Angaben macht, haftbar gemacht werden, „wenn sie es versäumt, bei der Einholung oder Übermittlung der Informationen ein angemessenes Maß an Sorgfalt und Sachverstand walten zu lassen". Restatement, § 552(1). Im Gegensatz zur arglistigen Täuschung ist der Schadenersatz für fahrlässige Täuschung auf die Mehraufwendungen beschränkt. Ibid. § 552B(1).

In einem kürzlichen Verfahren hat beispielsweise der Superior Court des US-Bundesstaats Connecticut für Recht erkannt, dass ein Versäumnis seitens eines Stromversorgungsunternehmens, seine Informationen über das Zahlungsverhalten von Kunden staatlichen Kreditauskunfteien offen zu legen, einen Grund darstellt, auf Täuschung zu klagen. Vergleiche Brouillard v. United Illuminating Co., 1999 Conn. Super. LEXIS 1754. In diesem Fall wurde der Klägerin ein Kredit verwehrt, da die Beklagte Zahlungen, die nicht innerhalb von dreißig Tagen nach Rechnungsdatum beglichen wurden, als „verspätet" meldete. Die Klägerin behauptete, dass sie von dieser Richtlinie nicht informiert worden sei, als sie bei der Beklagten ein Konto für die Bezahlung des Hausstroms eröffnete. Das Gericht befand insbesondere, dass „eine Klage auf fahrlässige Täuschung auf dem Versäumnis der Beklagten, sich zu äußern, wenn sie hierzu verpflichtet ist, basieren kann". Dieser Fall zeigt auch, dass eine „wissentliche Handlung" oder eine Täuschungsabsicht kein notwendiges Element eines Klagebegehrens auf fahrlässige Täuschung darstellt. Demzufolge könnte ein US-Unternehmen, das auf fahrlässige Weise versäumt, vollständig offen zu legen, wie es nach Maßgabe der Grundsätze des sicheren Hafens erhaltene personenbezogene Informationen verwendet, wegen Täuschung haftbar gemacht werden.

Soweit eine Verletzung der Grundsätze des sicheren Hafens einen Missbrauch personenbezogener Informationen nach sich zieht, könnte eine solche Verletzung auch einen Anspruch des Datensubjekts auf Verletzung der Privatsphäre im Rahmen der Regelungen des Common Law im Hinblick auf unerlaubte Handlungen begründen. Das US-amerikanische Recht anerkennt seit langem Klagegründe im Hinblick auf Verletzungen der Privatsphäre. Hinsichtlich eines Verfahrens im Jahr 1905 ([3]) befand der Supreme Court des US-Bundesstaats Georgia im Fall einer Privatperson, deren Foto von einer Lebensversicherung ohne ihre Zustimmung und ohne ihr Wissen für die Illustration einer Werbeanzeige verwendet worden war, dass ein in den Bestimmungen des Naturrechts und des Common Law verwurzeltes Recht auf Privatsphäre besteht. Indem es heute geläufige Themen der US-amerikanischen Rechtslehre in Bezug auf die Privatsphäre zum Ausdruck brachte, befand das Gericht, dass die Verwendung des Fotos „böswillig" und „falsch" und darauf ausgerichtet gewesen sei, „den Kläger vor der Welt lächerlich zu machen" ([4]). Die Grundlagen der Pavesich-Entscheidung waren, abgesehen von geringfügigen Abweichungen, stets maßgebend und wurden schließlich zum Kern des US-amerikanischen Rechts in Bezug auf dieses Thema. Einzelstaatliche Gerichte haben Klagebegehren im Bereich der Verletzung der Privatsphäre durchwegs bestätigt, und mindestens 48 Bundesstaaten kennen einige dieser Klagebegehren gerichtlich an ([5]). Des Weiteren verfügen mindestens zwölf Bundesstaaten über verfassungsmäßige Regelungen, die ihren Bürgern das Recht auf Schutz der Privatsphäre einräumen ([6]), wobei dieser Schutz in einigen Fällen auch für eine Verletzung der Privatsphäre durch nichtstaatliche Rechtssubjekte gelten könnte. Vergleiche z. B. Hill v. NCAA, 865 P.2d 633 (Ca. 1994); siehe auch S. Ginder, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 S.D. L. Rev. 1153 (1997). („Einige einzelstaatliche Verfassungen beinhalten Datenschutzregelungen, die über die diesbezüglichen Regelungen in der Bundesverfassung hinausgehen. Alaska, Arizona, Kalifornien, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina und Washington verfügen über weitreichendere Datenschutzregelungen.")

Die zweite Bearbeitung des Restatement, Sachgebiet unerlaubte Handlungen (Second Restatement of Torts) bietet in diesem Bereich einen maßgebenden rechtlichen Überblick. Durch Wiedergabe der üblichen gerichtlichen Praxis wird im Restatement dargelegt, dass das „Recht auf Privatsphäre" insgesamt vier verschiedene Ansprüche aus unerlaubter Handlung umfasst. Siehe Restatement, § 652A. Erstens kann eine Klage auf „Verletzung der Intimsphäre" gegen einen Beklag-

([3]) Pavesich v. New England Life Ins. Co., 50 S.E. 68/Ga. 1905.

([4]) Ibid. 69.

([5]) Eine elektronische Abfrage der Westland Datenbank ergab seit 1995 2 703 erfasste zivilrechtliche Verfahren an einzelstaatlichen Gerichten in Bezug auf „Datenschutz".

([6]) Siehe z. B. Verfassung des US-Bundesstaats Alaska, Artikel 1, Absatz 22; Arizona, Artikel 2, Absatz 8; Kalifornien, Artikel 1, Absatz 1; Florida, Artikel 1, Absatz 23; Hawaii, Artikel 1, Absatz 5; Illinois, Artikel 1, Absatz 6; Louisiana, Artikel 1, Absatz 5; Montana, Artikel 2, Absatz 10; New York, Artikel 1, Absatz 12; Pennsylvania, Artikel 1, Absatz 1; South Carolina, Artikel 1, Absatz 10 und Washington, Artikel 1, Absatz 7.

ten zulässig sein, der vorsätzlich, entweder körperlich oder auf sonstige Weise, in die Intimsphäre einer anderen Person bzw. in deren Privatangelegenheiten oder Belange eindringt. ([7]) Zweitens kann ein „Missbrauch" (appropriation) vorliegen, wenn jemand den Namen oder die Abbildung einer anderen Person für eigene Zwecke oder zum eigenen Nutzen verwendet. ([8]) Drittens kann bei einer „Veröffentlichung privater Sachverhalte" Klage erhoben werden, wenn die veröffentlichte Angelegenheit ihrer Art nach für eine vernünftige Person höchst beleidigend ist und für die Öffentlichkeit diesbezüglich kein legitimes Interesse besteht. ([9]) Eine Klage auf „irreführende Darstellung in der Öffentlichkeit" (false light publicity) ist schließlich angemessen, wenn der Beklagte eine andere Person wissentlich oder leichtfertig vor der Öffentlichkeit in einem falschen Licht erscheinen lässt und dies für eine vernünftige Person höchst beleidigend wäre. ([10])

Im Rahmen der Grundsätze des sicheren Hafens könnte eine „Verletzung der Intimsphäre" die unberechtigte Erhebung personenbezogener Informationen mit einschließen, wohingegen die unberechtigte Verwendung personenbezogener Informationen für geschäftliche Zwecke zu einer Klage auf Missbrauch (appropriation) führen könnte. Ebenso würde die Offenlegung nicht korrekter personenbezogener Informationen zu einer unerlaubten Handlung aufgrund „irreführender Darstellung in der Öffentlichkeit" führen, wenn die Angaben als für eine vernünftige Person höchst beleidigend einzustufen sind. Schließlich könnte eine Verletzung der Privatsphäre, die aus der Veröffentlichung bzw. Offenlegung sensibler personenbezogener Informationen resultiert, eine Klage auf „Veröffentlichung privater Sachverhalte" bewirken. (Siehe beispielsweise die dies veranschaulichenden nachstehenden Fälle.)

Was das Thema Schadenersatz anbelangt, so räumt eine Verletzung der Privatsphäre der verletzten Partei das Recht ein, Schadenersatz zu erhalten für:

a) die aus der Verletzung der Privatsphäre resultierende Verletzung seines Rechts auf Achtung der Privatsphäre;

b) sein nachweislich erlittenes psychisches Leid, falls dieses eine normalerweise aufgrund einer solchen Verletzung resultierende Art aufweist, und

c) besonderen Schaden, der mit der Verletzung in hinreichend engem Zusammenhang (legal cause) steht.

Restatement, § 652H. Angesichts der allgemeinen Gültigkeit des Rechts über unerlaubte Handlungen und der Vielzahl von Klagegründen, die verschiedene Aspekte des Rechts auf Achtung der Privatsphäre abdecken, erhalten diejenigen, deren Recht auf Achtung der Privatsphäre aufgrund der Nichteinhaltung der Grundsätze des sicheren Hafens verletzt wird, aller Wahrscheinlichkeit nach Schadenersatz in Form von Geld.

In der Tat sind bei den einzelstaatlichen Gerichten zahlreiche Verfahren anhängig, bei denen in analogen Situationen eine Verletzung der Privatsphäre geltend gemacht wird. Bei dem einseitigen Verfahren AmSouth Bancorporation u. a., 717 So. 2d 357, ging es beispielsweise um eine Gruppenklage, im Rahmen deren geltend gemacht wurde, dass die Beklagte „die von den Einlegern bei der Bank angelegten Gelder ausnutzte, indem sie vertrauliche Informationen über die Anleger und deren Konten weitergab", um es einer angeschlossenen Bank zu ermöglichen, offene Investmentfonds und sonstige Wertpapiere zu verkaufen. In solchen Fällen wird oftmals auf Schadenersatz erkannt. In dem Verfahren Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.App. 1985) hob ein Berufungsgericht das Urteil eines Gerichts der Vorinstanz auf, um für Recht zu erkennen, dass die Verwendung von Photographien des Klägers „vor" und „nach" einer Schönheitsoperation bei einer Vorführung in einem Kaufhaus aufgrund der Veröffentlichung privater Sachverhalte eine Verletzung der Privatsphäre darstellt. Im Verfahren Candebat v. Flanagan, 487 So.2d 207 (Miss. 1986) verwendete die beklagte Versicherungsgesellschaft in einer Werbekampagne einen Unfall, bei dem die Ehefrau des Klägers schwer verletzt worden war. Der Kläger klagte auf Verletzung der Privatsphäre. Das Gericht befand, dass der Kläger Schadenersatz für seelisches Leid und Identitätsmissbrauch erhalten kann. Eine Klage auf widerrechtliche Verwendung kann auch dann erhoben werden, wenn es sich bei dem Kläger um keine berühmte Person handelt. Siehe z. B. Staruski v. Continental Telephone C., 154 Vt. 568 (1990) (die Beklagte zog einen wirtschaftlichen Vorteil aus der Verwendung des Namens und der Abbildung des Angestellten in einem Zeitungsinserat). Im Verfahren Pulla v. Amoco Oil Co., 882 F.Supp. 836 (S.D Iowa 1995) verletzte ein Arbeitgeber die Intimsphäre des klagenden Angestellten, indem er einen anderen Angestellten seine Kreditkartenabrechnungen einsehen ließ, um seine Abwesenheit wegen Krankheit zu überprüfen. Das Gericht bestätigte die Entscheidung der Jury, die auf einen tatsächlichen Schadenersatz in Höhe von 2 USD und einen Strafe einschließenden Schadenersatz (punitive damages) in Höhe von 500 000 USD erkannte. Ein anderer Arbeitgeber wurde haftbar gemacht für die Veröffentlichung einer Geschichte in der Firmenzeitung über einen Angestellten, dem gekündigt worden war, da er angeblich seine Bewerbungsunterlagen gefälscht hatte. Siehe Zinda v. Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis.App. 1987). Die Geschichte stellte aufgrund der Veröffentlichung einer Privatangelegenheit eine Verletzung der Privatsphäre des Klägers dar, da die Zeitung innerhalb der Gemeinschaft im Umlauf war. Schließlich wurde ein College, das Studenten auf HIV testete, nachdem ihnen gesagt worden war, dass der Bluttest nur auf Röteln sei, wegen Verletzung der Intimsphäre haftbar gemacht. Siehe Doe v. High-Tech Institute, Inc., 972 P.2d 1060 (Colo.App. 1998). (Für weitere gesammelte Entscheidungen siehe Restatement, § 652H, Anhang.)

