C. Artikel 25 der Richtlinie

Der Artikel 25 der Richtlinie regelt die Grundsätze des Drittländertransfers.

Gemäß Absatz 1 ist eine Übermittlung in ein Drittland nur zulässig, sofern das Bestimmungsland einen angemessenen Datenschutz garantiert. Anhaltspunkte für die Bewertung des Schutzniveaus liefert der zweite Absatz der Vorschrift.[293]

In Absatz 3 ist darüber hinaus eine gegenseitige Pflicht der Mitgliedstaaten und der Kommission zur Unterrichtung über Fälle vorgesehen, in denen ein Drittland nicht über ein angemessenes Schutzniveau verfügt.

Die Absätze 4 bis 6 beschäftigen sich schließlich mit dem Verfahren der Europäischen Kommission gemäß Artikel 31 Absatz 2 der Richtlinie zur Feststellung des Vorliegens oder des Fehlens eines angemessenen Schutzniveaus:

Ist in dem betreffenden Drittland kein angemessenes Schutzniveau im Hinblick auf die angestrebte Übermittlung oder die geplanten Kategorien von Übermittlungen gewährleistet, müssen die Mitgliedstaaten für die Unterbindung weiterer gleichartiger Datentransfers Sorge tragen. Zudem soll die Kommission gemäß Absatz 5 Verhandlungen mit dem betreffenden Drittland einleiten, um der Lage Abhilfe zu schaffen.

Absatz 6 schließlich eröffnet die Möglichkeit zu der Feststellung eines angemessenen Schutzniveaus aufgrund der innerstaatlichen Rechtsvorschriften oder der internationalen Verpflichtungen, die das Drittland insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist. Eine positive Entscheidung der Kommission verpflichtet die Mitgliedstaaten gemäß Absatz 6 Satz 2, die aufgrund der Feststellung „gebotenen Maßnahmen“ zu treffen. Da es sich bei diesen Maßnahmen um einen unmittelbaren mitgliedstaatlichen Vollzug einer gemeinschaftsrechtlichen Entscheidung im Sinne des Artikels 249 Absatz 4 EGV handelt, gilt für sie das Effizienzgebot. Ein gleichartiger Transfer in das Drittland darf danach nicht mehr beziehungsweise nur noch unter

[293] Vgl. zur Angemessenheitsprüfung das Schaubild von *Bull*, 17 CLSR, S. 239, S. 240.

besonderen Umständen[294] mit der Begründung des Fehlens eines angemessenen Schutzniveaus verhindert werden.[295]

I. Die Grundsätze einer Angemessenheitsprüfung

Gemäß Artikel 25 Absatz 1 der Richtlinie dürfen personenbezogene Daten nur in solche Drittländer übermittelt werden, die über ein angemessenes Schutzniveau verfügen.

Eine Angemessenheitsprüfung setzt rein begrifflich voraus, dass zwei verschiedene Positionen zueinander in Relation gesetzt werden. Das wirft zunächst die Frage auf, woraus sich die Bezugsgröße ergibt, im Verhältnis zu der das Schutzniveau in dem Drittland angemessen sein soll. Darüber hinaus ist zu überlegen, welchen Maßstab der Begriff „angemessen“ an das Schutzniveau in dem Drittland anlegt.

1. Die Bezugsgröße der Angemessenheitsprüfung

Am Beginn jeder Angemessenheitsprüfung steht die Feststellung ihrer Bezugsgröße. Die Richtlinie selbst gibt keine Auskunft darüber, an welchem Grundwert das Schutzniveau in dem Drittland zu messen ist. Zunächst ist daher die rechtliche Quelle der Bezugsgröße zu ermitteln. Erst im Anschluss daran kann der Prüfungsradius für die Beurteilung des Schutzniveaus gezogen werden.

a. Die rechtliche Quelle

Als rechtliche Quelle kommen sowohl die jeweiligen mitgliedstaatlichen Datenschutzgesetze als auch ein ihnen gemeinsamer Standard sowie schließlich die Richtlinie 95/46/EG selbst in Betracht.

Die unmittelbare Rechtsgrundlage eines Drittländertransfers ergibt sich aus dem jeweiligen mitgliedstaatlichen Datenschutzgesetz, das die Schutzprinzipien der Richtlinie 95/46/EG in nationales Recht umsetzt.

---

[294] Sofern etwa der konkrete Datenempfänger in dem Drittland kein angemessenes Schutzniveau garantiert.

[295] Kaminski u. a. (*Blömer/Moos*), 2. Kap. D, Rn. 55; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 25, Rn. 24 f.; *Ehmann*, CR 1991, S. 234, S. 236; *Franzen*, DB 2001, S. 1867, S. 1869; Roßnagel (- *Hillenbrand-Beck*), 5.4, Rn. 80; *Klug*, RDV 2000, S. 212, S. 214; *Reimer*, DuD 2000, S. 309; a. A. Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 30, der bei einer positiven Entscheidung der Kommission keine bestimmte Verpflichtung der Mitgliedstaaten annimmt, dabei jedoch das Effizienzgebot übersieht; dem folgend: *Draf*, S. 103.

Der für die Verarbeitung Verantwortliche oder alternativ in einigen Mitgliedstaaten eine unabhängige Datenschutzstelle sind nach dieser innerstaatlichen Rechtsgrundlage zur Feststellung der Angemessenheit in dem jeweiligen Drittland verpflichtet. Indessen entfaltet die Richtlinie selbst gemäß Artikel 249 Absatz 3 EGV keine unmittelbare Wirkung in den einzelnen Mitgliedstaaten.

Aus dieser Perspektive muss sich der Prüfungsmaßstab der Angemessenheit eindeutig aus den nationalen Datenschutzgesetzen ermitteln. Dafür scheint ferner zu sprechen, dass die Mitgliedstaaten gemäß dem Erwägungsgrund (22) der Richtlinie dazu befugt sind, die Rechtmäßigkeitsbedingungen einer Verarbeitung zu präzisieren und bestimmte Verarbeitungen auch in Spezialgesetzen zu regeln. Betrifft ein konkreter Transfer einen solchen Bereich, ist eine unterschiedliche Bewertung der Angemessenheit in den einzelnen Mitgliedstaaten und im Verhältnis zu der Richtlinie durchaus wahrscheinlich.[296] Insbesondere den Mitgliedstaaten mit einem im Einzelfall höheren Schutzniveau käme daher eine Angemessenheitsprüfung anhand ihrer nationalen Gesetze auf den ersten Blick zugute. Andererseits bestünde aber ein großer Anreiz zur Umgehung dieser Vorschriften und somit zum Export über solche Mitgliedstaaten, die über ein niedrigeres Schutzniveau verfügten.[297] Eine Harmonisierung des Binnenmarktes, die nach einer gewissen Abschottung des europäischen Datenschutzsystems nach außen verlangt, ist auf diese Weise nicht zu erreichen. Ferner scheint eine Konfrontation der Drittländer mit verschiedenen Schutzstandards im Hinblick auf die angestrebte Kooperation bei der Herstellung eines angemessenen Schutzniveaus wenig sinnvoll. Dementsprechend besteht ein Bedürfnis nach einem gemeinsamen Maßstab für alle Mitgliedstaaten.[298]

---

[296] *Hoeren*, WM 1994, S. 1, S. 7; *Wuermeling*, Handelshemmnis Datenschutz, S. 111; *Schwartz*, 80 Iowa L. Rev., S. 471, S. 487 und S. 495 f., der zudem befürchtet, dass einige Mitgliedstaaten trotz der Pflicht zur Harmonisierung den Drittstaatentransfer von einem gleichwertigen Schutzniveau abhängig machen würden.

[297] Vgl. *Deutscher Bundestag*, Sicherheit und Schutz im Netz, S. 250, der auf die Gefahr von Wettbewerbsverzerrungen und Umgehungsmöglichkeiten bei einer unterschiedlichen Umsetzung der Richtlinie insgesamt hinweist; vgl. ferner *Ellger*, RDV 1991, S. 121, S. 132, der sich wegen der Umgehungsgefahr für eine einheitliche Auslegung der Übermittlungsvorschriften ausspricht.

[298] *Wuermeling*, Handelshemmnis Datenschutz, S. 112; a. A. Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 7; Dammann/Simitis, EG-Datenschutzrichtlinie (- *ders.*), Einleitung, Rn. 30; *ders.*, NJW 1997, S. 281, S. 285; der ohne maßgebliche Begründung als Maßstab zur Feststellung eines angemessenen Schutzniveaus das deutsche BDSG heranzieht; so wohl auch *Wohlgemuth*, BB 1996, S. 690, S. 694, für den Bereich des Arbeitnehmer-Datenschutzes, der das Persönlichkeitsrecht des Arbeitnehmers bei Datenübermittlungen in Drittstaaten nur dann für ausreichend geschützt hält, sofern die Angemessenheit des Schutzniveaus in deutlicher Anlehnung an das deutsche Datenschutzrecht bestimmt wird; vgl. auch *Stein* in: Festschrift f. Rudolf, S. 513, S. 520, der sich von den Mitgliedstaaten eine Konkretisierung der Drittländerregelung erhofft.

