

Das Safe-Harbor Modell

Datenschutzbestimmungen in der Relation EU-USA

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Medizinische Informatik

eingereicht von

Markus Wagner

Matrikelnummer 0527471

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer: Ass.-Prof. Mag. et Dr. iur. Markus Haslinger

Wien, 11.08.2011

(Markus Wagner)

(Dr. Markus Haslinger)

ERKLÄRUNG

Markus Wagner
7535 Güttenbach 368

„Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.“

Wien, 11.08.2011

(Markus Wagner)

KURZFASSUNG

Im Zeitalter des Internet, vor allem seit dem Aufkommen der Web 2.0 Technologien, werden personenbezogene Daten sehr leichtfertig preisgegeben und rasant an Dritte übertragen. Dadurch können Dienstbetreiber relativ einfach Personendaten sammeln und austauschen, wodurch über Personen mehr Informationen akquiriert werden können, als von diesen eigentlich gewollt.

Um Konsumenten zu schützen, haben das Europäische Parlament und der Rat bereits 1995 die Richtlinie 95/46/EG erlassen, welche unter anderem den Transfer personenbezogener Daten in Drittstaaten verbietet, wenn diese kein angemessenes Schutzniveau bieten. Die Datenschutzbestimmungen der Vereinigten Staaten von Amerika werden von der Europäischen Kommission als unsicher eingestuft, daher dürften grundsätzlich keine personenbezogenen Daten aus der EU in die USA übermittelt werden. Um eine folgenschwere Datenblockade zu verhindern, wurde im Jahr 2000 mit der Kommissionsentscheidung 2000/520/EG das Safe-Harbor Modell kreiert.

Safe-Harbor gestattet den Transfer personenbezogener Daten an Unternehmen in den USA, die sich den Safe-Harbor Grundsätzen unterworfen und sich selbst zertifiziert haben. Das Konzept basiert größtenteils auf Selbstkontrolle und sieht keine wirkungsvollen Überprüfungsmechanismen vor.

Das Modell ist nun mehr als 10 Jahre in Kraft und es muss eine erschütternde Bilanz gezogen werden: Der Großteil der Unternehmen hat sich selbst als Safe-Harbor-Teilnehmer zertifiziert, ohne jedoch die vorgeschriebenen Richtlinien einzuhalten. Da Datenschutzsünder de facto nicht mit Konsequenzen zu rechnen haben, stellt das Safe-Harbor Modell einen Freibrief für willkürlichen Umgang mit importierten personenbezogenen Daten dar. Die Ursache für diese Entwicklung liegt in der äußerst unzureichenden Realisierung des Durchsetzungsgrundsatzes, der jedoch in der Kommissionsentscheidung festgeschrieben ist. Aus diesem Grund ist eine Änderung der aktuellen Bestimmungen unumgänglich.

Diese Arbeit befasst sich mit der Analyse der Safe-Harbor-Problematik und der Suche nach Verbesserungsansätzen. Mittels ausführlicher Literaturrecherche und Rechtsvergleich wird die aktuelle Rechtslage der supranationalen Gemeinschaft EU und der Vereinigten Staaten von Amerika im Bereich Datenschutz beleuchtet sowie die aktuelle Safe-Harbor-Lösung analysiert. Weiters werden die Anforderungen an eine funktionierende Selbstregulierung erörtert. Schließlich werden bestehende Lösungsansätze und deren Schwächen begutachtet und daraus Verbesserungsmöglichkeiten erarbeitet. Dabei wird vor allem aufgezeigt, dass andere Prüfmechanismen als die bloße Selbstkontrolle notwendig sind, um eine nachhaltige Änderung erwirken zu können.

ABSTRACT

Browsing the web is a matter course in our society and interactive webservices such as social networks are developing rapidly. These technologies provide simple and fast collection and exchange of personal data enabling the gathering of more information about people than originally intended to be disclosed by the users.

In 1995 the European Parliament and the Council enacted the directive 95/46/EC to protect users rights in respect of personal data. This directive includes an article prohibiting transfers of personal data in countries which do not provide for adequate data protection laws. According to the European Commission the legislation of the US does not ensure appropriate data privacy, so transfers of personal data into the USA would be forbidden. To prevent the economic damage of such a ban the US-EU-Safe-Harbor framework was implemented in 2000.

This framework allows US companies to import personal data of european citizens under certain conditions. The importing company must fulfil the Safe-Harbor principles and perform the official self-certification process at the DOC. The frameworks enforcement is based on self-monitoring and does not include effective test-procedures.

This legal framework is active for ten years by now, but the enforcement is very unsatisfactory. Most companies have completed the self-certification process without observing the mandatory policies. Personal data can be abused easily, because of lack of meaningful penalties. This ominous development is a result of the inefficient implementation of the enforcement principle. There is a need for a widespread improvement of the Safe-Habor framework.

This thesis is analysing the issue of Safe-Harbor and developing approaches for improvement. Firstly, the basics of privacy laws of the US are compared to those of the EU. After analysing the principles of the Safe-Habor framework the requirements for effective self-regulation are discussed. Finally, the faults and existing approaches are surveyed and new proposals are presented. One basic finding is that new control mechanisms and operative sanctions are needed to guarantee reasonable privacy protection.

DANKSAGUNG

Zuerst möchte ich mich bei Prof. Dr. Markus Haslinger für die Betreuung und Unterstützung bei meiner Diplomarbeit bedanken. Seine Idee war es auch, das Safe-Harbor Modell als Themenstellung heranzuziehen.

Weiters danke ich meiner Familie und meinen Freunden, die mir während meines Studiums mit Rat und Tat zur Seite gestanden sind und mich immer wieder motiviert haben.

Ein Besonderer Dank gilt meinen Eltern, die es mir immer ermöglicht haben, meine eigenen Interessen zu verfolgen. Ohne ihre Unterstützung wäre mein Studium nur schwer vorstellbar gewesen.

INHALTSVERZEICHNIS

1	EINLEITUNG	13
1.1	Motivation und Fragestellungen	13
1.2	Aufbau der Arbeit.....	14
1.3	Begriffsdefinitionen	15
2	DATENSCHUTZRECHT IN DER EU UND DEN USA.....	17
2.1	Datenschutz in der EU.....	17
2.1.1	Datenschutz als europäisches Grundrecht.....	17
2.1.2	Datenschutzrichtlinie 95/46/EG.....	17
2.1.2.1	Qualität der Daten	17
2.1.2.2	Zulässigkeit der Verarbeitung von Daten.....	18
2.1.2.3	Besondere Kategorien der Verarbeitung.....	18
2.1.2.4	Information der betroffenen Person	18
2.1.2.5	Auskunftsrecht der betroffenen Person	18
2.1.2.6	Widerspruchsrecht der betroffenen Person	19
2.1.2.7	Vertraulichkeit und Sicherheit der Verarbeitung.....	19
2.1.2.8	Meldepflicht.....	19
2.1.2.9	Kontrolle und Sanktionierung.....	19
2.1.2.10	Drittstaatenregelung	20
2.1.2.11	Ausnahmen	22
2.1.3	Durchsetzung am Beispiel Österreichs	22
2.1.3.1	Einführung und Vorgaben durch die EG-DSRL.....	22
2.1.3.2	Die Datenschutzkommission	23
2.1.3.3	Rechtsschutz durch ein Kontroll- und Ombudsmannverfahren	23
2.1.3.4	Rechtsschutz durch Beschwerde an die Datenschutzkommission	25
2.1.3.5	Zivilrechtlicher Schutz durch die ordentlichen Gerichte.....	25
2.1.3.6	Schematische Darstellung des Rechtsschutzes nach dem DSG.....	26
2.2	Datenschutz in den USA.....	27
2.2.1	Privacy protection.....	27
2.2.2	Gesetzlicher Datenschutz.....	27
2.2.2.1	Die Verfassung	27
2.2.2.2	Einfachgesetzliche Bestimmungen	28
2.2.2.3	Privacy Act	28
2.2.2.4	Privacy Protection Act	29
2.2.2.5	Right to Financial Privacy Act.....	29
2.2.2.6	Fair Credit Reporting Act.....	29
2.2.2.7	Drivers Privacy Protection Act.....	30

2.2.2.8 Telephone Consumer Protection Act	30
2.2.2.9 Childrens Online Privacy Protection Act	30
2.2.2.10 Security Breach Information Act in Kalifornien	31
2.2.3 Selbstregulierung	32
2.2.4 Fazit.....	33
3 DAS SAFE-HARBOR MODELL	34
3.1 Notwendigkeit eines Datenschutzmodells	34
3.1.1 Drittstaatenregelung der Richtlinie 95/46/EG	34
3.1.2 Folgen	34
3.2 Rechtliche Grundlage	35
3.3 Inhalt des Safe-Harbor Modells	35
3.4 Safe-Harbor-Grundsätze	36
3.4.1 Informationspflicht	36
3.4.2 Wahlmöglichkeit.....	36
3.4.3 Weitergabe	37
3.4.4 Sicherheit.....	37
3.4.5 Datenintegrität	37
3.4.6 Auskunftsrecht	38
3.4.7 Durchsetzung.....	38
3.5 Häufig gestellte Fragen „FAQ“	39
3.6 Teilnahme am Safe-Harbor Modell	39
3.7 Sanktionen.....	42
3.7.1 Verbraucherrechte bei Verstoß gegen das Modell	42
3.7.2 Sanktionen der Streitschlichtungsstellen und der FTC	42
3.8 Ausnahmen	43
3.9 Bedeutung der Safe-Harbor Lösung.....	44
3.9.1 Bedeutung in Europa	44
3.9.2 Bedeutung in den USA.....	45
3.10 Alternativen zu Safe-Harbor	45
3.10.1 Standard-Vertragsklauseln	45
3.10.2 Binding Corporate Rules	46
3.11 Kritik der Artikel 29 – Datenschutzgruppe	47
3.11.1 Übertragung von Personaldaten.....	47
3.11.2 Recht auf Löschung.....	48
3.11.3 Wahlmöglichkeit.....	48
3.11.4 Durchsetzung	48
3.11.5 Fazit.....	49

4	GRUNDLAGEN DER SELBSTREGULIERUNG.....	50
4.1	Anforderungen an die Regeldurchsetzung.....	50
4.1.1	Anreiz zur Regeleinhaltung	50
4.1.2	Regelkontrolle als Voraussetzung für eine effektive Regeldurchsetzung	51
4.1.3	Sanktionsmechanismen zur Durchsetzung der Regeln	52
4.1.3.1	Private Sanktionierung.....	52
4.1.3.2	Staatlich-private Sanktionierung.....	52
4.1.3.3	Staatliche Sanktionierung	53
4.2	Risiken der Selbstregulierung	53
4.2.1	Defizite bei der Durchsetzung	53
4.2.2	Mangelnder Rechtsschutz	54
4.2.3	Mittel zur Verhinderung der Gesetzgebung	54
4.3	Fazit.....	55
5	KRITIK AN DER PRAXIS VON SAFE-HARBOR	56
5.1	Studien zur praktischen Umsetzung von Safe-Harbor	56
5.1.1	Prüfung durch die EU 2002.....	56
5.1.2	Prüfung durch die EU 2004.....	57
5.1.2.1	Allgemeine Probleme	57
5.1.2.2	Beteiligte Behörden	57
5.1.2.3	Kontrollmechanismen	58
5.1.2.4	Datenschutzrichtlinien der teilnehmenden Unternehmen	58
5.1.2.5	Safe-Harbor Teilnehmerliste	59
5.1.3	Studie des Consulting-Unternehmens Galexia	60
5.1.3.1	Mängel in den Privacy Policies.....	62
5.1.3.2	Mängel bezüglich Streitschlichtungsstellen.....	62
5.1.3.3	Werbung mit ungültigen Zertifikaten	64
5.1.3.4	Mitgliedschaft in Bezug auf eingeschränkte Datenkategorien.....	65
5.1.4	Fazit.....	66
5.2	Beispiele für Verstöße zertifizierter Teilnehmer	66
5.2.1	Verstöße des „social networks“ Facebook	66
5.2.1.1	Verarbeitung personenbezogener Daten von Nicht-Teilnehmern.....	67
5.2.1.2	Zugriff auf fremde Kontakte	67
5.2.1.3	Zwangswise Veröffentlichung von Benutzerdaten	67
5.2.1.4	Weitergabe von Daten an Dritte.....	68
5.2.2	Verstöße des Suchmaschinenbetreibers Google	68
5.2.2.1	Google Buzz	68
5.2.2.2	Google Analytics	69
5.2.2.3	Speicherung von Suchanfragen	70

5.2.2.4	Speicherung von WLAN-Informationen	70
5.3	Ursachen für die Fehlentwicklung	71
5.3.1	Keine qualitative Eingangsdatenprüfung	71
5.3.2	Mangelnde Sanktionen	71
5.3.3	Mangelnde Motivation der US-Behörden	72
5.3.4	Großer Anreiz, gegen das Modell zu verstoßen	73
5.3.5	Mängel im Rahmen der Unabhängigen Schiedsverfahren	73
5.3.5.1	Fehlende verbindliche Vorschriften im Durchsetzungsgrundsatz.....	73
5.3.5.2	Streitschlichtung durch private Datenschutzprogramme	74
5.3.5.3	Streitschlichtung durch das Unternehmen selbst	75
5.3.5.4	Worst-Case Szenario	75
5.3.6	Mangelnder internationaler Einfluss der FTC	75
5.3.7	Eingeschränkte Verpflichtung zu Ermittlungen der FTC.....	75
5.3.8	Langwieriges Sanktionsverfahren	76
5.3.9	Mangelnde Transparenz und fehlendes Bewusstsein.....	76
5.4	Fazit.....	77
6	BISHER GETÄTIGTE MAßNAHMEN	78
6.1	Maßnahmen und Initiativen in den USA.....	78
6.1.1	Sanktionen durch die FTC wegen ungültiger Zertifizierung	78
6.1.1.1	Kritik.....	78
6.1.2	Erstmalige Sanktion der FTC wegen Verstößen gegen Selbstverpflichtung	79
6.1.2.1	Sanktionen gegen Google	79
6.1.2.2	Kritik.....	79
6.1.3	Neue Datenschutzgesetze in den USA	80
6.1.3.1	Kritik.....	81
6.2	Maßnahmen und Initiativen auf EU-Ebene.....	82
6.2.1	Parlamentarische Anfrage betreffend den „sicheren Hafen“	82
6.2.2	Konkrete Pläne der EK.....	83
6.3	Maßnahmen und Initiativen in Deutschland	84
6.3.1	Entscheidung durch den Düsseldorfer Kreis	84
6.3.1.1	Was ist der Düsseldorfer Kreis?	84
6.3.1.2	Die Entscheidung betreffend Safe-Harbor	84
6.3.1.3	Folgen der Entscheidung.....	84
6.3.1.4	Kritik.....	85
6.3.2	Kleine Anfrage von Abgeordneten an die Bundesregierung	85
6.4	Fazit.....	86
7	NOTWENDIGE MAßNAHMEN	87

7.1	Ziele und Herausforderungen	87
7.2	Ansatz 1: Gesetzliche Regelung	87
7.3	Ansatz 2: Strenge Kontrollen der Safe-Harbor-Teilnehmer	88
7.3.1	Neustart der Safe-Harbor Datenbank	88
7.3.2	Aufrechterhalten der validen Teilnehmerliste	89
7.3.2.1	Prüfung der Privacy Policy	89
7.3.2.2	Generierte Privacy Policies	89
7.3.3	Adaptierung der anlassunabhängigen Kontrollen	89
7.3.4	Sicherstellung angemessener Sanktionierung	90
7.3.5	Vorteile	90
7.3.5.1	Sichere Kontrolle	90
7.3.6	Schwierigkeiten	90
7.3.6.1	Hoher Verwaltungsaufwand	90
7.3.6.2	Mangelnde Motivation der US-amerikanischen Behörden	90
7.4	Ansatz 3: Verbesserung der Selbstregulierung	91
7.4.1	Selbstzertifizierung	91
7.4.2	Überprüfung der Privacy Policy	91
7.4.3	Handhabung von Beschwerden betroffener Personen	92
7.4.4	Blacklist	92
7.4.5	Vorteile	93
7.4.5.1	Niedriger Verwaltungsaufwand	93
7.4.5.2	Transparenz	93
7.4.5.3	Klarheit der Vorgangsweise für Betroffene	93
7.4.5.4	Geringere Abhängigkeit von US-amerikanischen Behörden	94
7.4.5.5	Verkürzung der Verfahren	94
7.4.5.6	Einfachere Einführung des Systems	94
7.4.6	Mögliche Zweifel	94
7.4.6.1	Geringes Interesse an Mitarbeit	94
7.4.6.2	Fehlende Qualifikation der Prüfer	95
7.5	Ansatz 4: Kombination der vorhergehenden Ansätze	95
7.6	Unbedingt notwendige Maßnahmen	95
7.6.1	Standardisierung der Sanktionen	96
7.6.2	Erweiterung des internationalen Einflusses der FTC	96
7.6.2.1	Kooperation mit Generalstaatsanwälten	96
7.6.2.2	Anpassung der Befugnisse der FTC	96
7.6.2.3	Verpflichtung der FTC zu Ermittlungen	96
7.6.3	Verpflichtende Kooperation mit europäischen Datenschutzbehörden	97
7.6.4	Einführung schnellerer Sanktionsmöglichkeiten	98

7.7 Fazit.....	98
8 ZUSAMMENFASSUNG UND AUSBLICK.....	99
8.1 Zusammenfassung	99
8.1.1 Was ist Safe-Harbor und funktioniert dieses Modell?.....	99
8.1.2 Welche Mängel gibt es?.....	99
8.1.3 Wieso funktioniert das System nicht?.....	99
8.1.4 Wie konnte ein derartiger Missbrauch ohne Konsequenzen stattfinden?	100
8.1.5 Wie kann die Situation nachhaltig verbessert werden?.....	100
8.2 Ausblick	101
8.3 Offene Frage	101
Abbildungsverzeichnis.....	102
Tabellenverzeichnis	102
Literaturverzeichnis	102
Rechtsquellenverzeichnis	103
Verzeichnis der Onlinequellen	104

ABKÜRZUNGSVERZEICHNIS

Abs	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art	Artikel
Aufl.	Auflage
BCR	Binding Corporate Rules
BSt.	Buchstabe
COPPA	Children's Online Privacy Protection Act
DOC	Department of Commerce (Handelsministerium der USA)
DSG	Datenschutzgesetz
DSK	Datenschutzkommission
Ebd.	Ebenda
EK	Europäische Kommission
EG-DSRL	Europäische Datenschutzrichtlinie (95/46/EG)
EU	Europäische Union
FAQ	Frequently Asked Questions: (häufig gestellte Fragen); bezieht sich auf Anhang II der Entscheidung 2000/520/EG
FCRA	Fair Credit Reporting Act
f, ff	und die folgende(n)
FTC	Federal Trade Commission (Handelsaufsichtsbehörde der USA)
ITA	International Trade Administration
NGO	Non-Governmental Organization (nichtstaatliche Organisation)
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
SBIA	Security Breach Information Act
SH-E	Safe-Harbor Entscheidung (2000/520/EG)
SSID	Service Set Identifier (Name eines drahtlosen Netzwerks)
u. a.	unter anderem
US	United States (Vereinigte Staaten)
USA	United States of America (Vereinigte Staaten von Amerika)
VfGH	Verfassungsgerichtshof
Vgl.	Vergleiche
VwGH	Verwaltungsgerichtshof
WP	Working Paper (Arbeitspapier)
z.B.	zum Beispiel

1 EINLEITUNG

1.1 Motivation und Fragestellungen

Im Zeitalter des Internet, vor allem seit dem Aufkommen der Web 2.0 Technologien, werden personenbezogene Daten besonders leichtfertig preisgegeben und rasant an Dritte übertragen. Dadurch können Dienstbetreiber relativ einfach Personendaten sammeln und austauschen, sodass über Personen deutlich mehr Informationen akquiriert werden können, als von den Betroffenen eigentlich gewollt. Man kann sich personenbezogene Daten wie ein Puzzle vorstellen, wobei jede Information einen kleinen Teil darstellt. Je mehr Informationen man sammelt und auswertet, umso detaillierter ist das Bild, das man über Gewohnheiten, Vorlieben und Interessen einer Person erstellen kann, wodurch sich eine Art „gläserner Mensch“ entwickeln lässt. Vor allem die immer populärer werdenden sozialen Netzwerke und Suchmaschinen stellen eine größere Bedrohung dar, als den meisten Anwendern, vor allem Kindern und Jugendlichen, bewusst ist. Der Schutz der Konsumenten ist von besonders hoher Bedeutung, da den Anwendern in vielen Bereichen die notwendige Transparenz fehlt, um Gefahren im Zusammenhang mit der Datenverarbeitung richtig einschätzen zu können.

Die größten Gefahren einer Verletzung des Datenschutzes sind der Verkauf schutzwürdiger Daten durch das Unternehmen, das die Daten gesammelt hat, die unerlaubte Weitergabe durch Mitarbeiter sowie der Diebstahl durch Netzangriffe.

Innerhalb der EU gibt es strenge Datenschutzrichtlinien, die personenbezogene Daten relativ gut vor Missbrauch schützen, doch aufgrund der fortschreitenden Globalisierung werden immer mehr Daten in Drittländern, vor allem in den USA, verarbeitet. Sobald Informationen das EU-Hoheitsgebiet verlassen, bietet EU-Recht allein keinen Schutz mehr und man ist entweder auf die Rechtsordnung des Drittlandes, auf Verträge mit dem Datenimporteure oder auf Lösungen wie Safe-Harbor angewiesen.

Nachdem die Europäische Datenschutzrichtlinie aus dem Jahr 1995 den Transfer personenbezogener Daten in unsichere Drittstaaten, darunter auch die USA, verboten hat, ist im Jahr 2000 das Safe-Harbor Modell in Kraft getreten, das den Schutz personenbezogener Daten beim Transfer aus der EU in die USA sicherstellen sollte. Diese Lösung erlaubt es US-Unternehmen, die sich verpflichten, gewisse Datenschutzgrundsätze einhalten, personenbezogene Daten aus der EU zu importieren. Seither wird mit ruhigem Gewissen Transfers personenbezogener Daten in die Vereinigten Staaten zugestimmt, da die Informationen dort vermeintlich in sicheren Händen sind und angeblich ausschließlich zweckgebunden verwendet werden.

Zehn Jahre später werden nun immer mehr Untersuchungsergebnisse veröffentlicht, die deutlich aufzeigen, wie wirkungslos dieses Regelwerk in Wirklichkeit ist. Unzählige Unternehmen, die angeblich „Safe-Harbor zertifiziert“ sind, haben längst kein gültiges Zertifikat mehr oder sind dem Handelsministerium als Teilnehmer gänzlich unbekannt. Viele Unternehmen nutzen das Safe-Harbor-Modell als Freibrief für Datenmissbrauch aus, indem sie europäische personenbezogene Daten sammeln und diese willkürlich an Dritte weitergeben oder verkaufen, ohne mit ernstzunehmenden rechtlichen Konsequenzen rechnen zu müssen.

Das Thema Safe-Harbor ist daher aktueller denn je und es ist rasches Handeln der Verantwortlichen in der Politik notwendig, damit ein zuverlässiger Schutz personenbezogener Daten der EU-Bürger/innen schnellstmöglich wiederhergestellt wird.

Diese Arbeit befasst sich mit folgenden Fragestellungen, die sich in Zusammenhang mit diesem Thema aufdrängen:

- Was ist das Safe-Harbor Modell und wie funktioniert es?
- Welche Mängel gibt es?
- Wieso funktioniert das System nicht?
- Warum kann schwerwiegender Missbrauch ohne Konsequenzen stattfinden?
- Wie kann man das Datenschutzmodell effektiv und nachhaltig verbessern?

Bei der Suche nach neuen Ansätzen ist die große Herausforderung, Finanzierbarkeit, Effizienz und die unterschiedlichen Rechtsansichten der EU und der USA „unter einen Hut“ zu bringen.

1.2 Aufbau der Arbeit

Zu Beginn werden die wichtigsten Begriffe erläutert, die im Laufe dieser Arbeit immer wieder auftreten und einer Erklärung bedürfen. Danach wird ein Überblick über notwendige Grundlagen gegeben. Dazu werden zuerst die Datenschutzansätze der EU und der USA grob durchleuchtet und die gravierenden Unterschiede aufgezeigt. Danach wird die Safe-Harbor-Lösung im Detail beschrieben. Diese Darstellung enthält die Datenschutzprinzipien und den Modus deren Umsetzung. Als letzter Teil der Grundlagen werden die Anforderungen an ein funktionierendes Selbstregulierungssystem beschrieben und die relevanten Aspekte in Bezug auf das Safe-Harbor Modell betrachtet.

Im Anschluss daran werden die Mängel des aktuellen Safe-Harbor-Regelwerks aufgezeigt und die Ursachen analysiert. Danach werden Verbesserungsansätze diskutiert, die von unterschiedlichen Behörden und Organisationen erarbeitet wurden. Abschließend werden neue Verbesserungsmöglichkeiten präsentiert und die wichtigsten Erkenntnisse dieser Arbeit zusammengefasst.

1.3 Begriffsdefinitionen

Personenbezogene Daten

Im Sinne der EG-DSRL des Europäischen Parlaments und des Rates bezeichnet der Ausdruck "personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"). Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.¹

Verarbeitung personenbezogener Daten

Unter "Verarbeitung personenbezogener Daten" versteht man jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.²

Für die Verarbeitung Verantwortlicher

Unter einem "für die Verarbeitung Verantwortlichen" meint die EG-DSRL die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden.³

Auftragsverarbeiter

Ein Auftragsverarbeiter ist jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.⁴ Entscheidend ist, dass ein Auftragsverarbeiter ausschließlich für den Auftraggeber Leistungen in Bezug auf die Daten erbringt, die Informationen jedoch nicht für eigene Zwecke verwenden oder weitergeben darf.

„Dritter“

Unter "Dritter" wird die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der un-

¹ Vgl. EG-DSRL Art 2 BSt a.

² Vgl. EG-DSRL Art 2 BSt b.

³ Vgl. EG-DSRL Art 2 BSt d.

⁴ Vgl. EG-DSRL Art 2 BSt e.

mittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten, verstanden.⁵

Common Law

Das Common Law ist ein in vielen englischsprachigen Ländern vorherrschender Rechtskreis, der sich nicht nur auf Gesetze, sondern auch wesentlich auf maßgebliche richterliche Urteile der Vergangenheit – sogenannte Präzedenzfälle – stützt (Fallrecht) und auch durch richterliche Auslegung weitergebildet wird (Richterrecht).⁶ In dieser Bedeutung bildet es den Gegensatz zum sogenannten „Civil Law“ der kontinentaleuropäischen Länder, das auf von den jeweiligen Gesetzgebern kodifizierten Gesetzen basiert und in dem das Richterrecht eine untergeordnete Rolle spielt.⁷

IP-Adresse

Eine IP-Adresse ist eine Adresse in Computernetzen, die – wie z. B. das Internet – auf dem Internetprotokoll (IP) basieren.⁸ Sie wird Geräten zugewiesen, welche an das Netz angebunden sind und macht die Geräte so adressierbar und damit erreichbar.⁹

Opt-in

Opt-in bezeichnet ein Verfahren, bei dem die Verarbeitung von Daten standardmäßig verboten und erst nach Einholung einer expliziten Einverständniserklärung der betroffenen Person gestattet ist.

Opt-out

Beim Opt-out werden Daten standardmäßig verarbeitet, der Konsument muss jedoch darüber informiert werden und die Möglichkeit haben, die Verarbeitung zu unterbinden.

⁵ Vgl. EG-DSRL Art 2 BSt f.

⁶ Vgl. http://de.wikipedia.org/wiki/Common_Law.

⁷ Ebd.

⁸ Vgl. <http://de.wikipedia.org/wiki/IP-Adresse>.

⁹ Ebd.

2 DATENSCHUTZRECHT IN DER EU UND DEN USA

2.1 Datenschutz in der EU

2.1.1 Datenschutz als europäisches Grundrecht

Welcher Stellenwert dem Schutz personenbezogener Daten in der EU beigemessen wird, zeigt die Tatsache, dass Datenschutz in der Charta der Grundrechte der EU, konkret in Artikel 8, verankert ist.¹⁰ Demnach dürfen personenbezogene Daten nur zweckgebunden und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten Grundlage verarbeitet werden.¹¹ Weiters hat die betroffene Person das Recht auf Auskunft sowie Berichtigung der erhobenen Daten.¹² Zur Überwachung der Einhaltung sieht die Charta der Grundrechte eine unabhängige Stelle vor.¹³

Ähnliches wurde auch bereits 1981 in Artikel 8 der Konvention 108 des Europarates mit dem Titel „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ vereinbart.¹⁴

2.1.2 Datenschutzrichtlinie 95/46/EG

Das Herzstück des EU-Datenschutzes bildet die EG-DSRL, da sie das Thema Datenschutz deutlich detaillierter und umfassender regelt.¹⁵ Mit Ausnahme weniger Bereiche, wie der öffentlichen Sicherheit, der Landesverteidigung, der Staatssicherheit und des Strafrechts bildet sie eine einheitliche Vorgabe, die von allen Mitgliedsstaaten in nationales Recht umzusetzen ist.¹⁶ Diese Vorgabe enthält die folgenden Grundsätze, die die Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten schützen sollen.¹⁷

2.1.2.1 Qualität der Daten

Die Richtlinie sieht vor, dass personenbezogene Daten insbesondere nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden müssen sowie ausschließlich für festgelegte und rechtmäßige Zwecke verwendet werden dürfen.¹⁸ Sie müssen sachlich richtig sein und gegebenenfalls auf den neusten Stand gebracht werden.¹⁹ Außerdem dürfen Daten nicht länger, als für den erhobenen Zweck notwendig, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Person ermöglicht.²⁰

¹⁰ Vgl. Charta der Grundrechte der EU, Art 8.

¹¹ Ebd.

¹² Ebd.

¹³ Ebd.

¹⁴ Vgl. Konvention Nr. 108, Art 8.

¹⁵ Vgl. Genz, 19.

¹⁶ Vgl. Genz, 20.

¹⁷ Vgl. http://europa.eu/legislation_summaries/information_society/l14012_de.htm.

¹⁸ Vgl. EG_DSRL, Art 6.

¹⁹ Ebd.

²⁰ Ebd.

2.1.2.2 Zulässigkeit der Verarbeitung von Daten

Dieser Grundsatz schreibt vor, unter welchen Bedingungen personenbezogene Daten verarbeitet und transferiert werden dürfen. Dabei wird von einem grundsätzlichen Verbot ausgegangen, das entweder durch zweifelsfreie Einwilligung der betroffenen Personen oder durch einen der folgenden Gründe aufgehoben werden kann:²¹

- Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist
- Erfüllung von rechtlichen Verpflichtungen, denen der für die Verarbeitung Verantwortliche unterliegt
- Wahrung lebenswichtiger Interessen der betroffenen Person
- Wahrung einer Aufgabe, die im öffentlichen Interesse liegt
- Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird

2.1.2.3 Besondere Kategorien der Verarbeitung

Ausgewählte, als besonders sensibel geltende Datenkategorien dürfen nicht ohne der ausdrücklichen Zustimmung der betroffenen Person verarbeitet werden; dazu zählen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit und Sexualleben.²² Für diese Bestimmungen gelten Einschränkungen - unter anderem, wenn die Verarbeitung zum Schutze lebenswichtiger Interessen der betroffenen Person erforderlich oder aus Gründen der Gesundheitsvorsorge und der medizinischen Diagnostik notwendig ist.²³

2.1.2.4 Information der betroffenen Person

Der für die Verarbeitung Verantwortliche muss dem von der Datenverarbeitung Betroffenen unter anderem folgende Informationen zukommen lassen:²⁴

- Identität des Datenverarbeiters
- Zweck, zu dem die Daten erhoben werden
- Empfänger der Daten
- Hinweis auf Bestehen von Auskunfts- und Berichtigungsrechten

2.1.2.5 Auskunftsrecht der betroffenen Person

Datenverarbeiter haben Betroffenen Auskunft darüber zu geben, ob sie Gegenstand einer Datenverarbeitung sind und müssen im positiven Fall Einsicht in die Daten sowie in den Empfängerkreis gewähren.²⁵ Weiters hat der Betroffene das Recht auf Berichtigung, Sperrung oder Löschung der Daten, wenn diese nicht im

²¹ Vgl. EG-DSRL, Art. 7.

²² Vgl. EG-DSRL, Art. 8.

²³ Vgl. http://europa.eu/legislation_summaries/information_society/l14012_de.htm.

²⁴ Vgl. EG-DSRL, Art 10.

²⁵ Vgl. EG-DSRL, Art 12.

Einklang mit dieser Richtlinie erhoben oder verarbeitet wurden.²⁶ Im Falle einer Korrektur müssen diese Daten auch an Dritte, die unrichtige Daten erhalten haben, weitergegeben werden, sofern dies nicht unmöglich oder mit einem unverhältnismäßig hohen Aufwand verbunden ist.²⁷

2.1.2.6 Widerspruchsrecht der betroffenen Person

Dieser Grundsatz räumt betroffenen Personen das Recht ein, aus berechtigten Gründen Widerspruch gegen eine Verarbeitung sie betreffender Daten einzulegen.²⁸ Ist dieser Widerspruch berechtigt, darf sich der Datenverarbeiter nicht mehr auf die erhobenen Daten beziehen.²⁹ Weiters wird die Möglichkeit eines kostenfreien Antrags gegen eine beabsichtigte Verwendung oder Weitergabe für Zwecke der Direktwerbung zugesichert.³⁰

2.1.2.7 Vertraulichkeit und Sicherheit der Verarbeitung

Personenbezogene Daten dürfen nur auf Weisung des für die Verarbeitung verantwortlichen verarbeitet werden.³¹ Auftragsdatenverarbeiter dürfen die Daten nur ihnen unterstellten Personen zugänglich machen.³²

Außerdem müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um den Schutz der Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust, die unberechtigte Änderung oder der unberechtigten Zugang zu gewährleisten.³³

2.1.2.8 Meldepflicht

Der Grundsatz der Meldepflicht verlangt, dass für die Verarbeitung Verantwortliche vor der Durchführung eine Meldung bei der nationalen Kontrollstelle abgeben.³⁴ Nach Eingang der Meldung prüft die Kontrollstelle vorab, ob Risiken für die Rechte und Freiheiten der betroffenen Personen bestehen.³⁵ Es können vom jeweiligen Mitgliedsstaat verschiedene Bereiche der Datenverarbeitung von der Meldepflicht ausgenommen oder diese vereinfacht werden.³⁶

2.1.2.9 Kontrolle und Sanktionierung

Als weiterer wesentlicher Punkt sind unabhängige, öffentliche Stellen vorgesehen, die für die Kontrolle der Umsetzung dieser Richtlinie verantwortlich sind.³⁷ Neben der eigenständigen Überwachungstätigkeit können die Kontrollstellen auch von betroffenen Personen zum Schutz deren Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten konsultiert werden.³⁸ Diese Stellen sind mit um-

²⁶ Ebd.

²⁷ Ebd.

²⁸ Vgl. http://europa.eu/legislation_summaries/information_society/l14012_de.htm.

²⁹ Vgl. EG-DSRL, Art 14.

³⁰ Vgl. http://europa.eu/legislation_summaries/information_society/l14012_de.htm.

³¹ Vgl. EG-DSRL, Art 17.

³² Ebd.

³³ Ebd.

³⁴ Vgl. EG-DSRL, Art 18.

³⁵ Ebd.

³⁶ Ebd.

³⁷ Vgl. EG-DSRL, Art 28.