Die Vereinigten Staaten werden oft kritisiert, über die Maßen prozessfreudig zu sein; dies bedeutet jedoch auch, dass der Einzelne den Rechtsweg tatsächlich beschreiten kann und dies auch tut, wenn er glaubt, dass ihm Unrecht geschehen

([7]) Ibid. Kapitel 28, Absatz 652B.
([8]) Ibid. Kapitel 28, Absatz 652C.
([9]) Ibid. Kapitel 28, Absatz 652D.
([10]) Ibid. Kapitel 28, Absatz 652E.

ist. Viele Gesichtspunkte des US-amerikanischen Justizsystems machen es einem Kläger leicht, entweder als Einzelner oder als Gruppe einen Prozess anzustrengen. Durch die Anwaltschaft, die sich im Vergleich zu den meisten anderen Ländern wesentlich umfangreicher gestaltet, ist eine professionelle Vertretung leicht zugänglich. Die Anwälte der Kläger, die Einzelpersonen bei Privatklagen vertreten, arbeiten in der Regel auf der Grundlage eines Erfolgshonorars, wodurch es sogar armen oder mittellosen Klägern möglich ist, den Rechtsweg zu beschreiten. Dies führt zu einem wichtigen Faktor, so zahlt nämlich in der Regel jede Partei ihre eigenen Anwalts- und sonstigen Kosten. Im Gegensatz hierzu hat in Europa die unterliegende Partei der obsiegenen Partei ihre Kosten zu erstatten. Ohne auf die jeweiligen Vorteile der beiden Systeme näher einzugehen, lässt sich feststellen, dass aufgrund der Regelung in den Vereinigten Staaten die Wahrscheinlichkeit geringer ist, dass sich Einzelpersonen, die nicht in der Lage wären, im Unterliegensfall die Kosten beider Seiten zu tragen, davon abschrecken lassen, berechtigte Ansprüche geltend zu machen.

Einzelpersonen können den Rechtsweg sogar dann beschreiten, wenn ihre Ansprüche relativ gering sind. In den meisten, wenn nicht in allen Gerichtsbezirken der Vereinigten Staaten gibt es für Bagatellsachen zuständige Gerichte, die vereinfachte und weniger kostspielige Verfahren bei Rechtsstreitigkeiten, die in ihrem Streitwert unter der gesetzlichen Grenze liegen, anbieten.([11]) Die Möglichkeit des Strafe einschließenden Schadenersatzes (punitive damages) sieht auch eine finanzielle Belohnung für Einzelpersonen, die nur eine geringfügige direkte Verletzung erlitten haben, vor, wenn sie gegen verwerfliches ordnungswidriges Verhalten gerichtlich vorgehen. Schließlich können Einzelpersonen, die alle auf dieselbe Weise verletzt wurden, im Rahmen einer Gruppenklage ihre Mittel und Ansprüche bündeln.

Ein gutes Beispiel für die Möglichkeit von Einzelpersonen, einen Prozess anzustrengen, um hierdurch Schadenersatz zu erhalten, ist der gegen Amazon.com wegen Verletzung der Privatsphäre anhängige Prozess. Amazon.com, das große Online-Einzelhandelsunternehmen, ist Ziel einer Gruppenklage, in der die Kläger geltend machen, dass sie über die Erhebung personenbezogener Informationen über sie nicht unterrichtet wurden und hierzu nicht zugestimmt haben, als sie ein Softwareprogramm namens „Alexa", das Eigentum von Amazon ist, verwendeten. In diesem Fall haben die Kläger Verletzungen gegen den Computer Fraud and Abuse Act aufgrund eines rechtswidrigen Zugriffs auf ihre gespeicherten Mitteilungen sowie gegen den Electronic Communications Privacy Act aufgrund rechtswidrigen Abfangens ihrer elektronischen und telegrafischen Mitteilungen geltend gemacht. Sie machen auch eine Verletzung der Privatsphäre im Rahmen des Common Law geltend. Dies geht auf eine von einem Experten für Sicherheit im Internet im Dezember eingereichte Klage zurück. Es wird ein Schadenersatz in Höhe von 1 000 USD pro Gruppenmitglied, zuzüglich Anwaltskosten und Gewinne aufgrund der Rechtsverletzungen geltend gemacht. Angesichts der Tatsache, dass die Zahl der Gruppenmitglieder möglicherweise in die Millionen geht, könnte sich ein Schadenersatz in Milliardenhöhe ergeben. Die FTC untersucht auch die Anklagepunkte.

Die Rechtsvorschriften auf Bundes- sowie auf einzelstaatlicher Ebene hinsichtlich des Datenschutzes sehen oftmals private Klagen auf Schadenersatz in Form von Geld vor.

Sollten die Grundsätze des sicheren Hafens nicht eingehalten werden, so könnte hierdurch, abgesehen davon, dass dies eine zivilrechtliche Haftung im Rahmen des Rechts der unerlaubten Handlungen bewirkt, auch das ein oder andere der zu Hunderten bestehenden Bundes- oder einzelstaatlichen Gesetze zur Achtung der Privatsphäre verletzt werden. Viele dieser Gesetze, die eine Handhabung personenbezogener Informationen sowohl durch staatliche Stellen als auch im privaten Bereich betreffen, erlauben es Einzelpersonen, im Fall von Verletzungen auf Schadenersatz zu klagen. Zum Beispiel:

Electronic Communications Privacy Act von 1986. Das ECPA untersagt das unberechtigte Abhören bzw. Abfangen von über Mobiltelefon geführten Anrufen und Übertragungen von Computer zu Computer. Verletzungen können zu einem zivilrechtlichen Haftungsanspruch von mindestens 100 USD pro Tag, an dem diese Verletzung andauert, führen. Der Schutz des ECPA erstreckt sich auch auf den unberechtigten Zugang zu und die unberechtigte Preisgabe von gespeicherten elektronischen Mitteilungen. Personen, die gegen das Gesetz verstoßen, haften für entstandene Schäden oder die Einziehung der aufgrund einer Verletzung erzielten Gewinne.

Telecommunications Act von 1996. Nach Maßgabe von § 702 dürfen rechtlich geschützte kundenbezogene Netzwerkinformationen (customer proprietary network information (CPNI)) lediglich für die Erbringung von Telekommunikationsdiensten verwendet werden. Teilnehmer können entweder eine Beschwerde an die Bundesbehörde für das Fernmeldewesen (Federal Communications Commission) richten oder beim Bundesbezirksgericht (federal district court) Klage auf Schadenersatz und Erstattung der Anwaltsgebühren einreichen.

Consumer Credit Reporting Reform Act von 1996. Das Gesetz von 1996 stellt eine Ergänzung des Fair Credit Reporting Act von 1970 (FCRA) dar, wodurch die Regelungen in Bezug auf die Mitteilungspflicht und Zugangsrechte bei Kreditauskünften verbessert werden. Das Reformgesetz legte auch Wiederverkäufern von Verbraucherkreditauskünften neue Beschränkungen auf. Kunden können im Fall diesbezüglicher Verletzungen Zahlung von Schadenersatz und Erstattung der Anwaltsgebühren geltend machen.

([11]) Wir haben der Kommission bereits zu einem früheren Zeitpunkt Informationen über Bagatellsachen zukommen lassen.

In zahlreichen Situationen schützen auch die einzelstaatlichen Gesetze die Privatsphäre des Einzelnen. Bereiche, in denen die Bundesstaaten eingegriffen haben, beinhalten Bankdaten, Teilnahme an den Kabelfernsehdiensten, Kreditauskünfte, arbeitnehmerbezogene Daten, staatliche Daten, genetische Informationen und medizinische Daten, Versicherungsdaten, Schuldaten, elektronische Mitteilungen und Verleih von Videos. ([12])

B. **Ausdrückliche rechtliche Ermächtigungen**

Die Grundsätze des sicheren Hafens sehen eine Ausnahme vor, wenn aufgrund der Gesetze, Rechtsvorschriften oder des Fallrechts „widersprüchliche Verpflichtungen oder ausdrückliche Ermächtigungen entstehen, stets vorausgesetzt, dass ein Unternehmen bei der Ausübung einer solchen Ermächtigung demonstrieren kann, dass seine Nichtbefolgung der Grundsätze auf den Umfang beschränkt ist, der erforderlich ist, um den durch eine solche Ermächtigung geförderten ausschlaggebenden legitimen Interessen nachzukommen". Es steht jedoch eindeutig fest, dass, wenn aufgrund des US-amerikanischen Rechts eine den Grundsätzen des sicheren Hafens entgegenstehende Verpflichtung auferlegt wird, die US-Unternehmen die Gesetze einhalten müssen, und zwar ungeachtet dessen, ob sie auf die Grundsätze des sicheren Hafens verpflichtet sind oder nicht. Während die Grundsätze des sicheren Hafens darauf abzielen, die Unterschiede zwischen dem US-amerikanischen und den europäischen Rechtssystemen für den Schutz der Privatsphäre zu überbrücken, haben wir uns, was ausdrückliche Ermächtigungen betrifft, den Vorrechten unserer gewählten Gesetzgeber zu fügen. Durch die in beschränktem Umfang mögliche Abweichung von einer strikten Befolgung der Grundsätze des sicheren Hafens soll ein Gleichgewicht geschaffen werden, um somit den berechtigten Interessen beider Seiten nachzukommen.