Dafür sprechen auch die Regelungen des Artikels 25 Absatz 4 bis 6 der Richtlinie über das Verfahren der Europäischen Kommission zur Feststellung eines angemessenen Schutzniveaus in einem Drittland. Die Entscheidung der Kommission ist gemäß Artikel 25 Absatz 4 beziehungsweise Absatz 6 der Richtlinie für alle Mitgliedstaaten verbindlich. Infolgedessen dürfen Übermittlungen in solche Drittländer, deren Schutzniveau von der Kommission für angemessen erachtet wurde, nicht unterbunden werden, während ein Datentransfer in ein unsicheres Drittland verhindert werden muss.

Das Verfahren dient der Harmonisierung der mitgliedstaatlichen Übermittlungspraxis.[299] Aufgrund der Allgemeingültigkeit der Entscheidung kann die Kommission die Prüfung der Angemessenheit nicht an einem konkreten mitgliedstaatlichen Datenschutzgesetz ausrichten, sondern muss sich an einem gemeinsamen Nenner orientieren.[300]

Legten die Mitgliedstaaten bei ihren darüber hinaus gehenden Angemessenheitsprüfungen dennoch den Maßstab ihrer nationalen Gesetze an, gölten für die verschiedenen Drittländer unterschiedliche Beurteilungskriterien. Bestimmte Datenübermittlungen wären danach grundlos privilegiert. Von den handelspolitischen Konsequenzen im Verhältnis zu einigen Drittländern abgesehen wären auch Unternehmen benachteiligt, die ihren Sitz in einem Mitgliedstaat mit tendenziell strengeren Schutzgesetzen unterhielten. Sie erlitten einen erheblichen Wettbewerbsnachteil sowohl im eigenen Land als auch gegenüber den Unternehmen aus anderen Mitgliedstaaten, sofern ihre Geschäftspartner überwiegend in den nicht von der Kommission offiziell für sicher befundenen Drittländern niedergelassen wären. Einer solchen Wirkung des Datenschutzes soll aber die Umsetzung der Richtlinie in den Mitgliedstaaten gemäß Erwägungsgrund (7) gerade entgegenwirken.

Zudem erwiese sich die in Artikel 25 Absatz 3 der Richtlinie festgelegte gegenseitige Unterrichtungspflicht zwischen den Mitgliedstaaten und der Kommission über die Feststellungen hinsichtlich des Schutzniveaus in einem Drittland als ineffektiv, da jedes Land nur von der Beurteilung im Verhältnis zu dem eigenen Datenschutzgesetz berichten könnte.

---

[299] Grabitz/Hilf III (- *Brühann*), A 30, Art. 25, Rn. 22; *Schild*, EuZW 1996, S. 549, S. 553; *Thieffry*, Rn. 304.
[300] *Wuermeling*, Handelshemmnis Datenschutz, S. 112.

Eine einheitliche Bezugsgröße erscheint daher auch im Interesse der gemeinschaftlichen Verantwortung für eine wirkungsvolle Durchführung der Richtlinie geboten.

Es wird vertreten, dass sich der gemeinsame Maßstab aus der Gesamtheit der in Umsetzung der Richtlinie erlassenen mitgliedstaatlichen Datenschutzgesetze ergeben müsse.[301] Dieser aus den nationalen Gesetzen gebildete Standard könne wesentlich von dem Schutzniveau der Richtlinie abweichen. Es sei unter anderem möglich, dass einzelne Mitgliedstaaten den Umsetzungsspielraum der Richtlinie nutzen würden, um ein möglichst niedriges Schutzniveau zu erreichen. Unter diesen Umständen wäre zu besorgen, dass von einem Drittland bei Anlegung des Angemessenheitsmaßstabes der Richtlinie ein höherer Standard erwartet würde, als in dem betreffenden Mitgliedstaat selbst verwirklicht sei.

Ein solcher Sachverhalt ist jedoch eher unwahrscheinlich. Ein Mitgliedstaat, der nach der Übernahme der Richtlinienbestimmungen in sein nationales Recht über ein Schutzniveau verfügte, das hinter dem Angemessenheitserfordernis gegenüber Drittstaaten zurückbliebe, wird die Richtlinie kaum ordnungsgemäß umgesetzt haben.

Demgegenüber ist es sehr wahrscheinlich, dass alle Mitgliedstaaten in einzelnen Bereichen über das Schutzniveau der Richtlinie hinausgehen.[302] Da die Richtlinie 95/46/EG nur den Rahmen für den europäischen Datenschutz vorgibt, besteht dazu sogar unter Umständen eine Verpflichtung aus einer bereichsspezifischen Datenschutzrichtlinie[303].

Existiert andererseits keine gemeinsame Grundlage für die Abweichung, können die Modalitäten nicht nur in ihrer Strenge, sondern auch in ihrer Art und Weise erheblich divergieren und sich sogar in Einzelfällen gegenseitig widersprechen. Auf dieser Basis dürfte es sich in den meisten Fällen als unmöglich erweisen, ein gemeinsames Schutzniveau festzustellen, das nicht mit dem der Richtlinie identisch ist. Eine Mehrheitsentscheidung zugunsten der jeweils am häufigsten gewählten Umsetzungsmodalitäten könnte tatsächlich in einigen Mitgliedstaaten zu dem Wertungswiderspruch führen, dass inländische Verarbeitungen nachsichtiger behandelt würden als solche in Drittstaaten. Die gemein-

[301] So *Wuermeling*, Handelshemmnis Datenschutz, S. 112 f.
[302] *Blume*, CRi 2001, S. 11.
[303] Z. B. aus der Datenschutzrichtlinie 2002/58/EG für elektronische Kommunikation (ABl. EG Nr. L 201 vom 31.07.2002, S. 37).

same Grundlage einer Angemessenheitsprüfung ist demnach nicht in den mitgliedstaatlichen Datenschutzgesetzen zu suchen.

Ein einheitlicher Maßstab für alle Mitgliedstaaten ist sinnvoll im Grunde nur der Richtlinie selbst zu entnehmen. Die mitgliedstaatlichen Datenschutzgesetze verpflichten daher zur Bewertung des Schutzniveaus anhand der in das einzelstaatliche Recht übernommenen Richtlinienbestimmungen in deren ursprünglicher Richtlinienfassung, also ohne Rücksichtnahme auf nationale Eigenheiten. Da jedoch auch die bereichsspezifischen Datenschutzrichtlinien sowie zukünftige internationale, von allen Mitgliedstaaten ratifizierte Abkommen, etwa des Europarates oder der Vereinten Nationen,[304] das gemeinschaftliche Schutzniveau prägen und einheitlich ergänzen, sind die entsprechenden Bestimmungen in die Aussage der Schutzprinzipien zu integrieren.

b. Der Prüfungsradius

Weiterhin ist der Prüfungsradius für die Beurteilung des Schutzniveaus in dem Drittland zu bestimmen.

In Betracht kommt zunächst ein Vergleich der Schutzprinzipien mit dem gesamten Datenschutzsystem des Drittlandes im Hinblick auf sämtliche Übermittlungskonstellationen. Einen derart pauschalen Ländervergleich sah der erste Vorschlag zur Richtlinie noch vor. Der Nachteil einer abstrakten Bewertung des Datenschutzstandards eines Drittlandes liegt jedoch auf der Hand: Ein negatives Ergebnis auf nur einem einzelnen Sektor würde dabei zu einem den internationalen Handel hemmenden Transferverbot für das gesamte Drittland führen und somit unter Umständen erhebliche Beeinträchtigungen wirtschaftlicher Interessen sowohl der Mitgliedstaaten als auch des Drittlandes verursachen.