³⁸ Ebd.

fassenden Befugnissen ausgestattet, wie beispielsweise die Sperrung, Löschung oder Vernichtung von Daten anzuordnen oder das vorläufige oder endgültige Verbot einer Verarbeitung zu erlassen.³⁹

Den betroffenen Personen wird im Falle einer rechtswidrigen Datenverarbeitung die Möglichkeit garantiert, vor Gericht einen Rechtsbehelf einzulegen.⁴⁰ Wenn durch eine solche Datenverarbeitung dem Betroffenen ein Schaden entsteht, hat dieser Anspruch auf angemessenen Schadenersatz.⁴¹

2.1.2.10 Drittstaatenregelung

Abschließend sieht die Richtlinie eine Drittstaatenregelung vor, die den Transfer personenbezogener Daten grundsätzlich nur in Länder erlaubt, die ein angemessenes Schutzniveau aufweisen (Ausnahmen siehe Kapitel 2.2.1.11).⁴² Ziel dieser Regelung ist es, bei der Verarbeitung personenbezogener Daten die Einhaltung europäischer Datenschutzprinzipien zu gewährleisten.⁴³ Willigt ein Betroffener mit dem Wissen bzw. der Vorstellung, seine Daten werden nach europäischem Recht verarbeitet, in die Datenverarbeitung ein, muss dieses Schutzniveau bei jeder weiteren Verarbeitung dieser Daten eingehalten werden.⁴⁴ Da durch den Export in ein Drittland die EG-DSRL keine Anwendung findet, können dadurch die Rechte der Betroffenen unterlaufen werden.⁴⁵ Aus diesem Grund dürfen Daten nur in Länder transferiert werden, die über ein aus europäischer Sicht adäquates, jedoch nicht notwendigerweise äquivalentes, Datenschutzniveau verfügen.⁴⁶

Entscheidend ist die Frage, was unter „angemessen“ verstanden wird. Die Artikel 29-Arbeitsgruppe, eines der bedeutendsten Datenschutzgremien in der EU, hat sich mit dieser Frage beschäftigt und die folgende Sammlung an Grundsätzen erarbeitet, die den harten Kern des Datenschutzes bilden und als Mindestanforderungen für ein angemessenes Schutzniveau gelten müssen.⁴⁷

Inhaltliche Grundsätze:

- **Grundsatz der Beschränkung der Zweckbestimmung:**

„Daten sind für einen spezifischen Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit der Zweckbestimmung der Übermittlung nicht unvereinbar ist.“⁴⁸

- **Grundsatz der Datenqualität und Verhältnismäßigkeit:**

„Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Die Daten sollten angemessen, relevant und im Hinblick auf die Zweckbe-

³⁹ Ebd.

⁴⁰ Vgl. EG-DSRL, Art 22.

⁴¹ Vgl. EG-DSRL, Art 23.

⁴² Vgl. EG-DSRL, Art 25.

⁴³ Ebd.

⁴⁴ Vgl. Genz, 23f.

⁴⁵ Ebd.

⁴⁶ Ebd.

⁴⁷ Vgl. Genz, 27.

⁴⁸ Vgl. WP 12, 6.

stimmung, für die sie übertragen oder weiterverarbeitet werden, nicht exzessiv sein.“⁴⁹

- **Grundsatz der Transparenz:**

„Natürliche Personen müssen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies aus Billigkeitsgründen erforderlich ist.“⁵⁰

- **Grundsatz der Sicherheit:**

„Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Sicherheitsmaßnahmen für die Risiken der Verarbeitung zu treffen. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Verarbeiter, dürfen Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.“⁵¹

- **Recht auf Zugriff, Berichtigung und Widerspruch:**

„Die betroffene Person muss das Recht haben, eine Kopie aller sie betreffender Daten zu erhalten, die verarbeitet werden, sowie das Recht auf Berichtigung dieser Daten, wenn diese sich als unrichtig erweisen. In bestimmten Situationen muss sie auch Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen können.“⁵²

- **Beschränkung der Weiterübermittlung in andere Drittländer:**

„Weitere Übermittlungen personenbezogener Daten vom ursprünglichen Bestimmungsdrittland in ein anderes Drittland sind lediglich zulässig, wenn das zweite Drittland (d. h. der Empfänger der Weiterübermittlung) ebenfalls ein angemessenes Schutzniveau aufweist.“⁵³

Grundsätze in Bezug auf die Durchsetzung:

- *„Gewährleistung einer guten **Befolgungsrate der Vorschriften**. Ein gutes System zeichnet sich im allgemeinen dadurch aus, dass sich die für die Verarbeitung Verantwortlichen ihrer Pflichten und die betroffenen Personen ihrer Rechte und der Mittel für deren Wahrnehmung sehr stark bewusst sind. Die Existenz wirksamer, abschreckender Sanktionen ist wichtig, um die Einhaltung der Bestimmungen sicherzustellen; ebenso relevant sind natürlich auch Systeme der direkten Überprüfung durch Behörden, Buchprüfer oder unabhängige Datenschutzbeauftragte.“⁵⁴*
- *„**Unterstützung und Hilfe für einzelne betroffene Personen** bei der Wahrnehmung ihrer Rechte. Der Einzelne muss seine Rechte rasch und wirksam, ohne überhöhte Kosten durchsetzen können. Dafür muss es eine Art institutionellen Mechanismus geben, der eine unabhängige Prüfung von*

⁴⁹ Ebd.

⁵⁰ Ebd.

⁵¹ Ebd.

⁵² Ebd.

⁵³ Ebd.

⁵⁴ Vgl. WP 12, 7.

tionellen Mechanismus geben, der eine unabhängige Prüfung von Beschwerden ermöglicht.“⁵⁵

- *„Gewährleistung angemessener Entschädigung für die geschädigte Partei bei Verstoß gegen die Bestimmungen. Für dieses Schlüsselement muss ein System unabhängiger Schlichtung vorhanden sein, das die Zahlung von Entschädigungen oder auch die Auferlegung von Sanktionen ermöglicht.“⁵⁶*

Erfüllt das Datenschutzrecht eines Drittstaates diese Mindestkriterien nicht, so dürfen grundsätzlich keine personenbezogenen Daten in dieses Land übertragen werden.

2.1.2.11 Ausnahmen

Datenübermittlungen, deren Tätigkeiten in einen der folgenden Anwendungsbe-
reiche fallen, sind von der gesamten Richtlinie ausgenommen:

- Gemeinsame Außen- und Sicherheitspolitik
- Gemeinsame Verteidigungspolitik
- Öffentliche Sicherheit
- Landesverteidigung
- Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt)
- Tätigkeiten des Staates im strafrechtlichen Bereich.⁵⁷

Diese Transfers sind durch die Mitgliedsstaaten selbst zu regeln.

2.1.3 Durchsetzung am Beispiel Österreichs

2.1.3.1 Einführung und Vorgaben durch die EG-DSRL

Die EG-DSRL sieht in Art 22 vor, dass jede Person, deren Rechte bei der Verarbeitung ihrer personenbezogenen Daten verletzt wurden, vor Gericht einen Rechtsbehelf einlegen kann.⁵⁸

Weiters sind gemäß Art 28 EG-DSRL öffentliche Kontrollstellen einzurichten, die die Anwendung der vorgegebenen Richtlinien überwachen.⁵⁹ Diese Stellen müssen vollständig unabhängig sein, sind bei der Ausarbeitung von datenschutzrechtlichen Rechtsverordnungen und Verwaltungsvorschriften anzuhören und verfügen über Untersuchungsbefugnisse, Einwirkungsbefugnisse sowie ein Klagerecht.⁶⁰ Zusätzlich zu den eigenständigen Untersuchungen dieser Behörden kann sich laut Art 28 Abs 4 EG-DSRL jede Person mit einer Eingabe an die Kontrollstelle wenden.⁶¹

⁵⁵ Vgl. WP 12, 8.

⁵⁶ Ebd.

⁵⁷ Vgl. EG-DSRL Art 3 Abs 2.

⁵⁸ Jähnel, 495.

⁵⁹ Ebd.

⁶⁰ Ebd.

⁶¹ Ebd.

Das DSG 2000 setzt die Vorgaben des EG-DSRL in nationales Recht um und sieht bei Übertretungen zunächst die folgenden klassischen Rechtsschutzinstrumente vor:⁶²

- die Beschwerde an die Datenschutzkommission nach § 31
- die Anrufung der Gerichte nach § 32
- die strafrechtliche Verfolgung nach § 51 und
- die Verwaltungsstrafbestimmungen nach § 52.

Grundsätzlich ist bei Verletzungen im öffentlichen Bereich die DSK und im privaten Bereich das Landesgericht zuständig.⁶³ Die Durchsetzung des Rechts auf Auskunft stellt jedoch eine große Ausnahme dar und ist sowohl im privaten als auch im öffentlichen Bereich vor der DSK geltend zu machen.⁶⁴

Aufgrund der Vorgaben in Art 28 EG-DSRL sieht § 30 des DSG neben den klassischen Rechtsinstrumenten weitreichende Kontrollbefugnisse der DSK als Ergänzung zum Individualrechtsschutz vor.⁶⁵ Diese sind vor allem in Bereichen notwendig, in denen es dem durchschnittliche Konsumenten an der notwendigen Transparenz fehlt, wie zum Beispiel in der elektronischen Verarbeitung personenbezogener Daten.⁶⁶ Rechtsverletzungen im Datenschutzbereich sind für den Betroffenen oft nicht oder zu spät erkennbar, da die Auswirkungen nicht immer unmittelbar spürbar sind.⁶⁷

2.1.3.2 Die Datenschutzkommission

In Österreich ist die Datenschutzkommission das bedeutendste Kontrollorgan, das die Umsetzung und Einhaltung der Datenschutzrichtlinien sicherstellen soll. Die Mitglieder der DSK sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden.⁶⁸

2.1.3.3 Rechtsschutz durch ein Kontroll- und Ombudsmannverfahren

Das DSG sieht im § 30 die umfangreichste Kontrollbefugnis für die DSK im Datenschutzbereich in Form eines „Kontroll- und Ombudsmannverfahrens“ vor.⁶⁹ Dieses Verfahren ist vor allem im privaten Bereich ein praxistaugliches Mittel zur Beseitigung von datenschutzrechtlich relevanten Missständen, da die DSK dort mit Ausnahme von Verletzungen des Auskunftsrechts keine Zuständigkeit zur Durchführung förmlicher Bescheidverfahren besitzt.⁷⁰ Es können alle datenschutzrechtlich relevanten Sachverhalte dieser Prüfung vorgelegt werden, rechtsverbindliche Entscheidungen beinhaltet dieses Verfahren jedoch nicht; es endet mit einer Empfehlung der DSK.⁷¹

⁶² Ebd.

⁶³ Vgl. Jahnel, 496.

⁶⁴ Ebd.

⁶⁵ Ebd.

⁶⁶ Ebd.

⁶⁷ Ebd.

⁶⁸ Vgl. Jahnel, 499.

⁶⁹ Vgl. Jahnel, 512.

⁷⁰ Ebd.

⁷¹ Ebd.

Es kann sich jede betroffene Person, die behauptet, in ihren Datenschutzrechten verletzt worden zu sein, an die Datenschutzkommission wenden, unabhängig davon, ob sich die Beschwerde gegen öffentliche oder private Beschuldigte richtet.⁷² Daher ergibt sich eine Überschneidung, da Verletzungen im privaten Bereich grundsätzlich durch zivilrechtliche Klage zu behandeln sind, wobei der durchsetzbare Anspruch nur vor dem zuständigen Landesgericht erwirkt werden. Im Gegensatz dazu ist das Ombudsmannverfahren erheblich flexibler und es entfällt das Kostenrisiko.⁷³

Einschauverfahren

Die Datenschutzkommission ist in ihren Untersuchungen nicht unbedingt auf Beschwerden Betroffener angewiesen, sie kann auch von sich aus im Fall eines begründeten Verdachts Datenanwendungen überprüfen.⁷⁴

In solchen Fällen wird der Beschuldigte zuerst mit den Vorwürfen konfrontiert und zu einer Stellungnahme aufgefordert.⁷⁵ Wird dadurch der Verdacht bestätigt, kann eine Überprüfung durchgeführt werden, wobei die DSK das Recht hat, alle notwendigen Aufklärungen zu verlangen und Einschau in Datenverarbeitungen und Unterlagen zu nehmen.⁷⁶

Empfehlungen und deren Durchsetzung

Die DSK kann nach erfolgter Untersuchung Empfehlungen aussprechen, um eine weitere Verletzung zu unterbinden, wobei eine angemessene Frist für die Umsetzung festzulegen ist.⁷⁷ Wird die ausgesprochene Empfehlung innerhalb der gesetzten Frist nicht umgesetzt, kann die DSK anlassspezifisch die folgenden Maßnahmen setzen:⁷⁸

- Einleitung eines Verfahrens zur Überprüfung der Registrierung
- Erstatte einer Strafanzeige
- Klage vor dem zuständigen Gericht bei schwerwiegenden Verstößen im privaten Bereich

Die Empfehlung nach § 30 Abs 6 DSG stellt weder einen Bescheid, noch einen Akt unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt noch eine Verordnung dar, sondern eine eigene Form des Rechtsaktes.⁷⁹ Die Empfehlung ist nicht unmittelbar verbindlich, sie zieht lediglich die oben genannten Rechtsfolgen nach sich.⁸⁰

Untersagung einer Datenanwendung

Seit der DSG-Novelle 2010 hat die DSK laut § 30 Abs 6a die Möglichkeit, bei Gefahr in Verzug Datenanwendungen per Bescheid zu untersagen.⁸¹ Dies kann vor allem

⁷² Vgl. Jähnel, 513.

⁷³ Ebd.

⁷⁴ Vgl. Jähnel, 514.

⁷⁵ Ebd.

⁷⁶ Ebd.

⁷⁷ Vgl. Jähnel, 516.

⁷⁸ Ebd.

⁷⁹ Vgl. Jähnel, 517.

⁸⁰ Ebd.

⁸¹ Vgl. Jähnel, 519.

bei der rechtswidrigen Unterlassung einer Meldung oder bei der Datenanwendung auf eine Art und Weise, die den Grundsätzen des Datenschutzes enorm widerspricht (z.B. systematische Verarbeitung nicht aktueller oder im Hinblick auf den Verwendungszweck unrichtiger Daten), der Fall sein.⁸²

2.1.3.4 Rechtsschutz durch Beschwerde an die Datenschutzkommission

Bei behaupteten Verletzungen des Rechts auf Auskunft (bei Beschuldigten im privaten Bereich) oder der Rechte auf Geheimhaltung, auf Richtigstellung oder Löschung personenbezogener Daten (gegen Beschuldigte im öffentlichen Bereich) kann ein förmliches Beschwerdeverfahren durch die DSK eingeleitet werden.⁸³ Die DSK hat dabei dieselben Kontrollbefugnisse wie im zuvor behandelten Kontroll- und Ombudsmannverfahren.⁸⁴ Im Gegensatz dazu enden Beschwerdeverfahren nicht mit einer Empfehlung, sondern mit Bescheid.⁸⁵

Bei Beschuldigten des privaten Bereichs beinhaltet der Bescheid konkrete Leistungsaufträge.⁸⁶ Diese fordern den Beschwerdegegner auf, innerhalb einer bestimmten Leistungsfrist Auskunft über bestimmte Daten zu geben.⁸⁷ Die Nichterteilung einer Auskunft entgegen einem rechtskräftigen Bescheid ist mit einer Verwaltungsstrafe von bis zu 25.000,- € bedroht.⁸⁸

Im Verfahren gegen Beschuldigte des öffentlichen Bereichs ist keine Erlassung eines Leistungsbescheides möglich, es kann lediglich eine Rechtsverletzung durch die DSK festgestellt werden.⁸⁹ Die zuständige Stelle hat daraufhin die angemessene Rechtslage herzustellen.⁹⁰

Gegen Bescheide der DSK ist kein Rechtsmittel zulässig, wodurch die DSK erste und letzte Instanz ist; es kann lediglich der VfGH bzw. der VfGH durch die Parteien des Verfahrens angerufen werden.⁹¹

2.1.3.5 Zivilrechtlicher Schutz durch die ordentlichen Gerichte

Ansprüche gegen Beschuldigte des privaten Bereichs wegen Verletzungen der Rechte des Betroffenen auf Geheimhaltung, auf Richtigstellung oder Löschung können vom Betroffenen auf dem Zivilrechtsweg geltend gemacht werden.⁹² Dabei hat der Betroffene Anspruch auf Unterlassung sowie Beseitigung eines dem DSGVO widersprechenden Zustandes.⁹³ Zuständig ist das Landesgericht, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt hat, es kann aber auch vor dem Landesgericht, in dessen Sprengel der Beklagte seinen Sitz hat, geklagt werden.⁹⁴

⁸² Ebd.

⁸³ Vgl. Jahnel 520.

⁸⁴ Vgl. Jahnel, 523.

⁸⁵ Ebd.

⁸⁶ Ebd.

⁸⁷ Ebd.

⁸⁸ Vgl. Jahnel, 524.

⁸⁹ Vgl. Jahnel, 525.

⁹⁰ Ebd.

⁹¹ Ebd.

⁹² Vgl. Jahnel, 534.

⁹³ Ebd.

⁹⁴ Vgl. Jahnel, 535.

Beim begründeten Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs hat die DSK eine Feststellungsklage beim zuständigen Gericht zu erheben.⁹⁵ Diese Pflicht ist jedoch nur auf Fälle beschränkt, an deren Klärung öffentliches Interesse besteht.⁹⁶ Durch die Feststellungsklage der DSK soll das Prozessrisiko für den Betroffenen vermieden werden, dieser kann nach erfolgtem Feststellungsurteil entscheiden, ob er seine Unterlassungs- und Schadensersatzansprüche selbst weiterverfolgen will.⁹⁷

Der Betroffene kann auf zivilrechtlichem Weg sein Recht auf Schadenersatz nach den allgemeinen Bestimmungen des bürgerlichen Rechts geltend machen, wenn ein Auftraggeber oder Dienstleister Daten schuldhaft entgegen den Bestimmungen des DSG verwendet.⁹⁸ Auf dieser Grundlage kann nach den allgemeinen Regeln des Schadensersatzrechts der Vermögensschaden geltend gemacht werden.⁹⁹

Für bestimmte Arten von Daten ist auch der Ersatz immateriellen Schadens vorgesehen, und zwar in Fällen schwerwiegender rechtswidriger Datenanwendungen, die ihrem Wesen nach mit Tatbeständen vergleichbar sind, die nach dem Medien-gesetz zum Schadensersatz verpflichtet.¹⁰⁰ Voraussetzungen dafür sind:¹⁰¹

- Die Verwendung sensibler Daten, strafrechtlich relevanter Daten oder die Auskunft betreffend Kreditwürdigkeit
- die öffentlich zugängliche Verwendung einer dieser Datenarten
- die Verletzung schutzwürdiger Geheimhaltungsinteressen des Betroffenen in einer Weise, die einer Bloßstellung gleichkommt

2.1.3.6 Schematische Darstellung des Rechtsschutzes nach dem DSG

Abschließend skizziert die folgende Grafik den Instanzenzug bei der Durchsetzung des Datenschutzrechts in Österreich.

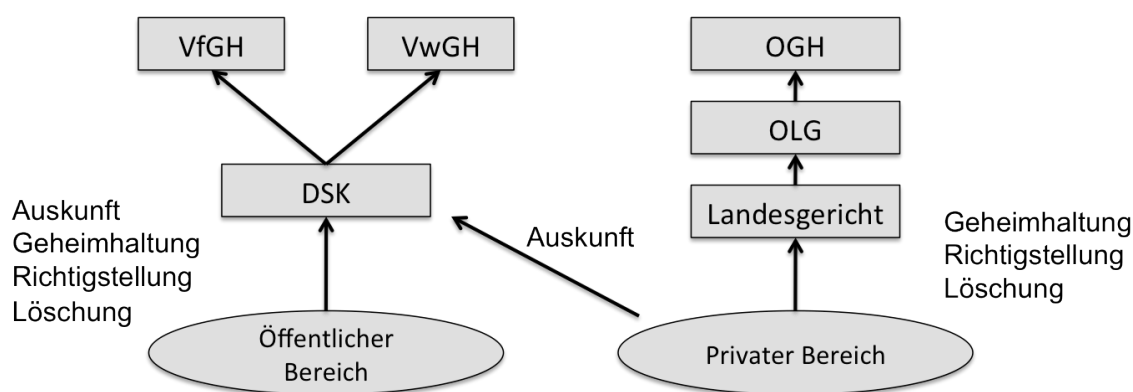


Abbildung 1: Rechtsschutz nach dem DSG

Quelle: Jahnelt, Handbuch Datenschutzrecht, 544

⁹⁵ Vgl. Jahnelt, 536.

⁹⁶ Ebd.

⁹⁷ Ebd.

⁹⁸ Vgl. Jahnelt 538.

⁹⁹ Ebd.

¹⁰⁰ Ebd.

¹⁰¹ Ebd.

2.2 Datenschutz in den USA

2.2.1 Privacy protection

Grundsätzlich ist das allgemeine Persönlichkeitsrecht als Ursprung für das Datenschutzrecht in den USA ebenso anerkannt wie in Europa.¹⁰² In Europa hat sich das Datenschutzrecht jedoch sowohl begrifflich als auch inhaltlich deutlich vom allgemeinen Persönlichkeitsrecht abgetrennt und entwickelt, während man in den USA weitgehend vom gemeinsamen Begriff der Privacy ausgeht.¹⁰³ Privacy kann als Zurückgezogenheit, das Alleinsein, das Privatleben, die Intimsphäre oder allgemein als Datenschutz übersetzt werden.¹⁰⁴ Je nach Kontext wird der Begriff unterschiedlich verwendet, wodurch eine Bewertung aus Sicht des Datenschutzes erschwert wird.¹⁰⁵

2.2.2 Gesetzlicher Datenschutz

Als erstes ist anzumerken, dass sich die US-amerikanische Rechtslage grundlegend von der europäischen unterscheidet.¹⁰⁶ Einerseits ist die Verfassungsanwendung eine vollkommen andere, da bei konkreten Rechtsfragen der direkte Bezug auf Verfassungstext zu erheblichen Schwierigkeiten führen kann.¹⁰⁷ Andererseits spielt neben dem Gesetzesrecht das Präjudizienrecht eine wesentliche Rolle, in welchem Richter auf Basis vergangener Einzelfallentscheidungen Urteile fällen.¹⁰⁸ Da erstens durch die enorme Anzahl der zu berücksichtigenden Fälle eine Beurteilung des Datenschutzes besonders schwierig ist und es zweitens für das gesamte Bundesgebiet kein einheitliches Common Law gibt, wird das Präjudizienrecht in dieser Beurteilung ausgeblendet.

2.2.2.1 Die Verfassung

In der US-Verfassung ist kein ausdrückliches Recht auf Privacy zu finden, daher ebenso auch kein Recht auf Schutz personenbezogener Daten.¹⁰⁹ Als Anknüpfungspunkt für den Schutz der Privatsphäre kann jedoch der vierte Verfassungszusatz gesehen werden.¹¹⁰ Dieser fordert das Recht der Menschen auf „Sicherheit ihrer Person, Häuser, Unterlagen und Eigentum gegen unbegründete Durchsuchungen und Beschlagnahmen“. ¹¹¹ Zwar nicht ausschließlich, jedoch hauptsächlich findet der vierte Verfassungszusatz Anwendung im Schutz gegenüber der Staatsgewalt (vor allem gegen Hausdurchsuchungen), weniger gegenüber sonstigen potenziellen Gefahren des Missbrauchs personenbezogener Daten.¹¹²

¹⁰² Vgl. Genz, 39f.

¹⁰³ Ebd.

¹⁰⁴ Ebd.

¹⁰⁵ Ebd.

¹⁰⁶ Vgl. Genz, 44f.

¹⁰⁷ Ebd.

¹⁰⁸ Vgl. Genz, 76.

¹⁰⁹ Vgl. Genz, 44f.

¹¹⁰ Ebd.

¹¹¹ Ebd.

¹¹² Ebd.

US-amerikanische Gerichte und Teile der Wissenschaft sehen auch Anknüpfungspunkte an den ersten Verfassungszusatz, das Recht auf Redefreiheit.¹¹³ Demnach ist das Sammeln von Daten ein wesentlicher Bestandteil der Ausübung der Redefreiheit, wodurch sich bei der Einschränkung der Datenerhebung verfassungsrechtliche Konflikte ergeben würden.¹¹⁴ Hier lässt sich bereits das Spannungsfeld zwischen dem Schutz der Privatsphäre und der Beschneidung der Freiheit des Individuums erkennen.¹¹⁵

2.2.2.2 Einfachgesetzliche Bestimmungen

Eine umfassende, bundesweit gültige Datenschutzregelung sucht man vergeblich, lediglich einige Bundesstaaten (beispielsweise Kalifornien) haben bereits weitreichende Datenschutzgesetze erlassen.¹¹⁶ Für die Bewertung der Angemessenheit des Datenschutzes der USA können solche gliedstaatliche Normen jedoch nicht herangezogen werden, da sich aus der einfachen Transferierbarkeit der Daten innerhalb der USA beträchtliche Risiken ergeben.¹¹⁷

Aus der folgenden exemplarischen Auflistung verschiedener Datenschutzgesetze soll erkennbar werden, wie Datenschutz in den USA durch viele Gesetze punktuell abgedeckt wird.¹¹⁸ In Bezug auf den Schutz der Privatsphäre gegen staatliche Eingriffe sind große Bemühungen erkennbar.¹¹⁹ Ein Gesetz, das alle personenbezogenen Daten schützt und für alle staatlichen Organe Geltung hat, fehlt jedoch.¹²⁰ Auch im nicht-öffentlichen Bereich existiert eine Vielzahl an Regelungen, die einzelne Bereiche teilweise abdecken, jedoch bei weitem keinen umfassenden Schutz garantieren können.¹²¹

2.2.2.3 Privacy Act

Der „Privacy Act“ ist ein Gesetz zum Schutz Privater gegen hoheitliche Eingriffe in deren Privatsphäre bei der Datensammlung durch Regierungsstellen des Bundes.¹²² Er sieht unter anderem vor, dass Datensammlungen, soweit möglich, direkt bei den Personen durchzuführen sind und räumt den Betroffenen das Recht auf Einsicht und gegebenenfalls Berichtigung ein.¹²³ Da der Privacy Act auf Behörden des Bundes begrenzt ist, hat er keine Auswirkung auf die Regierungsstellen in den einzelnen Gliedstaaten.¹²⁴ Außerdem hat der Privacy Act im Detail eine beträchtliche Schwäche: Er erlaubt nämlich die Offenlegung von Daten zum Zwecke des „Routinegebrauchs, übereinstimmend mit dem Zweck der ursprünglichen Datensammlung“, ohne jedoch den Begriff „Routinegebrauch“ näher einzuschränken.¹²⁵

¹¹³ Ebd.

¹¹⁴ Ebd.

¹¹⁵ Ebd.

¹¹⁶ Vgl. Genz, 74.

¹¹⁷ Ebd.

¹¹⁸ Vgl. Genz, 50ff.

¹¹⁹ Ebd.

¹²⁰ Ebd.

¹²¹ Vgl. Genz, 59ff.

¹²² Vgl. Genz, 50ff.

¹²³ Ebd.

¹²⁴ Ebd.

¹²⁵ Ebd.

Dadurch liegt die Befürchtung nahe, dass jeder Datenzugriff aus Routine geschieht und überhaupt kein Schutz vorhanden ist.¹²⁶

2.2.2.4 Privacy Protection Act

Der „Privacy Protection Act“ schränkt die staatlichen Eingriffsrechte gegenüber Verlegern hinsichtlich der Beschlagnahme ihrer Arbeitsmaterialien ein.¹²⁷ Eine Zulässigkeit von Beschlagnahmen ist danach nur mehr bei strafrechtlicher Relevanz oder der Gefährdung nationaler Sicherheit gegeben.¹²⁸ Datenschutzrechtlich ist das insofern von Bedeutung, als dadurch personenbezogene Daten, die der Verleger im Rahmen seiner Arbeit gespeichert hat, vor staatlichem Zugriff geschützt sind.¹²⁹

2.2.2.5 Right to Financial Privacy Act

Das US-amerikanische Recht bietet im Finanzsektor die größte Dichte an Bestimmungen zum Schutz personenbezogener Daten.¹³⁰ Der „Right to Financial Privacy Act“ schützt Kunden von Banken und anderen Finanzdienstleistern vor staatlichem Eingriff.¹³¹ Das Gesetz verhindert zwar nicht gänzlich den Zugriff staatlicher Behörden auf Bankdaten, es verlangt jedoch die umfassende Information des betroffenen Kunden.¹³²

2.2.2.6 Fair Credit Reporting Act

Der „Fair Credit Reporting Act“ (FCRA) ist ein bedeutendes Gegenstück zum „Right to Financial Privacy Act“ für den privaten Sektor.¹³³ Der FCRA soll für fairen Umgang mit Bank- und Finanzdaten sorgen, in dem er Verarbeitungsbedingungen für Informationsverwalter schafft.¹³⁴ Neben den Banken sind davon vor allem die in den USA üblichen Kreditauskunftagenturen, die „Consumer Reporting Agencies“, betroffen.¹³⁵ Dies sind Unternehmen, die ohne Wissen und Einwilligung des Betroffenen Informationen über Personen zusammentragen, um deren finanzielle Situation bzw. die Kreditwürdigkeit in Form von sogenannten „Consumer Reports“ darzustellen.¹³⁶ Als Quellen dienen öffentlich zugängliche Daten sowie Befragungen von Personen aus dem näheren Umfeld der Betroffenen.¹³⁷ Vor der Einführung des FCRA durften die Daten ohne jede Einschränkung gesammelt und für beliebige Zwecke nutzbar gemacht werden.¹³⁸ Art und Umfang der Datensammlungen werden zwar durch den FCRA nicht beschränkt, er sieht aber als eine von wenigen Vorschriften eine Gebrauchsbeschränkung vor.¹³⁹ Gemäß dem FCRA dürfen die

¹²⁶ Ebd.

¹²⁷ Vgl. Genz, 54.

¹²⁸ Ebd.

¹²⁹ Ebd.

¹³⁰ Vgl. Genz, 55f.

¹³¹ Ebd.

¹³² Ebd.

¹³³ Vgl. Genz, 60.

¹³⁴ Ebd.

¹³⁵ Ebd.

¹³⁶ Ebd.

¹³⁷ Ebd.

¹³⁸ Ebd.

¹³⁹ Ebd.

„Consumer Reports“ nur für folgende Zwecke bzw. unter den folgenden Bedingungen freigegeben werden:¹⁴⁰

- Gerichtliche Anforderung
- Kreditgewährung
- Arbeits- oder Versicherungsverhältnisse
- Bewilligung von Konzessionen und Beihilfen
- Wahrung berechtigter geschäftlicher Interessen, die durch ein Geschäft mit den Verbraucher berührt werden
- Einwilligung des Betroffenen

Außerdem haben die Betroffenen das Recht, die gesammelten Daten einzusehen und im Fehlerfall eine Berichtigung zu verlangen.¹⁴¹

2.2.2.7 Drivers Privacy Protection Act

Der „Drivers Privacy Protection Act“ regelt den Umgang staatlicher KFZ-Zulassungsbehörden mit personenbezogenen Daten.¹⁴² Bis 1994 war das Zulassungsregister öffentlich einsehbar.¹⁴³ Erst nach dem Mordfall an einer Schauspielerin, deren Mörder ihre Anschrift aus dem KFZ-Zulassungsregister ausfindig gemacht hatte, wurde dieses Gesetz erlassen, das den Zulassungsbehörden die Weitergabe personenbezogener Daten an Dritte grundsätzlich untersagt.¹⁴⁴

2.2.2.8 Telephone Consumer Protection Act

Dieses Gesetz soll das Problem des Telemarketings regeln.¹⁴⁵ Es verpflichtet Unternehmen, die Telefonmarketing betreiben, „do not call“-Listen zu berücksichtigen, auf welche sich Konsumenten setzen lassen können.¹⁴⁶ Dadurch wird den Telefonvermarktern angezeigt, wer nicht angerufen werden darf.¹⁴⁷ Die Wirksamkeit dieses Gesetzes lässt jedoch zu wünschen übrig, was die Vielzahl an kostenpflichtigen Angeboten der Telekommunikationsunternehmen zur Abwehr des Telefonmarketings zeigt.¹⁴⁸

2.2.2.9 Childrens Online Privacy Protection Act

Besonders hervorzuheben ist der „Childrens Online Privacy Protection Act“ (COPPA), der den Schutz personenbezogener Daten von Kindern unter 13 Jahren gewährleisten soll.¹⁴⁹ In erster Linie sieht der COPPA vor, dass Online-Dienste, die auf Kinder ausgerichtet sind, gegenüber den Eltern offenlegen müssen, ob und in welchem Umfang personenbezogene Daten erfasst, genutzt und veröffentlicht werden und dass sie vor der Erhebung personenbezogener Daten ein nachvoll-

¹⁴⁰ Ebd.

¹⁴¹ Ebd.

¹⁴² Vgl. Genz, 60.

¹⁴³ Ebd.

¹⁴⁴ Ebd.

¹⁴⁵ Vgl. Genz, 68f.

¹⁴⁶ Ebd.

¹⁴⁷ Ebd.

¹⁴⁸ Ebd.

¹⁴⁹ Ebd.

ziehbares Einverständnis der Eltern einholen müssen.¹⁵⁰ Weiters wird den Eltern auch das Recht auf Überwachung der Datenverwendung eingeräumt, wodurch diese die Möglichkeit haben, die Daten einzusehen, zu berichtigen oder die Löschung zu fordern.¹⁵¹ Die Eltern haben sogar das Recht, die weitere Nutzung bereits erfasster Daten ihrer Kinder sowie die weitere Datensammlung zu verhindern.¹⁵² Verstöße gegen den COPPA sind durch Sanktionen seitens der FTC in Form von Bußgeldern in Höhe von bis zu \$ 10.000 pro Verstoß bzw. pro Tag bei fortgesetztem Verstoß sowie durch den Justizminister verfolgbar.¹⁵³

Was den COPPA so besonders macht ist, dass in den USA erstmals ein Datenkategorien übergreifendes Regelwerk geschaffen wurde, dessen Schutz sich auf alle über das Internet erhobenen, personenbezogenen Daten erstreckt.¹⁵⁴ Es kommt erstmals nicht mehr auf die Art der personenbezogenen Daten (Finanzdaten, Personaldaten, usw.) an, wie es z.B. bei den Regelungen bezüglich Finanzdaten der Fall ist, sondern grundsätzlich auf den Umstand der Datenverarbeitung.¹⁵⁵

2.2.2.10 Security Breach Information Act in Kalifornien

Auch wenn der kalifornische „Security Breach Information Act“ (SBIA) für die bundesweite Beurteilung des Datenschutzes keine Relevanz findet, ist er als Beispiel und Vorreiter der aktuellen Entwicklungen im US-Datenschutzrecht erwähnenswert.

Nach dem SBIA unterliegt jedes Unternehmen, das in Kalifornien Geschäfte tätigt und persönliche Daten von Kunden sammelt, einer besonderen Anzeigepflicht.¹⁵⁶ Diese gilt, sobald Daten von Kunden oder Mitarbeitern versehentlich publik werden, verlorengehen oder Dritte unbefugt auf sie zugreifen.¹⁵⁷ In diesem Fall muss das Unternehmen schnellstmöglich und ohne schuldhafte Verzögerungen die betroffenen Kunden über den Vorfall informieren.¹⁵⁸ Das Office of Privacy of the California Department of Consumer Affairs empfiehlt, eine Frist von höchstens zehn Werktagen einzuhalten. Diese Anzeigepflicht gilt auch dann, wenn das Unternehmen den Datenschutz eingriff nicht verschuldet hat.¹⁵⁹ Von einer falsch weitergeleiteten Email über ein liegengelassenen Smartphone bis hin zum Hackerangriff auf den Datenbestand sind verschiedenste Szenarien vorstellbar.¹⁶⁰ Unter personenbezogenen Daten, auf das sich dieses Gesetz bezieht, werden im SBIA der Vor- und Nachname, die Sozialversicherungsnummer, die Führerscheinnummer, die Kontonummer unter Einschluss von Passwörtern und anderen Zugangscodes verstanden.¹⁶¹

¹⁵⁰ Vgl. <http://amlaw.us/kamps1.shtml>.