Ausnahmen sind beschränkt auf Fälle, bei denen eine ausdrückliche Ermächtigung vorliegt. Daher müssen in dieser Grenzsituation die entsprechenden Gesetze, Rechtsverordnungen oder Gerichtsentscheidungen das spezifische Verhalten der auf die Grundsätze des sicheren Hafens verpflichteten Unternehmen ausdrücklich genehmigen. ([13]) Anders ausgedrückt, würde die Ausnahme nicht in Fällen gelten, hinsichtlich deren keine entsprechende rechtliche Äußerung vorliegt. Darüber hinaus würde die Ausnahme nur gelten, wenn die ausdrückliche Ermächtigung der Befolgung der Grundsätze des sicheren Hafens entgegensteht. Auch in einem solchen Fall „beschränkt sich die Ausnahme auf das Maß, das erforderlich ist, um den durch eine solche Ermächtigung geförderten ausschlaggebenden rechtmäßigen Interessen nachzukommen". So würde beispielsweise in Fällen, bei denen das Recht eine Gesellschaft lediglich ermächtigt, staatlichen Stellen personenbezogene Informationen zu liefern, die Ausnahme nicht gelten. Umgekehrt wäre jedoch in Fällen, bei denen das Recht eine Gesellschaft explizit ermächtigt, staatlichen Stellen ohne die jeweilige Zustimmung des Einzelnen personenbezogene Informationen zu liefern, eine „ausdrückliche Ermächtigung" gegeben, auf eine Art und Weise zu handeln, die den Grundsätzen des sicheren Hafens entgegensteht. Oder aber spezifische Ausnahmen von den ausdrücklichen Erfordernissen, eine entsprechende Mitteilung zu machen und die Zustimmung einzuholen, würden in den Ausnahmebereich fallen (da dies einer spezifischen Ermächtigung gleichkommen würde, Informationen ohne entsprechende Mitteilung und Zustimmung offen zu legen). So könnte beispielsweise ein Gesetz, das Ärzten gestattet, die medizinischen Daten ihrer Patienten ohne die vorherige Zustimmung der Patienten an Beamte des Gesundheitsamts weiterzugeben, eine Ausnahme vom Mitteilungs- und Wahlmöglichkeitsgrundsatz gewähren. Diese Ermächtigung würde es einem Arzt nicht gestatten, dieselben medizinischen Daten an Gesundheitsvorsorgeeinrichtungen oder kommerzielle pharmazeutische Forschungslabors weiterzugeben, was das Maß der von Rechts wegen erteilten Ermächtigung übersteigen und daher die Reichweite des Ausnahmefalls überschreiten würde. ([14]) Bei der in Frage stehenden rechtlichen Ermächtigung kann es sich um eine „einzelne" Ermächtigung handeln, bestimmte Dinge mit personenbezogenen Daten zu tun; wie die nachstehenden Beispiele jedoch zeigen, handelt es sich eher um eine Ausnahme im Hinblick auf ein weitreichenderes Gesetz, das die Erhebung, Verwendung und Offenlegung personenbezogener Informationen verbietet.

Telecommunications Act von 1996

In den meisten Fällen entsprechen die genehmigten Verwendungen entweder den Erfordernissen der Direktive und den Grundsätzen oder diese würden aufgrund einer der anderen genehmigten Ausnahmen gestattet werden. So wird beispielsweise durch § 702 des Telecommunications Act (kodifiziert in 47 U.S.C. § 222) Fernmeldeunternehmen die Verpflichtung auferlegt, personenbezogene Informationen, die sie in der Zeit, in der sie dem Kunden gegenüber ihre Leistungen erbringen, erhalten, vertraulich zu behandeln. Diese Bestimmung gestattet es Fernmeldeunternehmen insbesondere,

1. Kundendaten für die Erbringung von Telekommunikationsdiensten, einschließlich der Herausgabe von Teilnehmerverzeichnissen zu verwenden;

2. Kundendaten auf schriftliches Ersuchen des Kunden an Dritte zu liefern und

3. Kundendaten in umfassender Form zu liefern.

([12]) Eine kürzlich durchgeführte elektronische Abfrage der Westlaw Datenbank ergab 994 erfasste einzelstaatliche Verfahren, die sich auf Schadenersatz und Verletzung der Privatsphäre bezogen.

([13]) Zur Klarstellung sollte darauf hingewiesen werden, dass die jeweilige Rechtsbehörde nicht explizit auf die Grundsätze des sicheren Hafens verweisen muss.

([14]) Ebenso könnte sich der in diesem Beispiel erwähnte Arzt nicht auf die gesetzliche Ermächtigung berufen, um sich über die in FAQ 12 vorgesehene Ausübung des Einzelnen seiner Wahlmöglichkeit (opt out) in Bezug auf das Direktmarketing hinwegzusetzen. Die Reichweite jedweder Ausnahme aufgrund „ausdrücklicher Ermächtigung" ist notwendigerweise auf die Reichweite der Ermächtigung im Rahmen des entsprechenden Gesetzes beschränkt.

Siehe 47 U.S.C. § 222(c)(1)-(3). Das Gesetz gestattet es Fernmeldeunternehmen hinsichtlich der Verwendung von Kundendaten auch, diese ausnahmsweise zu verwenden,

1. um ihre Dienste aufzunehmen, zu erbringen, in Rechnung zu stellen und das diesbezügliche Inkasso zu besorgen;

2. um sich gegen betrügerisches, missbräuchliches oder rechtswidriges Verhalten zu schützen und

3. im Rahmen eines vom Kunden initiierten Telefonats Telemarketing-, Vermittlungs- oder Verwaltungsdienste zu erbringen ([15]).

Ibid., § 222(d)(1)-(3). Schließlich sind Fernmeldeunternehmen verpflichtet, Herausgebern von Telefonbüchern Teilnehmerverzeichnisse zu liefern, die lediglich die Namen, Anschriften, Telefonnummern und im Fall von Geschäftskunden die Geschäftssparte beinhalten dürfen. Ibid., § 222(e).

Die Ausnahme der „ausdrücklichen Ermächtigung" könnte zum Tragen kommen, wenn Fernmeldeunternehmen geschützte kundenbezogene Netzwerkinformationen verwenden, um betrügerisches oder auf sonstige Weise rechtswidriges Verhalten zu vermeiden. Sogar hier könnten sich derartige Handlungen als „im öffentlichen Interesse" liegend erweisen und aus diesem Grund im Rahmen der Grundsätze des sicheren Hafens gestattet sein.

Vom US-Gesundheitsministerium (Department of Health and Human Services) vorgeschlagene Regelungen

Das US-Gesundheitsministerium (HHS) hat Regelungen hinsichtlich der Vorgaben für den Datenschutz in Bezug auf im Einzelfall identifizierbare Informationen über den Gesundheitszustand vorgeschlagen. Siehe 64 Fed. Reg. 59,918 (3. November 1999) (zu kodifizieren in 45 C.F.R. Punkte 160—164). Die Regelungen würden die Datenschutzerfordernisse des Health Insurance Portability and Accountability Act von 1996, Pub. L. 104—191 in Kraft setzen. Die vorgeschlagenen Regelungen würden es im Allgemeinen verdeckt tätigen Unternehmen (d. h. Gesundheitsprogramme, Abrechnungsstellen für Gesundheitsversorgung und Gesundheitsversorgungseinrichtungen, die Informationen über den Gesundheitszustand in elektronischer Form übermitteln) untersagen, geschützte Informationen über den Gesundheitszustand ohne die Zustimmung im Einzelfall zu verwenden oder offen zu legen. Siehe vorgeschlagenes 45 C.F.R. § 164.506. Die vorgeschlagenen Regelungen würden eine Offenlegung geschützter Informationen über den Gesundheitszustand lediglich für zwei Zwecke vorsehen, nämlich 1. um es Einzelpersonen zu gestatten, Informationen über ihren eigenen Gesundheitszustand zu überprüfen und zu kopieren, siehe ibid. § 164.512 und 2. um die Regelungen durchzusetzen, siehe ibid. § 164.522.

Die vorgeschlagenen Regelungen würden die Verwendungen bzw. Offenlegung geschützter Informationen über den Gesundheitszustand unter bestimmten Umständen ohne die ausdrückliche Genehmigung des Einzelnen gestatten, wie beispielsweise für die Überwachung des Gesundheitsversorgungssystems, zur Durchsetzung des Rechts und in Notfällen. Siehe ibid. § 164.510. Die vorgeschlagenen Regelungen legen die Beschränkungen für diese Verwendungen und Offenlegungen detailliert dar. Darüber hinaus wären genehmigte Verwendungen und Offenlegungen geschützter Informationen über den Gesundheitszustand auf ein Mindestmaß an erforderlichen Informationen beschränkt. Siehe ibid. § 164.506.

Die aufgrund der vorgeschlagenen Regelungen ausdrücklich genehmigten Verwendungen stimmen im Allgemeinen mit den Grundsätzen des sicheren Hafens überein bzw. sind auf andere Weise aufgrund einer sonstigen Ausnahmeregelung gestattet. So ist beispielsweise die Durchsetzung des Rechts und die Rechtsprechung ebenso wie die medizinische Forschung gestattet. Sonstige Verwendungen, wie beispielsweise die Überwachung des Gesundheitsversorgungssystems, des öffentlichen Gesundheitswesens und der staatlichen Gesundheitsdatensysteme dienen dem öffentlichen Interesse. Offenlegungen zur Abwicklung von Gesundheitsversorgungs- und Beitragszahlungen sind für die Erbringung der Gesundheitsversorgungsleistungen erforderlich. Verwendungen im Notfall, um Rücksprache mit den nächsten Familienangehörigen hinsichtlich der Behandlung zu halten, wenn eine Zustimmung vom Patienten „unter Anlegung praktischer und vernünftiger Maßstäbe nicht erteilt werden kann", oder um die Identität oder die Todesursache der verstorbenen Person festzustellen, sind von lebenswichtiger Bedeutung für die betroffene Person sowie für die anderen Personen. Eine Verwendung für die Verwaltung sich im militärischen Einsatz befindlicher Personen sowie sonstiger spezieller Personengruppen unterstützt die ordnungsgemäße Durchführung der militärischen Mission bzw. ähnlicher schwieriger Situationen, und eine derartige Verwendung findet, wenn überhaupt, nur geringe Anwendung auf Verbraucher im Allgemeinen.

Es verbleibt also lediglich die Verwendung personenbezogener Informationen durch Gesundheitsversorgungseinrichtungen, um Patientenverzeichnisse zu erstellen. Auch wenn einer solchen Verwendung nicht das Maß einer „lebenswichtigen" Bedeutung zukommt, so sind die Verzeichnisse für die Patienten sowie für deren Freunde und Verwandte von Nut-

([15]) Der Umfang dieses Ausnahmefalls ist sehr beschränkt. Entsprechend der Bestimmungen kann das Fernmeldeunternehmen geschützte kundenbezogene Netzwerkinformationen (CPNI) nur während eines vom Kunden initiierten Telefonats verwenden. Des Weiteren wurden wir von der FCC darüber in Kenntnis gesetzt, dass das Fernmeldeunternehmen die geschützten kundenbezogenen Netzwerkinformationen nicht verwenden darf, um Dienstleistungen, die über die Reichweite der Kundenanfrage hinausgehen, zu vermarkten. Schließlich stellt diese Regelung, da der Kunde die Verwendung der geschützten kundenbezogenen Netzwerkinformationen zu diesem Zweck genehmigen muss, eigentlich überhaupt keine „Ausnahmeregelung" dar.

zen. Der Umfang dieser genehmigten Verwendung ist des Weiteren von Natur aus begrenzt. Daher stellen Ausnahmen hinsichtlich der Richtlinien für die zu diesem Zweck von Rechts wegen „ausdrücklich genehmigten" Verwendungen ein minimales Risiko für den Datenschutz in Bezug auf Patienten dar.