Vor diesem Hintergrund sehen die Vorschriften über den Drittländertransfer seit dem geänderten Vorschlag[305] zur Richtlinie in Artikel 25 Absatz 2 vor, dass die Angemessenheit „unter Berücksichtigung aller Umstände (...), die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen“, zu ermitteln sei. Das Schutzniveau in dem Drittland muss daher nicht insgesamt im Verhältnis zu dem europäischen Datenschutzrecht angemessen sein, sondern

[304] *Wuermeling*, Handelshemmnis Datenschutz, S. 112.
[305] Dort noch in Artikel 26 Absatz 2.

nur im Hinblick auf die Erfordernisse einer konkreten Übermittlung.[306] Im Grunde ist also ein einzelfallbezogener Vergleich vorzunehmen zwischen dem Schutz, den das Drittland für die übermittelten Daten bietet, mit demjenigen Schutz, den die Daten bei einem innereuropäischen Transfer erfahren würden. Diese Vorgehensweise gewährleistet eine jeweils individuelle Beurteilung des Datenschutzniveaus im Hinblick auf die besonderen Bedürfnisse bei einem konkreten Transfer. Sie ermöglicht den Beteiligten, auf spezielle Anforderungen einer empfindlichen Gefährdungslage für das allgemeine Persönlichkeitsrecht des Betroffenen einzugehen, ohne dabei den internationalen Datenverkehr mit einem generell überhöhten Schutzmaßstab unverhältnismäßig zu behindern.

Die Richtlinie eröffnet allerdings auch die Möglichkeit zur Feststellung eines angemessenen Schutzniveaus für eine „Kategorie von Datenübermittlungen". Eine Kategorisierung setzt eine hinsichtlich der Rechte des Betroffenen vergleichbare Gefährdungslage voraus, die unter Berücksichtigung aller Umstände eine einheitliche Bewertung des Schutzniveaus rechtfertigt. Die Zugehörigkeit zu einer Gruppe von Übermittlungen bestimmt sich daher in erster Linie nach dem gemeinsamen Thema und derselben Zweckbestimmung der Verarbeitung.[307] Die Kategorie kann sich jedoch auch aus dem Anwendungsbereich eines in jeder Hinsicht angemessenen sektorspezifischen Datenschutzgesetzes ergeben. Verfügt das Drittland indessen über ein umfassendes Datenschutzsystem, ist sogar die Bescheinigung eines insgesamt angemessenen Schutzniveaus[308] für den gesamten Datenverkehr mit diesem Drittland möglich.[309]

---

[306] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 9; *Simitis*, CR 2000, S. 472, S. 475; *ders*. in: Datenverkehr ohne Datenschutz?, S. 177, S. 189.

[307] *Abel*, BDSG, S. 65; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 9; *Draf*, S. 77.

[308] So bereits von der Europäischen Kommission entschieden für die Schweiz (Entscheidung 2000/518/EG vom 26.7.2000, ABl. EG Nr. L 215 vom 25.8.2000, S. 1), Ungarn (Entscheidung 2000/519/EG vom 26.7.2000, ABl. EG Nr. L 215 vom 25.8.2000, S. 4), Kanada (Entscheidung 2002/2/EG vom 20.12.2001, ABl. EG Nr. L 002 vom 4.1.2002, S. 13), Argentinien (Entscheidung 2003/490/EG vom 30.6.2003, ABl. EG Nr. L 168 vom 5.7.2003, S. 19), Guernsey (Entscheidung 2003/821/EG vom 21.11.2003, ABl. EG Nr. L 308 vom 25.11.2003, S. 27) und Isle of Man (Entscheidung 2004/411/EG vom 28.4.2004, ABl. EG Nr. L 151 vom 30.4.2004, S. 51).

[309] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 13; kritisch dazu demgegenüber Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 64 f., da dies dem Charakter einer Einzelfallentscheidung widerspreche.

2. Der Maßstab der Angemessenheit

Weiterhin ist zu klären, welchen Maßstab der Begriff der Angemessenheit im Verhältnis zu dem Standard der Richtlinie an das Schutzniveau in dem Drittland anlegt.

Dem reinen Wortsinn entsprechend bedeutet ‚angemessen' beziehungsweise die in den anderen Sprachversionen der Richtlinie in der jeweiligen Sprache verwendete Vokabel ‚adäquat' „den gegebenen Umständen entsprechend".[310] Das kann im Grunde zweierlei meinen: Einerseits kommt eine Forderung nach einer funktionalen Äquivalenz im Verhältnis zu den Schutzprinzipien der Richtlinie in Betracht.[311] Andererseits könnte auch ein minderes Schutzniveau dem Angemessenheitserfordernis genügen,[312] da eine Abwägung der gegebenen Umstände ebenfalls eine Berücksichtigung der praktischen Notwendigkeit eines Drittländertransfers gestattet.

Für die Forderung nach einer funktionalen Äquivalenz spricht, dass der Schutz des Persönlichkeitsrechts des Betroffenen in seiner Intensität und Effektivität dem europäischen Standard im Hinblick auf die konkrete Situation entsprechen sollte.

Diese Erklärung erweist sich jedoch nur dann als plausibel, sofern eine funktionale Äquivalenz nicht identisch mit einer Gleichwertigkeit ist. Im Unterschied[313] zu einem angemessenen Schutzniveau strebt die Richtlinie einen gleichwertigen Schutz der Daten nur auf dem Binnenmarkt an.[314] Der Verzicht auf einheitliche Bedingungen für den Datenverkehr mit Drittstaaten[315] basiert auf ökonomischen Erwägungen. Da

---

[310] Vgl. die Definition im Bedeutungswörterbuch des Dudens.

[311] So etwa: *Poullet* in: UNESCO, S. 147, S. 167; *ders.*, Data Protection Conference, Brüssel 2002, S. 4; *Simitis*, CR 2000, S. 472, S. 475; *ders.*, NJW 1997, S. 281, S. 284 f.; vgl. aber Dammann/Simitis, EG-Datenschutzrichtlinie (- *ders.*), Einleitung, Rn. 29; *Köhler/Arndt*, S. 294, verlangen pauschal eine Vergleichbarkeit.

[312] So etwa *Dippoldsmann*, KJ 1994, S. 369, S. 377; *Draf*, S. 88; *Ellger*, CR 1993, S. 2, S. 9; *Körner-Dammann*, RDV 1993, S. 14, S. 18; *Riemann*, CR 1997, S. 762, S. 763, der danach fragt, wie hoch das Schutzniveau sein muss.

[313] Grabitz/Hilf III (- *Brühann*), A 30, Art. 25, Rn. 16; *Gola/Schomerus*, BDSG, § 4b, Rn. 7; *Koch*, S. 331; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 28; *ders.*, NJW 1997, S. 281, S. 284; a. A. *Ellger*, RDV 1991, S. 121, S. 131, der ein angemessenes Schutzniveau nur bei einer Gleichwertigkeit annimmt.

[314] Erwägungsgründe (8) und (9); Artikel 30 Absatz 2 der Richtlinie.

[315] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 28; *ders.*, NJW 1997, S. 281, S. 284; *Stein* in: Festschrift f. Rudolf, S. 513, S. 518; missverständlich *Büllesbach* in: Datenverkehr ohne Datenschutz?, S. 51, S. 60, der im Hinblick auf Drittstaaten von

bisher kaum ein Drittland über ein gleichwertiges Datenschutzkonzept verfügt, stünde anderenfalls eine massive Behinderung der globalen Wirtschaftsbeziehungen zu befürchten.[316]

Eine Kongruenz des Terminus der funktionalen Äquivalenz mit der Gleichwertigkeit drängt sich regelrecht auf, da die Äquivalenz den Begriff der Gleichwertigkeit als Synonym bereits in sich trägt. Etwas anderes kann nur gelten, sofern dem Erfordernis eines gleichwertigen Schutzes ausschließlich durch ein identisches Datenschutzrecht entsprochen werden könnte. „Gleichwertig" bedeutet aber eben nicht „gleich",[317] sondern aufgrund seiner Elemente und seiner Funktionsweise von gleichem Wert und somit äquivalent.

Allerdings könnte die Richtlinie zwei verschiedene Gleichwertigkeitsmaßstäbe an den Binnenmarkt und an Drittländer anlegen wollen. So differenziert *Ellger* zwischen einer rechtlichen und einer funktionellen Gleichwertigkeit.[318] Eine rechtliche Gleichwertigkeit liege vor, sofern in dem Drittland Datenschutzgesetze existierten, die denen des Herkunftslandes der Daten in ihrer Art, ihrem Anwendungsbereich und in ihrem Schutzgehalt entsprächen. Eine funktionale Äquivalenz erfordere demgegenüber ein Schutzniveau, das zwar ebenfalls inhaltlich mit dem des Herkunftslandes übereinstimme, jedoch bereits mithilfe eines Vertrages umgesetzt werden könne. Es liegt nahe, diese Unterscheidung auf das Verhältnis zwischen dem auf dem Binnenmarkt geltenden und dem von einem Drittland geforderten Schutzniveau zu übertragen.