¹⁵¹ Ebd.

¹⁵² Ebd.

¹⁵³ Vgl. <http://amlaw.us/kamps1.shtml>; Genz, 70.

¹⁵⁴ Vgl. Genz, 72.

¹⁵⁵ Ebd.

¹⁵⁶ Vgl. http://www.gtai.de/DE/Content/___SharedDocs/Links-Einzeldokumente-Datenbanken/fachdokument.html?fid=MK200709288001.

¹⁵⁷ Ebd.

¹⁵⁸ Ebd.

¹⁵⁹ Ebd.

¹⁶⁰ Ebd.

¹⁶¹ Ebd.

Ähnliche Regelungen in anderen Gliedstaaten

Andere Bundesstaaten schließen auch medizinische Daten, persönliche Zugangs-codes oder biometrische Daten ein.¹⁶² In New York wird unter personenbezogenen Daten alles verstanden, was geeignet ist, eine Person zu identifizieren.¹⁶³

Ein Verstoß gegen die Anzeigepflicht gilt in den meisten Bundesstaaten als Verstoß gegen das Wettbewerbsrecht und kann einen Schadensersatzanspruch der betroffenen Kunden nach sich ziehen.¹⁶⁴ Es drohen auch empfindliche Bußgelder, wie z.B. bis zu 500.000\$ im Bundesstaat Florida.¹⁶⁵

2.2.3 Selbstregulierung

Wie bereits erwähnt, enthält der gesetzliche US-amerikanische Datenschutz vornehmlich sektorale Regelungen und vermeidet umfassende und bereichsübergreifende gesetzliche Regelungen, da staatliche Regulierung privaten Handelns als Gefahr für die Rechte und Freiheiten der Bürger angesehen wird.¹⁶⁶ Daher ist die Rechtspolitik der USA überwiegend darauf ausgelegt, die Regulierung wesentlicher Bereiche gesellschaftlichen Lebens den Betroffenen selbst zu überlassen.¹⁶⁷ Aus diesem Grund muss auch ein Blick auf die Selbstregulierungsmechanismen geworfen werden, um das Datenschutzniveau beurteilen zu können.¹⁶⁸

Ausgangspunkt ist, dass der Benutzer frei über seine Daten verfügen kann und es ihm selbst überlassen ist, ob er diese preisgeben möchte oder nicht.¹⁶⁹ Daten können daher als Marktgüter angesehen werden, mit denen man handeln kann.¹⁷⁰ Damit dieser Handel fair ist, ist nur von Bedeutung, dass der Betroffene weiß, welche Daten von ihm erhoben werden und welchen Vorteil er dadurch hat.¹⁷¹ Aus Datenschutzsicht genügt also das Recht des Internetnutzers, zu entscheiden, ob er Informations- und Kommunikationsmöglichkeiten wahrnimmt, im Zuge deren Daten über ihn erhoben werden.¹⁷²

Die Selbstregulierung im Datenschutz basiert darauf, dass Dienstbetreiber um die Akzeptanz der Benutzer kämpfen, in dem sie besonders sorgfältig mit personenbezogenen Daten umgehen und dies öffentlich kundmachen.¹⁷³ Dienstanbieter können sich einem der vielen Gütesiegelprogramme (wie z.B. dem TRUSTe-Programm) anschließen, dazu müssen sie lediglich ihre Datenschutzpraktiken offenlegen und sich an diese halten.¹⁷⁴ Sie erhalten dafür ein „Trustmark“, das sie als Werbung auf der Webseite anbringen können und mit der Erklärung der Datenschutzpraktiken verlinken müssen.¹⁷⁵ Die Vertrauenswürdigkeit des Programms

¹⁶² Ebd.

¹⁶³ Ebd.

¹⁶⁴ Ebd.

¹⁶⁵ Ebd.

¹⁶⁶ Vgl. Genz, 85ff.

¹⁶⁷ Vgl. Genz, 85ff.

¹⁶⁸ Ebd.

¹⁶⁹ Vgl. Roßnagel.

¹⁷⁰ Ebd.

¹⁷¹ Ebd.

¹⁷² Ebd.

¹⁷³ Ebd.

¹⁷⁴ Ebd.

¹⁷⁵ Ebd.

wird durch Kontrolle der Webseiten sowie durch Beschwerdemöglichkeit der Nutzer sichergestellt.¹⁷⁶ Obwohl wiederholte Überprüfungen zur Einhaltung der Selbstverpflichtung vorgesehen sind, mangelt es an kontinuierlicher Verbesserung des Datenschutzes.¹⁷⁷ Viele Gütesiegelprogramme sehen nämlich keine materiellen Mindeststandards wie Recht auf Einsicht, Korrektur oder Löschung vor.¹⁷⁸ Daher erhöhen solche Gütesiegelprogramme letztlich nur die Transparenz im Umgang mit personenbezogenen Daten, nicht jedoch den Datenschutz.¹⁷⁹ Es erhalten auch Anbieter das Gütesiegel, die in ihrer Datenschutzerklärung offen beschreiben, dass sie Daten sammeln und diese auch an Dritte weitergeben.¹⁸⁰

2.2.4 Fazit

Abschließend muss festgestellt werden, dass weder auf gesetzlicher noch auf selbstregulativer Ebene ein das Europäische Gemeinschaftsrecht annähernd erreichendes Datenschutzniveau festgestellt werden kann. Während es dem legislativen Ansatz vor allem an einer umfassenden, bereichsübergreifenden Regelung mangelt, fehlt in der Selbstregulation in erster Linie ein Mindeststandard, der von Gütesiegelteilnehmern eingehalten werden müsste. Die große Gefahr liegt vor allem darin, dass die Sammlung und der Verkauf von Daten enorme wirtschaftliche Anreize bieten, wodurch viele Unternehmen motiviert werden, keine kundenorientierten Datenschutzmaßnahmen auf Selbstregulierungsbasis zu ergreifen.¹⁸¹

Aus europäischer Sicht kann einzig der COPPA als Schritt in die richtige Richtung erkannt werden, allerdings ist dieser auf Kinder bis zu einem Alter von 13 Jahren beschränkt.

¹⁷⁶ Ebd.

¹⁷⁷ Ebd.

¹⁷⁸ Ebd.

¹⁷⁹ Ebd.

¹⁸⁰ Ebd.

¹⁸¹ Vgl. Genz, 96.

3 DAS SAFE-HARBOR MODELL

3.1 Notwendigkeit eines Datenschutzmodells

3.1.1 Drittstaatenregelung der Richtlinie 95/46/EG

Am 24. Oktober 1995 haben das Europäische Parlament und der Rat die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-DSRL) erlassen. Unter anderem verbietet diese Richtlinie im Allgemeinen die Übermittlung personenbezogener Daten in Drittländer, sofern diese kein angemessenes Schutzniveau gewährleisten.¹⁸² Die Entscheidung, ob ein Drittstaat als sicher eingestuft wird, obliegt der Europäischen Kommission.¹⁸³

Da für die USA ein angemessenes Schutzniveau nicht festgestellt werden konnte, hat sich für die EU-Mitgliedsländer somit die Pflicht ergeben, Transfers personenbezogener Daten in die USA zu unterbinden. Wollte eine Organisation personenbezogene Daten, auf die keine Ausnahme (siehe Kapitel 3.8) zutrifft, in unsichere Drittstaaten übermitteln, so wäre das nur durch eine vertraglich festgesetzte Garantie des Datenimporteurs zulässig, in der er den Schutz der Privatsphäre des Betroffenen sicherstellt.¹⁸⁴

3.1.2 Folgen

Mit dem Inkrafttreten dieser Richtlinie war langfristig eine umfassende Blockade für personenbezogene Daten durch die EU-Mitgliedsstaaten zu befürchten.¹⁸⁵ Auch wenn eine solche Blockade aufgrund von Verzögerungen bei der Umsetzung in nationales Recht in absehbarer Zeit nicht zu erwarten war, führte die Richtlinie zu großer Verunsicherung, da die Rechtslage nicht mehr eindeutig schien.¹⁸⁶ Über die Reichweite der wirtschaftlichen und politischen Konsequenzen einer möglichen transatlantischen Datensperre soll an dieser Stelle nicht spekuliert werden.¹⁸⁷

Die EU versuchte, dem US-amerikanischen Gesetzgeber davon zu überzeugen, ein umfassendes Datenschutzgesetz, ähnlich der EG-DSRL, zu erlassen, doch dieses Vorhaben scheiterte an den grundsätzlich verschiedenen Auffassungen zur Freiheit des Bürgers.¹⁸⁸ Um eine Flut an Vertragsklauseln zu vermeiden und eine klare Rechtslage wiederherzustellen, hat die EK gemeinsam mit dem US-Handelsministerium ein Konzept zur Förderung des transatlantischen Handels unter dem Titel „Sicherer Hafen“ bzw. „Safe-Harbor“ beschlossen.¹⁸⁹

¹⁸² Vgl. EG-DSRL Art 25 Abs 1.

¹⁸³ Vgl. EG-DSRL Art 25 Abs 6.

¹⁸⁴ Vgl. EG-DSRL Art 26 Abs 2.

¹⁸⁵ Vgl. Genz, 129.

¹⁸⁶ Ebd.

¹⁸⁷ Ebd.

¹⁸⁸ Vgl. Leathers, 198f.

¹⁸⁹ Vgl. Genz, 129.

3.2 Rechtliche Grundlage

Das Konzept von Safe-Harbor wurde vom US-Handelsministerium in Kooperation mit der EK seit April 1998 vorbereitet und entwickelt und basiert auf einem komplexen Gerüst unterschiedlicher Grundlagendokumente und Stellungnahmen.¹⁹⁰

Den Kern des Safe-Harbor Modells bilden die beiden Dokumente „Grundsätze des sicheren Hafens“ und „Häufig gestellte Fragen – FAQ“. Diese Dokumente sind als Anlagen I und II in der Entscheidung 2000/520/EG der EK vom 26. Juli 2000 (SH-E) zu finden. Den inhaltlichen Kern der Lösung bilden zwar die Anlagen I und II, jedoch erhalten diese erst durch die Kommissionsentscheidung rechtliche Gültigkeit.¹⁹¹

Die Kommissionsentscheidung 2000/520/EG setzt auf Art 25 Abs 6 der EG-DSRL auf, welche der Kommission den Auftrag erteilt, Verhandlungen zu führen, mit deren Hilfe bisher als unsicher geltende Drittstaaten ein angemessenes Schutzniveau erreichen sollten.¹⁹²

3.3 Inhalt des Safe-Harbor Modells

Die Safe-Harbor Lösung ermöglicht es unbürokratisch und rechtlich zulässig personenbezogene Daten aus der EU in die USA zu exportieren. Es ändert grundsätzlich nichts am Status der USA als unsicheres Drittland. Es wird jedoch davon ausgegangen, dass Organisationen, die sich eindeutig und öffentlich dazu verpflichten, die Grundsätze des sicheren Hafens und die im Anhang enthaltenen „Frequently asked Questions“ (FAQ) einzuhalten, ein angemessenes Schutzniveau für die Übermittlung von Daten aus der EU erreichen.¹⁹³ Zusätzlich zu dieser Verpflichtung muss der Datenempfänger den gesetzlichen Befugnissen einer in Anhang VII der Entscheidung aufgeführten staatlichen Einrichtung unterliegen, die bei Nichteinhalten des Modells Beschwerden zu prüfen hat.¹⁹⁴

Festzuhalten ist, dass sich die Entscheidung jedoch nur auf die Angemessenheit des Schutzniveaus bezieht.¹⁹⁵ Daher bleiben andere Bestimmungen über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten innerhalb der Mitgliedstaaten unberührt.¹⁹⁶

Das heißt: Werden die oben genannten Voraussetzungen eingehalten, darf der Datenexporteur ohne weitere Garantien abgeben zu müssen, personenbezogene Daten aus der EU transferieren, wie es auch in Mitgliedstaaten erlaubt ist. Dies ist vor allem im Interesse der US-Datenverarbeiter, da sich diese nicht mehr auf die Gültigkeit von Ausnahmeregelungen verlassen müssen.¹⁹⁷

¹⁹⁰ Vgl. Genz, 130.

¹⁹¹ Ebd.

¹⁹² Ebd.

¹⁹³ Vgl. SH-E, Art 1 Abs 1.

¹⁹⁴ Vgl. SH-E, Art 1 Abs 2.

¹⁹⁵ Vgl. SH-E, Art 2.

¹⁹⁶ Ebd.

¹⁹⁷ Vgl. SH-E Anhang I, Vorwort.

3.4 Safe-Harbor-Grundsätze

Die Safe-Harbor-Grundsätze bilden den Anhang I der Entscheidung 2000/520/EG und sollen bei der Verarbeitung personenbezogener Daten europäischen Ursprungs in den USA die Anwendung von Datenschutzprinzipien mit angemessenem Schutzniveau sicherstellen.¹⁹⁸ Sie richten sich an die Organisationen, die am Safe-Harbor-Programm teilnehmen möchten. Die meisten Grundsätze sind der EG-DSRL entnommen, worauf im Folgenden jeweils hingewiesen wird.¹⁹⁹

3.4.1 Informationspflicht

In erster Linie sind Privatpersonen darüber zu informieren, zu welchem Zweck Daten erhoben und verwendet werden.²⁰⁰ Weiters ist klarzustellen, wie die Organisation bei Beschwerden kontaktiert werden kann, an wen die Daten weitergegeben werden und wie die Verwendung und Weitergabe der Daten eingeschränkt werden kann.²⁰¹ Diese Informationen sind dem Betroffenen unmissverständlich und deutlich bekannt zu geben, bevor zum ersten Mal Daten erhoben werden, wenn die Daten zu einem anderen als den ursprünglich angegebenen Zweck verwendet werden und auf jeden Fall, bevor Daten erstmals an Dritte (ausgenommen sind Dritte, die im Auftrag oder auf Anweisung der Organisation handeln)²⁰² weitergegeben werden.²⁰³

Die Informationspflicht stellt einen essentiellen Kernpunkt europäischen Datenschutzrechts dar, der in der EG-DSRL in den Abschnitten 10 bis 17 verankert ist.²⁰⁴

3.4.2 Wahlmöglichkeit

Bei der Wahlmöglichkeit wird grundsätzlich zwischen „Opt-out“ und „Opt-in“ unterschieden. Unter „Opt-out“ wird eine generelle Erlaubnis verstanden, bis diese explizit durch den Betroffenen aufgehoben wird. „Opt-in“ bezeichnet ein generelles Verbot, das durch den Betroffenen explizit aufgehoben werden kann.²⁰⁵

Die Betroffenen müssen eine leicht erkennbare Wahlmöglichkeit (zumindest „Opt-out“) haben, ob ihre personenbezogenen Daten an Dritte (ausgenommen sind Dritte, die im Auftrag oder auf Anweisung der Organisation handeln) weitergegeben werden dürfen und ob die Daten für einen anderen Zweck als ursprünglich vereinbart verwendet werden dürfen. Bei sensiblen Daten ist sogar eine ausdrückliche Zustimmung („Opt-in“) notwendig. Unter sensible Daten fallen 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.²⁰⁶

¹⁹⁸ Ebd.

¹⁹⁹ Genz, 134.

²⁰⁰ Vgl. SH-E, Anhang I: INFORMATIONSPFLICHT.

²⁰¹ Ebd.

²⁰² Details dazu folgen unter 3.4.3 Weitergabe.

²⁰³ Vgl. SH-E, Anhang I: INFORMATIONSPFLICHT.

²⁰⁴ Vgl. Genz, 135.

²⁰⁵ Vgl. Genz, 137.

²⁰⁶ Vgl. SH-E, Anhang I: WAHLMÖGLICHKEIT.

Dieses Prinzip findet sich in Art 7 der EG-DSRL, jedoch mit der zwingend notwendigen Einholung einer Einwilligung („Opt-in“).²⁰⁷

3.4.3 Weitergabe

Der Grundsatz der Weitergabe schützt personenbezogene Daten, wenn diese an Dritte weitergegeben werden, die im Auftrag oder auf Anweisung der Organisation tätig sind.²⁰⁸ Unter diesen Umständen finden nämlich die Grundsätze „Informationspflicht“ und „Wahlmöglichkeit“ keine Anwendung. Aus diesem Grund erlaubt der Grundsatz der Weitergabe einen solchen Datentransfer nur, wenn der Dritte, an den die Daten weitergegeben werden,

- dem sicheren Hafen angehört oder der Richtlinie unterliegt,
- von einer anderen Feststellung angemessenen Schutzniveaus erfasst wird (gilt aktuell für Unternehmen in Argentinien, Kanada, die Schweiz, Guernsey, Jersey, Färöer, Israel und auf der Isle of Man)²⁰⁹
- oder sich vertraglich zur Einhaltung der Safe-Harbor-Grundsätze verpflichtet hat.²¹⁰

Diese Vorschrift soll verhindern, dass personenbezogene Daten den sicheren Hafen verlassen, wodurch der Schutz dieser Daten nicht mehr gewährleistet wäre.²¹¹

3.4.4 Sicherheit

Der Grundsatz der Sicherheit besagt, dass jede Organisation, die personenbezogene Daten erstellt, verwaltet, verwendet oder verarbeitet, für die Sicherheit der Daten verantwortlich ist.²¹² Das heißt: Die Daten sind angemessen vor Verlust, Missbrauch, Zerstörung und auch vor unbefugtem Zugriff, unbefugter Weitergabe und Änderung zu schützen.²¹³

In der Europäischen Datenschutzrichtlinie spiegelt sich dieser Grundsatz in Art 16 und 17 wieder.²¹⁴

3.4.5 Datenintegrität

Unter dem Prinzip der Datenintegrität wird die Verpflichtung des qualifizierten Datenverarbeiters verstanden, die Daten für den vorgesehenen Zweck zuverlässig genau, vollständig und aktuell zu halten. Dadurch wird auch untersagt, personenbezogene Daten für einen anderen Zweck zu verwenden, wenn dieser mit dem ursprünglichen Erhebungszweck unvereinbar ist, auch wenn der Betroffene nachträglich zugestimmt hat.²¹⁵

²⁰⁷ Ebd.

²⁰⁸ Vgl. SH-E, Anhang I: WEITERGABE.

²⁰⁹ Vgl. <http://ec.europa.eu/justice/policies/privacy/thridcountries/>.

²¹⁰ Vgl. SH-E, Anhang I: WEITERGABE.

²¹¹ Vgl. Genz, 138.

²¹² Vgl. SH-E, Anhang I: SICHERHEIT.

²¹³ Ebd.

²¹⁴ Vgl. Genz, 139

²¹⁵ Vgl. SH-E, Anhang I: DATENINTEGRITÄT.

Das Prinzip der Datenintegrität ist in Art 6 EG-DSRL zu finden.²¹⁶

3.4.6 Auskunftsrecht

Eine Organisation, die personenbezogene Daten speichert, muss dem Betroffenen die Möglichkeit geben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind.²¹⁷ Allerdings gilt dies nur, wenn die Kosten der Korrektur bzw. der Einsichtnahme in angemessenem Verhältnis zu dem drohenden Nachteil stehen.²¹⁸ Dies ist im Einzelfall abzuwiegen. Laut FAQ 8 kann sogar die Erhebung einer angemessenen Gebühr für die Abfrage bzw. Änderung zulässig sein, um die Kosten zu decken.²¹⁹

Unklar bleibt einerseits jedoch, ob der Betroffene bei fehlerhaften Informationen auf Löschung des gesamten Datensatzes bestehen kann oder nur auf Beseitigung der fehlerhaften Information, andererseits auch, ob der Betroffene die Löschung vollständig korrekter Angaben veranlassen kann.²²⁰

Das Auskunftsrecht korreliert u. a. mit Art 6 EG-DSRL.²²¹

3.4.7 Durchsetzung

Der Durchsetzungsgrundsatz fordert Mechanismen, die

- die Einhaltung der Safe-Harbor-Grundsätze gewährleisten,
- im Fall von Verstößen Rechtsbehelfe für Betroffene vorsehen
- für Sanktionierung der Organisationen, die gegen die Grundsätze verstoßen haben, sorgen.²²²

Konkret müssen die qualifizierten Datenverarbeiter leicht zugängliche, erschwingliche und unabhängige Prüfungsverfahren ermöglichen, die Beschwerden behandeln und gegebenenfalls Betroffenen zu Schadenersatz verhelfen.²²³ Weiters müssen die Safe-Harbor-Teilnehmer Kontrollmaßnahmen durchführen, die sicherstellen, dass ihre Angaben in Bezug auf ihre Datenschutzmaßnahmen richtig sind und diese auch wie angegeben durchgeführt werden.²²⁴ Schließlich sind ausreichend strenge Sanktionen durch die Organisationen selbst vorgesehen, um die Einhaltung der Grundsätze sicherzustellen.²²⁵

Fragwürdig ist, warum auch die Kontroll- und Sanktionsmechanismen den Daten verarbeitenden Stellen selbst zugeschrieben werden. Diese sollten besser in der Verantwortung des Staates liegen, damit die korrekte Durchsetzung auch tatsächlich gewährleistet wird.²²⁶

²¹⁶ Vgl. Genz, 139

²¹⁷ Vgl. SH-E, Anhang 1: AUSKUNFTSRECHT.

²¹⁸ Ebd.

²¹⁹ Vgl. SH-E, Anhang II: FAQ 8, F6

²²⁰ Vgl. Genz, 140.

²²¹ Ebd.

²²² Vgl. SH-E, Anhang I: DURCHSETZUNG.

²²³ Ebd.

²²⁴ Ebd.

²²⁵ Ebd.

²²⁶ Vgl. Genz, 141.

3.5 Häufig gestellte Fragen „FAQ“

Die FAQ bilden Anhang II der SH-E, bestehen aus 15 Fragen mit den dazugehörigen Antworten und richten sich, wie auch die Grundsätze, direkt an die qualifizierten Datenverarbeiter. Sie sind ebenso bedeutend, da sie die oft sehr allgemein formulierten Grundsätze konkretisieren und wichtige Datenschutzfragen diskutieren. Ein bestimmtes System oder ein zwingend konkreter Bezug auf die Grundsätze ist nicht zu finden.²²⁷

Folgende Themen werden von den FAQ behandelt:²²⁸

FAQ 1 – Sensible Daten

FAQ 2 – Ausnahmen für den journalistischen Bereich

FAQ 3 – Hilfsweise Haftung

FAQ 4 – Investmentbanken und Wirtschaftsprüfer

FAQ 5 – Die Rollen der Datenschutzbehörden

FAQ 6 – Selbstzertifizierung

FAQ 7 – Anlassunabhängige Kontrolle

FAQ 8 – Auskunftsrecht

FAQ 9 – Personaldaten

FAQ 10 – Datenverarbeitung im Auftrag

FAQ 11 – Schiedsverfahren und Durchsetzungsprinzip

FAQ 12 – Wahlmöglichkeit – Zeitpunkt des Widerspruchs

FAQ 13 – Zeitpunkt des Widerspruchs

FAQ 14 – Arzneimittel und Medizinprodukte

FAQ 15 – Daten aus öffentlichen Registern und öffentliche zugängliche Daten

3.6 Teilnahme am Safe-Harbor Modell

Um unlimitiert Daten aus der EU empfangen zu dürfen, muss eine Organisation die Grundsätze des sicheren Hafens verbindlich anerkennen und offiziell am Safe-Harbor-Programm teilnehmen. Die Qualifikation erfolgt durch Selbstzertifizierung.²²⁹

Dazu ist die Vorlage eines Schreibens an das US-Handelsministerium bzw. eine von diesem benannte Stelle notwendig, in dem sich die Organisation eindeutig und öffentlich dazu verpflichtet, die Grundsätze und die FAQ einzuhalten.²³⁰ Die ITA führt eine öffentliche Liste²³¹ aller Teilnehmer, die auch die Zertifizierungsschreiben

²²⁷ Vgl. Genz, 142.

²²⁸ Vgl. SH-E, Anhang II

²²⁹ Vgl. SH-E, Anhang II: FAQ 6.

²³⁰ Ebd.

²³¹ Abrufbar unter <https://safeharbor.export.gov/list.aspx>.

enthält.²³² Diese Erklärung muss neben den Kontaktdaten folgende Informationen enthalten:

- Tätigkeit im Zusammenhang mit personenbezogenen Daten aus der EU
- Öffentliche Einsichtmöglichkeit der Datenschutz-Geschäftsbedingungen
- Datum des Inkrafttretens der Datenschutzvorkehrungen
- Kontaktstelle für die Bearbeitung von Beschwerden
- die Aufsichtsbehörde, die über Beschwerden gegen die Organisation entscheidungsbefugt ist (kann die FTC oder das US-Verkehrsministerium sein)
- Bezeichnung aller Datenschutzprogramme, an denen die Organisation teilnimmt
- die Art der anlassunabhängigen Kontrolle (intern oder extern)
- das unabhängige Schiedsverfahren zur Behandlung ungelöster Beschwerdefälle.²³³

Bei der Wahl des unabhängigen Schiedsverfahrens werden den Teilnehmern drei Möglichkeiten geboten: Zum einen kann ein von der Privatwirtschaft entwickeltes Datenschutzprogramm befolgt werden, das die Grundsätze des sicheren Hafens beinhaltet.²³⁴ Unter anderem stehen die folgenden Programme zur Verfügung:²³⁵

- BBBOnline
- TRUSTe
- Direct Marketing Association Safe Harbor Program
- Entertainment Software Rating Board Privacy Online EU Safe Harbor Programme
- Judicial Arbitration and Mediation Service (JAMS)
- American Arbitration Association

Zweitens kann sich der Safe-Harbor-Teilnehmer gesetzlich oder durch Rechtsverordnung vorgesehenen Kontrollorganen unterwerfen, die Beschwerden von Einzelpersonen nachgehen und Streitigkeiten schlichten.²³⁶ Als dritte Variante kann das Unternehmen einer Kooperation mit den europäischen Datenschutzbehörden zustimmen.²³⁷

Mit dem Tag der Selbstzertifizierung ist die Organisation offiziell Safe-Harbor-Teilnehmer und darf ab sofort personenbezogene Daten aus der EU importieren.²³⁸ Die Zertifizierung muss jährlich durch ein Zertifizierungsschreiben erneu-

²³² Vgl. SH-E, Anhang II: FAQ 6.

²³³ Ebd.

²³⁴ Vgl. SH-E, Anhang II: FAQ 11.

²³⁵ Vgl. www.bfdi.bund.de/DE/EuropaUndInternationales/Art29Gruppe/Artikel/SafeHarbor.html.

²³⁶ Vgl. SH-E, Anhang II: FAQ 11.

²³⁷ Ebd.

²³⁸ Vgl. SH-E, Anhang II: FAQ 6.

ert werden.²³⁹ Kommt eine Organisation dieser Pflicht nicht nach, verliert sie ihren Status als sicherer Hafen.²⁴⁰

Scheidet eine Organisation aus dem Programm aus, ist sie weiterhin verpflichtet, alle europäischen Daten, die sie während ihrer Safe-Harbor-Mitgliedschaft gesammelt hat, auch weiterhin zeitlich unbegrenzt unter der Berücksichtigung der Grundsätze zu behandeln.²⁴¹

Die folgende Abbildung zeigt ein Beispiel einer Safe-Harbor-Zertifizierung, die am 12. Mai 2011 aus der offiziellen Teilnehmerliste heruntergeladen wurde.

Organization Information:

Top Ten Global Publishing
182 Howard St., Ste. 645
San Francisco, California- 94105
Phone: (415) 869-8849
Fax: (415) 869-8849
<http://www.toptenglobal.com>

Organization Contact:

Contact Office: Privacy Matters c/o Top Ten Global, Inc.
Name: ,
Phone: (415) 869-8849
Fax: (415) 869-8849
Email: privacy@toptenglobal.com

Corporate Officer:

Corporate Officer: Marcus Ledergerber , Co-Founder, CIO
Phone: (415) 869-8849
Fax: (415) 869-8849
Email: marcus.ledergerber@toptenglobal.com

Safe Harbor Information:

Original Certification: 2/7/2007
Next Certification: 2/7/2010

Personal Information Received from the EU/EEA and/or Switzerland:
Review upon submission, published at the option of individual. Personal information is used to process customers' orders and to provide related services.

Privacy Policy Effective: 2/6/2007

Location: <http://www.toptenglobal.com/privacy.html>

²³⁹ Ebd.

²⁴⁰ Ebd.

²⁴¹ Vgl. SH-E, Anhang II: FAQ 6.

Regulated By: Federal Trade Commission

Privacy Programs:
Top Ten Global Publishing Privacy Program

Verification: In-house

Dispute Resolution:
Compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; JAMS' International Mediation Services

Personal Data Covered: off-line, on-line
Organization Human Resource Data Covered: No
Do You Agree to Cooperate and Comply with the EU and/or Swiss Data Protection Authorities? Yes

Relevant Countries from which Personal Information is Received:
Austria, Denmark, Germany, Greece, Ireland, Liechtenstein, Luxembourg, Netherlands, Sweden, United Kingdom

Industry Sectors:

Certification Status: Current
Compliance Status:

Abbildung 2: Beispiel einer Zertifizierung.

Quelle: <http://safeharbor.export.gov/companyinfo.aspx?id=7756> (12.5.2011)

3.7 Sanktionen

3.7.1 Verbraucherrechte bei Verstoß gegen das Modell

Konsumenten können bei Verstößen gegen die Grundsätze gegen den Datenverarbeiter Beschwerde oder auch zivilrechtliche Klage einreichen um gegebenenfalls Entschädigung zu erhalten.²⁴² Zeigt sich der beschuldigte Datenverarbeiter nicht kooperativ, kann der Betroffene eine zuständige Streitschlichtungsstelle konsultieren, die sich mit der Beschwerde befassen muss.

Schließlich können sich die Betroffenen an die nationale Datenschutzbehörde wenden. In Österreich ist dies die Datenschutzkommission, in Deutschland der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.²⁴³

Diese Sanktionsmöglichkeiten dienen in erster Linie natürlich dazu, Verbraucher zu schützen und zu entschädigen, in zweiter Linie sollen dadurch präventiv Verstöße durch die Organisationen verhindert werden.

3.7.2 Sanktionen der Streitschlichtungsstellen und der FTC

Theoretisch droht laut FAQ 11 Unternehmen, die sich Safe-Harbor unterworfen und trotzdem gegen die Grundsätze verstoßen haben, eine Reihe von Sanktionen:

Neben den bereits erwähnten Schadenersatzzahlungen kann die zuständige Streitschlichtungsstelle nach eigenem Ermessen den Verstoß öffentlich bekanntmachen, die Löschung der betreffenden Daten anordnen oder auch vorübergehend oder dauerhaft die Zuständigkeit für die Streitschlichtung abgeben.²⁴⁴ Während diese

²⁴² Ebd.

²⁴³ Vgl. www.bfdi.bund.de/DE/EuropaUndInternationales/Art29Gruppe/Artikel/SafeHarbor.html.

²⁴⁴ Vgl. SH-E, Anhang II FAQ11: Rechtsbehelfe und Sanktionen.

Maßnahmen vergleichsweise mild sind, steht der FTC ein strengeres Sanktionsmaß zur Verfügung:

Bei Verdacht eines Verstoßes gegen das Verbot unlauterer und irreführender Geschäftspraktiken kann sie eine behördliche Anordnung erwirken, die solche Handlungen untersagt, oder auch vor einem Bezirksgericht klagen.²⁴⁵ Gegen die Missachtung der behördlichen Unterlassungsanordnung kann die FTC Geldstrafen verhängen, gegen die Missachtung der Anordnung eines Bundesgerichts kann sie zivil- und strafrechtlich vorgehen.²⁴⁶

Werden die Grundsätze fortgesetzt verletzt, kann die Organisation ihren Status im Sicheren Hafen und die damit verbundenen Privilegien verlieren.²⁴⁷

3.8 Ausnahmen

Zum einen findet das Safe-Harbor Modell keine Anwendung auf Datentransfers, die von der gesamten EG-DSRL ausgenommen sind (siehe Kapitel 2.1.2.11).

Weiters sind für das Verbot der Übermittlung personenbezogener Daten in Drittländer im Speziellen in Art 26 Abs 1 der EG-DSRL mehrere Ausnahmen vorgesehen, wovon einige hervorzuheben sind:

Der Datentransfer ist auch in unsichere Drittländer zulässig, wenn

1. die betroffene Person zweifelsfrei ihre Zustimmung erteilt hat,
2. wenn die Übermittlung zur Erfüllung eines Vertrages zwischen dem Datenimporteur und dem Betroffenen oder einem Dritten im Interesse des Betroffenen notwendig ist,
3. die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist oder
4. die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist.²⁴⁸

Schließlich gibt es eine Reihe von Branchen, auf die das Safe-Harbor-Programm keine Anwendung findet.²⁴⁹ Die Ursache dafür ist, dass diese nicht unter die Befugnisse der FTC im Hinblick auf unfaire und irreführende Handlungen fallen.²⁵⁰ Aus diesem Grund hätte die FTC im Fall eines Verstoßes keine Sanktionsmöglichkeiten gegen Unternehmen dieser Branchen, wodurch eine Safe-Harbor-Teilnahme zwecklos wäre. Davon betroffene Organisationen müssen daher eine der Alternativen (siehe Kapitel 3.10) in Anspruch nehmen, um ein angemessenes Schutzniveau sicherzustellen. Davon betroffen sind:

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

²⁴⁵ Vgl. SH-E Anhang II FAQ11: Befassung der FTC.

²⁴⁶ Ebd.

²⁴⁷ Vgl. SH-E Anhang II FAQ11: Fortgesetzte Missachtung der Grundsätze.

²⁴⁸ Vgl. EG-DSRL Art 26 Abs 1 a), b) und c).

²⁴⁹ Vgl. SH-E Abs 6.

²⁵⁰ Vgl. SH-E, Anhang III, Ausnahmeregelungen des Abschnitts 5.

- Betreiber öffentlicher Telekommunikationsnetze und zwischenstaatlich tätige Transportunternehmen,
- Luftverkehrsunternehmen sowie
- Vieh- und Fleischhändler bzw. Fleischwarenproduzenten.²⁵¹

Versicherungsgesellschaften fallen grundsätzlich ebenfalls nicht unter die Verantwortung der FTC, davon ausgenommen sind Unternehmen, die zusätzlich zum Versicherungsgeschäft andere Tätigkeiten durchführen.²⁵²

Diese Ausnahmen geben viel Spielraum, Daten rechtmäßig unabhängig vom Schutzniveau des Zielstaates zu übertragen.²⁵³ Ist beispielsweise eine Zustimmung in den AGB eines Onlineportals eine eindeutige Zustimmung zur Übermittlung der Daten? Wie ist „im Interesse des Betroffenen“ auszulegen?

3.9 Bedeutung der Safe-Harbor Lösung

Das Safe-Harbor Modell hat auf Grund seiner komplexen Struktur eine unterschiedliche Auswirkung in Europa und den USA. Grundsätzlich wird gemäß EG-DSRL Art 25 ein Staat in seiner Gesamtheit bewertet, ob er ein angemessenes Schutzniveau bietet oder nicht. Durch die Einführung der Safe-Harbor-Lösung wird entscheidend davon abgewichen, indem eine unternehmensbezogene Regelung umgesetzt wurde. Dadurch ergeben sich enorme Probleme bei der Bestimmung der rechtlichen Bedeutung sowohl in Europa als auch den USA.