Fair Credit Reporting Act

Die Europäische Kommission hat ihre Bedenken dahin gehend geäußert, dass die Ausnahme der „ausdrücklichen Ermächtigung" für den Fair Credit Reporting Act (FCRA) „tatsächlich eine Angemessenheitsfeststellung schaffen würde". Das wäre nicht der Fall. Wenn im Rahmen des FCRA keine Angemessenheitsfeststellung gegeben wäre, so müssten US-Unternehmen, die sich ansonsten auf eine solche Feststellung berufen würden, versichern, dass sie die Grundsätze des sicheren Hafens in allen Aspekten befolgen. Dies bedeutet, dass in Fällen, in denen die Bestimmungen des FCRA das in den Grundsätzen vorgegebene Schutzmaß übersteigen, die US-Unternehmen lediglich die Bestimmungen des FCRA zu befolgen haben. Andererseits müssten diese Unternehmen in Fällen, bei denen die Bestimmungen des FCRA nicht ausreichend wären, ihre Vorgehensweise in Bezug auf die Handhabung von Informationen mit den Grundsätzen des sicheren Hafens in Einklang bringen. Durch den Ausnahmefall würde diese grundlegende Feststellung keine Änderung erfahren. Nach Maßgabe ihrer Bestimmungen gilt die Ausnahmeregelung nur in den Fällen, in denen die entsprechenden Gesetze ein Verhalten ausdrücklich genehmigen, das mit den Grundsätzen des sicheren Hafens nicht übereinstimmen würde. Die Ausnahmeregelung würde nicht für Fälle gelten, in denen die Bestimmungen des FCRA lediglich die Grundsätze des sicheren Hafens nicht erfüllen. ([16])

Anders ausgedrückt soll der Ausnahmefall nicht bedeuten, dass das, was nicht vorgeschrieben ist, deshalb „ausdrücklich genehmigt" wird. Des Weiteren gilt die Ausnahmeregelung nur, wenn das, was kraft US-amerikanischem Recht ausdrücklich genehmigt wird, den Erfordernissen der Grundsätze des sicheren Hafens entgegensteht. Das einschlägige Gesetz muss beide Elemente erfüllen, bevor eine Nichtbefolgung der Grundsätze genehmigt werden würde.

§ 604 des FCRA gestattet es Verbraucherberichterstattungsstellen beispielsweise ausdrücklich, in unterschiedlichen bezeichneten Situationen Verbraucherberichte herauszugeben. Siehe FCRA, § 604. Wenn es durch § 604 hierdurch Verbraucherberichterstattungsstellen gestattet werden würde, entgegen den Grundsätzen des sicheren Hafens zu handeln, so hätten sich diese auf den Ausnahmefall zu berufen (sofern natürlich nicht eine sonstige Ausnahme vorläge). Kreditauskunfteien haben Gerichtsbeschlüsse und Zwangsvorladungen der Anklagejury (grand jury) zu befolgen, und die Verwendung von Kreditauskünften durch staatliche Vollzugsstellen für Lizenzierungen, soziale Unterstützung und Kindesunterhalt dient einem öffentlichen Zweck. Ibid., § 604(a)(1), (3)(D) und (4). Folglich müsste sich die Kreditauskunftei für diese Zwecke nicht auf die „ausdrückliche Ermächtigung" im Ausnahmefall berufen. In Fällen, in denen die Kreditauskunftei gemäß den schriftlichen Anweisungen des Verbrauchers handelt, würde sie vollständig den Grundsätzen des sicheren Hafens entsprechen. Ibid., § 604(a)(2). Ebenso können Verbraucherberichte für arbeitnehmerbezogene Zwecke lediglich mit der schriftlichen Genehmigung des Verbraucher eingeholt werden (ibid., §§ 604(a)(3)(B) und (b)(2)(A)(ii)) und für Kredit- oder Versicherungstransaktionen, die nicht vom Verbraucher initiiert werden, nur, falls sich der Verbraucher nicht nach Maßgabe des Wahlmöglichkeitsgrundsatzes (opt out) dagegen verwehrt hat (ibid., § 604(c)(1)(B)). Das FCRA untersagt es Kreditauskunfteien auch, ohne die Zustimmung des Verbrauchers medizinische Informationen für arbeitnehmerbezogene Zwecke zu übermitteln. Ibid., § 604(g). Derartige Verwendungen lassen sich mit den Mitteilungs- und Wahlmöglichkeitsgrundsätzen vereinbaren. Sonstige durch § 604 genehmigte Zwecke beinhalten Transaktionen, bei denen der Verbraucher involviert ist, und die daher im Rahmen der Grundsätze des sicheren Hafens gestattet wären. Siehe ibid., § 604(a)(3)(A) und (F).

Die verbleibende durch § 604 „genehmigte" Verwendung bezieht sich auf sekundäre Kreditmärkte. Ibid., § 604(a)(3)(E). Zwischen der Verwendung von Verbraucherberichten zu diesem Zweck und den Grundsätzen des sicheren Hafens an sich besteht kein Widerspruch. Es ist richtig, dass Kreditauskunfteien nach Maßgabe des FCRA beispielsweise nicht verpflichtet sind, Verbraucher in Kenntnis zu setzen und ihre Zustimmung einzuholen, wenn sie zu diesem Zweck Berichte herausgeben. Wir weisen jedoch nochmal darauf hin, dass das Nichtbestehen eines Erfordernisses eine „ausdrückliche Ermächtigung", auf eine andere als die vorgeschriebene Art und Weise zu handeln, suggeriert. Gleichermaßen gestattet es § 608 Kreditauskunfteien, einige personenbezogene Informationen an staatliche Stellen weiterzugeben. Diese „Ermächtigung" wäre keine Rechtfertigung dafür, dass eine Kreditauskunftei ihre Verpflichtungen, die Grundsätze des sicheren Hafens zu befolgen, nicht einhält. Dies steht im Gegensatz zu unseren anderen Beispielsfällen, bei denen Ausnahmen in Bezug auf die Erfordernisse hinsichtlich der ausdrücklichen Mitteilungs- und Wahlmöglichkeitsgrundsätze dazu dienen, die Verwendung personenbezogener Informationen ohne die Einhaltung der Mitteilungs- und Wahlmöglichkeitsgrundsätze ausdrücklich zu genehmigen.

Schlussfolgerung

Sogar anhand unserer begrenzten Überprüfung dieser Gesetze lässt sich ein bestimmtes Muster erkennen:

— Die „ausdrückliche Ermächtigung" von Rechts wegen gestattet im Allgemeinen die Verwendung oder Offenlegung personenbezogener Informationen ohne die vorherige Zustimmung des Einzelnen; daher wäre die Ausnahme auf die Mitteilungs- und Wahlmöglichkeitsgrundsätze beschränkt.

([16]) Unsere Diskussion sollte an dieser Stelle nicht als Eingeständnis verstanden werden, dass das FCRA keinen „angemessenen" Schutz bietet. Bei jedweder Beurteilung des FCRA ist der durch das Gesetz als Ganzes gewährte Schutz zu betrachten, und es ist nicht nur auf die Ausnahmefälle abzustellen, wie wir es hier tun.

— In den meisten Fällen gelten die von Rechts wegen genehmigten Ausnahmefälle lediglich für bestimmte Situationen und bestimmte Zwecke. Ansonsten ist die nicht genehmigte Verwendung oder Offenlegung personenbezogener Informationen, die nicht in diesen begrenzten Bereich fällt, in allen Fällen von Rechts wegen untersagt.

— In den meisten Fällen dient die genehmigte Verwendung oder Offenlegung, unter Widerspiegelung ihres legislativen Charakters, einem öffentlichen Interesse.

— In beinahe allen Fällen entsprechen die genehmigten Verwendungen entweder vollständig den Grundsätzen des sicheren Hafens oder fallen unter eine der sonstigen genehmigten Ausnahmeregelungen.

Abschließend lässt sich festhalten, dass die Ausnahme aufgrund „ausdrücklicher Ermächtigung" von Rechts wegen von Natur aus in ihrer Reichweite ziemlich beschränkt ist.

C. **Fusionen und Übernahmen**

Die Artikel-29-Arbeitsgruppe brachte ihre Sorge darüber zum Ausdruck, dass in Situationen, in denen ein Safe-Harbour-Unternehmen von einer Gesellschaft übernommen wird bzw. mit dieser fusioniert, die sich nicht den Grundsätzen des sicheren Hafens verpflichtet hat. Die Arbeitsgruppe scheint jedoch davon ausgegangen zu sein, dass die übernehmende Gesellschaft nicht daran gebunden wäre, die Grundsätze des sicheren Hafens auf personenbezogene Informationen, die im Besitz der übernommenen Gesellschaft sind, anzuwenden. Dies ist jedoch nach Maßgabe des US-amerikanischen Rechts nicht notwendigerweise der Fall. Die allgemeine Regel in den Vereinigten Staaten im Hinblick auf Fusionen und Übernahmen lautet dahin gehend, dass eine Gesellschaft, die die ausgegebenen Aktien einer anderen Gesellschaft erwirbt, im Allgemeinen die Pflichten und Verbindlichkeiten der erworbenen Gesellschaft übernimmt. Siehe 15 Flechter Cyclopedia of the Law of Private Corporations § 7117 (1990); siehe auch Model Bus. Corp. Act § 11.06(3) (1979) („die übernehmende Gesellschaft hat alle Pflichten der an der Fusion beteiligten Gesellschaften"). Mit anderen Worten wäre bei einer Fusion oder einer Übernahme eines auf die Grundsätze des sicheren Hafens verpflichteten Unternehmens die übernehmende Gesellschaft aufgrund dieser Methode an die Zusicherungen der übernommenen Gesellschaft in Bezug auf die Grundsätze des sicheren Hafens gebunden.