Zweifelsohne besteht für die Mitgliedstaaten eine Verpflichtung zur Schaffung eines rechtlich äquivalenten Datenschutzes. Daraus kann jedoch nicht gefolgert werden, dass Drittstaaten über ein funktional äquivalentes Schutzniveau verfügen müssten. Schließlich gilt der Maßstab der Angemessenheit nicht nur für die rechtstechnische Umsetzung des Datenschutzes, sondern auch für die inhaltlichen Prinzipien. Eine von der funktionalen Äquivalenz vorausgesetzte inhaltliche Gleichwertigkeit würde dem jedoch widersprechen.

---

einem „vergleichbare(n) Datenschutzniveau" spricht; so auch *Tauss/Özdemir*, RDV 2000, S. 143, S. 144.

[316] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, vor Art. 25, Rn. 2; *Geis*, NJW 1997, S. 288, S. 290.

[317] *Ellger*, CR 1993, S. 2, S. 9; *Wuermeling*, Handelshemmnis Datenschutz, S. 103.

[318] *Ellger*, S. 406 ff.

Da der Terminus der funktionalen Äquivalenz daher schon mit dem Begriff der Gleichwertigkeit belegt ist, kann er nicht zugleich ein angemessenes Schutzniveau umschreiben.

Der Angemessenheit ist im Verhältnis zu den Schutzprinzipien der Richtlinie folglich bereits genügt, sofern das betreffende Drittland im Hinblick auf die Risiken einer konkreten Übermittlung zwar ein minderes, aber noch ausreichendes Datenschutzniveau garantiert.[319] Da es sich bei der Richtlinie allerdings um einen konkretisierten Grundrechtsschutz handelt, müssen stets noch der Schutz der Privatsphäre, die Grundrechte sowie die Grundfreiheiten des Betroffenen gewährleistet sein.[320]

Ausnahmsweise vermag auch mal nur ein gleichwertiges Schutzniveau diesen Kriterien gerecht zu werden.[321] Im Regelfall kommt es aber nicht darauf an, dass sämtliche Verarbeitungsbedingungen der Richtlinie Eingang in das Datenschutzrecht des Drittlandes gefunden haben.[322] Vielmehr können sogar fehlende Regelungselemente durch andere, besonders effektiv gestaltete Schutzmechanismen kompensiert werden.[323] Im Ergebnis entscheidet über die Bewertung des Schutzniveaus also die Funktionalität des Datenschutzsystems, die sich jedoch nur dadurch auszuzeichnen hat, dass sie den Risiken eines Transfers mit angemessenen und nicht zwingend mit gleichwertigen Mitteln begegnet. In Anlehnung an den Terminus der funktionalen Äquivalenz bietet sich mithin für die Charakterisierung des Angemessenheitserfordernisses der Begriff der funktionalen Adäquanz[324] an.

---

[319] Davon auch ausgehend *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 25, Rn. 5; *Däubler* in: Tinnefeld/Philipps/Heil, S. 110, S. 122; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 8, der aber trotz eines minderen Schutzniveaus eine ‚funktionale Äquivalenz im qualitativen Sinne' verlangt; *Swire/Litan*, S. 33; *Weber*, DS im europ. Umfeld, S. 83, S. 100; *Wendel*, S. 60; *Wuermeling*, Handelshemmnis Datenschutz, S. 103; vgl. aber Grabitz/Hilf III (- *Brühann*), A 30, Art. 25, Rn. 16 f., der das Angemessenheitskriterium im Vergleich zur Gleichwertigkeit nicht für schwächer, sondern für ein aliud hält. Es würden nicht Rechtsordnungen miteinander verglichen, sondern Risiken mit Garantien. Diese Ansicht schließt aber nicht aus, dass eine Angemessenheit bereits durch ein niedrigeres Schutzniveau erreicht werden kann; vgl. auch Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 29, der zwar eine funktionale Äquivalenz verlangt, damit aber die Existenz eines „harten Kerns" der von der Richtlinie formulierten Verarbeitungsanforderungen meint; dem zustimmend: *Stein* in: Festschrift f. Rudolf, S. 513, S. 519.

[320] Grabitz/Hilf III (- *Brühann*), A 30, Art. 25, Rn. 14 f.; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 8; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 25, Rn. 4 u. 12; *Simitis*, CR 2000, S. 472, S. 475 f.; *Terwangne/Louveaux*, MMR 1998, S. 451, S. 456.

[321] *Draf*, S. 88.

[322] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 29.

[323] *Wuermeling*, Handelshemmnis Datenschutz, S. 128 f.

[324] *Draf*, S. 95 f.

II. Die Bewertungskriterien im Einzelnen

Die Beurteilung des Schutzniveaus eines Drittlandes erfordert zunächst die Feststellung generell feststehender Datenschutzprinzipien im Sinne eines Standardmaßstabes, an dem sich die Prüfung der Angemessenheit in dem konkreten Einzelfall orientieren kann. In einem weiteren Schritt ist schließlich auf die in Artikel 25 Absatz 2 der Richtlinie aufgezählten Umstände einzugehen, die bei einer konkreten Übermittlung eine Rolle spielen. Einerseits ist dabei zu prüfen, ob sich im Einzelfall aufgrund des Charakters einer Übermittlung eine Anpassung des Standardmaßstabes in Form einer Verringerung oder einer Verschärfung einzelner Prinzipien empfiehlt. Andererseits muss festgestellt werden, inwieweit der in dem Drittland bestehende Datenschutz den Anforderungen der Angemessenheit bei der konkreten Übermittlung gerecht wird.

1. Die grundsätzlichen Prinzipien eines angemessenen Schutzniveaus

Die grundsätzlichen Prinzipien eines angemessenen Schutzniveaus erschließen sich aus dem Inhalt der Richtlinie 95/46/EG.[325]

Daraus hat die gemäß Artikel 29 der Richtlinie eingesetzte Datenschutzgruppe in ihrer beratenden Funktion gegenüber der Europäischen Kommission gemäß Artikel 30 Absatz 1b) der Richtlinie und im Interesse einer einheitlichen Anwendung der Vorschriften über den Drittländertransfer gewissermaßen Standardprinzipien eines angemessenen Schutzniveaus entwickelt, deren Anforderungsprofil entsprechend den Umständen des Einzelfalls sowohl erweitert als auch reduziert werden kann.[326]

Der Arbeitsunterlage WP 12 der so genannten Art. 29-Gruppe entsprechend beurteilt sich ein angemessenes Schutzniveau nach der Maßgabe zweier Grundelemente: den inhaltlichen Prinzipien des Datenschutzes sowie den Mitteln zur Sicherung ihrer wirksamen Durchsetzung.[327]

Während sich die inhaltliche Angemessenheit nach der Gewährleistung von Rechten für den Betroffenen sowie der Auferlegung von Pflichten für die verarbeitende Stelle (Kapitel I, II und IV der Richtlinie) bemisst, beurteilt sich die Effektivität des Durchsetzungsmechanismus

[325] Siehe dazu Gliederungspunkt C.I.1.a. dieses Kapitels.
[326] *WP 12*, das die Arbeitsunterlagen *WP 4, WP 7* und *WP 9* zusammenfasst.
[327] *WP 12*, S. 5 ff.; so bereits in *WP 4*, S. 6 ff.

anhand der bereitstehenden Rechtsbehelfe, der Sanktionen, der haftungsrechtlichen Aspekte (Kapitel III der Richtlinie) sowie der Einrichtung von Kontrollstellen (Kapitel VI der Richtlinie).

Da die Arbeitsunterlage WP 12 unter maßgeblicher Mitwirkung von Vertretern der mitgliedstaatlichen Kontrollbehörden zustande gekommen ist, wird im Allgemeinen davon ausgegangen, dass es sich bei dieser Stellungnahme zugleich um eine (nicht verbindliche) Verständigung der Mitgliedstaaten auf eine einheitliche Auslegung der Richtlinie mit dem Ziel einer homogenen Beurteilung der Angemessenheit handelt. Im Hinblick auf die dem Dokument sonach zukommende Vorbildfunktion[328] wird die Arbeitsunterlage WP 12 daher in der nachfolgenden Analyse zum Ausgangspunkt für die Ermittlung des maßgeblichen Inhalts eines angemessenen Schutzniveaus genommen.

a. Die allgemeinen inhaltlichen Grundsätze

Als Kern einer inhaltlichen Angemessenheit hat die Art. 29-Gruppe in ihrer Stellungnahme zu dem Tatbestandsmerkmal des angemessenen Schutzniveaus folgende Schutzprinzipien erarbeitet:

(I) den Grundsatz der Beschränkung der Zweckbestimmung,
(II) den Grundsatz der Datenqualität und –verhältnismäßigkeit,
(III) den Grundsatz der Transparenz,
(IV) den Grundsatz der Sicherheit,
(V) das Recht auf Zugriff, Berichtigung und Widerspruch
s o w i e
(VI). die Beschränkung der Weiterübermittlung in andere Drittländer.