3.9.1 Bedeutung in Europa

In Europa ist vor allem die Kommissionsentscheidung 2000/520/EG von Bedeutung, da durch diese qualifizierten Unternehmen die Erfüllung eines angemessenen Schutzniveaus zugesprochen wird.²⁵⁴ Mitgliedsstaaten müssen demnach „die aufgrund der Feststellung der Kommission gebotenen Maßnahmen“ treffen. Entscheidend ist daher die rechtliche Bindung der Entscheidung, ungehinderten Datenverkehr zwischen den Stellen der EU und den selbstzertifizierten US-Organisationen sicherzustellen.²⁵⁵ Formal besteht diese wegen Art 25 Abs 6 Satz 2 EG-DSRL zwar nicht, jedoch hat die Entscheidung rechtspraktisch aufgrund der Rechtsprechung des Gerichtshofs über die Bindungswirkung einer Entscheidung der Kommission und auch wegen des erforderlichen „effet utile“ (Effizienzgebot; nützliche, praktische Wirkung) mehr als nur indizierende Wirkung.²⁵⁶

Den Anhängen kommt in Europa keine eigenständige Bedeutung zu.²⁵⁷

²⁵¹ Ebd.

²⁵² Vgl. SH-E, Anhang VII.

²⁵³ Vgl. Genz, 22.

²⁵⁴ Genz, 156.

²⁵⁵ Ebd.

²⁵⁶ Ebd.

²⁵⁷ Ebd.

3.9.2 Bedeutung in den USA

In den USA ist Safe-Harbor vor allem für gewerbliche Datenverarbeiter von Bedeutung, die sich freiwillig den Prinzipien unterwerfen können.²⁵⁸ Für diese ist also in Form einer unternehmerischen Entscheidung abzuwiegen, ob sie den freien transatlantischen Datenverkehr nutzen wollen oder nicht.²⁵⁹

Weiters ist die Regelung für das US-Handelsministerium von Bedeutung, da dieses für die Verwaltung und Registrierung der Selbstzertifizierungen verantwortlich ist. Dabei beschränken sich die Tätigkeiten bei der Registrierung nur auf die Prüfung der Vollständigkeit der Unterlagen, inhaltlich und qualitativ sind keine Untersuchungen vorgesehen.²⁶⁰

Schließlich sind die FTC und das Verkehrsministerium betroffen, da diese für die Überwachung der Einhaltung verantwortlich sind.²⁶¹ Dabei greifen sie jedoch auf bestehende Befugnisse zurück, weshalb keine neue Ermächtigungsgrundlage notwendig ist.²⁶²

3.10 Alternativen zu Safe-Harbor

Für die Sicherstellung eines angemessenen Schutzniveaus, das für Übertragungen personenbezogener Daten in unsichere Drittstaaten notwendig ist, gibt es neben der Teilnahme am Safe-Harbor zwei weitere Möglichkeiten, nämlich die Verwendung von Standard-Vertragsklauseln sowie die Erstellung von sogenannten Binding Corporate Rules.²⁶³

3.10.1 Standard-Vertragsklauseln

Mit Hilfe von Standardvertragsklauseln kann für Unternehmen außerhalb der EU ein angemessenes Sicherheitsniveau sichergestellt werden, unabhängig davon, in welchem Land sich das Unternehmen befindet.²⁶⁴ Sie regeln die Rechte und Pflichten der Parteien beim Umgang mit personenbezogenen Daten und müssen unverändert übernommen werden.²⁶⁵ Abhängig von der Rolle des Datenimporteurs wird zwischen zwei Arten von Standardvertragsklauseln unterschieden: Für Übermittlungen an Auftragsdatenverarbeiter sind Klauseln für controller-processor Verhältnisse zu verwenden, für Transfers an verantwortliche Stellen finden Verträge für controller-controller Verhältnisse Anwendung.²⁶⁶

Standardvertragsklauseln sich relativ leicht umzusetzen, so lange man nur zu wenigen Gesellschaften in Drittländern Daten übermittelt.²⁶⁷ Bei mehreren Datenempfängern oder mehreren Konzernunternehmen steigt der Aufwand drastisch

²⁵⁸ Genz, 157.

²⁵⁹ Ebd.

²⁶⁰ Vgl. Genz, 157.

²⁶¹ Ebd.

²⁶² Ebd.

²⁶³ <http://www.thomashelbing.com/de/datenschutz-konzern-internationale-datentransfer-teil-2-safe-harbor-bcr-binding-corporate-rules-eu-standardvertragsklauseln>.

²⁶⁴ Ebd.

²⁶⁵ Ebd.

²⁶⁶ Ebd.

²⁶⁷ Ebd.

und das Vertragsnetzwerk wird zunehmend unübersichtlich.²⁶⁸ Erschwerend wirkt sich aus, dass manche Länder in der EU zusätzliche formale Anforderungen bzw. behördliche Zustimmungen verlangen.²⁶⁹

Ein erheblicher Nachteil für das Daten exportierende Unternehmen ist bei der Verwendung von Standardvertragsklauseln, dass sie eine gesamtschuldnerische Haftung der Parteien für Schadensersatzansprüche von Betroffenen bei Vertragsverletzungen vorsehen.²⁷⁰ Dadurch können betroffene Personen unabhängig von der Schadenverursachung wahlweise jede Vertragspartei haftbar machen, wenn ihre Daten missbräuchlich verwendet wurden.²⁷¹

Hinzu kommt, dass der Datenimporteur die Anwendung des im Land des Datenexporteurs geltenden Rechts akzeptiert und die damit verbundenen Untersuchungen durch europäische Datenschutzbehörden zulässt.²⁷² Schließlich erhalten Betroffene das Recht, zivilrechtliche Ansprüche gegen Unternehmen in Drittländern in ihrem Heimatland geltend zu machen.²⁷³

3.10.2 Binding Corporate Rules

Binding Corporate Rules sind ebenso wie Standardvertragsklauseln unabhängig vom Zielland des Datentransfers und sollen für einen gesamten Konzern ein angemessenes Datenschutzniveau sicherstellen, wodurch dieser zu einem sogenannten „Safe Haven“ gemacht wird.²⁷⁴ Es handelt sich dabei um ein rechtsverbindliches Regelwerk, das den Umgang mit personenbezogenen Daten innerhalb eines Unternehmens behandelt.²⁷⁵

BCR sind deutlich flexibler als Standardvertragsklauseln, da sie die individuellen Bedürfnisse des Konzerns berücksichtigen können.²⁷⁶ Außerdem sind sie ein gutes Mittel, um die Datenschutzrichtlinien eines Konzerns weltweit zu vereinheitlichen und dadurch auch zu verbessern.²⁷⁷ Die Einführung von BCR ist jedoch erheblich komplexer als die Verwendung von Standardvertragsklauseln.²⁷⁸ Die verbindlichen Regeln müssen konzernintern abgestimmt und die umfangreichen und detaillierten Vorgaben der EG-DSRL eingehalten werden.²⁷⁹ So müssen unter anderem Prüfungsmechanismen festgelegt werden, die den Umgang mit Beschwerden Betroffener regeln.²⁸⁰ Des Weiteren ist grundsätzlich die Zustimmung der Daten-

²⁶⁸ Ebd.

²⁶⁹ Ebd.

²⁷⁰ Ebd.

²⁷¹ Ebd.

²⁷² Ebd.

²⁷³ Ebd.

²⁷⁴ Vgl. <http://www.thomashelbing.com/de/datenschutz-konzern-internationale-datentransfer-teil-2-safe-harbor-bcr-binding-corporate-rules-eu-standardvertragsklauseln>.

²⁷⁵ Ebd.

²⁷⁶ Ebd.

²⁷⁷ Ebd.

²⁷⁸ Ebd.

²⁷⁹ Ebd.

²⁸⁰ Ebd.

schutzbehörden aller EU-Länder notwendig, in denen Konzernunternehmen ihren Sitz haben.²⁸¹

In Bezug auf die Haftung ziehen BCR folgenschwere Konsequenzen nach sich: Sie beinhalten nämlich die Verantwortung von Konzernteilen in der EU für solche Unternehmen, die sich außerhalb der EU befinden.²⁸² Für die Betroffenen berücksichtigen BCR, die von der EU als angemessen akzeptiert werden, ähnlich wie die Standardvertragsklauseln umfangreiche unmittelbare Rechte.²⁸³

Die Dauer, der Aufwand und damit auch die Kosten einer solchen Einführung sind nicht zu unterschätzen, daher ist eine Umsetzung nur mittelfristig realistisch und es werden oft Standardvertragsklauseln zumindest zur Überbrückung eingesetzt.²⁸⁴

3.11 Kritik der Artikel 29 – Datenschutzgruppe

Die Artikel 29 – Datenschutzgruppe ist ein unabhängiges Gremium zum Schutz von Personen bei der Verarbeitung personenbezogener Daten, das in Art. 29 der EG-DSRL vorgesehen und von der EK eingesetzt wurde.²⁸⁵ Die Gruppe setzt sich aus Vertretern der Datenschutzkontrollstellen der Mitgliedsstaaten (in Österreich die Datenschutzkommission), dem Europäischen Datenschutzbeauftragten sowie aus einem Kommissionsmitglied zusammen.²⁸⁶

Zu ihren Aufgaben zählen:²⁸⁷

- Die fachliche Beratung der Europäischen Kommission;
- die Förderung der einheitlichen Anwendung der EG-DSRL;
- die Beratung der EK zu allen EG-Rechtsvorschriften, die sich auf den Schutz personenbezogener Daten auswirken

Die Arbeitsgruppe hat die Verhandlung des Safe-Harbor-Programms verfolgt und regelmäßig Gutachten erstellt, deren Ergebnisse in das Regelwerk eingearbeitet wurden. Die folgenden Mängel, die in der letzten Review **vor der Unterzeichnung** des Modells vorgelegt wurden, fanden **keine Berücksichtigung** mehr.

3.11.1 Übertragung von Personaldaten

FAQ 9 der Entscheidung über das Safe-Harbor Modell befasst sich mit der Anwendung der Grundsätze auf Personaldaten, die in die USA exportiert werden.²⁸⁸

In der Antwort der ersten Frage aus FAQ 9 wird die Gültigkeit auf Personaldaten wie folgt eingeschränkt: „Die Grundsätze des sicheren Hafens gelten nur für die Übermittlung von und den Zugriff auf Daten über **identifizierte Einzelpersonen**.“²⁸⁹

²⁸¹ Ebd.

²⁸² Ebd.

²⁸³ Ebd.

²⁸⁴ Ebd.

²⁸⁵ Vgl. <http://www.edps.europa.eu/EDPSWEB/edps/lang/de/Cooperation/Art29>.

²⁸⁶ Ebd.

²⁸⁷ Ebd.

²⁸⁸ Vgl. WP 32, 4.

²⁸⁹ Ebd.

In der EG-DSRL sind personenbezogene Daten jedoch als „*Daten über eine bestimmte oder bestimmbare (direkt oder indirekt identifizierbar)*“ definiert.²⁹⁰ Da sich daraus die Gefahr ergeben könnte, dass im Safe-Harbor Modell nicht alle erforderlichen Datenkategorien berücksichtigt werden, hielt es die Gruppe für notwendig diese Definition auch in FAQ 9 anzuwenden.²⁹¹

3.11.2 Recht auf Löschung

Weiters wird der Umfang des Rechts auf Löschung personenbezogener Daten kritisiert. Dieses gilt gemäß dem Safe-Harbor-Grundsatz „Auskunftsrecht“ nämlich nur, wenn erhobene Daten nicht korrekt sind.²⁹² Die Datenschutzgruppe verlangte die Ausweitung auf einen Anspruch betroffener Personen, Daten auch dann löschen zu lassen, wenn diese ohne Zustimmung des Betroffenen oder auf eine Art und Weise, die gegen die Grundsätze verstößt, erhoben oder verarbeitet wurden.²⁹³

3.11.3 Wahlmöglichkeit

In Bezug auf die Wahlmöglichkeit wird bemängelt, dass diese nur für Betroffene gilt, deren personenbezogene Daten für einen Zweck verwendet werden, der mit dem ursprünglichen Erhebungszweck unvereinbar ist.²⁹⁴ Es wurde verlangt, dass dieser Grundsatz für alle vom ursprünglichen Zweck abweichenden Nutzungen gelten sollte.²⁹⁵

3.11.4 Durchsetzung

Die Gruppe hob die Wichtigkeit des Rechts auf Anhörung durch eine unabhängige Instanz im Falle einer Verletzung der Privatsphäre als Grundrecht hervor.²⁹⁶ Im Fall des Safe-Harbor Modells wurden große Zweifel daran geäußert, wie dieses Grundrecht bei Verletzung der Grundsätze gewährleistet werden könnte.²⁹⁷

Es kann sich zwar jeder Betroffene direkt an die FTC wenden, es gibt jedoch keine Garantie, dass diese den Fall tatsächlich prüft, da dies in ihrem freien Ermessen liegt.²⁹⁸ Daher hätte der Einzelne nicht das ausdrückliche Recht auf Anhörung vor der FTC, weder zum Zwecke der Durchsetzung der Entscheidung, noch um solche Entscheidungen (oder das Fehlen von Entscheidungen) anzufechten.²⁹⁹

Aus diesem Grund sieht die Gruppe eine unzureichende Umsetzung des Durchsetzungsgrundsatzes bezüglich zwei der drei Bedingungen aus der Arbeitsunterlage WP 22 (siehe Kapitel 2.1.2.10): „Unterstützung und Hilfe für einzelne betroffene

²⁹⁰ Ebd.

²⁹¹ Ebd.

²⁹² Vgl. WP 32, 6.

²⁹³ Ebd.

²⁹⁴ Ebd.

²⁹⁵ Ebd.

²⁹⁶ Vgl. WP 32, 7.

²⁹⁷ Ebd.

²⁹⁸ Ebd.

²⁹⁹ Ebd.

Personen“ und „Gewährleistung angemessener Entschädigung für die geschädigte Partei bei Verstoß gegen die Bestimmungen“.³⁰⁰

3.11.5 Fazit

Abschließend ist festzuhalten, dass die Artikel 29-Datenschutzgruppe das Safe-Harbor Modell für ein „**noch nicht funktionsfähiges System**“ hielt.³⁰¹ Sie begrüßte aus diesem Grund die Überprüfungsklausel, die eine Feststellung der Angemessenheit des Schutzniveaus im Laufe der Zeit ermöglicht.³⁰² Abschließend legte die Gruppe besonderen Wert auf die Einführung von Mechanismen zur Überprüfung der Entscheidung sowie auf weitere Schutzmechanismen.³⁰³

³⁰⁰ Vgl. WP 32, 8.

³⁰¹ Ebd.

³⁰² Ebd.

³⁰³ Vgl. WP 32, 9.

4 GRUNDLAGEN DER SELBSTREGULIERUNG

Das Safe-Harbor Modell ist eine Sonderform der Selbstregulierung. Während in der klassischen Form die Vorschriften von den Teilnehmern selbst erstellt werden, sind diese beim Safe-Harbor-Framework von der EK und der FTC verhandelt worden. Entscheidend ist, dass die Teilnahme auf freiwilliger Basis erfolgt.

Dieses Kapitel beschreibt die Voraussetzungen für eine funktionierende Selbstregulierung und prüft die Anwendung im Safe-Harbor Modell.

4.1 Anforderungen an die Regeldurchsetzung

4.1.1 Anreiz zur Regeleinhaltung

Selbstregulierung ist nur dann erfolgreich, wenn auch sichergestellt ist, dass die Adressaten die Vorschriften in der Praxis befolgen.³⁰⁴ Es muss daher einen Anreiz zu regelkonformem Verhalten geben.³⁰⁵ Die Zielgruppe muss den Zielen emotional zustimmen oder die Regeln müssen von einer echten moralischen Überzeugung getragen sein, auch wenn die Vorschrift im Einzelfall für den Teilnehmer ungünstig ist.³⁰⁶ Allerdings bilden der Eigennutzen und eine positive Kosten-Nutzenanalyse neben der Akzeptanz den stärksten Handlungsantrieb.³⁰⁷ Ist die generelle Regelakzeptanz dagegen sehr niedrig, rückt die drohende Sanktionierung einer Regelverletzung in den Mittelpunkt.³⁰⁸

Im Hinblick auf das Safe-Harbor Modell besteht ein großer Anreiz, sich den vorgegebenen Regeln zu widersetzen. Da personenbezogene Daten immer mehr an Wert für das personalisierte Marketing gewinnen, können diese teuer weiterverkauft werden. Erhobene personenbezogene Daten dürfen nur an Dritte weitergegeben werden, wenn der Betroffene ausdrücklich darüber informiert wird. Um leichter große Mengen an Daten zu sammeln, besteht daher für die Dienstbetreiber der Anreiz, falsche Informationen über die Datenverarbeitung zu machen.

Auch die emotionale Zustimmung zu den aufgestellten Regeln hält sich in Grenzen, da erstens Datenschutz in den USA keine so bedeutende Rolle spielt wie in Europa und zweitens das Modell nicht US-Bürger, sondern ausschließlich Konsumenten aus der EU betrifft. Safe-Harbor muss daher als ein Einsatzgebiet der Selbstregulierung gewertet werden, in dem die Notwendigkeit der Sanktionierung besonders hoch ist.

³⁰⁴ Vgl. Buck-Heeb, 290.

³⁰⁵ Ebd.

³⁰⁶ Ebd.

³⁰⁷ Ebd.

³⁰⁸ Ebd.

4.1.2 Regelkontrolle als Voraussetzung für eine effektive Regeldurchsetzung

Eine effektive Regeldurchsetzung setzt im Vorfeld eine ausreichende Regelkontrolle voraus.³⁰⁹ Deshalb zielt der Gesetzgeber dort, wo eine Selbstregulierung zugelassen ist, darauf ab, dass nicht nur eine Regel vorhanden ist, die inhaltlich einer gesetzlichen Bestimmung entspricht, sondern auch ein wirksamer Kontrollmechanismus besteht.³¹⁰

Die Anforderungen, die das Selbstregulierungsgremium zu erfüllen hat, hängen vom Umfang der staatlichen Einflussnahme ab.³¹¹ Je stärker die Einflussnahme des Staats ist, desto eher wird dieser die Überwachung der Regeleinhaltung übernehmen.³¹² Wenn die Selbstregulierung eine gesetzliche Lösung ersetzen soll, liegt die Kontrolle ganz bei der Selbstregulierungsorganisation.³¹³ Kann diese die Regelüberwachung nicht sicherstellen, besteht die Gefahr des Versagens des Selbstregulierungskonzeptes.³¹⁴

Der Erfolg der Selbstregulierung hängt u.a. auch davon ab, ob und inwiefern der Einzelne verpflichtet ist, bei einer Kontrolle mitzuwirken und z.B. Auskünfte gegenüber der Kontrollstelle zu erteilen.³¹⁵ Grundsätzlich kann die private Selbstregulierungsorganisation keine Zeugen laden, so dass es zur Aufdeckung eines Regelverstößes der Mitwirkung der Beteiligten bedarf.³¹⁶

Da wirksame Kontrolle regelmäßigen Einsatz finanzieller Mittel erfordert, ist zu klären, wer diese Kosten zu tragen³¹⁷ hat. Dies können die Mitglieder der jeweiligen Selbstregulierungsinstanz oder die von der Selbstregulierung Betroffenen sein.³¹⁸

Die Safe-Harbor Lösung ist von den USA initiiert worden um eine gesetzliche Lösung zu vermeiden. Die Prüfung der Regeleinhaltung ist zwar im Rahmen von anlassunabhängigen Kontrollen festgeschrieben, die Verantwortung dafür wurde jedoch den Teilnehmern selbst überlassen. Diese können die Kontrolle entweder selbst durchführen oder Drittorganisationen damit beauftragen, wobei in jedem Fall erhebliches Missbrauchspotenzial besteht.

Die Kosten der Kontrolle tragen die teilnehmenden Unternehmen, da sie entweder in firmeninterne Reviews investieren oder für die externen Kontrollen aufkommen müssen. Es besteht dadurch die Gefahr, dass Teilnehmer dazu motiviert werden, diese Kosten zu sparen und keine sinnvollen Kontrollen durchzuführen.

³⁰⁹ Ebd.

³¹⁰ Ebd.

³¹¹ Vgl. Buck-Heeb, 291.

³¹² Ebd.

³¹³ Ebd.

³¹⁴ Ebd.

³¹⁵ Vgl. Buck-Heeb, 291.

³¹⁶ Ebd.

³¹⁷ Ebd.

³¹⁸ Ebd.

4.1.3 Sanktionsmechanismen zur Durchsetzung der Regeln

In der Praxis ist häufig festzustellen, dass Sanktionen im Bereich der Selbstregulierung sehr zurückhaltend ausfallen.³¹⁹ Sehr oft wird im Wesentlichen auf den gesellschaftlichen Verruf als Folge eines Verstoßes abgestellt.³²⁰ In manchen Regelwerken sind dennoch unmittelbare Sanktionen vorgesehen, wobei die Verletzung der Vorschriften in einem eigens geregelten Verfahren festgestellt und geahndet wird.³²¹

4.1.3.1 Private Sanktionierung

Der Erfolg privater Regeldurchsetzung zeigt sich in der steigenden Relevanz verschiedener Formen alternativer Streitbeilegung, wie beispielsweise der Schiedsgerichtbarkeit und der Mediation.³²² Die Annahme, allein der Staat sei aufgrund seines Gewaltmonopols in der Lage, Vorschriften effektiv durchzusetzen, wird durch diese Mechanismen widerlegt, die in manchen Gebieten sogar effektiver als staatliche Zwangsvollstreckung sind.³²³

Eine effektive Form privater Regeldurchsetzung ist das Prinzip des „naming and shaming“.³²⁴ Es basiert darauf, den Regelbrecher beim Namen zu nennen und zu veröffentlichen, wodurch dieser soziale oder wirtschaftliche Schäden erleiden soll. Als Beispiel kann man sich ein Abkommen in einer Branche vorstellen, die sich zum Ziel gesetzt hat, keine Produkte aus Kinderarbeit zu vertreiben.³²⁵ Verstößt ein Teilnehmer gegen die Vereinbarung, kann es nach Veröffentlichung des Regelbruches dazu führen, dass Kunden nicht mehr bei diesem Unternehmen kaufen und dadurch erhebliche Umsatzeinbußen verursachen.³²⁶ Diese Art der Sanktion verliert nur ihre Wirkung, wenn der Staat die Veröffentlichung für unzulässig erklärt.³²⁷

Beim Safe-Harbor Modell wird dieses Prinzip kaum angewendet. Streitschlichtungsstellen hätten zwar die Möglichkeit, Verstöße zu veröffentlichen, haben es bisher jedoch nicht getan, vermutlich vor allem wegen der wirtschaftlichen Abhängigkeit von den Safe-Harbor-Teilnehmern. Die FTC publiziert zwar ihre Sanktionen gegen Unternehmen, dies ist jedoch erst zwei Mal vorgekommen und außerdem haben diese Informationen in Europa kaum die breite Öffentlichkeit erreicht. Das Problem hierbei ist unter anderem, dass Konsumenten in der EU kaum wissen, was das Safe-Harbor Modell überhaupt ist.

4.1.3.2 Staatlich-private Sanktionierung

Die Kombination aus privaten und staatlichen Mechanismen kann eine effektive Variante zur Durchsetzung eines Selbstregulierungskonzepts sein. Ein erfolgreiches Beispiel dafür ist das in Deutschland angewandte, sogenannte Enforcement-

³¹⁹ Vgl. Buck-Heeb, 292.

³²⁰ Ebd.

³²¹ Ebd.

³²² Vgl. Buck-Heeb, 293.

³²³ Ebd.

³²⁴ Vgl. Buck-Heeb, 294.

³²⁵ Ebd.

³²⁶ Ebd.

³²⁷ Ebd.

Verfahren im Bereich der Rechnungslegung, eine externe, zweistufig angelegte Kontrolle von Unternehmensabschlüssen.³²⁸

In erster Instanz kontrolliert ein privatrechtlich organisierter Verein, die Deutsche Prüfstelle für Rechnungslegung.³²⁹ Sollte die privatrechtliche Prüfung nicht funktionieren, da das zu prüfende Unternehmen nicht kooperiert oder das Ergebnis anzweifelt, übernimmt als zweite Instanz die Bundesanstalt für Finanzdienstleistungsaufsicht den Fall, die eine Prüfung verbindlich anordnen und mit hoheitlichen Kompetenzen durchsetzen kann.³³⁰

Ein solches System ist bei der Durchsetzung des Safe-Harbor Modells zumindest bei der Streitschlichtung vorgesehen. Allerdings scheitert die erfolgreiche Durchsetzung an den zuständigen Stellen, da diese offensichtlich nicht die notwendigen Maßnahmen treffen. Ursachen dafür werden in einem späteren Kapitel behandelt.

4.1.3.3 Staatliche Sanktionierung

Wenn private Maßnahmen alleine nicht ausreichen und ein unmittelbarer körperlicher Zwang zur Durchsetzung der Regeln erforderlich wird, ist man auf staatliche Hilfe angewiesen.³³¹ Wegen des hoheitlichen Gewaltmonopols ist es Privaten grundsätzlich (mit geringfügigen Ausnahmen) verboten, zur Selbsthilfe zu greifen.³³² Vertragliche Ansprüche wie Entschädigungszahlungen, Herausgabe einer Sache oder die Erwirkung von Handlungen und Unterlassungen müssen daher auf dem Weg der staatlichen Zwangsvollstreckung durchgesetzt werden.³³³

Staatliche Sanktionen sind im Safe-Harbor Modell zwar durch die FTC und das DOC vorgesehen, jedoch erst, nachdem das gegen die Regeln verstoßende Unternehmen zumindest einmal unmittelbar aufgefordert wurde, die regelwidrigen Handlungen zu unterlassen.

4.2 Risiken der Selbstregulierung

4.2.1 Defizite bei der Durchsetzung

Die härteste Kritik muss sich das Prinzip der Selbstregulierung dahingehend gefallen lassen, dass die Vorschriften oftmals unzureichend durchsetzbar sind und die interne und externe Überwachung häufig nicht angemessen funktioniert.³³⁴ Es wird daher oft vorgeworfen, dass das System zu sehr auf freiwillige Einhaltung und zu wenig auf Sanktionsmechanismen setzt.³³⁵

Bei staatlicher Regelsetzung besteht der Vorteil, dass der Gesetzgeber die Vorschriften gegenüber jedermann mit öffentlich-rechtlichen Zwangsmitteln durchsetzen kann.³³⁶ In der Selbstregulierung besteht die Durchsetzungsmöglichkeit für

³²⁸ Vgl. Buck-Heeb, 298.

³²⁹ Ebd.

³³⁰ Ebd.

³³¹ Vgl. Buck-Heeb, 298.

³³² Vgl. Buck-Heeb, 299.

³³³ Ebd.

³³⁴ Vgl. Buck-Heeb, 234.

³³⁵ Ebd.

³³⁶ Ebd.

Private nur, wenn diese bei der Regelschaffung vorgesehen wurde.³³⁷ Außerdem können private Kontrollorganisationen keine zwangsweise Durchsuchung vornehmen und Zeugen unter Androhung staatlicher Zwangsmaßnahmen vorladen.³³⁸

Trotz dieser Schwächen sollte nicht darauf vergessen werden, dass die wirtschaftlichen und sozialen Nachteile im Einzelfall für denjenigen, der gegen eine Bestimmung auf Selbstregulierungsbasis verstoßen hat, empfindlicher sein können als gesetzliche Sanktionen und Zwangsmaßnahmen.³³⁹ Im Extremfall kann ein Regelverstoß zum wirtschaftlichen Ruin führen, wenn Partnerunternehmen als Abnehmer oder Lieferanten nicht mehr mit dem Unternehmen, das gegen die Vorschrift verstoßen hat, zusammenarbeiten.³⁴⁰

4.2.2 Mangelnder Rechtsschutz

Ebenfalls bemängelt wird, dass den von Regelverletzungen Betroffenen zu geringe oder keine Rechtsschutzmöglichkeiten eingeräumt werden.³⁴¹ Da die Bestimmungen privatrechtlicher Natur sind, können Verstöße nicht auf öffentlich-rechtlichem Weg durchgesetzt werden, sondern auf zivilrechtlichem, der ein erheblich höheres Kostenrisiko nach sich zieht.³⁴² Aus diesem Grund ist der Rechtsschutz gewöhnlich geringer als bei staatlicher Gesetzgebung.³⁴³ Dieser Mangel kann durch die Einrichtung geeigneter Stellen behoben werden. Im Safe-Harbor Modell war dies durch Streitschlichtungsstellen vorgesehen, die jedoch nicht unabhängig sind, wodurch sich mangelnder Rechtsschutz ergeben hat.

4.2.3 Mittel zur Verhinderung der Gesetzgebung

Selbstregulierung kann unter Umständen auch dazu missbraucht werden, um eine gesetzliche Lösung zu verhindern.³⁴⁴ Unmittelbar nach der Einführung ist der Fokus auf die Umsetzung gerichtet, danach schwindet oft der Enthusiasmus für die Regelung.³⁴⁵ Als Folge könnte dann sowohl die Regeleinhaltung als auch die Kontrolle und die dazugehörige Sanktionierung inkonsequent werden oder völlig versagen. Dies führt dann so lange zu einem unsanktioniertem Zustand, bis das Thema neu zur Diskussion gebracht wird und entweder der Selbstregulierungsmechanismus verschärft oder ein gesetzliches Regelwerk erlassen wird.

Diesen Vorwurf müssen sich auch die für das Safe-Harbor Modell Verantwortlichen gefallen lassen. Das Regelwerk wurde geschaffen, um die Wirtschaftsbeziehungen mit europäischen Unternehmen unbürokratisch aufrechtzuerhalten, ohne die eigene Gesetzeslage anpassen zu müssen. Die Kritikpunkte am Modell, die durch die ersten Reviews aufgedeckt wurden, sind als Anfangsschwierigkeiten abgetan worden und danach ist es für lange Zeit still geworden. Erst nach zehn Jahren ist das Thema wieder aktuell geworden, nachdem eine Studie die völlige Nutzlosigkeit des Modells bewiesen hat.

³³⁷ Ebd.

³³⁸ Ebd.

³³⁹ Vgl. Buck-Heeb, 235.

³⁴⁰ Ebd.

³⁴¹ Vgl. Buck-Heeb, 236.

³⁴² Ebd.

³⁴³ Ebd.

³⁴⁴ Vgl. Buck-Heeb, 238.

³⁴⁵ Ebd.

4.3 Fazit

Ziel dieser Darstellung ist es, aufzuzeigen, dass Selbstregulierung nicht zwangsläufig zum Scheitern verurteilt ist, wie von vielen angenommen. Systeme auf Basis der Selbstregulierung funktionieren oft nicht, weil sie unzureichend durchdacht und mangelhaft umgesetzt sind. Das liegt unter anderem auch daran, dass dieses System oft als Notlösung eingesetzt wird, wenn aus verschiedenen Gründen keine Gesetzeslösung gewollt ist.

Unter der Voraussetzung, dass gute Kontrollmechanismen, die auf den Einsatz Dritter basieren, und greifende Sanktionen eingebunden werden, kann Selbstregulierung auf vielen Gebieten angemessene Stabilität sicherstellen.

5 KRITIK AN DER PRAXIS VON SAFE-HARBOR

5.1 Studien zur praktischen Umsetzung von Safe-Harbor

5.1.1 Prüfung durch die EU 2002

Nachdem die EK im Rahmen der Safe-Harbor Einführung aufgefordert wurde, die Anwendung der Grundsätze genau zu überwachen und regelmäßige Berichte vorzulegen, wurde bereits am 13.02.2002 die erste Review veröffentlicht.³⁴⁶ Darin wurden einige Kritikpunkte festgestellt, die teilweise auf Anfangsschwierigkeiten zurückgeführt wurden.³⁴⁷

In erster Linie wurde bemängelt, dass zahlreiche Unternehmen Datenschutzrichtlinien formuliert haben, die nicht mit den Safe-Harbor Grundsätzen übereinstimmen.³⁴⁸ In weniger als der Hälfte der Datenschutzrichtlinien der Organisationen spiegeln sich tatsächlich alle sieben Grundsätze wider.³⁴⁹ Viele ließen auch sonst jede öffentliche Erklärung über die Einhaltung dieser Grundsätze vermissen.³⁵⁰ Von Seiten des Handelsministeriums und der FTC wurde versichert, dass die Selbstzertifizierung an sich bereits eine öffentliche Bekanntgabe darstellt und als Grundlage für Durchsetzungsmaßnahmen der FTC zur Verhinderung irreführender Handlungen ausreicht.³⁵¹ Während die US-Behörden dem Akt der Selbstzertifizierung mehr Bedeutung beimessen, werden von der EK die Texte des „sicheren Hafens“ als Ganzes betrachtet und wird von den Teilnehmern eine vollständige Berücksichtigung verlangt.³⁵² Die Kommission befürchtet, dass die betroffenen Organisationen sich nicht über die Verpflichtungen, auf die sie sich im Rahmen des Safe-Harbor Modells eingelassen haben, im Klaren sind und diese daher auch nicht vollständig einhalten.³⁵³ Außerdem wirken sich diese Mängel negativ auf die Transparenz und die Klarheit vor allem gegenüber der Öffentlichkeit aus.³⁵⁴

Mangelnde Transparenz ortete die Kommission auch bei der Anwendung der Vorschriften: So bestand in vielen Fällen Unklarheit darüber, wie Konsumenten ihre Rechte in Bezug auf die Daten einfordern können, die ein Safe-Harbor Teilnehmer über sie gesammelt hat.³⁵⁵ Viele Organisationen gaben zum Beispiel an, dass bei der Speicherung sensibler Daten die Zustimmung des Betroffenen eingeholt wird, die wenigsten definierten jedoch, welche Daten als sensibel gelten. Außerdem informierte nur die Hälfte der Organisationen Konsumenten über die Regelungen, die für die Einreichung von Beschwerden bei unabhängigen Behörden gelten.³⁵⁶ Für Verwirrung sorgten auch Unternehmen, die mehrere Datenschutzrichtlinien angewandt haben, beispielsweise getrennte Policies für Daten, die in den USA ge-

³⁴⁶ Vgl. SEK(2002) 196, 2.

³⁴⁷ Vgl. SEK(2002) 196, 3.

³⁴⁸ Vgl. SEK(2002) 196, 9f.

³⁴⁹ Ebd.

³⁵⁰ Ebd.

³⁵¹ Ebd.

³⁵² Ebd.

³⁵³ Ebd.

³⁵⁴ Ebd.

³⁵⁵ Ebd.

³⁵⁶ Ebd.

sammelt wurden und für Daten, die in der EU erhoben wurden.³⁵⁷ Wenn auch diese Praxis nicht verboten ist, führt sie im Allgemeinen dazu, dass Konsumenten nicht wissen, welche Vorschriften für die Verarbeitung ihrer Daten gelten und wie sie ihre legitimen Rechte einfordern können.³⁵⁸

Die Ergebnisse dieser Review wurden von der Kommission an die US-amerikanischen Behörden weitergeben, um auf diesem Weg Verbesserungsmaßnahmen einzuleiten.³⁵⁹

5.1.2 Prüfung durch die EU 2004

Im Jahr 2004 wurde eine weitere Studie von der EK in Auftrag gegeben, die weitere Mängel aufgezeigt hat.