Darüber hinaus könnten, sogar wenn die Fusion oder Übernahme mittels Erwerb von Vermögenswerten bewirkt werden würde, die Pflichten des erworbenen Unternehmens das erwerbende Unternehmen dennoch unter bestimmten Umständen binden. 15 Flechter, § 7122. Auch wenn nach der Fusion Verpflichtungen nicht fortbestehen, ist darauf hinzuweisen, dass diese nach einer Fusion auch dann nicht fortbestehen würden, wenn die Daten von Europa nach Maßgabe eines Vertrags übermittelt worden wären, was die einzige realisierbare Alternative zu den Grundsätzen des sicheren Hafens für in die Vereinigten Staaten übermittelte Daten darstellt. Des Weiteren sind jedwede den Grundsätzen des sicheren Hafens verpflichtete Unternehmen aufgrund der Safe-Harbor-Dokumente in ihrer aktuellen Fassung verpflichtet, das Handelsministerium über jedwede Übernahmen in Kenntnis zu setzen, und es ist ihnen nur gestattet, Daten weiterhin an das Nachfolgeunternehmen zu übermitteln, wenn dieses sich den Grundsätzen des sicheren Hafens anschliesst (siehe FAQ 6). In der Tat haben die Vereinigten Staaten die Rahmenbestimmungen für die Grundsätze des sicheren Hafens dahin gehend abgeändert, dass US-Unternehmen in dieser Situation Informationen, die sie im Rahmen der Grundsätze des sicheren Hafens erhalten haben, löschen müssen, wenn ihre Zusicherungen in Bezug auf die Grundsätze des sicheren Hafens nicht weiter gelten bzw. keine sonstigen geeigneten Schutzmaßnahmen vorgenommen werden.

ANHANG V

14. Juli 2000

John Mogg
Direktor, GD Binnenmarkt
Europäische Kommission
Büro C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Brüssel

Sehr geehrter Herr Generaldirektor,

wie ich sehe, hat mein Schreiben an Sie vom 29. März 2000 eine Reihe von Fragen aufgeworfen. Um unsere Befugnisse in den fraglichen Bereichen zu erläutern, schreibe ich Ihnen diesen Brief. Um die weitere Bezugnahme zu erleichtern, enthält er nicht nur weitere Erläuterungen, sondern rekapituliert auch einen Teil des vorausgegangenen Schriftwechsels.

Bei Ihren Besuchen in unserer Dienststelle und in unserem Schriftwechsel warfen Sie einige Fragen nach den Befugnissen der United States Federal Trade Commission beim Datenschutz im Online-Verkehr auf. Ich halte es für sinnvoll, meine früheren Antworten zusammenzufassen und durch weitere Informationen über die Zuständigkeit unserer Dienststelle in Fragen des Verbraucherdatenschutzes zu ergänzen, die Sie in Ihrem letzten Schreiben angesprochen hatten. Sie stellten insbesondere folgende Fragen: 1. Ist die FTC in Fragen der Übermittlung von beschäftigungsrelevanten Daten zuständig, wenn bei der Übermittlung die US-Grundsätze des sicheren Hafens verletzt wurden? 2. Ist die FTC für nicht gewinnorientierte Programme zuständig, denen ein Vertrauenssiegel („seal" oder „trustmark") zuerkannt wurde? 3. Gilt der FTC Act sowohl für den Offline- als auch für den Online-Verkehr? 4. Was geschieht, wenn sich die Zuständigkeit der FTC mit der Zuständigkeit anderer Durchsetzungsinstanzen überschneidet?

Anwendung des FTC Act auf den Datenschutz

Die rechtlichen Befugnisse der Federal Trade Commission auf diesem Gebiet sind in Abschnitt 5 des Federal Trade Commission Act („FTC Act") geregelt; gemäß diesem Abschnitt sind unlautere und irreführende Praktiken verboten, die im Handel erfolgen oder den Handel beeinträchtigen ([1]). Irreführende Praktiken sind definiert als Darstellung, Unterlassung oder Handlung, die angetan ist, einen durchschnittlich informierten Verbraucher in erheblicher Weise zu täuschen. Praktiken sind unlauter, wenn sie dem Verbraucher einen erheblichen Schaden zufügen oder zufügen können, der nicht mit vertretbarem Aufwand zu vermeiden ist und nicht durch geldwerte Vorteile für den Verbraucher oder den Wettbewerb aufgewogen wird ([2]).

Bestimmte Praktiken zur Datenerhebung dürften gegen den FTC Act verstoßen. Beispiel: Wenn auf einer Web-Site fälschlicherweise behauptet wird, der Anbieter verfolge eine erklärte Datenschutzpolitik oder beachte Leitlinien zur Selbstregulierung, liefert Abschnitt 5 des FTC Act eine Rechtsgrundlage, auf der eine derarte Fehldarstellung als irreführend verfolgt werden kann. In der Tat haben wir das Recht erfolgreich durchgesetzt, das diesen Grundsatz begründet ([3]). Darüber hinaus hat sich die FTC das Recht vorbehalten, gravierende Datenschutzpraktiken als unlauter im Sinne von Abschnitt 5 zu verfolgen, falls Kinder oder hochsensible Daten, z. B. Finanz- ([4]) oder Medizindaten, davon betroffen sind. Die Federal Trade Commission hat derartige Durchsetzungsmaßnahmen in der Vergangenheit ergriffen und wird es auch in Zukunft tun; sie stützt sich dabei auf ihre eigene aktive Überwachungs- und Recherchetätigkeit, aber auch auf Fälle, die Selbstregulierungsorgane und andere Stellen, darunter die Mitgliedstaaten der Europäischen Union, an sie verweisen.

([1]) 15 U.S.C. § 45. Der Fair Credit Reporting Act (Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten) wäre ebenfalls auf Datenerhebung und -handel im Internet anwendbar, sofern sie die rechtlich definierten Konzepte „consumer report" (Konsumentendatei) und „consumer reporting agency" (Kreditauskunftei) betreffen.

([2]) 15 U.S.C. § 45(n).

([3]) Siehe GeoCities, Docket No. C-3849 (Final Order Feb. 12, 1999) (auf www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., Docket No. C-3891 (Final Order Aug. 12, 1999) (auf www.ftc.gov/opa/1999/9905/younginvestor.htm). Siehe auch Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. Part 312 (auf www.ftc.gov/opa/1999/9910/childfinal.htm). Die COPPA Rule, die letzten Monat in Kraft trat, verlangt von Betreibern von Web-Sites, die an Kinder unter 13 Jahren gerichtet sind oder die wissentlich personenbezogene Daten von Kindern unter 13 erheben, dass sie die in der Rule geforderten Standards für faire Datenpraktiken umsetzen.

([4]) Siehe FTC v. Touch Tone, Inc., Civil Action No 99-WM-783 (D.Co.) (eingereicht am 21. April 1999) auf www.ftc.gov/opa/1999/9904/touchtone.htm. Staff Opinion Letter vom 17. Juli 1997, als Antwort auf eine Petition des Center for Media Education auf www.ftc.gov/os/1997/9707/cenmed.htm.

Unterstützung bei der Selbstregulierung

Die FTC wird Fälle von Missachtung der Selbstregulierungsleitlinien, die Einrichtungen wie BBBOnline und TRUSTe ([5]) an zu verweisen, vorrangig behandeln. Dieses Vorgehen würde auch unseren langjährigen Beziehungen zum National Advertising Review Board (NARB) des Better Business Bureau gerecht, das Beschwerden über Werbemaßnahmen an die FTC verweist. Die National Advertising Division (NAD) von NARB regelt Beschwerden über inländische Werbemaßnahmen in Schiedsverfahren. Wenn sich eine Partei einer Entscheidung des NAD nicht beugt, wird der Fall an die FTC verwiesen. Mitarbeiter der FTC untersuchen die inkriminierte Werbemaßnahme vorrangig um festzustellen, ob sie gegen den FTC Act verstößt: oft gelingt es damit, dem inkriminierten Verhalten ein Ende zu setzen oder die Partei zur Rückkehr zum NARB-Verfahren zu bewegen.

Ebenso vorrangig wird die FTC Fälle von Missachtung der Grundsätze des sicheren Hafens behandeln, die Mitgliedstaaten der EU an sie verweisen. Was Fälle anbetrifft, die US-amerikanische Selbstregulierungsorgane an uns verweisen, so werden unsere Mitarbeiter alle Informationen würdigen, die Aufschluss darüber geben können, ob das inkriminierte Verhalten gegen Abschnitt 5 des FTC Act verstößt. Diese Verpflichtung ist außerdem in den Grundsätzen des sicheren Hafens festgeschrieben, und zwar in der häufig gestellten Frage Nr. 11 (FAQ 11) über das Durchsetzungsprinzip.

GeoCities: der erste Online-Fall der FTC zum Datenschutz

Der erste Fall der Federal Trade Commission, der den Datenschutz im Internet betraf, GeoCities, stützte sich auf die Befugnisse der FTC gemäß Abschnitt 5 ([6]). In diesem Fall brachte die FTC vor, GeoCities habe sowohl Erwachsene als auch Kinder falsch darüber informiert, wie ihre personenbezogenen Daten verwendet würden. In der Beschwerde der Federal Trade Commission heißt es, GeoCities habe den Eindruck erweckt, bestimmte auf ihrer Web-Site erhobene personenbezogene Daten würden nur zu internen Zwecken verwendet oder dazu, Verbrauchern bestimmte, von diesen angeforderte Werbeangebote, Produkte und Dienstleistungen nahe zu bringen, und bestimmte Zusatzinformationen freiwilliger Art würden nur mit Zustimmung der Verbraucher an Dritte weitergegeben. In Wirklichkeit wurden diese Informationen aber doch an Dritte weitergegeben; diese benutzten die Informationen, um bei Mitgliedern für Zwecke zu werben, denen die Mitglieder nicht zugestimmt hatten. In der Beschwerde heißt es ferner, GeoCities habe irreführende Praktiken angewandt, um Daten bei Kindern zu erheben. Der Beschwerde der FTC zufolge habe GeoCities dargestellt, dass das Unternehmen eine Kinderecke auf seiner Web-Site betreiben und dass die dort erhobenen Daten von dem Unternehmen selbst gepflegt würden. In Wirklichkeit wurde dieser Bereich auf der GeoCities-Web-Site jedoch von Dritten betrieben, die die Daten erhoben und pflegten.

Die Beilegungsvereinbarung verbietet GeoCities, den Zweck falsch darzustellen, zu dem das Unternehmen die personenbezogenen Daten von oder über Verbraucher, darunter auch Kinder, erhebt oder verwendet. Die Verfügung verlangt von dem Unternehmen, einen klaren und deutlich sichtbaren Datenschutzhinweis auf seiner Web-Site anzubringen, der Verbraucher darüber informiert, welche Daten zu welchem Zweck erhoben werden, an wen sie weitergegeben werden und wie der Verbraucher auf die Daten zugreifen und sie entfernen kann. Um die elterliche Kontrolle zu gewährleisten verlangt die Beilegungsvereinbarung darüber hinaus, dass GeoCities die Zustimmung der Eltern einholt, bevor das Unternehmen personenbezogene Daten von Kindern unter 13 Jahren erhebt. Die Verfügung verlangt, dass GeoCities seine Mitglieder benachrichtigt und ihnen die Möglichkeit einräumt, ihre Daten aus den Datenbanken von GeoCities und Dritten entfernen zu lassen. Die Beilegungsvereinbarung verlangt von GeoCities insbesondere, die Eltern von Kindern unter 13 Jahren zu benachrichtigen und deren Informationen zu löschen, sofern ein Elternteil der weiteren Speicherung und Nutzung nicht ausdrücklich zustimmt. Schließlich ist GeoCities auch verpflichtet, Dritte, an die das Unternehmen Daten weitergegeben hat, aufzufordern, diese Daten ebenfalls zu löschen ([7]).