[328] Erwägungsgrund (3) der „Safe Harbor"-Entscheidung der *Europäischen Kommission*, ABl. EG Nr. L 215 vom 25.08.2000, S. 7; *Europäisches Parlament*, Entschließung des Europäischen Parlaments zu dem Entwurf einer Entscheidung der Kommission über die Angemessenheit der US-Grundsätze des Sicheren Hafens und diesbezügliche häufig gestellte Fragen (FAQ), vorgelegt vom Handelsministerium der USA (C5-0280/2000 – 2000/2144(COS)) vom 5.7.2000, A5-0177/2000, ABl. EG C 121 vom 24.4.2001, S. 152, S. 153 f.; *Brühann* in: Datenverkehr ohne Datenschutz?, S. 35, S. 40 ff.; *Eul/Godefroid*, RDV 1998, S. 185, S. 189; *Heil*, DuD 1999, S. 458, S. 459 f.; *Jacob* in: Datenverkehr ohne Datenschutz?, S. 25, S. 28 ff.; *ders*., RDV 1999, S. 1, S. 4 f.; Roßnagel (- *Hillenbrand-Beck*), 5.4, Rn. 84; *Klug*, BDSG, S. 135 f.; *ders*., RDV 1999, S. 109, S. 110; *Kuner*, DuD 2002, S. 553, S. 555, der unter Hinweis auf die Bezugnahme einer englischen Gerichtsentscheidung auf eine Arbeitsunterlage der Art. 29-Gruppe die insgesamt wachsende Bedeutung dieser Dokumente anmerkt; *Räther/Seitz*, MMR 2002, S. 425, S. 427; *Schaar*, Datenschutz im Internet, S. 38; *Tröndle*, CR 1999, S. 717, S. 721; wohl auch *Verbiest/Wéry*, Rn. 892; *Simitis*, CR 2000, S. 472, S. 476 ff.; Simitis u. a. (- *ders*.), BDSG, § 4b, Rn. 64 ff., der jedoch insgesamt skeptisch gegenüber der Zuordnung der Gruppe zu der Generaldirektion Binnenmarkt ist. Die Gruppe unterliege dadurch einem starken Einfluss der von dieser Generaldirektion betriebenen Politik.

Aufschluss über den Aussagehalt der entwickelten Prinzipien geben die kurzen Erläuterungen der Datenschutzgruppe, die nachstehend dargestellt und kommentiert werden.

(I). Der *Grundsatz der Beschränkung der Zweckbestimmung* (vgl. Artikel 6 Absatz 1b) der Richtlinie) gebiete, dass Daten nur für einen spezifischen Zweck verarbeitet würden. Die Verarbeitung und die Weiterübermittlung in dem Drittland dürften nicht mit dem Zweck des Drittländertransfers unvereinbar sein. Eine Ausnahme komme nur in Betracht, sofern sie im Einklang mit Artikel 13 der Richtlinie notwendig sei (a) für die Sicherheit des Staates, die Landesverteidigung oder die öffentliche Sicherheit, (b) im Rahmen der Bekämpfung von Straftaten und von Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, (c) für wichtige wirtschaftliche oder finanzielle Interessen eines Mitgliedstaates, der Europäischen Union oder des Drittlandes sowie (d) für den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

Der Grundsatz der Beschränkung der Zweckbestimmung beziehungsweise der Zweckbindungsgrundsatz steht mit der Zulässigkeit der Verarbeitung quasi in einer Wechselwirkung.

Die Verarbeitung von personenbezogenen Daten ist gemäß Artikel 7 der Richtlinie nur zu einem der in den Buchstaben b) bis f) genannten Zwecke zulässig. Auch eine Einwilligung des Betroffenen entsprechend dem Buchstaben a) darf nicht pauschal, sondern nur für einen im Einzelnen konkretisierten Verarbeitungszweck eingeholt werden.[329]

Der Zweckbindungsgrundsatz verhindert sodann eine Verarbeitung, die nicht mit diesem Ursprungszweck der Erhebung vereinbar ist. Regelmäßig entfiele zwar bei einer zweckwidrigen Verarbeitung bereits die Zulässigkeitsvoraussetzung gemäß Artikel 7 der Richtlinie, ebenfalls mit der Folge der Rechtswidrigkeit der Verarbeitung. Über diese Deckungsgleichheit mit Artikel 7 der Richtlinie hinaus verbietet der Zweckbindungsgrundsatz jedoch zudem, dass Daten selbst zu solchen Sekundärzwecken nicht ohne weiteres genutzt werden dürfen, die an sich im Einklang mit Artikel 7 der Richtlinie stünden.[330] Anderenfalls wären sowohl die Effektivität des Transparenzgebotes als auch die Durchführung einer zuverlässigen Kontrolle des Verarbeitungsprozes-

[329] *Schild*, EuZW 1996, S. 549, S. 551; *Swire/Litan*, S. 34.
[330] *Brühann*, RDV 1996, S. 12, S. 15.

ses gefährdet,[331] da der Betroffene sowie die Kontrollbehörden den Weg der Daten nicht mehr sicher nachvollziehen könnten.

Der Zweckbindungsgrundsatz nimmt daher eine zentrale Rolle in einem effektiven Datenschutzsystem ein.[332] Ein Verzicht auf seine Geltung in dem betreffenden Drittland würde den Weg zu einer Verwendungsfreigabe eröffnen[333] und zum Beispiel eine Sammlung personenbezogener Daten in außereuropäischen Depots für zukünftige, noch nicht näher definierte Zwecke legalisieren.[334]

Das Fehlen einer den Erlaubnistatbeständen des Artikels 7 der Richtlinie nachgebildeten Zulässigkeitsregel beeinträchtigt die Angemessenheit des Schutzniveaus indessen nicht. Die Zulässigkeit der Verarbeitung für den Datenempfänger ergibt sich ohnehin aus seiner Bindung an den Übermittlungszweck. Für die Übermittlung selbst wiederum gilt in jedem Fall noch die dem Artikel 7 der Richtlinie entsprechende mitgliedstaatliche Datenschutzbestimmung.

(II). Der Grundsatz der *Datenqualität* setze voraus, dass die Daten sachlich richtig und, wenn nötig, auf dem neuesten Stand seien (vgl. Artikel 6 Absatz 1d) der Richtlinie). Nach dem Grundsatz der *Datenverhältnismäßigkeit* sollten die Daten angemessen, relevant und im Hinblick auf die Zweckbestimmung, für die sie übertragen oder weiterverarbeitet würden, nicht exzessiv sein (vgl. Artikel 6 Absatz 1c) der Richtlinie).

Diese Grundsätze der Datenpflege gewährleisten, dass der Schutz des Betroffenen nicht nach einer erstmaligen Prüfung der Rechtmäßigkeit der Verarbeitung abbricht.[335] Vielmehr muss sich der konkrete Datenbestand dauerhaft als gerechtfertigt erweisen. Zwar hat die Art. 29-Gruppe dabei die Pflicht zu einer Löschung der Daten nicht explizit angesprochen. Jedoch ergibt sich diese bereits unmittelbar aus dem

---

[331] *Simitis*, CR 2000, S. 472, S. 474; Simitis u. a. (- *ders.*), BDSG, § 4b, Rn. 58.
[332] Spindler/Wiebe (- *Bizer/Trosch*), Kap. I, Rn. 15; *Gounalakis/Mand*, CR 1997, S. 431, S. 436; *Jacob* in: Datenverkehr ohne Datenschutz?, S. 25, S. 28; *ders.*, RDV 1999, S. 1, S. 4; *Koch*, S. 32; *Schild*, EuZW 1996, S. 549, S. 551; *Schwartz/Reidenberg*, S. 13; *Simitis* in: Datenverkehr ohne Datenschutz?, S. 177, S. 182 f.; Dammann/Simitis, EG-Datenschutzrichtlinie (- *ders.*), Einleitung, Rn. 31; *ders.*, NJW 1997, S. 281, S. 285; *Stein* in: Festschrift f. Rudolf, S. 513, S. 523.
[333] Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 58; *ders.* in: Datenverkehr ohne Datenschutz?, S. 177, S. 184.
[334] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 31; *ders.*, NJW 1997, S. 281, S. 285.
[335] *Wuermeling*, Handelshemmnis Datenschutz, S. 116.