5.1.2.1 Allgemeine Probleme

Diese Studie wirft zunächst einige grundlegende Probleme auf, die zu Schwierigkeiten führen können. Beispielsweise wurde bisher von den US-Gerichten nicht bestätigt, ob die FTC tatsächlich die Gewalt hat, gegen Vergehen am Datenschutz vorzugehen.³⁶⁰ Während einige Verletzungen mit Sicherheit als unlautere Geschäftspraktiken gewertet werden können, gäbe es viele Graubereiche.³⁶¹ Außerdem bestehe berechtigter Zweifel daran, ob die FTC auch gegen Datenschutzverletzungen vorgehen kann, die personenbezogene Daten betreffen, die zu nicht-kommerziellen Zwecken erhoben wurden.³⁶² Ein weiterer Kritikpunkt sind Unterschiede in der Definition personenbezogener Daten zwischen dem Safe-Harbor Modell und der EG-DSRL, wodurch möglicherweise einige Datenkategorien nicht unter Safe-Harbor fallen obwohl sie von der EG-DSRL erfasst werden.³⁶³ Konkret wird die Frage aufgeworfen, was man unter „anonymisierten“ und „pseudonymisierten“ Daten versteht.³⁶⁴

5.1.2.2 Beteiligte Behörden

Hinsichtlich der beteiligten Behörden stellte die Studie fest, dass es bisher weder auf amerikanischer Seite durch die FTC noch in Europa durch das Data Protection Authority Panel Durchsetzungsmaßnahmen gegeben hat.³⁶⁵ Im Hinblick auf die US-Gerichte, die ebenfalls eine Anlaufstelle für Betroffene sein können, wurde festgestellt, dass diese nur in bestimmten Fällen erfolgreich sanktionieren können und Prozesse auf Grund des sehr hohen Kostenrisikos in Datenschutzfragen für gewöhnlich nicht leistbar sind.³⁶⁶

³⁵⁷ Vgl. SEK(2002) 196, 9f.

³⁵⁸ Ebd.

³⁵⁹ Vgl. SEK(2002) 196, 13.

³⁶⁰ Vgl. Crid, 14.

³⁶¹ Ebd.

³⁶² Vgl. Crid, 15.

³⁶³ Vgl. Crid, 16.

³⁶⁴ Ebd.

³⁶⁵ Vgl. Crid, 19.

³⁶⁶ Vgl. Crid, 23.

5.1.2.3 Kontrollmechanismen

In Bezug auf die Kontrollmechanismen wurde erhoben, dass 53% der Unternehmen an keinem Datenschutzprogramm teilnehmen, was jedoch auch nicht vorgeschrieben ist.³⁶⁷ Es wurde auch bezweifelt, ob die vielen ausgewählten Datenschutzprogramme und alternativen Streitschlichtungsstellen tatsächlich geeignet sind, um die Safe-Harbor Grundsätze durchzusetzen.³⁶⁸

Konkret wird dabei aufgezeigt, dass die wenigsten Datenschutzprogramme die folgenden Kriterien von ihren Teilnehmern verlangt haben:³⁶⁹

- Erklärung über die Safe-Harbor-Konformität
- Klare und deutliche Bereitstellung der Wahlmöglichkeit
- Opt-in Wahlmöglichkeit für sensible Daten
- Einholung einer Erklärung über die Verpflichtung der Einhaltung der Safe-Harbor-Grundsätze bei Datenverarbeitungen durch Dritte
- Datenverarbeitung ausschließlich für den Zweck der Erhebung
- Leistbares Auskunftsrecht für die Betroffenen
- Bereitstellen der Möglichkeit, falsche Daten löschen zu lassen

Der Großteil der Streitschlichtungsstellen wies folgende Mängel auf:³⁷⁰

- Unklarheit darüber, ob die Folgen eines Datenschutzvergehens behoben werden müssen
- Unklarheit über Entschädigungen der Betroffenen
- Keine vorgesehenen Sanktionen
- Keine Veröffentlichung der verhängten Sanktionen
- Unklarheit darüber, ob rechtswidrige Datenverarbeitungen eingestellt werden

Es bestehen vor allem Zweifel daran, ob sich im Rahmen der Streitschlichtung Datenschutz- bzw. Safe-Harbor-Experten mit den Fällen befassen.³⁷¹ Weiters haben sich 73% der Teilnehmer zwar bereit erklärt, mit dem europäischen DPA-Panel zu kooperieren, nur ein Bruchteil davon gab jedoch an, die Entscheidungen dieser Einrichtung letztlich auch zu respektieren.³⁷²

5.1.2.4 Datenschutzrichtlinien der teilnehmenden Unternehmen

Von besonders hoher Bedeutung ist die Kritik an den firmeninternen Datenschutzrichtlinien, die für die Zertifizierung verwendet wurden. Diesbezüglich wird kritisiert, dass die Datenschutzrichtlinien vieler Unternehmen sehr schwer zu lesen sind und oft nicht klar erkennbar machen, welche Datenverarbeitung stattfinden

³⁶⁷ Vgl. Crid, 35.

³⁶⁸ Vgl. Crid, 107.

³⁶⁹ Vgl. Crid, 56, 57.

³⁷⁰ Vgl. Crid, 57, 58.

³⁷¹ Ebd.

³⁷² Vgl. Crid, 35, 46.

und welche Risiken damit verbunden sind.³⁷³ Wie auch in der Studie aus dem Jahr 2002 ist man auch hier auf unzureichende Datenschutzrichtlinien gestoßen. Der Grundsatz der Wahlmöglichkeit wurde in vielen Policies nicht eindeutig behandelt oder vollkommen außer Acht gelassen.³⁷⁴ Die Wahlmöglichkeit stellt ein essentielles Kriterium dar um Konsumenten ein Minimum an Einfluss darüber zu sichern, was mit ihren Daten geschieht, denn ohne gute Wahlmöglichkeiten können die Daten fast uneingeschränkt verwendet und weitergegeben werden.³⁷⁵

In Bezug auf das Recht zur Weitergabe der Daten war in den Richtlinien nicht immer klar, was unter „Dritten“ verstanden wird - ob es sich um Partner- oder Tochterunternehmen handelt und ob diese in ausreichendem Einflussbereich des Unternehmens stehen.³⁷⁶ Es besteht die Gefahr, dass bei der Weitergabe Daten den sicheren Hafen verlassen und dadurch EU-Gesetze untergraben werden.³⁷⁷

Auch im Hinblick auf den Grundsatz der Datenintegrität wurden Mängel vorgefunden. Es konnte nicht festgestellt werden, ob die gesammelten Daten tatsächlich für den bestimmten Verwendungszweck relevant sind, da dieser oft nicht klar formuliert oder überhaupt nicht angegeben wurde.³⁷⁸

Schließlich war auch der Grundsatz der Auskunftspflicht unzureichend implementiert, da sich viele Unternehmen auf die Angabe von Kontaktdaten beschränkten oder überhaupt keine Auskunft zu diesem Thema gaben.³⁷⁹ Die Kosten einer Daten-Einsicht bzw. Änderung werden ebenso wie bei der Wahlmöglichkeit generell nicht angegeben.³⁸⁰

5.1.2.5 Safe-Harbor Teilnehmerliste

Bemängelt wurde auch das Fehlen einer Ansicht in der Safe-Harbor Teilnehmerliste, die alle Unternehmen darstellt, die ihre Mitgliedschaft gekündigt haben.³⁸¹ Diese Informationen sind notwendig, da alle Daten, die während der aufrechten Mitgliedschaft gesammelt wurden, auch weiterhin nur unter Berücksichtigung der Grundsätze verarbeitet werden dürfen.³⁸²

Der Bericht hält auch Mängel in der Selbstzertifizierung und in der Durchsetzung fest, auf diese wird im folgenden Kapitel im Detail eingegangen.

³⁷³ Vgl. Crid, 105.

³⁷⁴ Vgl. Crid, 106.

³⁷⁵ Ebd.

³⁷⁶ Ebd.

³⁷⁷ Ebd.

³⁷⁸ Ebd.

³⁷⁹ Ebd.

³⁸⁰ Ebd.

³⁸¹ Vgl. Crid, 47.

³⁸² Ebd.

5.1.3 Studie des Consulting-Unternehmens Galexia

Das australische Consulting-Unternehmen Galexia hat im Dezember 2008 eine Studie publiziert, die sich mit der Umsetzung des Safe-Harbor-Modells beschäftigt. Die Studie beschränkt sich auf die Überprüfung der korrekten Registrierung und der Einhaltung des Grundsatzes 7, die anderen sechs Grundsätze wurden außer Acht gelassen. Trotzdem ist das Ergebnis erschreckend und zeigt in aller Deutlichkeit, welcher dringender Handlungsbedarf besteht.

Am 17. Oktober 2008 wurde die Liste der Safe-Harbor-Teilnehmer abgerufen und enthielt 1597 Einträge, einschließlich Doppelt- und Dreifacheinträgen.³⁸³ Davon wurden 342 Zertifikate bereits vom Handelsministerium als „not current“ gekennzeichnet, 136 weitere Unternehmen haben die Rezertifizierungsfrist verstreichen lassen und müssten ebenfalls als „not current“ markiert sein.³⁸⁴

Nach Bereinigung dieser Meldungen sowie der Mehrfacheinträge bleiben 1109 Unternehmen aktuell zertifiziert, davon halten jedoch nur 348 die wichtigsten Safe-Harbor-Kriterien ein.³⁸⁵ Zahlreiche Teilnehmer verfügen über keine öffentliche Privacy Policy, viele erwähnen in der Policy Safe-Harbor in keiner Weise.³⁸⁶ Ein beträchtlicher Anteil erfüllt die Anforderungen des Grundsatzes 7 nicht, da keine Streitschlichtungsstelle beauftragt wurde, 209 Unternehmen haben Streitschlichtungsstellen gewählt, die nicht leistbar sind.³⁸⁷

Die folgende Tabelle zeigt im Detail, wie die Safe-Harbor-Liste von 1597 Einträgen auf 348 reduziert wurde:

Membership Requirement	Notes	Number of entries	Number of unique entries removed	Total
Organisation is listed.	All organisations listed on 17 October 2008.	1597	0	1597
Unique entry	Removes doubles, triples and the test file	19	19	1578
Collects EU personal information	Removes irrelevant organisations who do not collect any EU personal information	7	7	1571
Listed as current by DOC	Removes organisations listed by the Department of Commerce as 'not current'	342	329	1242
Listed as current by certification renewal date	Removes organisations that failed to renew by 17 October 2008.	477	133	1109

³⁸³ Vgl. Galexia. 7.

³⁸⁴ Ebd.

³⁸⁵ Ebd.

³⁸⁶ Ebd.

³⁸⁷ Ebd.

Website privacy policy is accessible	Removes organisations who claim to have a website privacy policy, but it is unreachable.	175	57	1052
Privacy policy mentions Safe Harbor	Removes organisations who have a public privacy policy but it does not mention the Safe Harbor at all	218	127	925
Privacy policy complies with the enforcement principle	Removes organisations who have a public privacy policy that does not provide information on the selected dispute resolution provider.	587	279	646
Affordable dispute resolution provider.	Removes organisations who have selected AAA or JAMS as their dispute resolution provider in either their certification record or their public privacy policy.	209	107	539
Verified member of TRUSTe dispute resolution.	Removes organisations who have selected TRUSTe as their dispute resolution provider when they are not current members.	29	11	528
Verified member of TRUSTe privacy program	Removes organisations who claim to be members of the TRUSTe privacy program when they are not current members	30	2	526
Verified member of the BBB Safe Harbor program	Removes organisations who claim to be members of the BBB Safe Harbor program when they are not current members.	4	3	523
Dispute resolution provider exists	Removes organisations who have selected BBB Online Privacy as their dispute resolution provider (closed in July 2008)	21	15	508
Privacy program exists	Removes organisations who claim to be members of BBB Online Privacy (closed in July 2008)	31	3	505
No website privacy policy	Removes organisations who require a password or direct contact in order to obtain their privacy policy.	246	151	354
No misleading information	Removes organisations who are using unauthorised Safe Harbor seals or who claim they have been certified by the Department of Commerce or the EU	32	6	348

Tabelle 1: Überprüfung der Safe-Harbor-Teilnehmerliste auf valide Zertifikate

Quelle: Galexia, The US-Safe Harbor - Fact or Fiction, 7

5.1.3.1 Mängel in den Privacy Policies

Da die Privacy Policy die rechtliche Basis für eine Safe-Harbor-Teilnahme darstellt, ist eine ordnungsgemäße Veröffentlichung von höchster Bedeutung.³⁸⁸ Wie aus der folgenden Tabelle ersichtlich wird, haben viele Teilnehmer keine Policy veröffentlicht, den Zugang dazu eingeschränkt oder falsch verlinkt:³⁸⁹

Availability	Number of Organisations
Not Available - Contact Required Requires contact with the organisation, often an email address is supplied or the location requires a password.	246
Not Available - Absent The website does not have a privacy policy or access to the privacy policy is permanently broken. In this study access was attempted using both Internet Explorer and Mozilla Firefox. Searches included home pages, contact sections, "about us", FAQs etc.	175
Available - Findable using search The Department of Commerce self-certification entry was incorrect, but the privacy policy could be found using simple site searches.	208
Available - Accurate link provided Accurately linked or clearly on the home page (includes correcting basic typos).	966

Tabelle 2: Verfügbarkeit von Privacy Policies

Quelle: Galexia, The US-Safe Harbor - Fact or Fiction, 11

Der Großteil der Einträge enthält zwar eine Privacy Policy, deren Qualität jedoch sehr hohen Schwankungen unterliegt.³⁹⁰ Viele Policies sind zwischen einer und drei Zeilen lang und enthalten praktisch keine brauchbaren Informationen für Konsumenten.³⁹¹ Während einige Unternehmen einfach einen Link zur Safe-Harbor-Webseite setzen, begnügen sich andere mit Einträgen wie: „Wir setzen Maßnahmen, die den Safe-Harbor-Anforderungen gerecht werden“.³⁹²

5.1.3.2 Mängel bezüglich Streitschlichtungsstellen

Im Zuge des Safe-Harbor-Grundsatzes 7 – Durchsetzung - muss eine Streitschlichtungsstelle bestimmt werden, an die sich betroffene Konsumenten im Beschwerdefall wenden können.³⁹³ Die wichtigsten Anforderungen an eine Streitschlichtungsstelle sind Unabhängigkeit, Leistbarkeit und die Möglichkeit, wirksame Sanktionen zu setzen.³⁹⁴

³⁸⁸ Vgl. Galexia, 11.

³⁸⁹ Ebd.

³⁹⁰ Vgl. Galexia, 12.

³⁹¹ Ebd.

³⁹² Ebd.

³⁹³ Vgl. Galexia, 13f.

³⁹⁴ Ebd.

209 Teilnehmer wählten die beiden Stellen American Arbitration Association mit einem Stundensatz von 120\$ bis 1.200\$ zuzüglich einer Verwaltungsgebühr von 950\$ und den Judicial Arbitration Mediation Service, der zwischen 350\$ und 800\$ pro Stunde und eine Verwaltungsgebühr von 275\$ verrechnet.³⁹⁵ Keiner der Teilnehmer hat diese Kosten in seiner Privacy Policy angeführt, einige Unternehmen erwähnten lediglich, dass der Konsument die Kosten der Streitschlichtungsstelle mittragen müsse.³⁹⁶

Außerdem gaben beinahe alle Unternehmen, die TRUSTe als Streitschlichtungsstelle gewählt haben an, dies sei eine unabhängige Non-profit-Organisation, was jedoch seit Juli 2008 nicht mehr der Wahrheit entspricht. Andere wiederum gaben Streitschlichtungsstellen an, die überhaupt nicht mehr existieren.³⁹⁷

Die folgende Tabelle gibt eine Übersicht über die Angaben, die Unternehmen in ihren Zertifizierungseinträgen bezüglich Streitschlichtungsstellen gemacht haben:

Dispute Resolution Provider	Number of Organisations	Compliance	Notes
Entry is blank	9	Non compliant	
Entry provides an email address only	2	Non compliant	
AAA	184	Non compliant	The American Arbitration Association (AAA) costs between \$120 and \$1,200 per hour (with a four-hour minimum charge plus a \$950 administration fee).
BBB	106	Confusing	The BBB Safe Harbor program is compliant, but it is often unclear whether an organisation is indicating that it is a member of another BBB program (eg the Reliability program), a former BBB program (e.g. the closed Online Privacy program), or whether they just mean a consumer can take their complaint to a generic BBB office.
BBB EU	37	Compliant	This number is likely to be higher as some organisations that have stated "BBB" will actually belong to the BBB EU program.
BBB Online Privacy	32	Non compliant	This program is closed. This number is likely to be slightly higher as many organisations that have stated "BBB" will actually belong to the BBB Online Privacy program.
DMA	112	Compliant	
EU DPA Panel	870	Compliant	
JAMS	25	Non compliant	The Judicial Arbitration Mediation Service (JAMS) costs \$350 to \$800 per hour (plus a \$275 administration fee).

³⁹⁵ Ebd.

³⁹⁶ Ebd.

³⁹⁷ Ebd.

TRUSTe	61	Confusing	The generic TRUSTe program cannot receive complaints regarding offline data, and may therefore not be suitable in all circumstances. This number is likely to be lower as some organisations have only entered “TRUSTe” on the form without indicating the specific TRUSTe scheme they belong to.
TRUSTe Safe Harbor	110	Confusing	This number is likely to be higher as some organisations have only entered “TRUSTe” on the form without indicating the specific TRUSTe scheme they belong to.

Tabelle 3: Einträge bezüglich Streitschlichtungsstellen

Quelle: Galexia, The US-Safe Harbor - Fact or Fiction, 13

5.1.3.3 Werbung mit ungültigen Zertifikaten

Die Studie hat ergeben, dass 206 Unternehmen auf ihren Webseiten angeben, Mitglied des Safe-Harbor-Programms zu sein, obwohl sie es in Wirklichkeit nicht sind.³⁹⁸ Während in Europa Fehlinformationen dieser Art mit Sicherheit rechtliche Konsequenzen nach sich ziehen würden, gibt es in den USA keine Anzeichen dafür, dass ein Unternehmen wegen eines solchen Verstoßes sanktioniert wurde, obwohl es im Laufe der Jahre hunderte Vergehen gegeben hat.³⁹⁹

Für weitere Verwirrung der Konsumenten sorgen Unternehmen, die angeben vom US-Handelsministerium oder sogar von der EU zertifiziert zu sein, obwohl Safe-Harbor auf Selbstzertifizierung basiert.⁴⁰⁰ Dies führt soweit, dass auf der Webseite mit diversen Logos geworben wird, die zum Teil selbst kreiert wurden. Das folgende offizielle Logo kann von den Teilnehmern als äußeres Zeichen der Selbstzertifizierung an der Webseite angebracht werden:



Abbildung 3: Safe-Harbor-Logo

Quelle: Galexia, The US-Safe Harbor - Fact or Fiction, 10

Dieses wurde auf 26 Webseiten gefunden, wovon aber nur 13 Organisationen tatsächlich Safe-Harbor zertifiziert waren.⁴⁰¹ Die folgenden Logos sind Beispiele für Eigenkreationen, die im Rahmen der Studie gefunden wurden:

³⁹⁸ Vgl. Galexia, 8.

³⁹⁹ Ebd.

⁴⁰⁰ Ebd.

⁴⁰¹ Vgl. Galexia, 10.



Abbildung 4: Ungültiges Logo 1

Quelle: Galexia, The US-Safe Harbor - Fact or Fiction, 10

Hierbei handelt es sich um Eigenkreationen, die das Logo des US-Handelsministeriums enthalten.



Abbildung 5: Ungültiges Logo 2

Quelle: Galexia, The US-Safe Harbor - Fact or Fiction, 10

Eine Safe-Harbor-Policy enthielt das Logo des Handelsministeriums, ohne weitere Erklärungen oder Kommentare.



Abbildung 6: Ungültiges Logo 3

Quelle: Galexia, The US-Safe Harbor - Fact or Fiction, 10

Es besteht ein erhebliches Risiko, dass Konsumenten und Organisationen durch solche Angaben irreführt werden und sich auf sichere Datenbehandlung verlassen, die nicht gegeben ist.⁴⁰²

5.1.3.4 Mitgliedschaft in Bezug auf eingeschränkte Datenkategorien

Auch wenn ein Unternehmen gültig zertifiziert ist, kann es sein, dass sich der Schutz der Daten nur auf ausgewählte Datenkategorien bezieht.⁴⁰³ Eine Information darüber muss nicht unbedingt in der öffentlichen Privacy Policy enthalten sein, ist aber gewöhnlich im Selbstzertifizierungseintrag zu finden.⁴⁰⁴

Von den 348 Unternehmen, die die grundlegendsten Kriterien einhalten, beziehen nur 54 ihre Mitgliedschaft auf alle gesammelten Daten, bezogen auf alle 1.579 Einträge in der Safe-Harbor Liste ergibt das eine magere Quote von 3%.⁴⁰⁵ Die übrigen Teilnehmer beschränken ihre Teilnahme auf ausgewählte Datenkategorien.⁴⁰⁶ Die folgende Tabelle stellt dar, wie oft bestimmte Datenkategorien von Safe-Harbor-

⁴⁰² Vgl. Galexia, 10.

⁴⁰³ Vgl. Galexia, 16.

⁴⁰⁴ Ebd.

⁴⁰⁵ Ebd.

⁴⁰⁶ Ebd.

Teilnehmern miteinbezogen wurden (Unique Selection steht für Unternehmen, die ausschließlich diese eine Kategorie gewählt haben):

Category of Data	Selected	Unique Selection
Human Resources	152	41
Online	294	75
Offline	181	4
Manual	134	2
Other	6	6

Tabelle 4: Datenkategorien

Quelle: Galexia, *The US-Safe Harbor - Fact or Fiction*, 16

5.1.4 Fazit

Zusammenfassend kann man aus den drei Studien folgende Aussage treffen:

- Viele der teilnehmenden Unternehmen haben überhaupt keine Datenschutzrichtlinien veröffentlicht.
- Von den vorhandenen Datenschutzrichtlinien sind viele sehr mangelhaft, die meisten decken nicht alle sieben Grundsätze ab.
- Von den wenigen vollständigen Zertifizierungen beschränken sich viele nur auf ausgewählte Datenkategorien.
- Die Datenschutzprogramme entsprechen nicht den qualitativen Ansprüchen des Safe-Harbor-Regelwerks.
- Die alternativen Streitschlichtungsstellen sorgen für keinen angemessenen Rechtsschutz für die Betroffenen.
- Unternehmen täuschen Konsumenten, indem sie mit ihrer Safe-Harbor Zertifizierung werben, ohne das entsprechende Schutzniveau zu bieten.

5.2 Beispiele für Verstöße zertifizierter Teilnehmer

5.2.1 Verstöße des „social networks“ Facebook

Facebook ist das weltweit größte soziale Netzwerk mit mittlerweile mehr als 750 Millionen Mitgliedern weltweit und knapp 160 Millionen innerhalb Europas. Da das Unternehmen im Wege seiner Userinnen und User personenbezogene Daten in der EU erfasst und diese dann verarbeitet, ist es vom Safe-Harbor Modell betroffen, weshalb sich Facebook zertifiziert hat.⁴⁰⁷ Bezüglich des Umgangs mit Benutzerdaten muss sich Facebook viel Kritik gefallen lassen, viele Beschwerden betreffen Verstöße gegen das Safe-Harbor Modell.

⁴⁰⁷ <http://www.heise.de/newsticker/meldung/Facebook-verstoest-gegen-europaeische-Datenschutzstandards-915756.html>

5.2.1.1 Verarbeitung personenbezogener Daten von Nicht-Teilnehmern

Facebook bietet eine Synchronisationsmöglichkeit für Smartphones, die alle Vornamen, Nachnamen, Telefonnummern, Emailadressen und Geburtsdaten hochlädt und speichert (Friend Finder).⁴⁰⁸ Diese Informationen werden jedoch nicht nur in Form eines Adressbuchs gespeichert, sondern auch für das Verknüpfen neuer Bekanntschaften verarbeitet.⁴⁰⁹ Im Falle der Anmeldung einer Person, bekommt diese gleich eine Liste mit Vorschlägen von möglichen Bekannten, da bereits vor der Teilnahme Daten verarbeitet wurden.⁴¹⁰

Dadurch verstößt Facebook eindeutig gegen die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Datenintegrität. Die betroffene Person wird nämlich nicht darüber informiert, dass sie betreffende personenbezogene Daten verarbeitet werden und sie kann auch die Weitergabe nicht beeinflussen. Außerdem werden die Daten für einen anderen Zweck als den bei der Erhebung angegebenen verwendet, da die Informationen zweckmäßig nur für das Finden von Kontakten mit Hilfe der Emailadresse vorgesehen waren.

5.2.1.2 Zugriff auf fremde Kontakte

Bei der Erstellung eines Facebook-Accounts ist es möglich, eine fremde E-Mailadresse anzugeben, vorausgesetzt, es gibt noch kein Profil mit dieser Adresse. Der Besitzer der Adresse bekommt zwar eine Verständigung über das Anlegen eines Accounts zugeschickt, es ist jedoch keine Bestätigung der Adresse notwendig.⁴¹¹ Man kann sich unmittelbar nach der Registrierung auf dem Portal einloggen und bekommt sofort 20 mögliche Kontakte als Freunde vorgeschlagen.⁴¹² Versuche haben ergeben, dass von diesen 20 Vorschlägen dem Besitzer der E-Mailadresse ca. 18 tatsächlich bekannt sind, obwohl er mit Facebook noch nie etwas zu tun hatte.⁴¹³ Außerdem kann man sich als Besitzer des Profils ausgeben und dem tatsächlichen Eigentümer schaden, bis dieser auf die Willkommensnachricht entsprechend reagiert und bei Facebook interveniert.⁴¹⁴

Diese Möglichkeit stellt einen Verstoß gegen den Grundsatz der Sicherheit dar, da Unbefugten durch bloße Kenntnis der E-Mailadresse der Zugang zu personenbezogenen Daten ermöglicht wird und die Daten daher nicht ausreichend geschützt sind.

5.2.1.3 Zwangsweise Veröffentlichung von Benutzerdaten

2009 Änderte Facebook die Standardeinstellungen für die Sichtbarkeit der Benutzerdaten dahingehend, dass sehr viele Informationen für jedermann zugänglich waren.⁴¹⁵ Außerdem waren Name, Profilfoto, Freunde und Gruppenzugehörigkeiten immer öffentlich sichtbar.⁴¹⁶ Nach großen Benutzer-Protesten wurde 2010 die

⁴⁰⁸ Vgl. <http://de.wikipedia.org/wiki/Facebook>.

⁴⁰⁹ Ebd.

⁴¹⁰ Ebd.

⁴¹¹ <http://www.faz.net/s/Rub594835B672714A1DB1A121534F010EE1/Doc~E5205C93A4508472CB610D9565E72C5BD~ATpl~Ecommon~Scontent.html>.

⁴¹² Ebd.

⁴¹³ Ebd.

⁴¹⁴ Ebd.

⁴¹⁵ Vgl. <http://de.wikipedia.org/wiki/Facebook>.

⁴¹⁶ Ebd.

Möglichkeit geschaffen, diese Sichtbarkeit in den Kontoeinstellungen zu beschränken, jedoch ist die Veröffentlichung des Profilfotos nach wie vor verpflichtend.⁴¹⁷ Diese Praxis verstößt gegen das Prinzip der Wahlmöglichkeit, da dem Benutzer das Recht verwehrt wird, zu entscheiden, an wen seine Daten weitergegeben werden.

5.2.1.4 Weitergabe von Daten an Dritte

Anfang 2011 hat Facebook einen Dienst, der personenbezogene Daten an andere Webseiten weitergibt, auf Europa ausgeweitet.⁴¹⁸ Diese Übertragung findet standardmäßig statt, kann jedoch grundsätzlich vom Benutzer in seinen Kontoeinstellungen deaktiviert werden.⁴¹⁹ Selbst dann können immer noch Daten an Partnerwebseiten weitergegeben werden, falls ein Facebook-Freund diese Option nicht abgeschaltet hat.⁴²⁰ Die Wahrscheinlichkeit, dass tatsächlich alle Freunde die Übertragung an Partner-Sites verbieten, ist äußerst gering, da Facebook diesen Dienst unangekündigt gestartet hat.⁴²¹

Auch dabei handelt es sich um einen Verstoß gegen den Grundsatz der Wahlmöglichkeit, da man keinen ausreichenden Einfluss auf die Kontoeinstellungen seiner Facebook-Freunde hat.

5.2.2 Verstöße des Suchmaschinenbetreibers Google

Google ist der größte Suchmaschinenbetreiber der Welt mit einem Marktanteil von mehr als 80% aller Suchanfragen im Internet.⁴²² Google hat seine Dienste neben der Suchfunktionalität ausgeweitet und bietet unter anderem auch einen Emaildienst, ein soziales Netzwerk (seit 29.6.2011 plus.google.com) und Analysesoftware für Webseitenzugriffe an.

5.2.2.1 Google Buzz

Google Buzz ist eine Social-Network-Plattform, die es unter anderem ermöglicht Statusnachrichten, Fotos und Videos mit anderen Personen auszutauschen.

Als Google diesen Onlinedienst einführte, wurden Benutzer der Google-Emailplattform Gmail beim Login mit den beiden Optionen „Sweet! Check out Buzz“ und „Nah, go to my inbox“ gefragt, ob sie dieses Service nutzen möchten.⁴²³ Selbst wenn man sich dafür entschieden hat, nicht an Google Buzz teilzunehmen, wurden einige Funktionen trotzdem aktiviert.⁴²⁴ Benutzer, die sich für den Dienst entschieden haben, mussten feststellen, dass ihre gespeicherten Email-Kontakte zu anderen Personen zum Allgemeingut wurden.⁴²⁵

Diese Vorgehensweise stellt massive Verstöße gegen die Grundsätze der Wahlmöglichkeit und der Weitergabe dar. Vor allem die Aktivierung einiger Dienste

⁴¹⁷ Vgl. <http://de.wikipedia.org/wiki/Facebook>.

⁴¹⁸ Vgl. <http://www.futurezone.at/stories/1665356>.

⁴¹⁹ Ebd.

⁴²⁰ Vgl. <http://bazonline.ch/digital/internet/Tipps-fuer-mehr-Privatsphaere-in-Facebook/story/10923444>.

⁴²¹ Vgl. <http://www.futurezone.at/stories/1665356/>.

⁴²² Vgl. <http://de.wikipedia.org/wiki/Google>.

⁴²³ Vgl. <http://www.intern.de/internet-news/9052-google-hat-gegen-das-safe-harbor-abkommen-verstossen-muss-datenschutz-audits-ueber-sich-ergehen-lassen.html>.

⁴²⁴ Ebd.

⁴²⁵ Ebd.

trotz der Verneinung durch den Benutzer stellt einen Datenmissbrauch dar, da eine bewusste Täuschung der Anwender stattfindet.

5.2.2.2 Google Analytics

Google Analytics ist eine Analysesoftware, die Betreibern von Webseiten umfangreiche Statistiken über die Zugriffe auf ihre Seite ermöglicht.⁴²⁶ Durch diese Statistiken lassen sich detaillierte Benutzerprofile erstellen.⁴²⁷ Die Software stellt die ermittelten Informationen nicht nur den Seitenbetreibern zur Verfügung, sondern leitet sie auch an Google in die USA weiter.⁴²⁸ Die meisten Informationen, die dabei übermittelt werden, stellen datenschutzrechtlich kein Problem dar.⁴²⁹ Neben dem Surfverhalten der Benutzer wird jedoch auch die vollständige IP-Adresse jedes Zugriffs übermittelt, wodurch die Benutzer unter Umständen auch identifizierbar werden.⁴³⁰

Da IP-Adressen auf direktem Weg nur Geräte identifizieren und nicht Personen, gilt es (vor allem in Ländern wie Deutschland, in denen der Begriff „indirekt personenbezogene Daten“ nicht existiert) als Streitfrage, ob es sich bei IP-Adressen um personenbezogene Daten handelt. In Österreich können IP-Adressen jedenfalls direkt (für den Internet Service Provider, dem die Zuordnung zum Benutzer möglich ist) und indirekt personenbezogene Daten darstellen.⁴³¹ Erst nach Löschung der Zuordnungstabelle durch den Provider handelt es sich um kein personenbezogenes Datum mehr.⁴³²

Das rechtliche Problem in der Verarbeitung dieser Daten liegt nicht in der Einhaltung der Safe-Harbor-Grundsätze, sondern in der Einhaltung geltenden europäischen bzw. nationalen Rechts. Eine Safe-Harbor-Teilnahme des Datenimporteurs alleine genügt nicht, um personenbezogene Daten transferieren zu dürfen.⁴³³ Die Übertragung ist nur dann zulässig, wenn auch die Verarbeitung an sich erlaubt ist.⁴³⁴ Unter der Annahme, dass IP-Adressen unter personenbezogene Daten fallen, ist gemäß EG-DSRL (und damit nach jeweils geltendem, nationalem Recht) eine eindeutige Zustimmung des Betroffenen notwendig.⁴³⁵

Die Zustimmung für die Erhebung personenbezogener Daten muss ausdrücklich vor der Erhebung erfolgen.⁴³⁶ Die gängige Praxis ist, dass beim Betreten der Startseite bereits Daten erhoben werden und man im Impressum oder in den AGB einen Hinweis auf Google Analytics findet. Dieses Vorgehen kann nicht als Einholen einer ausdrücklichen Zustimmung ausgelegt werden.⁴³⁷

⁴²⁶ Vgl. <http://www.akademie.de/programmierung-administration/website-administration/tipps/webmaster-tricks/google-analytics-datenschutz-abmahnung.html>.

⁴²⁷ Ebd.

⁴²⁸ <http://www.sumomag.at/knowhow/medienlandschaft/72-datenschutz-google-analytics.html>.

⁴²⁹ Vgl. <http://www.akademie.de/programmierung-administration/website-administration/tipps/webmaster-tricks/google-analytics-datenschutz-abmahnung.html>.

⁴³⁰ Ebd.

⁴³¹ Vgl. Sonntag, 231.

⁴³² Vgl. Sonntag 232.

⁴³³ Vgl. Knyrim, 470.

⁴³⁴ Ebd.

⁴³⁵ Vgl. EG-DSRL, Art. 7.

⁴³⁶ Vgl. SH-E, INFORMATIONSPFLICHT.

⁴³⁷ Ebd.

Für manche Browser gibt es Erweiterungen, die es ermöglichen, die Weitergabe der IP-Adresse zu unterbinden. Solche Schutzmechanismen sind eher nur erfahrenen Internetbenutzern zuzutrauen und können daher das gesetzliche Verbot nicht „abschwächen“.⁴³⁸

5.2.2.3 Speicherung von Suchanfragen

Der Durchschnitts-Internetbenutzer wird vermutlich glauben, dass bei einer Suchanfrage an Google lediglich der Suchbegriff transferiert und ausgewertet wird und daraufhin die Liste der Ergebnisse übertragen wird. In Wahrheit geschieht im Hintergrund jedoch viel mehr: Es wird nämlich auch die IP-Adresse des Clients mitgesendet und gemeinsam mit allen Suchbegriffen laut Angaben von Google bis zu neun Monate gespeichert.⁴³⁹ Diese Informationen können von Google gemeinsam mit den Daten, die mit Hilfe von Google Analytics erhoben werden, ausgewertet werden. Es gibt seit kurzem zwar die Möglichkeit, das Speichern der Suchhistorie zu unterbinden, jedoch ist den meisten Nutzern nicht klar, welchen Nutzen die Übertragung der Suchanfragengeschichte und der IP-Adresse für den Suchmaschinenbetreiber haben kann.

Da die Speicherung der IP-Adresse weder für die Erbringung des Suchresultats, noch für das Erstellen von anonymen Profilen für zielgruppenorientiertes Marketing notwendig ist, wird dadurch der Grundsatz der Datenintegrität verletzt, demzufolge die erhobenen Daten für den beabsichtigten Verwendungszweck erheblich sein müssen.

5.2.2.4 Speicherung von WLAN-Informationen

Im Rahmen des Google Street View Projekts lässt Google mit Kameras ausgestattete Fahrzeuge durch die Straßen fahren, um Fotos aufzunehmen.⁴⁴⁰ Nebenbei betreiben die Fahrzeuge auch Scanner, die alle WLAN-Netze katalogisieren.⁴⁴¹ Dabei werden die weltweit eindeutigen MAC-Adressen der WLAN-Geräte, die SSID's der WLAN-Netze und Informationen darüber gespeichert, ob das Netzwerk verschlüsselt ist.⁴⁴² Diese Daten werden in Kombination mit der Standortinformation in den USA verarbeitet.⁴⁴³ Mit diesen Daten könnte Google einen öffentlichen WLAN-Katalog erstellen, der Datenmissbrauch erleichtern würde: Während einerseits das „Schwarzsurfen“ erleichtert werde, werden auch unauthorisierte Zugriffe auf Daten in diesen Netzwerken gefördert.⁴⁴⁴

Da die Eigentümer dieser Netzwerke darüber nicht konkret informiert sind und auch keine Möglichkeit haben, diese Aufnahmen zu verhindern, wird dadurch gegen die Grundsätze der Informationspflicht und Wahlmöglichkeit verstoßen.