ReverseAuction.com

Im Januar 2000 hatte die FTC einer Beschwerde über ReverseAuction.com stattgegeben und eine Konsensvereinbarung mit diesem Unternehmen getroffen. ReverseAuction ist eine Site für Online-Auktionen, die beschuldigt wurde, sich über die Site eines Mitbewerbers (eBay.com) Zugang zu personenbezogenen Daten von Verbrauchern verschafft zu haben. Anschließend habe das Unternehmen unaufgefordert irreführende E-Mail-Nachrichten an Verbraucher geschickt ([8]).

([5]) Die FTC hat kürzlich beim Federal District Court gegen Toysmart.com, eine Firma, die ein TRUSTe-Siegel hat, eine Unterlassungs- und Feststellungsklage erhoben, um damit den Verkauf vertraulicher personenbezogener Kundendaten zu verhindern, die im Widerspruch zur eigenen Datenschutzpolitik auf der Website der Firma erhoben wurden. Die FTC war von TRUSTe direkt von der möglichen Rechtsverletzung in Kenntnis gesetzt worden. FTC v. Toysmart.com, LLC, Civil Action No. 00-11341-RGS (D.Ma.) (Klage eingereicht am 11. Juli 2000) (verfügbar unter folgender Adresse: www.ftc.gov/opa/2000/07/toysmart.htm).

([6]) GeoCities, Docket No. C-3849 (Final Order 12. Februar 1999) (auf www.ftc.gov/os/1999/9902/9823015d%26o.htm).

([7]) Die FTC legte danach noch eine weitere Angelegenheit bei, in der es ebenfalls um die Online-Erhebung personenbezogener Daten von Kindern ging. Liberty Financial Companies Inc. betrieb die Website Young Investor, die sich an Kinder und Heranwachsende richtete und auf Themen über Geld und Investitionen abstellte. Die FTC brachte vor, die Site habe fälschlicherweise dargestellt, dass Daten, die von Kindern bei einer Umfrage erhoben wurden, anonym blieben und den Teilnehmern ein E-Mail-Mitteilungsblatt und Gewinne zugeschickt würden. In Wirklichkeit wurden die personenbezogenen Daten über das Kind und die finanziellen Verhältnisse der Familie identifizierbar aufbewahrt, und es wurden auch kein Mitteilungsblatt und keine Gewinne verschickt. Die Konsensvereinbarung verbietet künftig derartige Fehldarstellungen und verpflichtet Liberty Financial, einen Datenschutzhinweis auf den Web-Sites für Kinder anzubringen sowie die nachweisliche Zustimmung der Eltern einzuholen, bevor das Unternehmen personenbezogene Daten von Kindern erhebt. Liberty Financial Cos., Docket No. C-3891 (Final Order 12. August 1999) (auf www.ftc.gov/opa/1999/9905/younginvestor.htm).

([8]) Siehe ReverseAuction.com, Inc., Civil Action No. 000032 (D.D.C.) (vom 6. Januar 2000) (Pressemitteilung und Schriftsatz unter www.ftc.gov/opa/2000/01/reverse4.htm).

Unsere Beschwerde stellte ab auf einen Verstoß von ReverseAuction gegen Abschnitt 5 FTC Act wegen der Beschaffung personenbezogener Daten, darunter die E-Mail-Adressen von eBay-Benutzern und ihre persönlichen Benutzerkennungen („user IDs"), sowie wegen des Versands der irreführenden E-Mail-Nachrichten.

Wie in der Beschwerde ausgeführt, registrierte sich ReverseAuction vor der Informationsbeschaffung zuerst als eBay-Benutzer und verpflichtete sich, die Nutzungsvereinbarung und die Datenschutzpolitik von eBay zu respektieren. Vereinbarung und Politik schützen eBay-Benutzer vor der Erhebung und Nutzung personenbezogener Daten zu unzulässigen Zwecken wie z. B. dem unaufgeforderten Versand von E-Mail-Nachrichten zu Werbezwecken. Daher stellte unsere Beschwerde erstens darauf ab, dass ReverseAuction fälschlicherweise dargestellt habe, die Nutzungsvereinbarung und die Datenschutzpolitik von eBay zu respektieren, was eine irreführende Praktik nach Abschnitt 5 darstelle. Ersatzweise habe die Nutzung der Daten durch ReverseAuction zum unaufgeforderten Versand von E-Mail-Nachrichten zu Werbezwecken die Nutzungsvereinbarung und die Datenschutzpolitik verletzt, was eine unlautere Handelspraktik gemäß Abschnitt 5 darstelle.

Zweitens stellte die Beschwerde darauf ab, dass die E-Mail-Nachricht an die Verbraucher eine irreführende Betreff-Zeile enthalten habe, in der ihnen mitgeteilt worden sei, dass die Gültigkeit ihrer eBay-Benutzerkennung demnächst ablaufe. In den E-Mail-Nachrichten sei fälschlich dargestellt worden, dass eBay die Firma ReverseAuction direkt oder indirekt mit personenbezogenen Daten von eBay-Benutzern beliefert habe bzw. auf sonstige Weise an der unaufgeforderten Verbreitung von E-Mail beteiligt gewesen sei.

Die von FTC erreichte Beilegung der Auseinandersetzung verbietet ReverseAuction weitere Verstöße dieser Art. Sie verpflichtet ReverseAuction außerdem dazu, die Verbraucher zu benachrichtigen, die sich als Reaktion auf die E-Mail von ReverseAuction bei ReverseAuction registriert haben oder noch registrieren werden. Die Benachrichtigung muss diese Verbraucher ferner darüber informieren, dass die Gültigkeit ihrer eBay-Benutzerkennung demnächst nicht abläuft und dass eBay weder von dem unaufgeforderten E-Mail-Versand von ReverseAuction wusste noch einem etwaigen Versand zugestimmt hat. Mit der Benachrichtigung muss den Verbrauchern ferner die Möglichkeit eingeräumt werden, ihre Registrierung bei ReverseAuction zu annullieren und ihre personenbezogenen Daten aus der Datenbank von ReverseAuction löschen zu lassen. Darüber hinaus verpflichtet die Verfügung die Firma ReverseAuction, die personenbezogenen Daten aller eBay-Mitglieder zu löschen und von deren Nutzung oder Weitergabe abzusehen, die die E-Mail von ReverseAuction zwar erhalten, sich aber nicht bei ReverseAuction registriert hatten. Schließlich verlangt die Vereinbarung getreu früherer Datenschutzverfügungen, die unsere Dienststelle erwirkt hat, von der Firma ReverseAuction, ihre Datenschutzpolitik auf ihrer Internet-Site zu veröffentlichen. Ferner verpflichtet die Vereinbarung die Firma, umfassende Aufzeichnungen zu führen, damit die FTC die Einhaltung überwachen kann.

Der Fall ReverseAuction veranschaulicht, dass die FTC ihre Möglichkeiten zur Durchsetzung konsequent nutzt, um die Bemühungen der Industrie zur Selbstregulierung beim Verbraucherdatenschutz im Online-Verkehr zu unterstützen. In diesem konkreten Fall wurde ein Verhalten direkt abgemahnt, das eine Datenschutzpolitik sowie eine diesbezügliche Nutzungsvereinbarung unterlaufen hatte und das Vertrauen der Verbraucher in Datenschutzmaßnahmen von Online-Unternehmen untergraben könnte. Da sich in diesem Fall ein Unternehmen unrechtmäßig Verbraucherdaten eines anderen Unternehmens angeeignet hat, die durch eine Datenschutzpolitik geschützt waren, kommt dem Fall unter Umständen eine besondere Bedeutung für Datenschutzbelange zu, die sich beim Austausch von Daten zwischen Unternehmen in unterschiedlichen Ländern ergeben.

Ungeachtet der Durchsetzungsmaßnahmen der FTC in den Fällen GeoCities, Liberty Financial Cos. und ReverseAuction sind die Befugnisse unserer Dienststelle in einigen Bereichen des Online-Datenschutzes stärker begrenzt. Wie bereits erwähnt, muss die Erhebung und Nutzung von personenbezogenen Daten ohne Zustimmung der Betroffenen als unlautere oder irreführende Praktik gelten, damit sie auf der Grundlage des FTC Act verfolgt werden kann. So wird der FTC Act wohl nicht wirksam, wenn eine Web-Site personenbezogene Daten von Verbrauchern erhebt, ohne den Erhebungszweck falsch darzustellen oder ohne die Informationen in einer Weise weiterzugeben, die den Verbrauchern erheblichen Schaden zufügen könnte. Es liegt möglicherweise auch gegenwärtig nicht in der Macht der FTC, auf breiter Basis zu verlangen, dass Einrichtungen, die Informationen über das Internet erheben, sich in der einen oder anderen Form eine Datenschutzpolitik verordnen [9]. Wie aber bereits erwähnt, wird der Verstoß eines Unternehmens gegen eine erklärte Datenschutzpolitik wahrscheinlich als irreführende Praktik geahndet.

---

[9] Aus diesem Grund erklärte die Federal Trade Commission vor dem Kongress, dass wohl weitere Rechtsvorschriften erforderlich sind, die allen kommerziellen, verbraucherorientierten US-amerikanischen Web-Sites bestimmte faire Informationspraktiken vorschreiben. „Consumer Privacy on the World Wide Web", vor dem Subcommittee on Telecommunications, Trade and Consumer Protection des House Committee on Commerce United States House of Representatives, 21. Juli 1998 (siehe www.ftc.gov/os/9807/privac98.htm). Die FTC sah vorläufig davon ab, derartige Vorschriften zu fordern, damit die Selbstregulierung zeigen kann, ob sie in der Lage ist, auf breiter Basis faire Informationspraktiken auf Web-Sites durchzusetzen. Im Bericht der Federal Trade Commission an den Kongress über den Online-Datenschutz („Privacy Online: A Report to Congress") vom Juni 1998 (siehe www.ftc.gov/reports/privacy3/toc.htm) empfahl die FTC Vorschriften, wonach kommerzielle Web-Sites das Einverständnis der Eltern einholen müssen, bevor sie personenbezogene Daten von Kindern unter 13 Jahren erheben. Siehe Fußnote 3 oben. Letztes Jahr kam der FTC-Bericht („Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress", Juli 1999; siehe www.ftc.gov/os/1999/9907/index.htm#13,) zu dem Schluss, dass die Selbstregulierung genügend Fortschritte erzielt habe und deshalb derzeit keine Gesetzgebungsmaßnahmen empfohlen würden.
Im Mai 2000 hat die FTC dem Kongress einen dritten Bericht vorgelegt „Privacy Online: Fair Information Practices in the Electronic Marketplace" (der Bericht ist unter folgender Adresse zu finden: www.ftc.gov/os/2000/05/index.htm#22). Darin werden die jüngste Erhebung der FTC über kommerzielle Websites und die Frage erörtert, inwieweit bei diesen Websites faire Informationspraktiken angewandt werden. In dem Bericht wird auch (von einer Mehrheit der FTC-Mitglieder) empfohlen, dass der Kongress ein Gesetz verabschiedet, das für verbraucherorientierte kommerzielle Websites einen grundlegenden Schutz der Privatsphäre vorschreibt.