Zweckbindungsgrundsatz: Da auch die Aufbewahrung eine Verarbeitung im Sinne des Artikel 2b) der Richtlinie ist, müssen Daten, deren Vorhaltung nicht mit dem Übermittlungszweck vereinbar ist, zwangsläufig gelöscht werden.

(III). Entsprechend dem *Transparenzgebot* sei der Betroffene über die Zweckbestimmung der Verarbeitung, die Identität des außereuropäischen Verantwortlichen und, sofern sich dies aus Billigkeitsgründen als erforderlich erweise, über andere Modalitäten der Verarbeitung zu informieren (vgl. Artikel 10 und 11 Absatz 1 der Richtlinie). Eine Ausnahme könne sich nur aus Artikel 13 der Richtlinie ergeben sowie aus dem Umstand, dass die Daten nicht bei der betroffenen Person erhoben worden seien und sich die Information des Betroffenen entweder als unmöglich darstelle, einen unverhältnismäßigen Aufwand erfordere oder die Speicherung beziehungsweise die Weitergabe der Daten durch Gesetz ausdrücklich vorgesehen sei (vgl. Artikel 11 Absatz 2 der Richtlinie).

Das Transparenzgebot soll verhindern, dass der Betroffene über die Verarbeitung seiner Daten im Ungewissen bleibt. Er muss überblicken, wer über welche Informationen hinsichtlich seiner Person verfügt, um sein Verhalten koordinieren zu können. Diesbezügliche Unsicherheiten vermögen den Betroffenen in der unbefangenen Ausübung seiner Freiheitsrechte in seinem sozialen und politischen Umfeld zu hemmen.[336] Zudem soll der Betroffene die Risiken einer Verarbeitung abschätzen können. Das gilt besonders für eine Verarbeitung in Drittländern,[337] da die Daten hier aus der Sicht des Betroffenen noch eher unkalkulierbaren Gefahren ausgesetzt sind als in den Mitgliedstaaten.

(IV). Gemäß dem Grundsatz der *Datensicherheit* obliege es dem für die Verarbeitung Verantwortlichen, geeignete technische und organisatorische Sicherheitsmaßnahmen für die Verarbeitung zu treffen, indem zum Beispiel alle unter seiner Verantwortung tätigen Personen nur auf seine Anweisung hin Daten verarbeiten dürften (vgl. Artikel 16 und 17 der Richtlinie).

Das Prinzip der Datensicherheit ergänzt die Bestimmungen über den Datenschutz. Ohne technische und organisatorische Vorkehrungen können die Daten nicht zuverlässig gegen unrechtmäßige Zugriffe und Kenntnisnahmen geschützt werden. Die datenschutzrechtlichen Rechte

[336] *BVerfGE* 65, S. 1, S. 42 f.; *Schwartz/Reidenberg*, S. 15.
[337] *Simitis*, CR 2000, S. 472, S. 477.

und Pflichten im Verhältnis zwischen dem Betroffenen und dem Verantwortlichen wären sonach in ihrer Wirkung stark beeinträchtigt.

(V). Nach dem *Recht auf Zugriff, Berichtigung* und *Widerspruch* könne der Betroffene eine Kopie aller ihn betreffenden Daten verlangen, die verarbeitet werden, sowie nötigenfalls auf deren Berichtigung bestehen (vgl. Artikel 12 der Richtlinie). Zudem sei ihm unter bestimmten Umständen[338] ein Widerspruchsrecht gegen zu spezifischen Zwecken durchgeführte Verarbeitungen einzuräumen (vgl. Artikel 14 der Richtlinie). Ausnahmen hiervon könnten sich nur aus Artikel 13 der Richtlinie ergeben.

Mithilfe der genannten Rechte kann der Betroffene Einfluss auf die Verarbeitung nehmen. Da er zur Ausübung seiner Ansprüche die wesentlichen Elemente einer Verarbeitung kennen muss, setzt die effektive Gewährleistung des Rechts auf Zugriff, Berichtigung und Widerspruch eine zuverlässige Informationsstruktur voraus[339] und ist folglich eng mit dem Transparenzgebot verwoben.

(VI). Zudem müsse für den Verarbeiter in dem Drittland ein *Übermittlungsverbot an weitere Drittländer* gelten. Ein etwaiger Transfer dürfe nur unter der Bedingung erlaubt sein, dass dieses zweite Drittland ebenfalls über ein angemessenes Schutzniveau verfüge; es sei denn, es liege eine Ausnahme des Artikels 26 Absatz 1 der Richtlinie vor (vgl. Artikel 25 und 26 der Richtlinie).

Die mit den Artikeln 25 und 26 der Richtlinie vergleichbare Übermittlungshürde rundet die Voraussetzungen an das Schutzniveau des Drittlandes ab. Sofern ein weiterer Transfer nicht schon mit dem ursprünglichen Übermittlungszweck unvereinbar wäre, könnten die Daten anderenfalls an beliebige Bestimmungsorte versandt werden und wären dort ihrer Schutzlosigkeit ausgesetzt. Ein derart durchlässiges System würde letztlich den Sinn und Zweck der Artikel 25 und 26 der Richtlinie nachträglich infrage stellen.

Sofern das angemessene Schutzniveau in dem ersten Drittland nur für eine bestimmte Übermittlung oder Kategorie von Übermittlungen be-

[338] Gemäß Artikel 14 a) der Richtlinie soll der Betroffene zum Beispiel Verarbeitungen nach Artikel 7e) und 7f) der Richtlinie widersprechen können, wenn dazu ein überwiegender, schutzwürdiger, sich aus der besonderen Situation ergebender Grund vorliegt.

[339] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 33; *ders.*, NJW 1997, S. 281, S. 285.

steht, muss im Hinblick auf die Effektivität des Systems darüber hinaus ein den Artikeln 25 und 26 der Richtlinie entsprechendes Übermittlungsverbot an weitere Empfänger aus demselben Drittland vorgesehen sein.[340]

b. Die besonderen inhaltlichen Grundsätze

Bei der Beurteilung des Schutzniveaus im konkreten Einzelfall kann das Anforderungsprofil unter Berücksichtigung des Ausmaßes der Gefahren, die für den Betroffenen der Datenübermittlung entstehen, gelockert oder verschärft werden. Die Arbeitsunterlage WP 12 der Art. 29-Gruppe detailliert einige sich aus den besonderen Merkmalen eines Transfers ergebenden Verarbeitungsmodalitäten wie folgt:

Der Transfer *sensibler Daten* im Sinne des Artikels 8 der Richtlinie erfordere zusätzliche Sicherheitsvorkehrungen wie beispielsweise das Einholen einer ausdrücklichen Einwilligung des Betroffenen.

Ferner solle bei einer Übermittlung zum Zwecke des *Direktmarketings* dem Betroffenen die Option einer jederzeitigen Entscheidung gegen eine derartige Verwendung („opt-out“) der Daten eingeräumt werden (vgl. Artikel 14b) der Richtlinie).

Eine *automatisierte Einzelentscheidung* (vgl. Artikel 15 der Richtlinie) begründe demgegenüber ein gesteigertes Informationsinteresse des Betroffenen, zum Beispiel hinsichtlich der einer Entscheidung zugrunde liegenden Logik (vgl. Artikel 12a), 3. Spiegelstrich, der Richtlinie).

Damit greift die Arbeitsunterlage WP 12 alle von der Richtlinie eigens genannten Verarbeitungsmodalitäten auf, die zusätzliche Anforderungen an das Schutzniveau in dem Drittland stellen.

Zu nennen ist in diesem Zusammenhang aber auch der Artikel 9 der Richtlinie, der sich mit den Ausnahmen für Verarbeitungen zu ausschließlich journalistischen, künstlerischen und literarischen Zwecken befasst. Danach kann das Recht auf freie Meinungsäußerung zu Abweichungen von den Richtlinienbestimmungen zwingen und somit zugleich eine Reduktion der Anforderungen an ein angemessenes Schutzniveau in einem Drittland rechtfertigen.

[340] *WP 12*, S. 12, sowie bereits *WP 7*, S. 3, im Hinblick auf die Weitergabe von Daten an eine Stelle, die einem angemessenen Selbstkontrollkodex nicht angeschlossen ist.

c. Die Durchsetzung des Schutzniveaus

Das zweite Grundelement eines angemessenen Schutzniveaus ist entsprechend der Arbeitsunterlage WP 12 der Art. 29-Gruppe die Existenz eines verfahrensrechtlichen Mechanismus beziehungsweise die Bereitstellung effektiver Instrumente zur Durchsetzung der inhaltlichen Schutzprinzipien.