⁴³⁸ Ebd.

⁴³⁹ Vgl. <http://www.google.com/intl/de/privacy/faq.html>.

⁴⁴⁰ Vgl. <http://www.netzwelt.de/news/82527-datenschutz-google-street-view-speichert-wlan-netze.html>.

⁴⁴¹ Ebd.

⁴⁴² Ebd.

⁴⁴³ Ebd.

⁴⁴⁴ Ebd.

5.3 Ursachen für die Fehlentwicklung

5.3.1 Keine qualitative Eingangsdatenprüfung

Ein bedeutendes Problem in der Handhabung der Safe-Harbor Lösung ist, dass die Selbstzertifizierungen bei der Einreichung nicht auf die Qualität des Inhalts kontrolliert werden. Es wird weder überprüft, ob die Privacy Policy den Safe-Harbor-Grundsätzen entspricht, noch ob eine konforme zuständige Streitschlichtungsstelle angegeben wurde. Dadurch wurde die Entwicklung zu einer praktisch wertlosen Teilnehmerdatenbank, wie sie aktuell existiert, erst möglich. Eine Prüfung der Registrierungen auf einen Mindeststandard würde in jedem Fall das Niveau des Verzeichnisses drastisch heben, auch wenn diese aller Voraussicht nach eine Reduktion der Teilnehmerzahlen auf einen Bruchteil mit sich ziehen würde.

Die Ursache für die mangelnde Überprüfung liegt am deutlich zu geringen Budget.⁴⁴⁵ Das DOC hat für das Safe-Harbor-Programm jährlich nur 190.250 \$ veranschlagt, weshalb nur 550 Arbeitsstunden im Jahr zu Verfügung stehen.⁴⁴⁶ Aus diesem Grund werden in jede Onlineregistrierung lediglich 20 Minuten und in jede Anmeldung in Papierform 40 Minuten für die Beurteilung investiert.⁴⁴⁷

5.3.2 Mangelnde Sanktionen

Eine der Hauptursachen, warum so viele Unternehmen gravierende Mängel in ihren Privacy Policies aufweisen, ist mit Sicherheit die Tatsache, dass sie offensichtlich mit keinen Konsequenzen zu rechnen haben.

Die Privacy Policies stellen die rechtliche Basis für eine Safe-Harbor-Teilnahme dar, denn sie ermöglichen den Vergleich zwischen Datenschutzversprechen und Datenschutzpraktiken.⁴⁴⁸ Ein Unternehmen ist nur dann von der FTC rechtlich verfolgbar, wenn sich Theorie und Praxis der Datenschutzmaßnahmen von einander unterscheiden, also wenn irreführende oder falsche Angaben gemacht werden.⁴⁴⁹ Auch wenn die FTC gegenüber der EK zugesichert hat, dass eine Selbstzertifizierung an sich bereits als Grundlage für Durchsetzungsmaßnahmen der FTC zur Verhinderung irreführender Handlungen ausreicht, sieht die Realität scheinbar anders aus.⁴⁵⁰ Die Praxis hat gezeigt, dass ein Teilnehmer, der trotz Zertifizierung keine Privacy Policy veröffentlicht hat, keine Konsequenzen zu befürchten, da der FTC in diesem Fall jegliche gesetzliche Basis fehlt, um Sanktionen zu setzen.⁴⁵¹ Dieser Umstand motiviert natürlich zahlreiche Unternehmen, sich mit fadenscheinigen Datenschutzrichtlinien zu zertifizieren und auf dieser Basis beliebig Daten aus der EU zu importieren.

Es muss daher entweder dafür Sorge getragen werden, dass die Datenschutzrichtlinien aller Teilnehmer den Safe-Harbor-Grundsätzen vollständig entsprechen, oder dass Unternehmen, die sich mit Richtlinien unter dem Safe-Harbor-Niveau

⁴⁴⁵ Vgl. Leathers, 222.

⁴⁴⁶ Ebd.

⁴⁴⁷ Ebd.

⁴⁴⁸ Vgl. Galexia, 11.

⁴⁴⁹ Ebd.

⁴⁵⁰ Ebd.

⁴⁵¹ Ebd.

zertifiziert haben, tatsächlich wegen irreführender Handlungen wirksam und konsequent sanktioniert werden.

5.3.3 Mangelnde Motivation der US-Behörden

Auf US-amerikanischer Seite hält sich die Motivation in Grenzen, die Durchsetzung des Safe-Harbor Modells zu gewährleisten.⁴⁵² Dafür gibt es zwei Ursachen:

Erstens entspricht die Anzahl der Teilnehmer am Safe-Harbor-Programm bei weitem nicht den Erwartungen, was für große Enttäuschung sorgt.⁴⁵³ Es wurde ursprünglich von 1500 Registrierungen pro Jahr ausgegangen, tatsächlich sind es nach neun Jahren insgesamt nur etwas mehr als 1600, wovon viele der jährlichen Rezertifizierung nicht nachgekommen sind.⁴⁵⁴ Die geringe Teilnehmerzahl wird als geringer Ertrag für die hohen Kosten der Verhandlung und Einrichtung des Modells angesehen.⁴⁵⁵

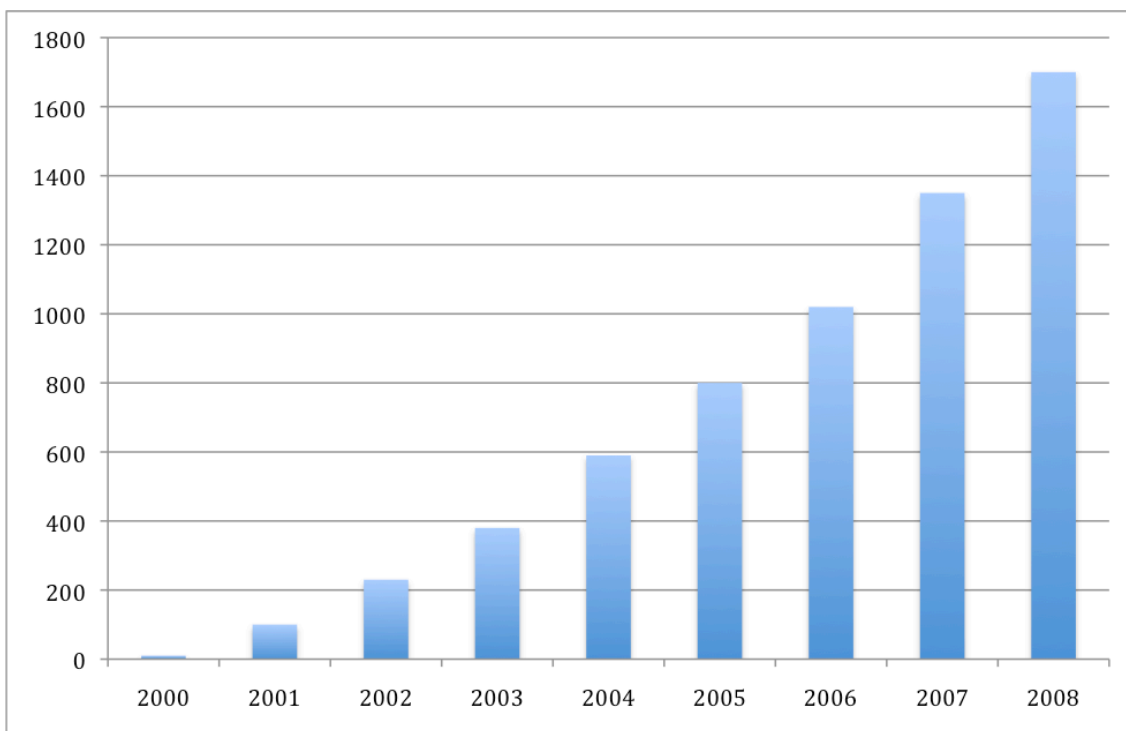


Abbildung 7: Entwicklung der Safe-Harbor Teilnehmerzahl

Quelle: Galexia, *The US-Safe Harbor - Fact or Fiction*, 6

Im März 2005 versuchte das DOC, potenzielle Teilnehmer zu einer Zertifizierung zu motivieren, in dem die Registrierungsgebühr von 150-500 \$ auf einheitlich 50 \$ gesenkt wurde.⁴⁵⁶ Es ist jedoch äußerst unwahrscheinlich, dass diese geringe

⁴⁵² Vgl. Leathers, 222f.

⁴⁵³ Vgl. Leathers, 222f.

⁴⁵⁴ Ebd.

⁴⁵⁵ Ebd.

⁴⁵⁶ Vgl. Leathers, 223f.

Gebühr eine Barriere für millionenschwere Unternehmen dargestellt hat.⁴⁵⁷ Vermutlich wurden auch aus diesem Grund die Gebühren im Jahr 2009 auf 200 \$ pro Registrierung und 100 \$ pro Verlängerung erhöht.⁴⁵⁸

Es scheitert viel mehr am fehlenden Bewusstsein vieler Organisationen, was es mit Safe-Harbor auf sich hat.⁴⁵⁹ Die meisten Unternehmen verzichten aus den folgenden Gründen auf eine Registrierung:⁴⁶⁰

- Unternehmen sehen keine Notwendigkeit, Safe-Harbor beizutreten;
- Zögern der Unternehmensjuristen;
- mangelndes Bewusstsein, mit welchen Maßnahmen begonnen werden muss;
- fehlendes Bewusstsein, welche Vorteile das Programm mit sich bringt.

Der zweite Grund für die Passivität der US-amerikanischen Behörden ist schlicht und einfach der fehlende Anreiz, sich für die Rechte der EU-Bürger einzusetzen.⁴⁶¹ Betroffene in der EU sind gezwungen sich auf Organe zu verlassen, die für sie nicht politisch angreifbar sind und auch sonst keinen Anlass zum Handeln sehen.⁴⁶²

5.3.4 Großer Anreiz, gegen das Modell zu verstoßen

Das Prinzip der Selbstregulierung ist grundsätzlich kein schlechter Ansatz, jedoch ist es nur dann effektiv, wenn es mit Selbstverpflichtung zur Einhaltung von Mindeststandards und konsequenter Sanktionierung im Missbrauchsfall kombiniert wird. Selbstregulierung zielt darauf ab, dass durch Werbung mit guten Datenschutzpraktiken ein Wettbewerbsvorteil erzielt werden kann. Da die meisten Konsumenten dazu tendieren, Sicherheitsrichtlinien nicht im Detail zu lesen und sich auf das Vorhandensein von Gütesiegeln zu verlassen, haben Unternehmen oft bereits durch die bloße Teilnahme an einem Gütesiegelprogramm erheblichen Wettbewerb gewonnen, ohne wirklich Verpflichtungen einzugehen. Diese Tatsache in Verbindung mit dem enormen Ertrag, der durch Verkauf personenbezogener Daten erzielt werden kann, stellt eine große Motivation für Unternehmen dar, ihre unaufmerksamen Kunden zu täuschen.

5.3.5 Mängel im Rahmen der Unabhängigen Schiedsverfahren

5.3.5.1 Fehlende verbindliche Vorschriften im Durchsetzungsgrundsatz

Der Safe-Harbor Durchsetzungsgrundsatz lässt den unabhängigen Schiedsstellen die Freiheit, einen mehr oder weniger willkürlichen Grad an Sanktionen anzuwenden, da es an vorschreibenden Formulierungen mangelt.⁴⁶³ Es macht zwar den Anschein, als gäbe es ausreichend Rechtsbehelfe, diese sind jedoch nur in Soll-Vorschriften verankert und nicht verpflichtend anzuwenden.⁴⁶⁴

⁴⁵⁷ Ebd.

⁴⁵⁸ Vgl. http://www.export.gov/safeharbor/eg_main_020436.asp.

⁴⁵⁹ Ebd.

⁴⁶⁰ Ebd.

⁴⁶¹ Vgl. Leathers, 208.

⁴⁶² Ebd.

⁴⁶³ Vgl. Leathers, 224.

⁴⁶⁴ Ebd.

Beispielsweise „**soll** die Inanspruchnahme eines Rechtsbehelfs 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 den Beschwerdeführer betreffenden Daten künftig entweder im Einklang mit den Grundsätzen des sicheren Hafens schützt oder nicht mehr verarbeitet.“⁴⁶⁵

Es gibt zwar eine Vorschrift, die besagt: „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 im beauftragte Stelle) unterrichten.“, diese kommt jedoch nie zur Anwendung, falls die Streitschlichtungsstelle keine Sanktionen verhängt hat.⁴⁶⁶

Die unabhängigen Schiedsstellen haben daher freies Ermessen und machen die zur Verfügung stehenden Rechtsmittel ineffektiv. Unternehmen, die sich am Safe-Harbor Modell beteiligen, werden dadurch motiviert, sich einer Streitschlichtungsstelle zu unterwerfen, die sehr milde oder überhaupt keine Strafen verhängt.⁴⁶⁷

5.3.5.2 Streitschlichtung durch private Datenschutzprogramme

Neben der Kooperation mit europäischen Datenschutzbehörden kann ein Unternehmen auch durch die Teilnahme an privaten Datenschutzprogrammen oder durch Beauftragung sonstiger privater Schiedsstellen dem Durchsetzungsgrundsatz gerecht werden.⁴⁶⁸ BBBOnline, ein privates Datenschutzprogramm, das u.a. große Unternehmen wie Amazon oder Careerbuilder betreut, die sensible Kundendaten speichern, sieht beispielsweise keine fixen Sanktionen in den Streitschlichtungsrichtlinien⁴⁶⁹ vor.⁴⁷⁰ Ein Klient, der keine angemessenen Datenschutzrichtlinien online stellt oder gegen diese verstößt, hat demnach die Möglichkeit, alternative Maßnahmen einzubringen, um den Verstoß zu korrigieren.⁴⁷¹ Außerdem kann es im Extremfall bis zu sechs Monaten dauern, bis BBBOnline ein Vergehen bei der FTC anzeigt.⁴⁷²

Aktuelle Entwicklungen zeigen, dass immer mehr Safe-Harbor Teilnehmer private Schiedsstellen beauftragen. Streitschlichtung auf Basis des Safe-Harbor Modells fällt definitiv in den internationalen Bereich, weshalb es in die Gesetzgebung der Bundesregierung fällt und daher durch den Federal Arbitration Act geregelt wird.⁴⁷³ Dieser verlangt von den Schiedsstellen nicht, dass sie sich in ihren Entscheidungen an Gesetze halten, was sehr beunruhigend ist.⁴⁷⁴ Hinzu kommt die Tatsache, dass private Streitschlichtungsstellen wirtschaftlich stark von ihren Klienten abhängig sind, weshalb sie dazu neigen, zu deren Gunsten zu entscheiden.⁴⁷⁵

⁴⁶⁵ Vgl. SH-E, Anhang II, FAQ 11.

⁴⁶⁶ Vgl. Leathers, 224; 200/520/EG Anhang II, FAQ 11.

⁴⁶⁷ Vgl. Leathers, 225.

⁴⁶⁸ Vgl. SH-E, Anhang II, FAQ 11.

⁴⁶⁹ Vgl. <http://www.bbbonline.org/privacy/DataPrivacyDRRules.pdf>.

⁴⁷⁰ Vgl. Leathers, 225.

⁴⁷¹ Ebd.

⁴⁷² Ebd.

⁴⁷³ Vgl. Leathers, 226.

⁴⁷⁴ Ebd.

⁴⁷⁵ Ebd.

Es ist daher wenig verwunderlich, dass immer mehr Unternehmen diese Lücke nutzen, um drohenden Sanktionen aus dem Weg zu gehen.

5.3.5.3 Streitschlichtung durch das Unternehmen selbst

Offensichtlich gibt es Unternehmen, die den Durchsetzungsgrundsatz so interpretieren, dass mit der Einrichtung unabhängiger Schiedsstellen auch die firmeninterne Beschwerdeverwaltung gemeint ist.⁴⁷⁶ Die Vorstellung, dass eine Organisation gegen sich gerichtete Beschwerden selbst in Form einer „unabhängigen Streitschlichtungsstelle“ regeln soll ist absurd und ein Widerspruch in sich.⁴⁷⁷ Es liegt daher auf der Hand, dass jedes Unternehmen, das interne Prozesse als unabhängige Schiedsstelle angegeben hat, den Sinn des Safe-Harbor Modells nicht verstanden hat oder die Absicht hat, dieses vorsätzlich zu missbrauchen.⁴⁷⁸

5.3.5.4 Worst-Case Szenario

Diese Lücken im Durchsetzungsgrundsatz ermöglichen das folgende Worst-Case Szenario: Ein Safe-Harbor-Teilnehmer kann sich selbst zertifizieren, ohne eine Datenschutzrichtlinie zu veröffentlichen, in der Hoffnung dass die Registrierung von der Annahmestelle akzeptiert wird, wodurch eine Verfolgung durch die FTC bereits ausgeschlossen ist.⁴⁷⁹ Als anlassunabhängige Kontrolle kann der Teilnehmer interne Mechanismen angeben und daher die Umsetzung der Richtlinie selbst bescheinigen.⁴⁸⁰ Als unabhängige Schiedsstelle kann dieses Unternehmen eine private Streitschlichtungsstelle wählen, die dafür bekannt ist, zu Gunsten des Teilnehmers zu entscheiden.⁴⁸¹ Dadurch wird es für Betroffene sehr schwierig, ihr Recht durchzusetzen und das Unternehmen hat mit keinen Sanktionen zu rechnen.⁴⁸²

5.3.6 Mangelnder internationaler Einfluss der FTC

Bei der Verhandlung des Safe-Harbor Modells ist den europäischen Datenschutzbehörden ein gravierender Fehler unterlaufen.⁴⁸³ Der FTC-Act erlaubt der FTC zwar, den Handel mit anderen Staaten zu regulieren, jedoch nur, wenn nicht ausschließlich Ausländer davon betroffen sind.⁴⁸⁴ Das heißt, die Autorität der FTC erstreckt sich nur auf Fälle, die auch Einfluss auf US-Amerikaner haben.⁴⁸⁵

5.3.7 Eingeschränkte Verpflichtung zu Ermittlungen der FTC

Grundsätzlich erlaubt der FTC-Act der FTC, Untersuchungen im Auftrag des Justizministers, des Präsidenten, des Kongresses, der US-Gerichte, der allgemeinen Öffentlichkeit und im eigenen Auftrag durchzuführen.⁴⁸⁶ Im Fall von Safe-Harbor hat die FTC ihre Befugnisse jedoch selbst eingeschränkt: Betreffend Beschwerden im Zusammenhang mit Safe-Harbor müssen nur Ermittlungsanfragen von den zu-

⁴⁷⁶ Ebd.

⁴⁷⁷ Ebd.

⁴⁷⁸ Ebd.

⁴⁷⁹ Vgl. Leathers, 229.

⁴⁸⁰ Ebd.

⁴⁸¹ Ebd.

⁴⁸² Ebd.

⁴⁸³ Vgl. Leathers, 233.

⁴⁸⁴ Ebd.

⁴⁸⁵ Ebd.

⁴⁸⁶ Vgl. Leathers. 234f.

ständigen Streitschlichtungsstellen angenommen werden.⁴⁸⁷ Selbst im Falle einer solchen Aufforderung einer Streitschlichtungsstelle muss die FTC den Fall nicht zwangsläufig bearbeiten, da im Safe-Harbor Modell lediglich angegeben wird, die FTC wolle Anträge von Selbstregulierungsorganen „priorisieren“.⁴⁸⁸

Das heißt, ein betroffener EU-Bürger hat keinen Anspruch auf Entschädigung, wenn die FTC keine Untersuchungen gegen ein Unternehmen einleitet, selbst wenn die zuständige Streitschlichtungsstelle einen entsprechenden Antrag gestellt hat.⁴⁸⁹

5.3.8 Langwieriges Sanktionsverfahren

Laut FAQ 11 des Safe-Harbor Modells kann die FTC im Fall des Verstoßes eines Unternehmens gegen die Richtlinien als erste Maßnahme eine Abmahnung aussprechen und solche Handlungen untersagen.⁴⁹⁰ Andere Sanktionen sind beim ersten Verstoß nicht vorgesehen, erst bei fortgesetzter Missachtung können weiter reichende Maßnahmen gesetzt werden.

Es stellt sich daher die Frage, welchen Charakter die freiwillige Selbstverpflichtung hat. Grundsätzlich soll die Teilnahme am Modell eine verbindliche Verpflichtung darstellen. Da aber bis zur Abmahnung durch die FTC keine Sanktionen angedroht werden, ist es wenig verwunderlich, wenn Safe-Harbor von den teilnehmenden Unternehmern als Empfehlung verstanden wird. So können sich Teilnehmer, die vorsätzlich gegen die Datenschutzbestimmungen verstoßen, so lange in Sicherheit wiegen, bis ihnen offiziell von der FTC die Nicht-Einhaltung der Richtlinien verboten wird.

Wollte also die FTC wirksam gegen Datenschutzsünder vorgehen, hätte sie mit enormem bürokratischen Aufwand zu kämpfen, da sie gegen jedes betroffene Unternehmen offiziell eine Abmahnung aussprechen müsste.

5.3.9 Mangelnde Transparenz und fehlendes Bewusstsein

Wenn Selbstregulierung im Datenschutzbereich eingesetzt wird, ist es von enormer Bedeutung, dass jeder Verstoß den aktuellen und auch den potentiellen zukünftigen Konsumenten publik gemacht wird. Während diese Maßnahme einerseits den Verletzer des Modells anschwärzen und ihm schaden soll, ist es andererseits noch von viel wichtiger, dass sich Betroffene dadurch schützen können. Verbraucher haben nur dann die Möglichkeit, sich vor „schwarzen Schafen“ zu schützen (beispielsweise durch Meiden der angebotenen Dienste), wenn ihnen diese auch bekannt sind.

Die Anzahl der Unternehmen, gegen die bisher offiziell durch die FTC vorgegangen wurde, hält sich zwar stark in Grenzen, doch auch diese Maßnahmen (siehe 6.1) sind der breiten Öffentlichkeit in Europa überhaupt nicht bekannt. Lediglich datenschutzinteressierte Personen, die sich in einschlägigen Foren und auf Webseiten erkundigen, haben davon gehört oder darüber gelesen.

⁴⁸⁷ Ebd.

⁴⁸⁸ Ebd.

⁴⁸⁹ Ebd.

⁴⁹⁰ Vgl. SH-E, Anhang II, FAQ 9.

Ein größeres Problem ist jedoch das fehlende Bewusstsein über die Risiken, die Datenschutzverletzungen mit sich bringen können. Es hat vermutlich jeder Nutzer des sozialen Netzwerks Facebook in den Medien gehört und gelesen, dass der Betreiber personenbezogene Daten an Dritte weitergibt und dass dadurch identifizierbare Benutzerprofile erstellt werden können. Trotzdem geben Millionen von Benutzern, vor allem Kinder und Jugendliche, aber auch unzählige Erwachsene, private und sensible Informationen preis.

Auch wenn der Großteil der Betroffenen mit Informationen bezüglich Datenschutzverletzungen von US-amerikanischen Organisationen nichts anfangen möchte, ist es dennoch essentiell, dass für die wenigen Interessierten Transparenz geschaffen wird. Es genügt nämlich schon, wenn wenige Betroffene die weiteren Handlungen eines beschuldigten Unternehmens verfolgen und gegebenenfalls die notwendigen Maßnahmen ergreifen.

5.4 Fazit

Diese Untersuchungen zeigen deutlich auf, wie wirkungslos das Safe-Harbor Modell in der praktischen Umsetzung ist, obwohl die Grundsätze des sicheren Hafens an sich geeignet wären, um ihren Zweck zu erfüllen.

- Die Mängel im Durchsetzungsgrundsatz erlauben es Unternehmen, sich mit unzureichenden oder nicht vorhandenen Privacy Policies zu zertifizieren, ohne mit Konsequenzen rechnen zu müssen.
- Konsumenten in der EU werden daher durch Werbung mit dem Safe-Harbor-Zertifikat in die Irre geführt.
- Es gibt praktisch keine greifenden, anlassunabhängigen Kontrollverfahren, die die Umsetzung der Datenschutzrichtlinien überprüfen.
- Dadurch müssen auch Unternehmen, die Safe-Harbor-konforme Datenschutzrichtlinien entwickelt haben, im Falle von Verstößen häufig nicht mit Sanktionen rechnen.
- Betroffenen Personen ist nicht garantiert, dass sie bei Missbrauch ihrer personenbezogenen Daten ihre Rechte durchsetzen können.

Das einzige Ziel, das durch das Safe-Harbor Modell tatsächlich erreicht wurde, ist die Erleichterung und Entbürokratisierung des transatlantischen Datenverkehrs. Dieses Ziel wurde jedoch auf Kosten des Schutzes personenbezogener Daten, der eigentlich die primäre Aufgabe des Modells sein sollte, erreicht.

6 BISHER GETÄTIGTE MAßNAHMEN

Seit dem Bekanntwerden der Studie des Consultingunternehmens Galexia wurden auf unterschiedlichsten Ebenen Maßnahmen getroffen, die das Datenschutzniveau bei Transfers personenbezogener Daten heben sollen. Diese Ansätze werden im Folgenden zusammengefasst.

6.1 Maßnahmen und Initiativen in den USA

6.1.1 Sanktionen durch die FTC wegen ungültiger Zertifizierung

Im Herbst 2009 ist die FTC erstmals gegen sechs Unternehmen vorgegangen, die falsche Angaben über ihre Safe-Harbor-Zertifizierung gemacht haben.⁴⁹¹

In allen sechs Fällen waren die Unternehmen ursprünglich Safe-Harbor registriert, jedoch haben sie die Zertifizierung nicht jährlich erneuert und trotzdem auf ihrer Webseite mit der Safe-Harbor-Teilnahme geworben.⁴⁹² Es wurden keine Untersuchungen bezüglich Verstößen gegen die Grundsätze durchgeführt, es wurde allein auf Grund der falschen Angaben über die Teilnahme reagiert.⁴⁹³ Den betroffenen Unternehmen wurde es untersagt, irreführende Angaben in Bezug auf Safe-Harbor oder andere Gütesiegelprogramme zu machen.⁴⁹⁴ Von Bußgeldern oder sonstigen Strafen musste zwar abgesehen werden, trotzdem wird die Maßnahme als Signal dafür gewertet, dass die FTC künftig aktiver gegen nicht regelkonforme Safe-Harbor-Teilnehmer vorgehen wird.⁴⁹⁵

6.1.1.1 Kritik

Obwohl es einerseits positiv zu sehen ist, dass die FTC die Initiative ergriffen hat, lässt dieses Verfahren, das lediglich mit einer Unterlassungsaufforderung geendet hat, doch eine gewisse abschreckende Wirkung vermissen. Dadurch wird die Frage aufgeworfen, ob durch diese Handhabung Datenschutzsünder, die sich vor Sanktionen sicher gefühlt haben, nicht in ihrem Glauben bestärkt werden. Aufgrund der aktuellen Rechtslage hat die FTC jedoch beim ersten Verstoß keine anderen Mittel, als die unlauteren Praktiken zu untersagen. Erst, wenn gegen die behördliche Unterlassungsanordnung verstoßen wird, können Geldstrafen verhängt werden.⁴⁹⁶ Entscheidend wird sein, wie die FTC in absehbarer Zeit mit vergleichbaren Fällen umgehen wird.

⁴⁹¹ Vgl. <http://www.ftc.gov/opa/2009/10/safeharbor.shtm>.

⁴⁹² Vgl. <http://www.huntonprivacyblog.com/2009/09/articles/enforcement-1/ftcs-first-safe-harbor-enforcement-action>.

⁴⁹³ Ebd.

⁴⁹⁴ Ebd.

⁴⁹⁵ Vgl. <http://www.hldataprotection.com/2009/10/articles/international-compliance-inclu/ftc-settles-safe-harbor-enforcement-actions-with-six-companies/>

⁴⁹⁶ Vgl. SH-E, Anfang II, FAQ 11.

6.1.2 Erstmalige Sanktion der FTC wegen Verstößen gegen Selbstverpflichtung

6.1.2.1 Sanktionen gegen Google

Am 30.3.2011 gab die FTC in einer Aussendung bekannt, dass sie in der Einführung von Googles sozialem Netzwerk „Google Buzz“ einen Verstoß gegen die Safe-Harbor-Richtlinien festgestellt hat.⁴⁹⁷ Die Untersuchung erfolgte aufgrund einer Beschwerde durch das Electronic Privacy Information Center.⁴⁹⁸

Der konkrete Vorwurf lautete, dass Google, ohne die Nutzer zu informieren bzw. ohne Wahlmöglichkeit zu geben, Daten für andere Zwecke verwendet hat, als bei der Erhebung angegeben.⁴⁹⁹

Die FTC traf daher mit Google eine Vereinbarung, die Google zur Einführung eines umfassenden Datenschutzprogramms verpflichtet.⁵⁰⁰ Dieses beinhaltet die Pflicht, für die nächsten 20 Jahre alle zwei Jahre Datenschutz-Audits durch externe Stellen durchführen zu lassen.⁵⁰¹ Weiters verbietet die Vereinbarung, die Safe-Harbor-Richtlinien oder die Auflagen anderer Datenschutzprogramme, an denen Google teilnimmt, zu missachten.⁵⁰² Außerdem wird Google aufgefordert, künftig bei Neueinführungen oder Anpassungen von Diensten das Einverständnis der Nutzer einzuholen, bevor Daten an Dritte weitergegeben werden oder in einer Art und Weise verarbeitet werden, die nicht mit den ursprünglichen Datenschutzbestimmungen im Einklang steht.⁵⁰³

Erwähnenswert ist in diesem Zusammenhang, dass die FTC IP-Adressen ausdrücklich als personenbezogene Daten in die Vereinbarung einbezieht.⁵⁰⁴ Darüber ist in der Vergangenheit viel diskutiert worden.

Es ist dies laut der Aussendung das erste Mal, dass die FTC gegen einen Verstoß gegen das Safe-Harbor Modell vorgeht und auch ein Novum, dass in den USA einem Unternehmen ein verpflichtendes Datenschutzprogramm auferlegt wird.⁵⁰⁵

6.1.2.2 Kritik

Erst eineinhalb Jahre nach dem ersten Einschreiten der FTC im Zusammenhang mit dem Safe-Harbor Modell wurden erneut Maßnahmen gesetzt. Außerdem bleibt offen, welche Auswirkungen diese Abmachung auf Google's Datenschutzpraktiken haben wird. Im Zusammenhang mit dem regelmäßigen Audit bezieht sich das Modell nämlich auf die eigene Policy und nicht auf die Safe-Harbor-Grundsätze.⁵⁰⁶ Details hinsichtlich der Inhalte des Datenschutzprogramms sind der Vereinbarung nur wenige zu entnehmen. Es bleibt daher die Entwicklung abzuwarten.

⁴⁹⁷ Vgl. <http://ftc.gov/opa/2011/03/google.shtm>.

⁴⁹⁸ ebd

⁴⁹⁹ Ebd.

⁵⁰⁰ Ebd.

⁵⁰¹ Ebd.

⁵⁰² Ebd.

⁵⁰³ Ebd.

⁵⁰⁴ Vgl. <http://ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf>.

⁵⁰⁵ Vgl. <http://ftc.gov/opa/2011/03/google.shtm>.

⁵⁰⁶ Vgl. <http://www.intern.de/internet-news/9052-google-hat-gegen-das-safe-harbor-abkommen-verstossen-muss-datenschutz-audits-ueber-sich-ergehen-lassen.html>.

6.1.3 Neue Datenschutzgesetze in den USA

In den USA herrscht aktuell ein großes Umdenken in Datenschutzfragen, als Folge dessen werden in Zukunft gesetzliche Datenschutzregelungen eine viel größere Rolle einnehmen als bisher. Es sind viele Gesetzesvorschläge zum Datenschutz in Arbeit und es wurde ein neuer Senatsunterausschuss für Datenschutz, Technik und Recht eingerichtet.⁵⁰⁷

Die besten Chancen, vom Senat akzeptiert zu werden, hat laut Experten der Entwurf der beiden Senatoren John Kerry und John McCain „The Commercial Privacy Bill of Rights Act of 2011“.⁵⁰⁸ Der Gesetzesentwurf beschränkt sich nicht nur auf Online-Daten, er ist viel mehr als technologieunabhängiges Regelwerk zu verstehen, das ausreichend flexibel ist, um auf Technologieänderungen angepasst zu werden und auch auf Datenverarbeitungen Anwendung zu finden, die offline erfolgen.⁵⁰⁹

Die folgenden Regelungen sind im Entwurf vorgesehen:⁵¹⁰

- **Datensicherheit**
Der Datenverarbeiter ist für die Sicherheit vor unbefugtem Zugriff verantwortlich.
- **Informationspflicht, Wahlmöglichkeit, Rechte auf Zugriff und Korrektur**
Der Sammler der Daten muss eindeutig kennzeichnen, welche Daten zu welchem Zweck gespeichert werden. Es muss weiters eine Opt-out-Möglichkeit für alle Datenkategorien und eine Opt-in-Möglichkeit für sensible Daten geschaffen werden. Außerdem sollen Betroffene das Recht haben, ihre Daten entweder einzusehen und zu korrigieren oder die Einstellung der Verwendung und Weitergabe zu verlangen.
- **Datenintegrität**
Das Sammeln von Daten soll auf ein Minimum beschränkt werden, so dass nur Daten, die zum Zweck der Durchführung des Dienstes notwendig sind, gespeichert werden dürfen. Bei Weitergabe der Informationen an Dritte müssen diese vertraglich dazu verpflichtet werden, die Daten nur in Einklang mit diesem Gesetz zu verarbeiten.
- **Vollziehung**
Für die Durchsetzung sind die Generalstaatsanwälte der Bundesstaaten sowie die FTC verantwortlich, es darf bei der Sanktionierung jedoch zu keinen Kollisionen dieser Behörden kommen. Die Generalstaatsanwälte sollen

⁵⁰⁷ Vgl. <http://www.heise.de/newsticker/meldung/US-Senat-befragt-Apple-und-Google-zu-Datenschutz-1241671.html>.

⁵⁰⁸ Vgl. <http://paidcontent.org/article/419-kerry-mccain-privacy-billopt-outs-are-in-do-not-track-is-out/>.

⁵⁰⁹ Ebd.

⁵¹⁰ Vgl.

<http://kerry.senate.gov/imo/media/doc/Commercial%20Privacy%20Bill%20of%20Rights%20Summary.pdf>.

Bußgeldzahlungen bis zu 3.000.000\$ verhängen können und die FTC bis zu 16.000\$ pro Tag.⁵¹¹

- **Safe-Harbor-Programme**

Das Gesetz soll der FTC auch die Möglichkeit geben, Organisationen zu akkreditieren, die freiwillige Safe-Harbor-Programme überwachen sollen. Diese Programme müssen mindestens so streng wie der Commercial Privacy Bill of Rights Act selbst sein und sollen den Teilnehmern Flexibilität bei der Umsetzung von Datenschutzrichtlinien geben.

6.1.3.1 Kritik

Prinzipiell ist es sehr positiv zu bewerten, dass in den USA Datenschutz vermehrt legislativ geregelt wird. Viele der vorgeschlagenen Datenschutzrichtlinien sind sehr an europäische Grundsätze angelehnt. Sollte dieser Gesetzesentwurf vom Kongress akzeptiert werden, würden die USA wohl trotzdem nicht von der EK als Drittstaat mit angemessenem Schutzniveau angesehen werden, da einige wesentliche Voraussetzungen fehlen, auf die seitens der EU hoher Wert gelegt wird:

Ein großes Manko ist im Bereich des Rechtsschutzes festzustellen. Die Durchsetzung dieses Gesetzes kann nur durch die Generalstaatsanwälte und durch die FTC initiiert werden, es bestehen daher keine Rechtsmittel für betroffene Personen.⁵¹² Dadurch haben von Datenschutzverletzungen Betroffene nicht zwangsläufig die Möglichkeit ihre Datenschutzrechte geltend zu machen. Sie können sich nur darauf verlassen, dass die FTC oder der zuständige Generalstaatsanwalt die Initiative ergreift.