Darüber hinaus gilt die Zuständigkeit der FTC in diesem Bereich nur für unlautere und irreführende Praktiken, die im Handel erfolgen oder die den Handel beeinträchtigen. Datenerhebung durch kommerzielle Waren- oder Dienstleistungsanbieter und die Erhebung und Nutzung von Daten zu kommerziellen Zwecken erfüllen vermutlich das „Handelskriterium". Andererseits gibt es viele Einzelpersonen oder Stellen, die möglicherweise Daten im Online-Verkehr erheben, ohne einen kommerziellen Zweck zu verfolgen, womit sie aus dem Zuständigkeitsbereich der Federal Trade Commission herausfallen dürften. Ein Beispiel für diese Einschränkung liefern „chat rooms", wenn sie von nicht kommerziell ausgerichteten Stellen betrieben werden, z. B. von einer karitativen Einrichtung.

Zu guter Letzt gibt es noch Fälle, die ganz oder teilweise von der Basiszuständigkeit der FTC für kommerzielle Praktiken gesetzlich ausgenommen sind, sodass die FTC keine umfassende Antwort auf die Datenschutzproblematik im Internet liefern kann. Ausnahmen gelten unter anderem für viele datenintensive Wirtschaftszweige wie z. B. Banken, Versicherungen und Luftfahrtgesellschaften. Wie Sie wissen, sind andere Einrichtungen auf Bundes- oder Staatsebene zuständig für diese Stellen, so z. B. die Bankinstitute des Bundes oder das Verkehrsministerium.

Wo die FTC zuständig ist, akzeptiert und verfolgt sie im Rahmen der Mittelverfügbarkeit Verbraucherbeschwerden, die per Post oder Telefon in ihrem Consumer Response Center („CRC") und neuerdings auch auf ihrer Web-Site eintreffen ([10]). Das CRC nimmt Beschwerden aller Verbraucher entgegen, auch solcher, die ihren Wohnsitz in einem Mitgliedstaat der Europäischen Union haben. Der FTC Act ermächtigt die Federal Trade Commission, die Unterlassung weiterer Verstöße gegen den FTC Act sowie Schadenersatz für geschädigte Verbraucher zu erwirken. Wir würden allerdings prüfen, ob das Unternehmen sich in typischer Weise unangemessen verhalten hat, da wir keine individuellen Verbraucherstreitigkeiten regeln. In der Vergangenheit hat die Federal Trade Commission sowohl Bürgern aus den Vereinigten Staaten als auch aus anderen Ländern beigestanden ([11]). Die FTC wird ihre Befugnisse in geeigneten Fällen weiter ausüben, um Bürgern in anderen Ländern, die durch irreführende Praktiken innerhalb ihres Zuständigkeitsbereichs geschädigt wurden, zu ihrem Recht zu verhelfen.

Beschäftigungsdaten

In Ihrem jüngsten Schreiben baten Sie um weitere Erläuterungen zur Zuständigkeit der FTC im Zusammenhang mit Beschäftigungsdaten. Zuerst stellten Sie die Frage, ob die FTC gemäß Abschnitt 5 gegen ein Unternehmen vorgehen könne, das zwar nach eigenen Angaben die US-Grundsätze des sicheren Hafens respektiere, aber beschäftigungsbezogene Daten in einer Weise übermittele oder nutze, die gegen diese Grundsätze verstoße. Wir möchten Ihnen versichern, dass wir die rechtlichen Möglichkeiten der FTC genau geprüft haben, neben den einschlägigen Vorschriften auch sonstige Unterlagen sowie die einschlägige Rechtsprechung; danach sind wir zu dem Schluss gelangt, dass die FTC bei Beschäftigungsdaten dieselbe Zuständigkeit besitzt wie in allen anderen Fällen gemäß Abschnitt 5 des FTC Act ([12]). Dies bedeutet folgendes: Wenn ein Fall unseren Kriterien (Unsauberkeit oder Irreführung) für eine Durchsetzungsmaßnahme zum Datenschutz entspricht, dann können wir auch bei Beschäftigungsdaten tätig werden.

Wir würden auch gerne der Ansicht widersprechen, die Möglichkeiten der FTC bei Durchsetzungsmaßnahmen zum Datenschutz beschränkten sich auf Situationen, in denen ein Unternehmen einzelne Verbraucher in die Irre geführt hätte. Die kürzliche Maßnahme der FTC im Fall ReverseAuction ([13]) belegt, dass die FTC den Datenschutz auch in Situationen durchsetzt, in denen es um die Übermittlung von Daten zwischen Unternehmen geht, falls ein Unternehmen gegenüber einem anderen Unternehmen ungesetzlich handelt und dadurch Verbraucher und Unternehmen potentiell schädigt. Wir gehen davon aus, dass sich die Frage der Beschäftigungsdaten am ehesten in Konstellation stellt, da Beschäftigungsdaten über europäische Staatsbürger von europäischen an amerikanische Unternehmen übermittelt werden, die sich verpflichtet haben, die Grundsätze des sicheren Hafens zu respektieren.

Wir möchten jedoch auf eine andere Konstellation hinweisen, unter der ein Tätigwerden der FTC umgangen werden könnte. Dies könnte vorkommen, falls die Angelegenheit bereits Gegenstand eines traditionellen Streitbeilegungsverfahrens innerhalb einer arbeitsrechtlichen Auseinandersetzung wäre, in den meisten Fällen wohl ein Beschwerde- oder Schiedsverfahren oder eine Beschwerde wegen unlauterer Beschäftigungspraktik beim National Labor Relations Board.

([10]) Siehe http://www.ftc.gov/ftc/complaint.htm (Online-Beschwerdeformular der Federal Trade Commission).

([11]) Beispiel: Ein Fall jüngeren Datums betraf ein Internet-Pyramidensystem; dort erwirkte die FTC Rückzahlungen für 15 622 Kunden in einer Gesamthöhe von etwa 5,5 Mio. USD. Die Verbraucher hatten ihren Wohnsitz in den Vereinigten Staaten bzw. in einem von 70 ausländischen Staaten. Siehe www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

([12]) Abgesehen von den ausdrücklichen Ausnahmen in den Rechtsvorschriften über die Befugnisse der FTC deckt sich die Zuständigkeit der FTC gemäß dem FTC Act bei Praktiken, die im Handel erfolgen oder die den Handel beeinträchtigen, mit den verfassungsrechtlichen Befugnissen des Kongresses gemäß der Commerce Clause (United States v. American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1975)). Danach umfasst die Zuständigkeit der FTC auch beschäftigungsbezogene Praktiken in Unternehmen und in der Industrie im internationalen Handel.

([13]) Siehe „Online Auction Site Settles FTC Privacy Charges", Pressemitteilung der FTC (6. Januar 2000) auf http://www.ftc.gov/opa/2000/01/reverse4.htm.

Dies könnte vorkommen, wenn z. B. ein Arbeitgeber in einer Tarifauseinandersetzung um die Nutzung personenbezogener Daten eine Zusage gemacht hätte und ein Arbeitnehmer oder eine Gewerkschaft den Arbeitgeber des Bruchs der Vereinbarung beschuldigen würde. Die FTC würde einem derartigen Verfahren vermutlich nicht vorgreifen ([14]).

Zuständigkeit bei Programmen mit Vertrauenssiegel

Zweitens fragten Sie, ob die FTC zuständig sei für Vertrauenssiegel-Programme, die Streitbeilegungsinstrumente in den Vereinigten Staaten anböten und ihre Rolle bei der Durchsetzung der Grundsätze des sicheren Hafens und bei der Behandlung von Beschwerden von Einzelpersonen falsch darstellen würden, auch wenn derartige Stellen aus technischer Sicht nicht gewinnorientiert seien. Bei der Bestimmung, ob wir für Stellen zuständig sind, die sich als nicht gewinnorientiert bezeichnen, analysiert die FTC sehr genau, ob diese Stellen Gewinne zwar nicht für sich selbst, wohl aber für ihre Mitglieder anstreben. Die FTC hat mit Erfolg ihre Zuständigkeit für derartige Stellen behauptet. Noch am 24. Mai 1999 bekräftigte der Oberste Gerichtshof der Vereinigten Staaten im Fall California Dental Association gegen Federal Trade Commission einstimmig, dass die FTC für den Fall eines freiwilligen, nicht gewinnorientierten Zusammenschlusses lokaler Zahnärzteverbände zuständig ist, der eine Kartellangelegenheit betraf. Der Gerichtshof kam zu folgendem Schluss:

> Der FTC Act ist darauf bedacht, nicht nur Stellen einzubeziehen, die organisatorisch auf die Erwirtschaftung von Gewinnen ausgerichtet sind (15 U.S. C. § 44), sondern auch Stellen, deren Tätigkeit darauf ausgerichtet ist, ihren Mitgliedern Gewinne zukommen zu lassen. … Man kann in der Tat kaum annehmen, dass der Kongress den Begriff einer versteckt unterstützenden Organisation derart restriktiv auslegen und damit die Möglichkeit zur Umgehung der Zuständigkeit schaffen wollte, wo doch der FTC Act diese Zuständigkeit offensichtlich gerade sichern soll.

Kurz gesagt: um die Zuständigkeit für eine bestimmte, nicht gewinnorientierte Stelle, die ein Vertrauenssiegel-Pogramm durchführt, zu klären, muss zunächst faktisch gewürdigt werden, in welchem Maß die Stelle ihren gewinnorientierten Mitgliedern wirtschaftliche Vorteile verschafft. Wenn eine solche Stelle ihr Vertrauenssiegel-Programm in einer Weise betreibt, die ihren Mitgliedern einen wirtschaftlichen Vorteil verschafft, dann wird die FTC wohl ihre Zuständigkeit geltend machen. Daneben ist die FTC wahrscheinlich auch für betrügerische Vertrauenssiegel-Programme zuständig, die sich fälschlicherweise als nicht gewinnorientiert ausgeben.

Schutz der Privatsphäre in der Offline-Welt

Drittens weisen Sie darauf hin, dass sich unser vorausgegangener Schriftwechsel auf den Datenschutz in der Online-Welt konzentriert habe. Obwohl die FTC ihr Hauptaugenmerk auf den Online-Schutz richtet, da ihm eine kritische Funktion bei der Entwicklung des elektronischen Handels zukommt, darf nicht übersehen werden, dass der FTC Act bis ins Jahr 1914 zurückreicht und gleichermaßen für die Offline-Welt gilt. Wir können somit Offline-Unternehmen belangen, die unlautere oder irreführende Handelspraktiken im Zusammenhang mit dem Verbraucherdatenschutz anwenden ([15]). In der Tat wurde in einem von der FTC eingebrachten Fall (FTC gegen TouchTone Information Inc.) ein Informationsvermittler beschuldigt, sich unrechtmäßig personenbezogene Finanzdaten von Verbrauchern beschafft und diese veräußert zu haben. Die FTC stellte darauf ab, TouchTone habe sich unter Vorspiegelung falscher Tatsachen („pretexting") Zugang zu den Verbraucherdaten verschafft. Pretexting ist ein Kunstbegriff, der im privaten Recherchegeschäft für Praktiken geprägt wurde, bei denen unter falschen Vorgaben personenbezogene Daten eingeholt werden, vor allem per Telefon. Der Fall, der am 21. April 1999 beim Bundesgericht von Colorado eingereicht wurde, zielt auf eine einstweilige Verfügung und eine Entschädigung für alle unrechtmäßig erzielten Gewinne.