Ein direkter Vergleich der Verfahrensregeln der Richtlinie mit den in Drittländern bestehenden Durchsetzungsmechanismen gestaltet sich jedoch überwiegend problematisch. Während die Richtlinie 95/46/EG in ihren wesentlichen Aussagen zum Inhalt eines effektiven Datenschutzes einen weitestgehend gemeinsamen Nenner in den Festlegungen des Übereinkommens Nr. 108 des Europarates[341] findet, das wiederum ähnliche Richtwerte vorgibt wie die diesbezüglichen Leitlinien der OECD[342] (1980) und der UNO[343] (1990),[344] geht sie hinsichtlich des verfahrensrechtlichen Mechanismus zur Durchsetzung der Datenschutzprinzipien, abgesehen von der Europaratskonvention, über die Vorgaben dieser Abkommen weit hinaus.

Nach europäischen Vorstellungen zeichnet sich ein effektiver Datenschutz durch eine gesetzliche Verankerung seiner Schutzprinzipien sowie durch eine Sanktionierung von Verstößen und eine Schadensersatzhaftung zugunsten jedes Geschädigten aus. Als unabdingbar gilt zudem die Einrichtung von externen und unabhängigen Kontrollstellen, die Überwachungsaufgaben wahrnehmen und Beschwerden nachgehen.

In diesem Sinne schreibt zwar das Übereinkommen des Europarates seinen Parteien eine gesetzliche Umsetzung seiner inhaltlichen Grundsätze vor und verlangt in seinem Zusatzprotokoll vom 8.11.2001 darüber hinaus nach der Einrichtung einer unabhängigen Kontrollstelle. Von den aufgezählten Maßnahmen mahnen indessen die OECD-Leitlinien lediglich eine Berücksichtigung ihrer inhaltlichen Vorgaben

---

[341] *Europarat*, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS 108) vom 28. Januar 1981 in der Fassung der vom Ministerkomitee am 15.6.1999 angenommenen Änderung und Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS 108) bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 8.11.2001 (ETS 181).

[342] *OECD*, Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten vom 23. September 1980, OECD-Dokument C (80) 58 (FINAL).

[343] *Vereinte Nationen*, Richtlinien betreffend personenbezogene Daten in automatisierten Dateien von der Generalversammlung beschlossen am 14. Dezember 1990.

[344] *Brühann*, RDV 1996, S. 12, S. 14; *Mei*, 25 L.P.Int'l.B., S. 305, S. 306 ff.

in der nationalen Gesetzgebung an, während die Leitlinien der UNO zwar Aussagen über Kontrollmaßnahmen und Sanktionen treffen, jedoch wie die OECD-Leitlinien nicht verbindlich umzusetzen sind.

Da eine unmittelbare Vergleichbarkeit der verfahrensrechtlichen Bedingungen demzufolge oftmals nicht gegeben sein wird, hat die Art. 29-Gruppe lediglich die Ziele eines Durchsetzungsmechanismus definiert. Anhand dieser Vorgaben sollen im konkreten Einzelfall die in dem betreffenden Drittland bestehenden Optionen zu einem gerichtlichen oder einem außergerichtlichen Verfahren gemessen werden. Die einzelnen Ziele sind wie folgt beschrieben:

(I) die Gewährleistung einer guten Befolgungsrate der Vorschriften,
(II) die Unterstützung und Hilfe für einzelne Personen bei der Wahrnehmung ihrer Rechte s o w i e
(III) die Gewährleistung einer angemessenen Entschädigung des Betroffenen bei Verstoß gegen die Datenschutzbestimmungen.

(I). Die *Befolgungsrate* könne zwar nicht empirisch in Prozent ermittelt werden. Das jeweilige Datenschutzsystem lasse jedoch Rückschlüsse auf die Effektivität der materiellen Datenschutzbestimmungen zu. So könne von einem funktionierenden Mechanismus ausgegangen werden, sofern sich der für die Verarbeitung Verantwortliche seiner Pflichten sowie der Betroffene seiner Rechte und der Mittel ihrer Wahrnehmung sehr stark bewusst seien. Abschreckende Sanktionen sowie Systeme der direkten Überprüfung durch Behörden, Buchprüfer oder unabhängige Datenschutzbeauftragte trügen ebenfalls zu einer positiven Bewertung des Schutzniveaus bei.

Das Erfordernis einer guten Befolgungsrate verdeutlicht, dass selbst sehr strenge und detaillierte inhaltliche Anforderungen nur von geringem Wert sind, sofern sie nicht beachtet werden.[345] Der Schwerpunkt einer effektiven Umsetzung der Datenschutzprinzipien muss daher stets auf der tatsächlichen Verwirklichung der Rechte und der Freiheiten des Betroffenen liegen.[346]

[345] *Riemann*, CR 1997, S. 762, S. 764; so auch *Mütsch*, DuD 1994, S. 187, S. 188 für die Überwachung der Durchführung der Datenschutzbestimmungen in den Mitgliedstaaten.
[346] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 28.

Ferner stellt die Datenschutzgruppe klar, dass die Unterstützung einer wirkungsvollen Durchsetzung des Datenschutzes im Wege einer unabhängigen Überwachung nicht zwingend die Einrichtung einer Kontrollstelle im Sinne des Artikels 28 der Richtlinie voraussetzt. Die Datenschutzaufsicht darf demnach auch von einer Stelle ausgeübt werden, die in ihrer Hauptfunktion mit einem anderen Aufgabenbereich betraut ist. Als solche in Betracht kommt zum Beispiel eine Einrichtung des Verbraucherschutzes[347] oder eine Regulierungsbehörde.[348]

Diese Freiheit bei der Wahl eines geeigneten Durchsetzungsinstruments sollte aber nicht darüber hinwegtäuschen, dass die Anzahl der Mittel zur Erzielung einer guten Befolgungsrate verhältnismäßig gering ist. Die Unabhängigkeit der Kontrolle, die auch bereits im Vorfeld der Arbeitsunterlage WP 12 der Art. 29-Gruppe durchweg als elementar für einen angemessenen Datenschutz angesehen wurde,[349] wird daher im Regelfall dennoch unverzichtbar sein.

Das Ziel einer hohen Befolgungsrate rief allerdings zum Teil Kritik hervor, da auch innerhalb der Europäischen Union eine mangelhafte Um- und Durchsetzung der Schutzprinzipien in einzelnen Mitgliedstaaten geduldet würde.[350]

Das mag für die Phase der Umsetzung der Richtlinie in nationales Recht zutreffend gewesen sein. Inzwischen hat sich die Europäische Kommission in ihrem ersten Bericht über die Durchführung der Datenschutzrichtlinie[351] und in einer diesem im Anhang beigefügten technischen Analyse[352] über die Umsetzung in den Mitgliedstaaten jedoch zu diesem Thema geäußert und Feststellungen über anzustrebende Ände-

---

[347] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 11; Simitis u. a. (- *Simitis*), § 4b, Rn. 62; *Wuermeling*, Handelshemmnis Datenschutz, S. 189 f.
[348] *WP 15*, S. 4.
[349] Z. B. *Ellger*, CR 1993, S. 2, S. 9; *Heil*, DuD 1999, S. 458 und S. 461; *Schwartz/Reidenberg*, S. 17; Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 62; Dammann/Simitis, EG-Datenschutzrichtlinie (- *ders.*), Einleitung, Rn. 29; *Wuermeling*, Handelshemmnis Datenschutz, S. 117; vgl. auch *WP 78*, S. 11, das im Hinblick auf die Zulässigkeit einer Weitergabe von Flugpassagierdaten an die US-amerikanische Verwaltung eine wirksame Kontrolle und Durchsetzung von Schutzgarantien fordert; vgl. auch *Gellman* in: Governance of Global Networks, S. 71, S. 81, der generell eine unabhängige Kontrolle zur Gewährleistung des Datenschutzes für notwendig hält.
[350] So *Wuermeling*, Handelshemmnis Datenschutz, S. 116 und S. 129 f., allerdings ohne Nennung von Beispielen.
[351] *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig.
[352] *Europäische Kommission*, Analysis and impact study on the implementation of the Directive EC 95/46 in Member States, Annex zu dem ersten Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.5.2003, KOM(2003) 265.

rungen und Verbesserungen bei der Umsetzung und Durchsetzung der Richtlinie in den Mitgliedstaaten getroffen. Der Vorwurf sollte sich daher mittlerweile erledigt haben.

(II). Dem Betroffenen müsse darüber hinaus die Möglichkeit eingeräumt werden, seine *Rechte* rasch, wirksam und ohne überhöhte Kosten im Rahmen eines institutionellen Mechanismus zur unabhängigen Prüfung von Beschwerden *durchzusetzen*.