Ein weiteres schwerwiegendes Defizit im vorgelegten Entwurf ist die fehlende Geltung für staatliche Einrichtungen. Die angesprochenen Datenschutzprinzipien richten sich nur an Unternehmen und NGOs, nicht jedoch an staatliche Einrichtungen wie Regierungen und die Polizei.⁵¹³ Dieser Bereich wird jedoch schon teilweise von existierenden Gesetzen geregelt (z.B. Privacy Act, siehe 2.2.2.3).

Außerdem wird kritisiert, dass der Entwurf keine verpflichtende Benachrichtigung der Betroffenen im Falle einer Verletzung der Datensicherheit (zum Beispiel durch Datendiebstahl) vorsieht.⁵¹⁴

Datenschützer sind auch enttäuscht darüber, dass der Commercial Privacy Bill of Rights Act keine verpflichtende Einhaltung von sogenannten „Do-not-track-Mechanismen“ verlangt.⁵¹⁵ Dabei handelt es sich um einen HTTP-Header, den der Browser bei jeder Seitenanfrage an den Server überträgt, der angibt, ob der User von Werbeanbietern mittels Cookies über mehrere Webseiten hinweg wiedererkannt und getrackt werden darf.⁵¹⁶ Ohne eine gesetzliche Regelung bleibt es jedem

⁵¹¹ Vgl. <http://www.reuters.com/article/2011/04/12/us-congress-privacy-idUSTRE73B59E20110412>.

⁵¹² Vgl. Kerry, 37.

⁵¹³ Vgl. http://news.cnet.com/8301-31921_3-20053367-281.html.

⁵¹⁴ Ebd.

⁵¹⁵ Vgl. <http://paidcontent.org/article/419-kerry-mccain-privacy-billopt-outs-are-in-do-not-track-is-out/>.

⁵¹⁶ Vgl. <http://www.golem.de/1101/80917.html>.

Seitenanbieter überlassen, wie er mit dieser Information umgeht bzw. ob er sie überhaupt berücksichtigt.⁵¹⁷

Im Hinblick auf das Safe-Harbor Modell zwischen der EU und den USA kann dieses Gesetz, abhängig von der tatsächlichen Reichweite, eine große Chance für eine bessere Durchsetzung sein. Der Entwurf ließ offen, welche Durchsetzungsgewalt die FTC konkret im Rahmen der freiwilligen Safe-Harbor-Programme hat und mit welchen Handlungsfreiheiten die akkreditierten Prüforganisationen ausgestattet sein sollen. Falls den zuständigen Stellen ausreichende Kompetenzen zugeschrieben werden und auch zufriedenstellender Rechtsschutz für Betroffene sicherstellt wird, könnte man dieses Durchsetzungsprinzip auf das EU-Safe-Harbor Modell anwenden.

6.2 Maßnahmen und Initiativen auf EU-Ebene

6.2.1 Parlamentarische Anfrage betreffend den „sicheren Hafen“

Die Abgeordneten zum Europäischen Parlament Sophia in 't Veld und Jan Philipp Albrecht stellten am 14. Dezember 2010 eine schriftliche Parlamentarische Anfrage an die EK, in der sie diese mit den aktuellen Entwicklungen in Bezug auf die Durchsetzung des Safe-Harbor Modells einschließlich der Studie von Chris Connolly konfrontierten.⁵¹⁸ Die Initiative hinterfragte, welche Schlüsse die Kommission aus den Ergebnissen der erwähnten Studie zieht; was die Kommission unternimmt, um die Einhaltung der Datenschutzgrundsätze zu gewährleisten und ob die Kommission die Ansicht teilt, dass dringend Ermittlungen einzuleiten bzw. Neuverhandlungen notwendig sind.⁵¹⁹ Außerdem wurde die Möglichkeit in den Raum gestellt, Safe-Harbor durch das bevorstehende transatlantische Datenschutzabkommen abzulösen.⁵²⁰

Die Antwort der Kommissarin Viviane Reding gibt wenig Hoffnung auf drastische Maßnahmen seitens der Kommission.⁵²¹ Sie verweist lediglich auf die regelmäßige Prüfung der Umsetzung des Modells, insbesondere auf den kommenden Bericht, der im ersten Halbjahr 2011 zu erwarten ist.⁵²² Weiters wies sie auf die enge Kooperation der Kommission mit den zuständigen US-Behörden hin, die im Rahmen einer im Juni 2009 gegründeten Arbeitsgruppe stattfindet, bestehend aus Vertretern des US-Wirtschaftsministeriums, der FTC sowie der Kommission und zwei nationalen Datenschutzbehörden.⁵²³

Die möglichen Auswirkungen eines zukünftigen transatlantischen Datenschutzabkommens auf Safe-Harbor möchte die EK nicht kommentieren, da bisher keine Verhandlungen über ein solches Abkommen begonnen haben.⁵²⁴

Die von der Kommissarin erwähnte Privacy Contact Group hat ihre Arbeit vor nun knapp zwei Jahren aufgenommen, bisher wurden jedoch keine Empfehlungen oder

⁵¹⁷ ebd.

⁵¹⁸ Vgl. E-010411/2010

⁵¹⁹ Ebd.

⁵²⁰ Ebd.

⁵²¹ Ebd.

⁵²² Ebd.

⁵²³ Ebd.

⁵²⁴ Ebd.

Kommentare im Zusammenhang mit dem Safe-Harbor Modell veröffentlicht, wodurch sich auch die in diese Arbeitsgruppe gesetzten Hoffnungen in Grenzen halten.

6.2.2 Konkrete Pläne der EK

Im Rahmen des Privacy Platform Meetings am 26. März 2011 gab die EU-Kommissarin für Justiz, Viviane Reding, ihre Pläne für eine Reform der Datenschutzrichtlinie bekannt.⁵²⁵ Die folgenden vier Punkte sollen dabei höchste Priorität genießen:⁵²⁶

- **Das Recht auf Vergessen.** Dieses Recht soll es Personen erlauben, ihre Erlaubnis zu einer Datenverarbeitung nachträglich effektiv zurückzuziehen.
- **Mehr Transparenz.** Bestimmungen über die Nutzung, Sammlung und Speicherung personenbezogener Daten müssen leicht verständlich, nachvollziehbar und auffindbar sein (vor allem im Bereich sozialer Netzwerke und in Bezug auf Kinder).
- **Standardmäßiger Datenschutz.** Privacy Einstellungen müssen standardmäßig komplett aktiviert sein und nicht, wie bisher oft üblich, standardmäßig deaktiviert sein (privacy by default).
- **Standortunabhängiger Datenschutz.** Datenschutz soll unabhängig vom geografischen Ort der Datensammlung- und Verarbeitung gelten, ohne Ausnahmen für Betreiber aus Drittstaaten.

Die Einführung standortunabhängiger Datenschutzbestimmungen würde das Safe-Harbor Modell obsolet machen, da personenbezogene Daten ohnehin in allen Drittstaaten geschützt wären. Voraussetzung dafür ist aber eine effektive Umsetzung. Die Kommissarin hielt fest, dass die EU nicht zögern werde, gegen Unternehmen außerhalb der EU vorzugehen, wenn diese gegen EU-Bestimmungen in Hinblick auf die Sammlung und Speicherung von Daten verstoßen.⁵²⁷ Dazu schlug sie die Bestellung von nationalen Datenschutzeinrichtungen vor, die Datenverarbeiter außerhalb der EU überprüfen sollen.⁵²⁸ Diese Einrichtungen müssen jedoch mit ausreichenden Kontrollbefugnissen und Sanktionsmöglichkeiten ausgestattet sein um die Ziele wirkungsvoll durchsetzen zu können. Dabei sind große Schwierigkeiten vorhersehbar.

⁵²⁵ Vgl. http://www.unwatched.org/EDRigram_9.6_Privacy_Platform_Meeting.

⁵²⁶ Ebd.

⁵²⁷ Ebd.

⁵²⁸ Ebd.

6.3 Maßnahmen und Initiativen in Deutschland

6.3.1 Entscheidung durch den Düsseldorfer Kreis

6.3.1.1 Was ist der Düsseldorfer Kreis?

Der Düsseldorfer Kreis ist eine informelle Vereinigung der obersten deutschen Datenschutzbehörden, die sich mit der Einhaltung des Datenschutzes im nicht-öffentlichen Bereich befasst.⁵²⁹ Die Beschlüsse des Kreises haben entsprechend zwar keine unmittelbar rechtssetzende Wirkung, gelten aber als verlässliche Leitlinie für das künftige Handeln der Datenschutzbehörden.⁵³⁰

6.3.1.2 Die Entscheidung betreffend Safe-Harbor

Der Düsseldorfer Kreis hat als erstes Gremium folgenschwere Konsequenzen aus dem unzureichenden Schutz durch das Safe-Harbor Modell gezogen. Die Vereinigung hat am 29. April 2010 beschlossen, dass sich deutsche Daten exportierende Unternehmen nicht mehr allein auf die Behauptung einer Safe-Harbor-Zertifizierung des Datenimporteurs verlassen dürfen.⁵³¹ Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe-Harbor-Zertifizierungen tatsächlich vorliegen und deren Grundsätze auch eingehalten werden.⁵³² Als Mindestkriterium ist die Gültigkeit der Safe-Harbor-Zertifizierung zu prüfen.⁵³³ Außerdem muss sich das exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten gegenüber den von der Datenverarbeitung Betroffenen nachkommt.⁵³⁴ Diese Notwendigkeit besteht auch deshalb, damit das Unternehmen die Informationen an den von der Verarbeitung Betroffenen weitergeben kann.⁵³⁵

Die Mindestprüfung muss dokumentiert und auf Verlangen den Aufsichtsbehörden vorgelegt werden.⁵³⁶ Sollten nach einer Prüfung Zweifel an der Einhaltung der Safe-Harbor-Kriterien bestehen, so wird die Verwendung von Standard-Vertragsklauseln empfohlen.⁵³⁷ Ergibt die Prüfung eine nicht mehr gültige Zertifizierung oder mangelnde Informationen für die Betroffenen, dann sollen die zuständigen Behörden über diesen Umstand informiert werden.⁵³⁸

6.3.1.3 Folgen der Entscheidung

Aufgrund der hohen Bedeutung bisheriger Entscheidungen des Düsseldorfer Kreises wird diese Entscheidung für deutsche Unternehmen faktisch zur Voraussetzung für den Datentransfer in die USA.⁵³⁹ Die Nichteinhaltung dieser Entscheidung

⁵²⁹ Vgl. http://blog.dlapiper.com/detechnology/entry/duesseldorfer_kreis_richtlinien_zu_safe.

⁵³⁰ Ebd.

⁵³¹ Vgl. Düsseldorfer Kreis.

⁵³² Ebd.

⁵³³ Ebd.

⁵³⁴ Ebd.

⁵³⁵ Ebd.

⁵³⁶ Ebd.

⁵³⁷ Ebd.

⁵³⁸ Ebd.

⁵³⁹ Vgl. <http://www.datenschutzbeauftragter-online.de/usa-datenschutz-safe-harbor-aenderungen-entscheidung-aufsichtsbehoerden-duesseldorfer-kreis/>.

kann schwerwiegende Folgen haben, da bei Verstößen gegen das Bundesdatenschutzgesetz Bußgelder in Höhe von bis zu 300.000€ vorgesehen sind und außerdem Schadensersatzklagen erhoben werden können.⁵⁴⁰

6.3.1.4 Kritik

Die Entscheidung des Düsseldorfer Kreises ist als Sofortmaßnahme im deutschen Hoheitsgebiet zu begrüßen, langfristig sind mit Sicherheit umfassendere Ansätze notwendig.

Als erstes ist zu bemängeln, dass die Lösung nur für Deutschland Gültigkeit hat, doch auch eine Ausweitung auf den gesamten EU-Raum wäre auf Dauer wenig zufriedenstellend. Weiters ist zwar von einer Prüfung der Datenexporteure hinsichtlich der Einhaltung der Grundsätze durch die Datenimporteure die Rede, in der Praxis werden wohl nur die verlangten Mindestprüfungen von Bedeutung sein. Diese beinhalten ausschließlich das Vorhandensein einer aktuellen Selbstzertifizierung sowie die Einhaltung der Informationspflicht, daher bekämpft dieser Ansatz nur einen Teil der bestehenden Schwächen des Safe-Harbor-Systems.

Praktisch außer Acht gelassen wird die Frage, ob die übrigen Grundsätze eingehalten werden und ob die Durchsetzung durch die amerikanischen Behörden gewährleistet ist.

6.3.2 Kleine Anfrage von Abgeordneten an die Bundesregierung

Am 6.10.2010 stellten Abgeordnete des Deutschen Bundestags eine Anfrage an die Bundesregierung in Bezug auf die Einhaltung der Safe-Harbor-Grundsätze bei der transatlantischen Datenübermittlung.⁵⁴¹

In dieser konfrontierten sie die Bundesregierung mit den Mängeln des Safe-Harbor-Modells und der Frage, wie diese dazu stehe und ob sie Handlungsbedarf sehe.⁵⁴² Ziel der federführenden Abgeordneten war es, die Bundesregierung dazu zu motivieren, eine Neuverhandlung des Safe-Harbor-Modells anzustoßen. Aus der Antwort der Bundesregierung vom 25.10.2010 war jedoch klar ersichtlich, dass diese keinen Anlass dazu sieht.⁵⁴³ Bei den entscheidenden Fragen wurde mangels Zuständigkeit auf den Bundesbeauftragten für Datenschutz verwiesen oder die Angemessenheit des Modells festgestellt.⁵⁴⁴

Es sind daher keinerlei Folgen aus dieser Anfrage zu erwarten, möglicherweise war sie auch an den falschen Adressaten gerichtet. Sinnvoller wäre es, die Forderungen gegenüber den unabhängigen Datenschutzgremien zu deponieren.

⁵⁴⁰ Ebd.

⁵⁴¹ Vgl. BT Drs-Nr. 17/3250.

⁵⁴² Ebd.

⁵⁴³ Vgl. BT Drs-Nr. 17/3375.

⁵⁴⁴ Ebd.

6.4 Fazit

Zusammenfassend wird festgestellt, dass alle bisher durchgeführten Maßnahmen und Initiativen einen Beitrag leisten, der bei weitem zu gering ist, um an der aktuellen Situation Grundlegendes zu ändern.

Das Einschreiten der FTC in einigen wenigen Fällen kann als schwaches Lebenszeichen des längst tot geglaubten Durchsetzungsmechanismus gewertet werden. Die parlamentarische Anfrage an die EK sowie die Kleine Anfrage an die deutsche Bundesregierung können als Initiativen beurteilt werden, die im Keim erstickt wurden und deutlich aufzeigen, wie wenig Änderungsbedarf innerhalb der EU gesehen wird.

Die Pläne der zuständigen EU-Kommissarin klingen zwar vielversprechend, es bleibt jedoch abzuwarten, wie diese Ideen in die Praxis umgesetzt werden sollen.

Die Entscheidung durch den Düsseldorfer Kreis kann positive Konsequenzen mit sich bringen, sie kann jedoch nur als temporäre Lösung gedacht sein.

Es sind daher neue Ideen notwendig, deren Umsetzung seitens der EU konsequent verfolgt werden muss, denn vor allem von europäischer Seite ist bisher kein Druck erzeugt worden, um an der aktuellen Lage rasch etwas zu ändern. Von den zuständigen Behörden in den USA sind mit Sicherheit keine Initiativen zu erwarten das Modell besser durchzusetzen, solange die EK in den aktuellen Praktiken keinen Handlungsbedarf sieht. Überraschend sind jedoch die Entwicklungen in den USA, die auf Ebene des Bundes und der Bundesstaaten immer mehr bemüht sind, Datenschutz besser gesetzlich zu verankern.

7 NOTWENDIGE MAßNAHMEN

7.1 Ziele und Herausforderungen

Während die sechs inhaltlichen Grundsätze des Safe-Harbor Modells eine ausreichende Grundlage darstellen, führt an der Neuverhandlung der Details des Durchsetzungsgrundsatzes kein Weg vorbei. Zu schwerwiegend sind die Erkenntnisse, die in der Praxis im Umgang mit unternehmensinternen Datenschutzrichtlinien festgestellt wurden, als dass man die aktuelle Regelung beibehalten könnte.

Da die Aussagekraft einer Safe-Harbor-Zertifizierung auf ein Minimum gesunken ist, sind qualitätssteigernde Maßnahmen notwendig, die folgende Ziele gewährleisten sollen:

- Im Falle einer Beibehaltung der Safe-Harbor-Lösung muss entweder jedem Eintrag in der Safe-Harbor-Liste eine gültige Zertifizierung inklusive eine den Grundsätzen entsprechende Datenschutzerklärung zu Grunde liegen oder der Eintrag muss klar und deutlich als abgelaufen gekennzeichnet sein.
- Es muss wirksame, anlassunabhängige Prüfungsmechanismen geben, die sicherstellen, dass die Datenschutzrichtlinien in der Praxis tatsächlich eingehalten werden.
- Jeder Beschwerde durch eine betroffene Person muss auf jeden Fall nachgegangen werden, um die Einhaltung ihrer Rechte sicher zu stellen.

Die große Herausforderung liegt darin, viele verschiedene, sich teilweise widersprechende Kriterien zu vereinbaren.

Es ist auf jeden Fall ein EU-weit einheitliches System notwendig, das Sonderregelungen, wie die Auflagen des Düsseldorfer Kreises, ablösen kann. Außerdem soll eine möglichst einfache und unbürokratische Zusammenarbeit zwischen Unternehmen in der EU und den USA gefördert werden. Im Mittelpunkt steht jedenfalls die ordnungsgemäße Durchsetzung der Grundsätze, wodurch die Wahrung der Rechte europäischer Bürger sichergestellt wird. Erschwert wird die Lösungsfindung durch knappe budgetäre Voraussetzungen sowie die US-amerikanische Datenschutzpolitik, die sich grundsätzlich von der europäischen unterscheidet.

7.2 Ansatz 1: Gesetzliche Regelung

Bedingt durch die US-amerikanische Gesetzeslage ist eine wirksame Durchsetzung des Safe-Harbor Modells nur durch relativ aufwändige Mechanismen möglich. Die einfachste Lösung wäre daher eine Kündigung des Regelwerks und die Einführung eines neuen, gesetzesbasierten Systems.

Dieses könnte auf dem Vorschlag der EU-Kommissarin Viviane Reding aufbauen, der die Erweiterung der EG-DSRL um standortunabhängigen Datenschutz vorsieht.⁵⁴⁵ Dadurch wäre nach erfolgter Umsetzung in nationales Recht eine gesetzliche Grundlage geschaffen, die jedoch ohne weiterführende Maßnahmen auf Grund fehlender Hoheitsgewalt in den USA an die Grenzen der Durchsetzbarkeit stoßen

⁵⁴⁵ Vgl. http://www.unwatched.org/EDRigram_9.6_Privacy_Platform_Meeting.

würde. Es müsste daher in weiterer Folge eine unabhängige Datenschutzbehörde in den USA eingesetzt werden, um die Durchsetzung zu ermöglichen.

Diese Behörde nach europäischem Vorbild sollte als Anlaufstelle für Betroffene fungieren und dazu verpflichtet sein, jede Beschwerde zu untersuchen. Sie müsste daher mit umfassenden Rechten (z.B. Einsichtnahme in Unterlagen, Befragung von Zeugen) ausgestattet sein. Weiters müsste die Behörde die Möglichkeit haben, Verstöße wirksam zu sanktionieren und rechtlich bindende Weisungen auszusprechen. Neben der Behandlung von Beschwerden sollte die Institution auch selbstständig Untersuchungen aufnehmen und mit europäischen Datenschutzbehörden kooperieren. Außerdem müsste die Möglichkeit bestehen, Betroffenenrechte vor Gericht durchzusetzen.

Die größte Schwierigkeit bei der Realisierung dieses Ansatzes ist das notwendige Entgegenkommen der US-amerikanischen Gesetzgebung. Um eine solche Institution einzurichten, müssen in den USA zuerst die gesetzlichen Voraussetzungen geschaffen werden, vor allem im Hinblick auf die erforderlichen Kompetenzen dieser Datenschutzbehörde und die Möglichkeit der gerichtlichen Durchsetzung. Die Bereitschaft dazu hält sich bisher in Grenzen, wie die Reaktionen aus Washington auf derartige Forderungen zeigen: „Wie können unser System nicht ändern, um den Europäern einen Gefallen zu tun.“⁵⁴⁶

Da dieses fehlende Entgegenkommen eine unüberwindbare Hürde in der Realisierung darstellen könnte, werden noch weitere mögliche Ansätze vorgeschlagen.

7.3 Ansatz 2: Strenge Kontrollen der Safe-Harbor-Teilnehmer

Im Gegensatz zum ersten Ansatz basieren diese und die folgenden Varianten auf die Weiterführung des Safe-Harbor Modells, verlangen jedoch verschiedene Anpassungen und damit eine teilweise Neuverhandlung.

7.3.1 Neustart der Safe-Harbor Datenbank

Da die meisten Zertifizierungen Mängel enthalten, sollten alle bisherigen Einträge entfernt und es könnte damit ein Neustart gemacht werden. Die online verfügbare Teilnehmerliste sollte in einigen Punkten adaptiert werden, um ausreichende Aktualität zu gewährleisten und Verwaltungskosten zu sparen. Die Datenbank sollte nicht nur einen Link auf die Privacy Policy enthalten, sondern den Volltext, damit eine Verbindung zum Inhalt nicht „verschwinden“ kann, wie es aktuell mehrfach der Fall ist. Außerdem sollten abgelaufene Zertifikate automatisch als „not current“ angezeigt werden. Das zertifizierte Unternehmen sollte rechtzeitig vor Ablauf der Gültigkeit eine automatische Benachrichtigung erhalten, um eine fristgerechte Verlängerung zu unterstützen. Einträge, die länger als beispielsweise sechs Monate abgelaufen sind, sollten aus der öffentlich sichtbaren Anzeige automatisch entfernt werden.

⁵⁴⁶ Vgl. <http://www.welt.de/die-welt/wirtschaft/article7801328/Europa-draengt-USA-zu-strengem-Datenschutz.html>.

7.3.2 Aufrechterhalten der validen Teilnehmerliste

Da die von den Unternehmen formulierten und eingereichten Datenschutzrichtlinien die Basis für eine bindende Safe-Harbor-Teilnahme darstellen, muss sichergestellt werden, dass diese in allen Punkten konform mit den Safe-Harbor-Richtlinien sind. Um die dauerhafte Zulassung von ausschließlich konformen Registrierungen sicherzustellen, sind wirksame Mechanismen notwendig.

7.3.2.1 Prüfung der Privacy Policy

Eine gründliche Prüfung jeder Selbstzertifizierung wäre eine Möglichkeit, das Niveau der Privacy Policies angemessen hoch zu halten. Nur wenn allen Grundsätzen entsprochen wird, sollte das sich zertifizierende Unternehmen in die Safe-Harbor-Liste aufgenommen werden. Dadurch wäre ein wesentliches Schlupfloch – die Registrierung mit überhaupt nicht vorhandenen oder mit Alibi-Datenschutzrichtlinien – beseitigt. Als Folge wäre jedes Unternehmen, das gegen die selbst auferlegten (durch die Prüfung auch garantiert Safe-Harbor konformen) Datenschutzrichtlinien verstößt, zumindest auf jeden Fall durch die FTC sanktionierbar.

7.3.2.2 Generierte Privacy Policies

Alternativ dazu könnte man den Entstehungsprozess der Privacy Policies grundlegend ändern. Aktuell werden diese von den teilnehmenden Unternehmen formuliert und bei der Selbstzertifizierung eingereicht. Frei formulierter Text ist für die Kontrollstellen nur mit sehr aufwändigen Mitteln überprüfbar und außerdem sind die Kontrollen durch komplexe Formulierungen sehr fehleranfällig und die Richtlinien für Konsumenten schwer verständlich.

Aus diesem Grund könnte man die Safe-Harbor Teilnehmer einen computergestützten, umfangreichen Fragebogen auf multiple-choice Basis ausfüllen lassen. Dieses Formular könnte erheben, wie das Unternehmen personenbezogene Daten verarbeitet, die Daten könnten elektronisch ausgewertet werden. Entspricht die Art und Weise der Verarbeitung den Grundsätzen des sicheren Hafens, so wird aus dem Formular ein Vertrag generiert, den das Unternehmen unterzeichnen muss.

Auf diese Weise könnte man den Aufwand für die Überprüfung einsparen, ohne bei der Qualität der Datenschutzrichtlinien Einbußen hinnehmen zu müssen.

7.3.3 Adaptierung der anlassunabhängigen Kontrollen

Da das Vorhandensein einer Safe-Harbor konformen Datenschutzrichtlinie noch lange nicht heißt, dass diese auch ordnungsgemäß umgesetzt wird, sind auch hier Maßnahmen notwendig, um dies sicherzustellen. Dazu sollte die in FAQ 7 geregelte, anlassunabhängige Kontrolle geändert werden.

In erster Linie muss auf jeden Fall die Möglichkeit, diese Kontrolle selbst durchzuführen, abgeschafft werden. Unternehmen, die ihre eigenen Datenschutzrichtlinien bewusst nicht einhalten, werden im Rahmen dieser selbst durchgeführten Überprüfungen auch keine Mängel aufzeigen. Außerdem kann durch die Zulassung von ausschließlich externen Prüfungen einer Betriebsblindheit vorgebeugt werden. Es kann durchaus sein, dass Unternehmen ihre Richtlinien teils ohne Absicht nicht einhalten. Im Zuge interner Prüfungen ist die Wahrscheinlichkeit, solche Fehler zu „übersehen“, höher als im Rahmen unabhängiger Prüfungsverfahren. Externe Prü-

fer haben einen neutralen Blick auf die Tätigkeiten des Unternehmens und verfügen im Normalfall auch über effektivere Prüfungsmethoden.

Als zweite Maßnahme sollte der Kreis der befugten Prüfer eingeschränkt werden. Aktuell ist die Rechtslage so, dass grundsätzlich jeder Prüfungen durchführen darf, die der anlassunabhängigen Kontrollpflicht gerecht werden, ohne eine geeignete Qualifikation bzw. die Unbefangenheit nachweisen zu müssen. Daher sollte man in Zukunft Kontrollen nur durch ausgewählte, qualifizierte Organisationen zulassen. Dadurch wäre ein Mindestniveau der Prüfungen sichergestellt.

7.3.4 Sicherstellung angemessener Sanktionierung

Um eine angemessene Sanktionierung sicherzustellen, muss Sorge getragen werden, dass ebenso wie die Kontrollorgane auch die Streitschlichtungsstellen wirtschaftlich unabhängig von den Safe-Harbor Teilnehmern sind.

Dies könnte gewährleistet werden, indem Unternehmen ihre Prüf- und Streitschlichtungsstellen nicht mehr selbst engagieren dürften, sondern von der FTC zugewiesen bekämen. Die Kosten für Kontrollen könnten bei der Safe-Harbor Zertifizierung erhoben werden. Verstöße sollten verpflichtend der FTC gemeldet werden, um einen willkürlichen Umgang zu verhindern.

7.3.5 Vorteile

7.3.5.1 Sichere Kontrolle

Dieser Ansatz stellt sicher, dass alle firmeninternen Datenschutzrichtlinien, die für eine Registrierung verwendet wurden, sofort ab Anmeldedatum auch tatsächlich konform sind.

7.3.6 Schwierigkeiten

7.3.6.1 Hoher Verwaltungsaufwand

Eine mögliche Schwierigkeit bei diesem Ansatz könnten der hohe Verwaltungsaufwand und die damit verbundenen Kosten darstellen. Da bisher beinahe alle Anträge ohne Beanstandung akzeptiert wurden, würde eine ausführliche Prüfung erheblich länger dauern. Außerdem würde die Anzahl der zu prüfenden Anträge steigen, da vermutlich jede Ablehnung eine weitere Prüfung einer nachgebesserten Version nach sich ziehen würde. Hinzu kommt, dass jede Änderung der Datenschutzrichtlinie durch das teilnehmende Unternehmen eine erneute Prüfung notwendig machen würde. Die Dauer solcher Überprüfungen auf geringfügige Änderungen könnte man jedoch durch den Einsatz von Vergleichssoftware drastisch senken.

Der Einsatz automatisch generierter Datenschutzrichtlinien würde diese Kostenexplosion verhindern und die Realisierung dieses Modells deutlich realistischer machen.

7.3.6.2 Mangelnde Motivation der US-amerikanischen Behörden

Da die US-amerikanischen Behörden bisher beschränkte Motivation an den Tag legten, das Safe-Harbor Modell durchzusetzen, liegt die Befürchtung nahe, dass sich daran auch durch die Pflicht einer umfassenden Eingangsdatenprüfung nichts

ändert. Diesem Risiko ist auf jeden Fall mittels strichprobenartiger Überprüfungen zu begegnen, zum Beispiel durch die Artikel 29-Datenschutzgruppe. Sollte sich der Verdacht bewahrheiten, könnte man das Prüfverfahren in die EU verlagern und durch nationale Datenschutzbehörden durchführen lassen. Dadurch wäre zwar die angemessene Qualität der Datenschutzrichtlinien sichergestellt, es würde jedoch eine Finanzierungsfrage aufgeworfen werden, auf die an dieser Stelle nicht eingegangen wird.

7.4 Ansatz 3: Verbesserung der Selbstregulierung

Durch geeignete Maßnahmen gegen die aktuellen Schwächen im Selbstregulierungsmechanismus ist eine wirksame Alternative zur strikten staatlichen Kontrolle vorstellbar. Diese Alternative basiert in erster Linie auf Transparenz, denn diese ist ein effektives Werkzeug, um Unternehmen zu motivieren, ihre Datenschutzrichtlinien einzuhalten. Als Mittel zum Zweck sollte dabei auf bewährte Web 2.0 Technologien gesetzt werden, die einen entscheidenden Beitrag zur effektiven und effizienten Kommunikation leisten können.

Grundvoraussetzung ist eine zentrale Online-Plattform, die vor allem die Zusammenarbeit der einzelnen teilnehmenden Unternehmen, Behörden und der Betroffenen transparent darstellen und erleichtern sowie alle Prozesse des Safe-Harbor-Zyklus koordinieren soll. Darunter ist zu verstehen, dass (von der Zertifizierung über die Kontrolle bis hin zur Sanktionierung) alle Schritte online begleitet werden.

7.4.1 Selbstzertifizierung

Unternehmen, die am Safe-Harbor Modell teilnehmen möchten, müssen sich ähnlich wie bisher selbst zertifizieren. Dazu müssen sie sich in der Online-Plattform registrieren und ihre firmenweite Privacy Policy übermitteln, die mit den Safe-Harbor Grundsätzen konform sein muss. Die Datenschutzrichtlinie ist für jedermann öffentlich zugänglich. Sobald die Anmeldung abgeschlossen ist, gilt das Unternehmen offiziell als Safe-Harbor-Teilnehmer mit allen Rechten und Pflichten.

Im Zuge der Zertifizierung geht der Teilnehmer einen Vertrag ein, der garantiert, dass seine Policy mindestens den Safe-Harbor Kriterien entspricht. Im Fall einer Abweichung von den Safe-Harbor Grundsätzen sieht dieser Vertrag hohe Strafzahlungen sowie den Verlust der Zertifizierung vor.

Eine Eingangsdatenprüfung der Datenschutzrichtlinien ist bei diesem Ansatz nicht zwingend notwendig. Dadurch wäre diese Variante kostengünstiger als der zuerst genannte Ansatz. Entscheidend bei dieser Alternative wäre jedenfalls, dass Abweichungen von den Safe-Harbor-Richtlinien auf jeden Fall sanktioniert werden, ohne Datenschutzverletzungen in der Praxis nachweisen zu müssen.

7.4.2 Überprüfung der Privacy Policy

Das System sieht ein Rating vor, das das Niveau der Datenschutzrichtlinie visualisieren soll, wobei jeder Teilnehmer mit einem Einstiegslevel beginnt. Jede interessierte Person kann sich auf der Plattform registrieren und die Privacy Policy bewerten. Zielpersonen sind vor allem betroffene Private und Datenschützer in der EU. Deutet das Rating auf eine unzureichende Datenschutzrichtlinie hin, wird au-

tomatisch und für jedermann sichtbar die FTC verständigt. Diese muss nach der Review der Privacy Policy das Ergebnis samt Begründung online dokumentieren. Wenn die FTC die Mängel in den Datenschutzrichtlinien bestätigt, wird unter Androhung des Verlustes der Zertifizierung eine Nachbesserung durch das betroffene Unternehmen verlangt. Ist das Unternehmen zu Unrecht im Rating schlecht bewertet worden, kann die FTC das Rating korrigieren.

7.4.3 Handhabung von Beschwerden betroffener Personen

Die Abwicklung einer Beschwerde soll ebenfalls über diese Plattform erfolgen und wie nachstehend erläutert ablaufen:

Die betroffene Person muss sich in der Online-Plattform registrieren und ihren Beschwerdetext online einreichen. Dieser wird nur an das entsprechende Unternehmen weitergeleitet, öffentlich ist lediglich sichtbar, dass am jeweiligen Datum eine Beschwerde mit offenem Status gegen das Unternehmen eingegangen ist.

Nachdem die beiden Parteien unter Ausschluss der Öffentlichkeit die Beschwerde behandelt haben, muss der Betroffene den Status der Beschwerde publik auf „erledigt“ oder „nicht erledigt“ setzen. Konnte keine Einigung erzielt werden, wird durch die Änderung des Status die Beschwerde an die zuständige Streitschlichtungsstelle weitergeleitet und der Status auf „In Bearbeitung der Streitschlichtungsstelle“ gesetzt.

Nachdem die Streitschlichtungsstelle die Prüfung abgeschlossen hat, muss sie ihre Entscheidung samt Begründung und eventueller Sanktionen online stellen. Der Status kann danach entweder „Abgeschlossen“ sein oder die Streitschlichtungsstelle leitet den Fall an die FTC weiter. Falls das Beschwerdeverfahren für abgeschlossen erklärt wurde, kann der Betroffene angeben, ob er mit der Lösung zufrieden ist oder nicht. Sollte er der Lösung nicht zustimmen, kann er seinen Fall über die Plattform an die zuständige nationale Datenschutzbehörde weiterleiten lassen, die den Sachverhalt prüft und an die FTC weiterleitet, falls sie diesen Schritt für angemessen hält. In jedem Fall wird die entsprechende Entscheidung, sowohl von der Datenschutzbehörde als auch von der FTC auf der Online-Plattform vermerkt.

Weiters gibt es ein eigenes Rating für die Abwicklung von Beschwerden. Dieses ist vergleichbar mit Bewertungsmechanismen bei Auktionsplattformen, die eine Bewertung der Verkäufer ermöglichen. Dadurch sollen die betroffenen Unternehmen zusätzlich motiviert werden, mit Betroffenen bestmöglich zu kooperieren.

7.4.4 Blacklist

Aus diesen Ratings kann eine Blacklist generiert werden, die Unternehmen mit auffallend unsicheren Datenschutzrichtlinien oder schlechtem Beschwerdemanagement klar und deutlich anzeigt. Dadurch werden dem Konsumenten leicht lesbare Informationen zur Verfügung gestellt, mit deren Hilfe er besser entscheiden kann, ob er einem Unternehmen seine Daten anvertrauen möchte oder nicht. Diese Blacklists wären auch für die Kontrollbehörden hilfreich, da sie ihre Kapazitäten schwerpunktmäßig für die Überprüfung und Sanktionierung schlecht bewerteter Unternehmen nutzen könnten.