Diese Erfahrung mit der Durchsetzung von Rechtsvorschriften und jüngste Bedenken hinsichtlich der Zusammenfassung von Online- und Offline-Datenbanken wie auch die Tatsache, dass sich die Grenzen zwischen Online- und Offline-Handel verwischen und dass ein Großteil der personenbezogenen Informationen offline erfasst und verarbeitet wird, machen deutlich, dass der Frage des Schutzes der Privatsphäre im Offline-Bereich große Aufmerksamkeit gewidmet werden muss.

Überschneidungen bei der Zuständigkeit

Abschließend stellten Sie die Frage nach der Vereinbarkeit der FTC-Zuständigkeit mit der Zuständigkeit anderer Durchsetzungsgremien, vor allem in Fällen, in denen sich die Zuständigkeiten möglicherweise überlappen. Wir haben inten-

([14]) Die Entscheidung darüber, ob ein Verhalten als unlautere Beschäftigungspraktik oder als Verstoß gegen eine tarifvertragliche Vereinbarung gilt, ist technischer Art; sie bleibt in der Regel den dafür zuständigen Arbeitsgerichten vorbehalten, die die Beschwerden entgegennehmen, also Schiedsstellen und dem NLRB.

([15]) Wie Sie bereits aus früheren Erörterungen wissen, gibt der Fair Credit Reporting Act der FTC die Befugnisse zum Schutz der Finanzdaten von Verbrauchern im Anwendungsbereich des Act, und die FTC veröffentlichte vor kurzem einen Beschluss zu dieser Frage. Siehe In the Matter of Trans Union, Docket No. 9255 (1. März 2000) (Pressemitteilung und Stellungnahme unter www.ftc.gov/os/2000/03/index.htm#1).

sive Arbeitsbeziehungen zu vielen anderen Durchsetzungsgremien geknüpft, darunter auch zu den Bankinstituten des Bundes und der Generalstaatsanwaltschaft der Bundesstaaten. Wir koordinieren sehr häufig unsere Nachforschungen, um unsere Ressourcen in Fällen überlappender Zuständigkeit zu maximieren. Wir verweisen zu prüfende Angelegenheiten ferner häufig an die zuständigen Stellen auf Bundes- oder Staatsebene.

Ich hoffe, dass Ihnen diese Übersicht weiterhilft. Bitte lassen Sie mich wissen, falls Sie weitere Informationen benötigen.

Mit freundlichen Grüßen

Robert Pitofsky

ANHANG VI

John Mogg
Direktor, GD XV
Europäische Kommission
Büro C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Brüssel

Sehr geehrter Herr Generaldirektor,

ich sende Ihnen diesen Brief auf Bitten des US-Handelsministeriums, um die Rolle zu erläutern, die das Verkehrsministerium beim Schutz der Privatsphäre von Verbrauchern spielt, wenn diese den Luftverkehrsgesellschaften Informationen überlassen.

Das Verkehrsministerium befürwortet die Selbstregulierung als unaufdringlichstes und wirksamstes Instrument zur Geheimhaltung personenbezogener Daten, die Verbraucher den Luftverkehrsgesellschaften überlassen. Das Ministerium unterstützt daher die Schaffung eines „sicheren Hafens", denn damit könnten die Luftverkehrsgesellschaften den Anforderungen der Datenschutzrichtlinie der Europäischen Union im Hinblick auf den Transfer in Drittstaaten entsprechen. Das Ministerium räumt jedoch ein, dass Selbstregulierung nur funktionieren kann, wenn die Fluggesellschaften, die die Grundsätze des sicheren Hafens annehmen, sich auch an diese Grundsätze halten. Dazu sollte die Selbstregulierung aber auf dem Rechtsweg durchsetzbar sein. Aus diesem Grund wird das Ministerium von seinen rechtlichen Befugnissen zum Verbraucherschutz Gebrauch machen und sicherstellen, dass die Luftfahrtgesellschaften ihrer Datenschutzverpflichtung gegenüber der Öffentlichkeit nachkommen. Es wird Fällen von Nichteinhaltung der Vorschriften nachgehen, die von Selbstregulierungsorganen und anderen Stellen, darunter auch die Mitgliedstaaten der Europäischen Union, an das Ministerium verwiesen werden.

Die Durchsetzungsbefugnisse des Ministeriums auf diesem Gebiet ergeben sich aus 49 U.S.C. 41712. Diese Vorschrift verbietet Luftfahrtgesellschaften, unlautere und irreführende Praktiken beim Verkauf von Flugtickets anzuwenden, die den Verbraucher schädigen bzw. schädigen könnten. Abschnitt 41712 ist nach dem Vorbild von Abschnitt 5 Federal Trade Commission Act (15 U.S.C. 45) aufgebaut. Fluggesellschaften wurden von der Federal Trade Commission gemäß 15 U.S.C. 45(a)(2) allerdings von den Bestimmungen in Abschnitt 5 ausgenommen.

Meine Dienststelle untersucht und verfolgt Fälle, die 49 U.S.C. 41712 betreffen. (Siehe z. B. folgende DOT Orders: 99-11-5 vom 9. November 1999; 99-8-23 vom 26. August 1999; 99-6-1 vom 1. Juni 1999; 98-6-24 vom 22. Juni 1998; 98-6-21 vom 19. Juni 1998; 98-5-31 vom 22. Mai 1998 und 97-12-23 vom 18. Dezember 1997.) Wir leiten aufgrund eigener Untersuchungen Verfahren ein und bearbeiten formelle und informelle Beschwerden von Privatpersonen, Reisebüros, Luftfahrtgesellschaften sowie US-amerikanischen und ausländischen staatlichen Stellen.

Ich möchte darauf hinweisen, dass der Verstoß einer Luftfahrtgesellschaft gegen die Geheimhaltung personenbezogener Daten von Passagieren nicht per se eine Verletzung von Abschnitt 41712 darstellt. Sobald aber eine Luftfahrtgesellschaft sich öffentlich und formell zu den Grundsätzen des sicheren Hafens und zum Schutz der bereitgestellten Verbraucherinformationen bekennt, kann das Ministerium von den rechtlichen Befugnissen gemäß Abschnitt 41712 Gebrauch machen und die Einhaltung dieser Grundsätze sicherstellen. Gibt also ein Passagier Informationen an eine Luftfahrtgesellschaft, die sich zur Einhaltung der Grundsätze des sicheren Hafens verpflichtet hat, dann würde ein Verstoß gegen diese Grundsätze dem Verbraucher wahrscheinlich zum Schaden gereichen und eine Verletzung der Bestimmungen des Abschnitts 41712 darstellen. Meine Dienststelle würde der Untersuchung und Verfolgung aller entsprechenden Fälle hohe Priorität einräumen. Wir werden darüber hinaus das Handelsministerium über die Untersuchungsergebnisse in diesen Fällen unterrichten.

Eine Verletzung der Bestimmungen des Abschnitts 41712 kann Unterlassungsanordnungen nach sich ziehen; der Verstoß gegen diese Anordnungen kann zivilrechtlich verfolgt werden. Obwohl wir nicht das Recht haben, beschwerdeführenden Privatpersonen Schadenersatz oder finanzielle Entschädigungen anzuerkennen, dürfen wir doch Vereinbarungen genehmigen, die sich aus Untersuchungen und vom Ministerium eingebrachten Fällen ergeben und dem Verbraucher als Abgeltung oder als Ausgleich für andernfalls zu verhängende Geldstrafen einen geldwerten Vorteil verschaffen. Wir haben dies in der Vergangenheit so gehandhabt, und wir können und werden dies auch im Zusammenhang mit den Grundsätzen des sicheren Hafens so handhaben, falls die Umstände dies erfordern. Sollte eine US-Luftfahrtgesellschaft die Bestimmungen des Abschnitts 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. (Siehe DOT Orders 93-6-34 vom 23. Juni 1993 sowie 93-6-11 vom 9. Juni 1993. Obwohl sich dieses Verfahren nicht auf

Abschnitt 41712 stützte, führte es zum Widerruf der Betriebsgenehmigung für eine Luftfahrtgesellschaft wegen völliger Missachtung der Vorschriften des Federal Aviation Act, eines bilateralen Abkommens sowie der Vorschriften des Ministeriums.)

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

Mit freundlichen Grüßen

Samuel Podberesky

Assistant General Counsel for
Aviation Enforcement and Proceeding

ANHANG VII

Staatliche Einrichtungen in den Vereinigten Staaten im Sinne von Artikel 1 Absatz 2 Buchstabe b), die berechtigt sind, im Fall der Nichtbeachtung der entsprechend den FAQ umgesetzten Grundsätze Beschwerden zu prüfen und Abhilfe bei unlauteren und irreführenden Praktiken sowie Schadenersatz für Privatpersonen zu erwirken, und zwar ungeachtet des Landes, in dem sie ihren Wohnsitz haben, oder ihrer Nationalität, sind:

1. die Federal Trade Commission und

2. das US-Verkehrsministerium.

Die Federal Trade Commission wird auf der Grundlage von Section 5 des Federal Trade Commission Act tätig. Die Zuständigkeit der Federal Trade Commission nach Abschnitt 5 für unlautere oder irreführende Handlungen ist ausgeschlossen in Bezug auf: Banken, Spar-, Darlehens- und Kreditgenossenschaften, Telekommunikationsunternehmen, bundesstaatübergreifend tätige Transportunternehmen, Luftverkehrsgesellschaften, Verlader und Lagerbetriebe. Die Versicherungswirtschaft ist in der Liste der Ausnahmen in Abschnitt 5 zwar nicht ausdrücklich genannt, aber das entsprechende Gesetz, der McCarran-Ferguson Act [1], überlässt die Regulierung des Versicherungsgeschäfts im Allgemeinen den einzelnen Bundesstaaten. Die Bestimmungen des FTC Act gelten jedoch für die Versicherungswirtschaft insoweit, als das Versicherungsgeschäft nicht durch das Recht von Bundesstaaten geregelt ist. Ebenso hat die FTC weiterhin die Befugnis, im Fall unlauterer oder irreführender Praktiken von Versicherungsgesellschaften tätig zu werden, wenn diese andere Geschäfte als Versicherungsgeschäfte tätigen.

Das US-Verkehrsministerium wird auf der Grundlage von Title 49 United States Code Section 41712 tätig. Das US-Verkehrsministerium leitet Verfahren aufgrund eigener Ermittlungen sowie aufgrund förmlicher und formloser Beschwerden von Einzelpersonen, Reisebüros, Fluggesellschaften und staatlichen US- und ausländischen Einrichtungen ein.

[1] 15 U.S.C. § 1011 et seq.