Weiters sollte die Plattform eine Liste aller Unternehmen anbieten, die ihre Teilnahme am Modell nicht verlängert haben. Dadurch wäre leichter überprüfbar, ob

diese die Daten, die sie während ihrer Teilnahme gesammelt haben, nach wie vor entsprechend den Grundsätzen verarbeiten.

7.4.5 Vorteile

7.4.5.1 Niedriger Verwaltungsaufwand

Da durch die Verteilung eines wesentlichen Teils der Überprüfungsaktivität auf interessierte Privatpersonen die Kontrollen durch die US-amerikanischen Behörden entfallen, wird viel Verwaltungsaufwand eingespart, wodurch die Finanzierung dieses Systems erleichtert wird.

7.4.5.2 Transparenz

Bisher war es ohne relativ aufwändige Recherche nicht möglich, sich zu erkundigen, wie sicher die Datenschutzrichtlinien eines Unternehmens in den USA sind, wie viele Beschwerden im Zusammenhang mit Datenschutzfragen bereits gegen das Unternehmen gerichtet waren, wie diese behandelt wurden und welche Konsequenzen daraus folgten. Gerade dies sind jedoch die entscheidenden Fragen, wenn man auf das Prinzip der Selbstregulierung setzt. An der mangelnden Transparenz in Verbindung mit der Untätigkeit der Behörden ist nämlich das aktuelle Safe-Harbor System gescheitert.

Durch den Einsatz einer solchen Plattform wären solche Fragen auf einem Blick beantwortet. Dadurch wäre auch für Laien leicht ersichtlich, ob sich ein Unternehmen an die Safe-Harbor-Grundsätze hält oder nicht. Davon profitierten einerseits die Betroffenen, für die der Beschwerdeprozess transparenter wird und auch Daten exportierende Unternehmen in Europa, die über das tatsächliche Datenschutzniveau des Geschäftspartners Bescheid wüssten. Weiters wüchse der Druck auf alle beteiligten Parteien in den USA:

Teilnehmende, nicht seriös agierende Unternehmen könnten nicht mehr teils fast unverschämt mit dem Safe-Harbor-Zertifikat werben und sich darauf verlassen, dass diese Täuschung nicht publik wird. Streitschlichtungsstellen könnten nicht mehr zu Unrecht zu Gunsten der beklagten Unternehmen entscheiden, da auch ihre Arbeit kontrolliert würde. Nicht zuletzt wäre auch die FTC zum Handeln gezwungen, denn auch sie hat bisher vom mangelnden Überblick über die Beschwerden „profitiert“.

7.4.5.3 Klarheit der Vorgangsweise für Betroffene

Gleichzeitig soll dieses System alle Betroffenen bei der Durchführung eines Beschwerdeverfahrens unterstützen und solche Personen, die bisher aus Angst vor unüberwindbaren bürokratischen Hürden von einer Beschwerde abgesehen haben, zum Einfordern ihrer Rechte motivieren.

Viele lassen sich durch unbegründete Abweisungen seitens der Unternehmen aufhalten, wissen nicht, welche Instanzen in welchen Fällen zu kontaktieren sind oder welche Rechte sie überhaupt haben. Dieses Problem fällt durch die Onlineplattform weg, da sie den Instanzenweg vorgibt und die Unterlagen „auf Knopfdruck“ an die entsprechenden Stellen weiterleitet. Dadurch könnte die Anzahl der Beschwerden deutlich steigen und eine positive Auswirkung auf die Datenschutzpraktiken der Unternehmen bewirkt werden.

7.4.5.4 Geringere Abhängigkeit von US-amerikanischen Behörden

Wie bereits erwähnt, mangelt es der FTC an Motivation, Verstöße gegen das Safe-Harbor Modell zu sanktionieren, da nur EU-Bürger davon betroffen sind. Da dieser Ansatz ohnehin den Schwerpunkt auf Selbstregulierung setzt und dabei die Transparenz in den Mittelpunkt stellt, werden voraussichtlich die meisten Beschwerden spätestens auf Ebene der Streitschlichtungsstellen gelöst. Daher wird es vermutlich nur wenige Verstöße geben, die tatsächlich von der FTC bearbeitet werden müssen. Diese bleiben dann überschaubar und sollten im schlimmsten Fall nach Intervention der zuständigen nationalen Datenschutzbehörde des EU-Mitgliedstaats erfolgreich sanktioniert werden.

7.4.5.5 Verkürzung der Verfahren

Ein weiterer Vorteil des Einsatzes einer zentralen Onlineplattform ist die Verkürzung der Beschwerdeverfahren. Durch die Onlineabwicklung entfallen Wartezeiten, die sich bei transatlantischen Sendungen deutlich auswirken. Außerdem können sich unbegründet lange Bearbeitungszeiten der betroffenen Unternehmen negativ auf das Ranking auswirken, wodurch diese zusätzlich zur raschen Abwicklung motiviert werden sollen.

7.4.5.6 Einfachere Einführung des Systems

Dieser Ansatz kann das Datenschutzniveau in der Relation zu Unternehmen in den USA erheblich verbessern, ohne dass eine gesetzliche Regelung notwendig ist. Dadurch ist es wahrscheinlich, dass die Kooperation mit den USA im Rahmen der Umsetzung reibungslos funktioniert. Außerdem könnten die USA diese Regelung auch für US-amerikanische, personenbezogene Daten anwenden, was zu einer Verbesserung der Durchsetzung führen würde.

7.4.6 Mögliche Zweifel

7.4.6.1 Geringes Interesse an Mitarbeit

Es liegt natürlich die Frage nahe, ob die Öffentlichkeit ausreichend Interesse an der Mitarbeit an einem solchen Projekt zeigt und ob es dadurch genügend Reviews der Datenschutzrichtlinien gibt.

Dieser Gefahr kann durch Bewusstseinsbildung mittels Informationskampagnen entgegengewirkt werden. Das Wikipedia-Projekt beweist, wie effektiv Informationen durch öffentliche Zusammenarbeit gesammelt und koordiniert werden können. Natürlich spricht die Safe-Harbor-Problematik einen viel kleineren Interessentenkreis an als eine Enzyklopädie, die im alltäglichen Leben hilfreich ist. Es ist jedoch auch nur ein Bruchteil der Wikipedia-Teilnehmer notwendig, da die Anzahl der Safe-Harbor zertifizierten Unternehmen (aktuell ca. 1600), die es zu überprüfen gilt, sehr überschaubar ist. Es gibt mit Sicherheit ausreichend am Datenschutz interessierte Privatpersonen und auch Organisationen (z.B. das Electronic Privacy Information Center oder die Electronic Frontier Foundation), die sich freiwillig bereiterklären könnten, für eine gut organisierte Plattform Kurzgutachten zu erstellen.⁵⁴⁷

⁵⁴⁷ Vgl. Leathers, 236.

Um einen erfolgreichen Start sicherzustellen, könnte man Mitarbeiter europäischer Datenschutzbehörden einsetzen, die die ersten Bewertungen durchführen. Auf diese Weise könnte man verhindern, dass das System mangels Aktivität stirbt, bevor es überhaupt zu „leben“ begonnen hat.

7.4.6.2 Fehlende Qualifikation der Prüfer

Eine weitere Befürchtung könnte sein, dass die freiwilligen „Prüfer“ keine ausreichende juristische Qualifikation haben, um ein ausreichendes Niveau der Gutachten zu bewirken.

Dem ist entgegenzusetzen, dass die meisten an Datenschutz ernsthaft Interessierten in der Praxis eine gewisse juristische Ausbildung oder entsprechenden beruflichen Hintergrund haben. Außerdem muss man kein Jurist sein, um eine Datenschutzrichtlinie auf die Einhaltung der Safe-Harbor-Grundsätze überprüfen zu können. Man könnte als weitere Hilfestellung eine Checkliste erstellen und auf der Plattform zur Verfügung stellen, die Bewerter dabei unterstützt, eine lückenlose Überprüfung durchzuführen.

7.5 Ansatz 4: Kombination der vorhergehenden Ansätze

Unter der Annahme, dass Ansatz 1 aufgrund mangelnder Kooperation der USA nicht umsetzbar ist, könnte man den besten Schutz gewährleisten, in dem man die effektivsten Aspekte der Ansätze 2 und 3 kombiniert und einen guten Mittelweg zwischen Selbstregulierung und Kontrolle wählt.

Dazu wäre eine Onlineplattform, wie im Ansatz 3, der Ausgangspunkt. Im Gegensatz zu diesem Ansatz wird jedoch jede Selbstzertifizierung durch eine Behörde (eventuell auch mit Sitz in der EU) auf Einhaltung der Safe-Harbor-Richtlinien überprüft. Die Teilnahme am Modell ist erst nach positiver erfolgreicher Überprüfung gültig. Man ist daher zumindest im Bereich der Registrierungen nicht mehr auf die Kontrolle durch die Öffentlichkeit angewiesen.

In Bezug auf anlassunabhängige Kontrollverfahren ist (wie im Ansatz 2) keine Beschränkung auf interne Mechanismen zulässig und es muss durch qualifizierte Organisationen geprüft und bescheinigt werden, dass die Datenschutzrichtlinien ordnungsgemäß umgesetzt wurden. Das Beschwerdemanagement soll jedoch weiterhin über die Onlineplattform durchgeführt werden, um die Vorteile der einfachen Handhabung und der Transparenz als Druckmittel nutzen zu können.

Diese Variante erhöht das Schutzniveau, in dem sie die Vorteile der beiden zuerst genannten Ansätze verbindet. Wie die Ansätze 2 und 3, sind auch bei dieser Variante keine gravierenden Einschnitte in US-amerikanisches Recht notwendig.

Als Schwächen sind eine höhere finanzielle Belastung und die weiterhin bestehende Abhängigkeit von US-amerikanischen Behörden festzuhalten, da man auf die sorgfältige Überprüfung der Datenschutzrichtlinien aufbaut.

7.6 Unbedingt notwendige Maßnahmen

Höchste Priorität bei der Umsetzung des Safe-Harbor Modells hat die Sicherstellung des Rechtsschutzes der betroffenen Personen. Die folgenden Maßnahmen sind daher deutlich wichtiger als die anlassunabhängigen Kontrollverfahren und müssen

unabhängig vom gewählten Ansatz durchgeführt werden (bei erfolgreicher Einführung des ersten Ansatzes sind einige Punkte nicht unbedingt zwingend).

7.6.1 Standardisierung der Sanktionen

Da der aktuelle Durchsetzungsgrundsatz den unabhängigen Schiedsstellen erlaubt, Sanktionen nach eigenem Ermessen zu verhängen, sind die Sanktionsmaßstäbe der verschiedenen Organisationen sehr unterschiedlich oder teilweise nicht vorhanden. Um in Zukunft eine angemessene Durchsetzung sicherzustellen, sollte das Safe-Harbor Modell einen einheitlichen und strengen Maßnahmenkatalog gegen Verstöße vorsehen.

7.6.2 Erweiterung des internationalen Einflusses der FTC

Um das Problem, dass die FTC keine ausreichende Autorität hat, um Verstöße ohne inländischen Bezug zu sanktionieren, zu lösen, gibt es zumindest zwei mögliche Varianten.

7.6.2.1 Kooperation mit Generalstaatsanwälten

Die FTC könnte sich vom Generalstaatsanwalt des jeweils betroffenen Bundesstaates vertreten lassen um gegen Safe-Harbor-Sünder vorgehen zu können.⁵⁴⁸ Denn Bundesstaaten haben erstens die Gewalt, einige Datenschutzaspekte zu regulieren und zweitens dürfen sie auch internationale Angelegenheiten behandeln.⁵⁴⁹

7.6.2.2 Anpassung der Befugnisse der FTC

Eine einfachere und unbürokratischere Alternative ist es, die Handlungsgewalt der FTC in Bezug auf die Durchführung irreführender und betrügerischer Handlungen auszuweiten.⁵⁵⁰ Diese Änderung könnte die FTC relativ einfach eigenständig durchführen.⁵⁵¹ Die FTC besitzt die Freiheit, Statuten aus dem ihr zu Grunde liegendem FTC-Act unterschiedlich zu interpretieren, solange die ursprüngliche Interpretation nicht zweifelfrei war.⁵⁵² Grundsätzlich gestattet der FTC-Act der FTC zwar ausdrücklich, den Handel mit ausländischen Nationen zu regulieren, diese Erlaubnis wurde durch US-Gerichte jedoch eingeschränkt.⁵⁵³ Die FTC könnte einfach ihre eigene Interpretation veröffentlichen, die ihr Sanktionen gegen irreführende und betrügerische Handlungen im Ausland erlauben.⁵⁵⁴ Diese eigene Interpretation hätte Vorrang gegenüber den bisherigen Entscheidungen und wäre daher rechtlich bindend.⁵⁵⁵

7.6.2.3 Verpflichtung der FTC zu Ermittlungen

Die Tatsache, dass die FTC nur Untersuchungsanträge von Selbstregulierungsorganen behandeln darf und selbst diesen nicht zwingend nachkommen muss, ist ein

⁵⁴⁸ Vgl. Leathers, 233.

⁵⁴⁹ Ebd.

⁵⁵⁰ Ebd.

⁵⁵¹ Ebd.

⁵⁵² Vgl. Leathers, 234.

⁵⁵³ Ebd.

⁵⁵⁴ Ebd.

⁵⁵⁵ Ebd.

Mangel im Safe-Harbor Modell, der im Zuge einer Neuverhandlung überarbeitet werden muss.

Einerseits sollte die FTC künftig Beschwerden von unabhängigen Schiedsstellen, europäischen Datenschutzorganisationen und auch von den betroffenen EU-Bürgern selbst entgegennehmen dürfen.⁵⁵⁶ Andererseits sollten Anträge europäischer Datenschutzbehörden und Streitschlichtungsstellen sogar verpflichtend bearbeitet werden. Dadurch wäre zumindest sichergestellt, dass selbst aktiv gewordene Betroffene ihre Rechte durchsetzen können.

Ein weiterer enormer Vorteil dieser Änderung wäre, dass die FTC ihre beschränkten Kapazitäten besser nutzen könnte.⁵⁵⁷ Sie müsste in vielen Fällen keine eigenständigen Untersuchungen durchführen, indem sie auf bestehende Unterlagen und Ergebnisse europäischer Institutionen zugreifen könnte.⁵⁵⁸ Es handelt sich auch um eine Frage der Motivation: Organisationen aus der EU, wie die nationalen Datenschutzbehörden, werden ihre Ressourcen zur Bekämpfung von Safe-Harbor-Verletzungen effektiver und motivierter einsetzen, da das Recht europäischer Bürger durchzusetzen ist.⁵⁵⁹

7.6.3 Verpflichtende Kooperation mit europäischen Datenschutzbehörden

Im Rahmen der FAQ 11 des Safe-Harbor Modells wird zur Erfüllung der Forderung nach unabhängigen Schiedsstellen als eine von drei Optionen die Möglichkeit geboten, sich zu verpflichten, mit den Datenschutzbehörden in der Europäischen Union oder mit deren bevollmächtigten Vertretern zusammenzuarbeiten. Viele Safe-Harbor-Teilnehmer haben sich bereits dieser Verpflichtung unterworfen. Trotzdem sollte diese Kooperation in Zukunft nicht mehr auf freiwilliger Basis stattfinden, sondern ein verpflichtender Bestandteil des Modells sein. Weiters ist es notwendig, diese Zusammenarbeit genau zu definieren, damit auch zweifelfrei sichergestellt ist, dass die Unternehmen Entscheidungen der europäischen Behörden respektieren müssen.

Da Safe-Harbor auf die Einhaltung europäischer Regeln abzielt und mit der FTC eine amerikanische Behörde die Entscheidung über Sanktionen trifft, sollte es im Sinne des Konsumentenschutzes bei jedem Beschwerdeverfahren die Möglichkeit geben, eine europäische Datenschutzbehörde einzuschalten, die den Betroffenen vertritt.

Dafür spricht zum einen die höhere Bereitschaft europäischer Institutionen, die Interessen europäischer Bürger zu vertreten. Weiters sind Datenschutzbehörden in der EU in jedem Fall wirtschaftlich unabhängig von US-amerikanischen Unternehmen, wodurch das Risiko vermieden wird, dass zu Unrecht gegen den Konsumenten entschieden wird. Schließlich werden auch Probleme wie sprachliche Barrieren, die für manche Konsumenten eine nicht zu unterschätzende Schwierigkeit darstellen können, beseitigt.

⁵⁵⁶ Vgl. Leathers, 236.

⁵⁵⁷ Ebd.

⁵⁵⁸ Ebd.

⁵⁵⁹ Ebd.

7.6.4 Einführung schnellerer Sanktionsmöglichkeiten

Wie bereits erörtert, kann die FTC laut FAQ 11 nach einer Beschwerde als erste Konsequenz nur eine Verwarnung aussprechen und Handlungen, die gegen das Modell verstoßen, untersagen. Um zu verhindern, dass jedes Unternehmen so lange gegen die Datenschutzrichtlinien verstößt, bis es erstmals ermahnt wurde, sollte diese Regelung angepasst werden.

Der Durchsetzungsgrundsatz des Safe-Harbor Modells sollte daher auch bei erstmaligen Verstößen eines Unternehmens Sanktionen ermöglichen, die das Unternehmen unmittelbar treffen. Verwarnungen sind durchaus zielführend und wünschenswert, jedoch sollten diese ohnehin bereits durch die zuständige Streitschlichtungsstelle ausgesprochen worden sein. Man kann daher davon ausgehen, dass sich Beschwerden, die tatsächlich auf Ebene der FTC behandelt werden, auf bewusste Vergehen beziehen. Da die FTC grundsätzlich nur Beschwerden behandelt, für deren Klärung die Befugnisse der Streitschlichtungsstellen nicht ausgereicht haben, wären sofortige Sanktionen seitens der FTC durchaus angemessen.

Dies sollte vor allem in Fällen angewandt werden, deren Verstöße große Ähnlichkeit zu vergangenen, bereits sanktionierten Vergehen anderer Unternehmen haben. Dadurch könnte man einerseits den Verwaltungsaufwand der FTC senken und andererseits eine abschreckende Wirkung erzielen.

7.7 Fazit

Es gibt genügend mögliche Maßnahmen, um das Safe-Harbor-Programm bedeutend sicherer und damit auch wieder glaubwürdig zu machen. Während nur einige wenige Anpassungen tiefgreifende Änderungen US-amerikanischer Gesetze voraussetzen, werden ausreichend Alternativen angeboten, die lediglich höhere finanzielle Mittel und eine teilweise Neuverhandlung des Safe-Harbor Modells erfordern.

8 ZUSAMMENFASSUNG UND AUSBLICK

8.1 Zusammenfassung

Zusammenfassend werden Antworten auf die folgenden Fragen gegeben:

8.1.1 Was ist Safe-Harbor und funktioniert dieses Modell?

Nachdem die EU durch Erlass der EG-DSRL Transfers personenbezogener Daten in Drittstaaten mit unsicherem Datenschutzniveau grundsätzlich untersagt hat und auch die USA als solches Land klassifiziert wurden, würde die daraus resultierende Datenblockade schwere Folgen für die transatlantische Wirtschaft nach sich ziehen. Um dies zu verhindern wurde ein Modell verhandelt, das Datentransfers in die USA unter gewissen Auflagen ermöglicht. US-amerikanische Unternehmen, die sich dazu verpflichten, sieben Grundsätze bei der Verarbeitung personenbezogener Daten einzuhalten, nehmen demnach am Safe-Harbor teil und sind daher von diesem Verbot ausgenommen. Die Verpflichtung basiert auf Selbstzertifizierung in Verbindung mit der Erstellung firmeninterner Datenschutzrichtlinien.

8.1.2 Welche Mängel gibt es?

Wie Studien aufzeigen, haben sich zahlreiche Unternehmen selbst zertifiziert, ohne sich dabei auf die vollständigen Richtlinien zu beziehen. Die Teilnehmer können daher Daten beliebig importieren, ohne sich an die Grundsätze des sicheren Hafens zu halten. In der Praxis hat sich gezeigt, dass bei Verstößen keine Sanktionen verhängt werden.

8.1.3 Wieso funktioniert das System nicht?

Für das Scheitern des Systems gibt es mehrere Ursachen. Ein wichtiger Grund ist der große Anreiz, gegen das Modell zu verstoßen, da personenbezogene Daten einen enormen finanziellen Wert für die Werbebranche haben.

Die Hauptursache ist jedoch, dass die Durchsetzungsmechanismen vollständig versagen. Kontrolle der Qualität der firmeninternen Datenschutzrichtlinien bei der Einreichung der Selbstzertifizierung ist praktisch nicht gegeben und die Überprüfung der Einhaltung weist ebenfalls schwere Mängel auf. Diese kann bizarrerweise durch das Unternehmen selbst oder durch beliebige Dritte durchgeführt werden.

Streitschlichtungsstellen haben einerseits keine klaren Vorgaben, an die sie sich zu halten haben und sind andererseits zum Teil wirtschaftlich von den Safe-Harbor-Teilnehmern abhängig, weshalb sie bevorzugt zu deren Gunsten entscheiden.

Ein wichtiger Faktor ist, dass die FTC als die für Sanktionierung zuständige Stelle zehn Jahre lang gegen keinen einzigen Verstoß vorgegangen ist.

So ist es wenig verwunderlich, dass die Safe-Harbor-Grundsätze von den teilnehmenden Unternehmen mehr als Empfehlung statt als Verpflichtung betrachtet und ohne drohende Konsequenzen ignoriert werden. Außer Frage steht, dass sich nun Gravierendes an diesem Modell ändern muss.

Dass gegen diese Entwicklung so lange Zeit nichts unternommen worden ist, ist vor allem den Verantwortlichen in der EU zuzuschreiben. Diese haben ihre im Mo-

dell festgelegten Review-Aufgaben nicht ausreichend wahrgenommen bzw. den Ergebnissen keine Konsequenzen folgen lassen. Der Druck, etwas zu verändern, muss jedenfalls von europäischer Seite erzeugt werden, da für die US-Behörden der Schutz personenbezogener Daten von EU-Bürgern keine wesentliche Rolle spielt, so lange keine Maßnahmen seitens der EK gesetzt werden.

8.1.4 Wie konnte ein derartiger Missbrauch ohne Konsequenzen stattfinden?

Die Ursache dafür ist in der Passivität der EK zu suchen. Es wurden zwar Studien in Auftrag gegeben, die Probleme und Mängel bei der Umsetzung des Modells aufgezeigt haben, aus den Resultaten wurden jedoch nicht die notwendigen Maßnahmen abgeleitet. Die Untersuchungen haben sich mit Schwächen des Modells befasst, die zu Missbrauch führen können. Wären rechtzeitig konkrete schwerwiegende Missbrauchsfälle medienwirksam aufgedeckt worden, hätte man vermutlich früher Konsequenzen gezogen.

8.1.5 Wie kann die Situation nachhaltig verbessert werden?

Die wahrscheinlich beste Lösung wäre die Einrichtung einer unabhängigen Datenschutzbehörde in den USA, wie es auch die EU-Kommissarin für Justiz, Viviane Reding, anstrebt. Um diesen Plan zu verwirklichen, sind jedoch Änderungen im US-amerikanischen Recht notwendig, da diese Behörde mit umfangreichen Kompetenzen ausgestattet sein muss. Da bezweifelt werden darf, dass diese Umsetzung tatsächlich in absehbarer Zeit gelingt, sollten auf jeden Fall auch andere Maßnahmen in Betracht gezogen werden. Alternativen müssen darauf basieren, dass sich die teilnehmenden Unternehmen nicht mehr ausschließlich selbst kontrollieren dürfen, da diese Vorgangsweise für großes Missbrauchspotenzial sorgt.

Ein möglicher Ansatz wäre, verstärkte Prüfungen der firmeninternen Datenschutzrichtlinien im Rahmen der Selbstzertifizierung durchzuführen und für die Kontrolle der Einhaltung ausschließlich unabhängige, zertifizierte Stellen zuzulassen. Außerdem sind die Sanktionsbefugnisse der FTC in Bezug auf das Safe-Harbor Modell auszuweiten, damit diese effektivere Maßnahmen ergreifen kann. Weiters soll Betroffenen die Möglichkeit gegeben werden, Beschwerden über europäische Datenschutzbehörden abwickeln zu können.

Eine Alternative wäre die Verbesserung des Selbstregulierungsmechanismus durch Erhöhung der Transparenz und Vereinfachung des Beschwerdewegs. Dazu müsste die Safe-Harbor-Datenbank auf einer Web 2.0 Plattform basieren, auf der die Datenschutzrichtlinien der Teilnehmer durch Interessierte (Crowdsourcing) bewertet und kommentiert werden sollen. Beschwerden sollten ebenfalls über dieses Portal abgewickelt und Verstöße veröffentlicht werden. Dadurch sollen teilnehmende Unternehmen in die Verantwortung genommen werden, den Verpflichtungen nachzukommen, die zum Führen des Gütesiegels aufgelegt werden.

Als letzte Option könnten die beiden vorherigen Ansätze kombiniert werden, wodurch man die Wirksamkeit erhöhen würde. Daraus ergäben sich jedoch höhere Kosten.

8.2 Ausblick

Es ist von größter Bedeutung, dass die EK diesem Thema hohe Priorität beimisst und mit Entschlossenheit die Durchsetzung der Rechte europäischer Bürger in den Verhandlungen mit den USA einfordert. Dabei ist es wichtig, sich nicht mit unzureichenden Kompromissen zufrieden zu geben, sondern ein Ergebnis zu erreichen, das auch langfristig hohen Datenschutz sicherstellen kann.

Sollten die Vertreter der USA keiner angemessenen Lösung zustimmen, kommt eine Beendigung des Safe-Harbor-Modells als Druckmittel durchaus in Frage. Da es zur transatlantischen Übermittlung personenbezogener Daten zwei weitere Möglichkeiten (Standardvertragsklauseln und Binding Corporate Rules) gibt, würde eine Beendigung des Modells zwar schwerwiegende Folgen für die betroffenen Unternehmen haben, jedoch keine vollständige Datenblockade nach sich ziehen.

8.3 Offene Frage

Abschließend muss betont werden, dass der Schutz personenbezogener Daten kein Thema ist, das die EU nur in Verbindung mit den USA betrifft, sondern dass es sich um eine Problematik handelt, die viele weitere unsichere Drittstaaten betrifft, in denen ebenso essentielle Wirtschaftspartner ihren Sitz haben.

Offen bleibt daher die spannende Frage, wie die EU generell internationale Verstöße gegen EU-Datenschutzrecht sanktionieren möchte, die nicht unter das Safe-Harbor Modell fallen. Dazu zählen vor allem Betreiber von Online-Diensten, die keinen Sitz innerhalb der EU haben, unabhängig davon, ob die Daten in die USA oder einen anderen unsicheren Drittstaat übertragen werden.

Besonders der Vorstoß der EU-Kommissarin für Justiz, Datenschutz standortunabhängig wirksam machen zu wollen, lässt mit Spannung auf die Durchsetzung warten.

ABBILDUNGSVERZEICHNIS

Abbildung 1: Rechtsschutz nach dem DSGVO.....	26
Abbildung 2: Beispiel einer Zertifizierung.....	42
Abbildung 3: Safe-Harbor-Logo.....	64
Abbildung 4: Ungültiges Logo 1.....	65
Abbildung 5: Ungültiges Logo 2.....	65
Abbildung 6: Ungültiges Logo 3.....	65
Abbildung 7: Entwicklung der Safe-Harbor Teilnehmerzahl.....	72

TABELLENVERZEICHNIS

Tabelle 1: Überprüfung der Safe-Harbor-Teilnehmerliste auf valide Zertifikate ...	61
Tabelle 2: Verfügbarkeit von Privacy Policies.....	62
Tabelle 3: Einträge bezüglich Streitschlichtungsstellen.....	64
Tabelle 4: Datenkategorien.....	66

LITERATURVERZEICHNIS

- Buck-Heeb*, Petra, Dieckmann Andreas: Selbstregulierung im Privatrecht
Tübingen, 2010
- Crid*: Safe Harbour Decision Implementation Study
Jan Dhont, María Verónica Pérez Asinari, Yves Poulet; 2004
- Galexia*, Chris Conolly: The US Safe Harbor - Fact or Fiction
Pyrmont, 2008
- Genz*, Alexander: Datenschutz in Europa und den USA, 1. Aufl.
Wiesbaden, 2004
- Jahnel*, Dietmar: Handbuch Datenschutzrecht
Wien, 2010
- Knyrim*, Rainer: Checkliste: Zulässigkeit eines internationalen Datenverkehrs nach
DSG 2000, Ecolex 2002, 470-472
- Leathers*, Daniel R.: Giving bite to the EU-U.S. Data Privacy Safe Harbor: Model
Solutions for Effective Enforcement, 2009
- Roßnagel*, Alexander: Regulierung und Selbstregulierung im Datenschutz
Telekommunikation und Gesellschaft 2000, Band 8, Heidelberg, 2000
- Sonntag*, Michael: Einführung in das Internetrecht
Wien, 2010

RECHTSQUELLENVERZEICHNIS

- EG-DSRL: 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.
Amtsblatt Nr. L 281 vom 23/11/1995 S. 31 - 50
- SH-E: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen 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.
Amtsblatt Nr. L 215 vom 25/08/2000 S. 7 - 47
- Beschluss des
Düsseldorfer Kreises: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover.
- BT Drs-Nr. 17/3250: Kleine Anfrage mehrerer Abgeordneter zum Deutschen Bundestag zur Einhaltung der Safe-Harbor-Grundsätze bei der transatlantischen Datenübermittlung.
- BT Drs-Nr. 17/3375: Antwort der Bundesregierung auf die Anfrage zur Einhaltung der Safe-Harbor-Grundsätze bei der transatlantischen Datenübermittlung.
- E-010411/2010: Anfrage zur schriftlichen Beantwortung an die Kommission durch die Abgeordneten zum Europäischen Parlament Sophia in 't Veld und Jan Philipp Albrecht sowie die Antwort der Kommission.
- Kerry: Gesetzesentwurf der Senatoren Kerry und McCain: The Commercial Privacy Bill of Rights Act of 2011.
- SEK(2002) 196: Arbeitsdokument der Kommissionsdienststellen über die Umsetzung der Entscheidung 520/2000/EG 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. Feber 2002.
- WP 12: Arbeitsunterlage der Gruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten (Artikel 29-Datenschutzgruppe): „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU“. Angenommen am 24. Juli 1998.

DLA Piper

http://blog.dlapiper.com/detechnology/entry/düsseldorfer_kreis_richtlinien_zu_safe
(abgerufen am 22.2.2011)

Europäische Kommission

<http://ec.europa.eu/justice/policies/privacy/thridcountries/>
(abgerufen am 9.3.2011)

Export.gov

http://www.export.gov/safeharbor/eg_main_020436.asp
(abgerufen am 21.3.2011)

Federal Trade Commission

<http://www.ftc.gov/opa/2009/10/safeharbor.shtm>

(abgerufen am 3.3.2011)

<http://ftc.gov/opa/2011/03/google.shtm>

(abgerufen am 19.4.2011)

<http://ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf>

(abgerufen am 19.4.2011)

Frankfurter Allgemeine Zeitung, 17.10.2010

<http://www.faz.net/s/Rub594835B672714A1DB1A121534F010EE1/Doc~E5205C93A4508472CB610D9565E72C5BD~ATpl~Ecommon~Scontent.html>

(abgerufen am 24.10.2011)

Futurezone.at

<http://www.futurezone.at/stories/1665356/>

(abgerufen am 24.2.2011)

German American Law Journal

<http://amlaw.us/kamps1.shtml>

(abgerufen am 3.1.2011)

Germany Trade & Invest, [http://www.gtai.de/DE/Content/_SharedDocs/Links-](http://www.gtai.de/DE/Content/_SharedDocs/Links-Einzeldokumente-Datenbanken/fachdokument.html?fid=MK200709288001)

Einzeldokumente-Datenbanken/fachdokument.html?fid=MK200709288001

(abgerufen am 22.2.2011)

Golem.de

<http://www.golem.de/1101/80917.html>

(abgerufen am 4.5.2011)

Google FAQ

<http://www.google.com/intl/de/privacy/faq.html>

(abgerufen am 28.2.2011)

Heise.de

[http://www.heise.de/newsticker/meldung/US-Senat-befragt-Apple-und-Google-zu-](http://www.heise.de/newsticker/meldung/US-Senat-befragt-Apple-und-Google-zu-Datenschutz-1241671.html)

[Datenschutz-1241671.html](http://www.heise.de/newsticker/meldung/US-Senat-befragt-Apple-und-Google-zu-Datenschutz-1241671.html)

(abgerufen am 25.5.2011)

Heise.de

[http://www.heise.de/newsticker/meldung/Facebook-verstoest-gegen-europaeische-](http://www.heise.de/newsticker/meldung/Facebook-verstoest-gegen-europaeische-Datenschutzstandards-915756.html)

[Datenschutzstandards-915756.html](http://www.heise.de/newsticker/meldung/Facebook-verstoest-gegen-europaeische-Datenschutzstandards-915756.html)

(abgerufen am 28.7.2011)

Intern.de

[http://www.intern.de/internet-news/9052-google-hat-gegen-das-safe-harbor-](http://www.intern.de/internet-news/9052-google-hat-gegen-das-safe-harbor-abkommen-verstwikossen-muss-datenschutz-audits-ueber-sich-ergehen-lassen.html)

[abkommen-verstwikossen-muss-datenschutz-audits-ueber-sich-ergehen-lassen.html](http://www.intern.de/internet-news/9052-google-hat-gegen-das-safe-harbor-abkommen-verstwikossen-muss-datenschutz-audits-ueber-sich-ergehen-lassen.html)

(abgerufen am 19.4.2011)

Netzwelt.de

<http://www.netzwelt.de/news/82527-datenschutz-google-street-view-speichert-wlan-netze.html>

(abgerufen am 25.2.2011)

PaidContent.org – The Economics of Digital Content

<http://paidcontent.org/article/419-kerry-mccain-privacy-billopt-outs-are-in-do-not-track-is-out/>

(abgerufen am 3.5.2011)

Privacy and Information Security law blog

<http://www.huntonprivacyblog.com/2009/09/articles/enforcement-1/ftcs-first-safe-harbor-enforcement-action/>

(abgerufen am 3.3.2011)

Reuters.com

<http://www.reuters.com/article/2011/04/12/us-congress-privacy-idUSTRE73B59E20110412>

(abgerufen am 4.5.2011)

SUMO – Das junge online Magazin

<http://www.sumomag.at/knowhow/medienlandschaft/72-datenschutz-google-analytics.html>

(abgerufen am 25.2.2011)

ThomasHelbing.com

<http://www.thomashelbing.com/de/datenschutz-konzern-internationale-datentransfer-teil-2-safe-harbor-bcr-binding-corporate-rules-eu-standardvertragsklauseln>

(abgerufen am 9.3.2011)

Unwatched.org, Das Datenschutzportal

http://www.unwatched.org/EDRigram_9.6_Privacy_Platform_Meeting

(abgerufen am 27.4.2011)

Welt online

<http://www.welt.de/die-welt/wirtschaft/article7801328/Europa-draengt-USA-zu-strengem-Datenschutz.html>

(abgerufen am 5.5.2011)

Wikipediaeintrag zu „Common Law“

http://de.wikipedia.org/wiki/Common_Law

(abgerufen am 28.2.2011)

Wikipediaeintrag zu „Google“

<http://de.wikipedia.org/wiki/Google>

(abgerufen am 19.4.2011)

Wikipediaeintrag zu „Facebook“

<http://de.wikipedia.org/wiki/Facebook>

(abgerufen am 24.2.2011)

Wikipediaeintrag zu „IP-Adresse“

<http://de.wikipedia.org/wiki/IP-Adresse>

(abgerufen am 28.2.2011)