Dabei sind insbesondere jene Hindernisse zu berücksichtigen, die dem Betroffenen aufgrund der grenzüberschreitenden Geltendmachung seiner Ansprüche in dem betreffenden Drittland gegenüberstehen. Die faktischen Hürden dürfen allerdings nur bedingt ins Gewicht fallen, da dem Betroffenen auch bei einer Rechtsdurchsetzung in anderen Mitgliedstaaten keine Hilfestellungen im Hinblick auf die Grenzüberschreitung angeboten werden. Die Angemessenheit des Durchsetzungsmechanismus bemisst sich daher nicht an einem rein innerstaatlichen Sachverhalt, sondern an dem Verfahren einer grenzüberschreitenden Rechtsdurchsetzung auf dem Binnenmarkt.[353]

Als Hauptschwierigkeit für den Betroffenen im Rahmen einer Beschwerde stellt sich regelmäßig die Feststellung des konkreten Verstoßes dar. Oftmals ist für den Betroffenen die Ursache eines spezifischen Einzelproblems kaum nachvollziehbar. Im Rahmen einer Übermittlung vermag er häufig nicht einmal zu verifizieren, ob die Verletzung in den Verantwortungsbereich des Datenübermittlers oder des Datenempfängers fällt, sodass er nur selten ermitteln kann, ob tatsächlich ein rechtlicher Anspruch gegen einen bestimmten Verarbeiter besteht.

Angesichts dieser Schwierigkeiten ist das Beschwerdeverfahren innerhalb der Europäischen Union dergestalt geregelt, dass der Betroffene sich gemäß Artikel 28 Absatz 4 der Richtlinie mit seiner Beschwerde an jede mitgliedstaatliche Kontrollstelle wenden darf. Die angerufene Beschwerdestelle untersucht sodann die tatsächliche Verletzung des jeweils einschlägigen mitgliedstaatlichen Datenschutzgesetzes, nötigenfalls gemäß Artikel 28 Absatz 6 der Richtlinie in Zusammenarbeit mit den Kontrollstellen anderer Mitgliedstaaten, und ermittelt im Rahmen ihrer entsprechend dem Artikel 28 Absatz 3 der Richtlinie gesetzlich eingeräumten Eingriffsbefugnisse gegen die verarbeitende Stelle.

[353] *Wuermeling*, Handelshemmnis Datenschutz, S. 129.

Ein effektives Beschwerdeverfahren im Rahmen eines angemessenen Schutzniveaus setzt sonach eine mit entsprechenden Untersuchungsbefugnissen gegenüber den verarbeitenden Stellen ausgestattete unabhängige Kontrollinstanz voraus, die im Rahmen ihrer Aufsichtspflicht jeder nicht offensichtlich unbegründeten Beschwerde nachgeht und gegebenenfalls abhilft.[354]

Ungeachtet der Option zur Anrufung einer aufsichtsbehördlichen Kontrollinstanz gewährleistet der Artikel 22 der Richtlinie dem Betroffenen eine Rechtsweggarantie, die ihm ein gerichtliches Vorgehen sowohl gegen einen öffentlichen als auch gegen einen privaten Datenverarbeiter ermöglicht.

Eine wirkungsvolle Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte setzt daher zudem die Möglichkeit zur Herbeiführung einer Streitschlichtung vor einer unabhängigen, möglichst staatlichen Instanz voraus, deren Entscheidung für den Betroffenen vollstreckbar ist.

(III). Für die *Entschädigung* des Betroffenen sei schließlich die Existenz eines Systems unabhängiger Schlichtung erforderlich, das die Zahlung von Entschädigungen sowie die Auferlegung von Sanktionen ermögliche.

Dieses „Schlüsselelement“[355] des Verfahrensmechanismus soll sicherstellen, dass dem Betroffenen in Anlehnung an die Regelung des Artikels 23 der Richtlinie eine Schadenskompensation sowie eine Genugtuung für die erlittenen Einbußen seiner Privatsphäre zugesprochen werden kann.

d. Gesamtwürdigung

Insgesamt hat die Art. 29-Gruppe in ihrer Stellungnahme ein Angemessenheitsprofil entworfen, das entsprechend dem Prinzip der funktionalen Adäquanz sehr an der geforderten Wirkungs- und Funktionsweise des Datenschutzsystems orientiert ist. Während die Datenschutzgruppe diese Ausrichtung im Hinblick auf den verfahrensrechtlichen Mechanismus selbst betont, werden jedoch auch die Prinzipien zum Inhalt an Zielvorgaben gemessen.

---

[354] *Brühann*, DuD 1998, S. 700, S. 701 f.
[355] *WP 9*, S. 6.

Im Unterschied zu der Vorgehensweise bei den verfahrensrechtlichen Grundsätzen ist allerdings zusätzlich die Art und Weise beschrieben, in der die inhaltlichen Anforderungen umgesetzt sein sollen. Dabei werden quasi alle materiellen Vorschriften der Richtlinie in mehr oder weniger ausführlicher Form berücksichtigt. Die beinahe erschöpfende Nennung der Schutzprinzipien mag insofern erstaunen, als dass sogar ihre Erläuterungen fast wörtlich den entsprechenden Richtlinientext zitieren. Es erschließt sich daher, dass die eigentlichen Zugeständnisse an die Intensität des Schutzniveaus im Verhältnis zu einer Gleichwertigkeit erst in dem konkreten Einzelfall zu machen sind.

Da sich die Aufstellung von Prinzipien zur Durchsetzung des Datenschutzes aus bereits erwähnten Gründen nur an der Wirkungsweise der entsprechenden Richtlinienbestimmungen ausrichten kann, fließen demgegenüber im Hinblick auf die Verfahrensvorschriften bereits bei der Formulierung der Bezugsgröße flexible und moderate Elemente in die Beurteilung des Schutzniveaus ein.

Diese Strategie erweist sich insgesamt als sehr geschickt. Indem sowohl die verfahrensrechtlichen als auch die inhaltlichen Kerngrundsätze von klaren Zielvorgaben in Bezug auf ihre Wirkungsweise ausgehen, verlieren sie sich nicht in unübersichtlichen Details. Gerade im Hinblick auf die angestrebte Kooperation der Drittländer bei der Herstellung eines angemessenen Schutzniveaus wäre es völlig unzweckmäßig, den Maßstab durch die bloße Beschreibung einzelner Rechtmäßigkeitsvoraussetzungen festzulegen und das Herausfiltern der entscheidenden Zielsetzung den Drittländern selbst zu überlassen.[356] Zudem wird auf diese Weise der Eindruck vermieden, ein angemessenes Schutzniveau könne nur bei einer vollständigen Übernahme der jeweiligen Richtlinienbestimmungen erreicht werden. Ein derartiger Ansatz wäre zwar bei einer Forderung nach einem gleichen Schutzniveau sinnvoll. Bereits eine funktionale Äquivalenz im Rahmen einer Gleichwertigkeitsprüfung kann sich aber aufgrund des Erfordernisses flexibler Modalitäten nur an Schutzzielen orientieren.[357]

[356] So offenbar noch der Ansatz von *Ellger*, CR 1993, S. 2, S. 9, der jedoch damit seine Forderung nach der Voraussetzung eines gleichwertigen Schutzniveaus in Drittstaaten illustriert.
[357] A. A. *Wuermeling*, Handelhemmnis Datenschutz, S. 114, der sich ohne nähere Begründung auch eine Gleichwertigkeitsprüfung noch anhand von formal rechtlichen Gesichtspunkten vorstellen kann.

Die Praktikabilität dieser Vorgehensweise der Arbeitsunterlage WP 12 der Art. 29-Gruppe bestätigt auch eine bereits zuvor von der Europäischen Kommission bei der Goethe-Universität in Frankfurt am Main in Auftrag gegebene Studie über das Datenschutzniveau in den USA.[358] Anhand einer Auflistung der wesentlichen Inhalte und Ziele der Schutzprinzipien der Richtlinie wurden darin die einzelnen Sektoren des US-amerikanischen Rechts danach untersucht, ob sie im Vergleich zu den europäischen Grundsätzen überhaupt funktional äquivalente[359] Regelungen enthalten.[360] Es ging hier allerdings nicht direkt um die Feststellung eines angemessenen Datenschutzes. Vielmehr erarbeitete die Studie einen Überblick über das in den USA vorhandene Schutzniveau und schaffte somit eine Grundlage für die Beurteilung seiner Angemessenheit durch die Europäische Kommission.

Indessen erweisen sich auch die Erläuterungen über die Art und Weise der Umsetzung der inhaltlichen Kernaussagen als unverzichtbar. Ohnehin sind die materiellen Richtlinienbestimmungen recht allgemein formuliert. Eine von vornherein definierte Reduktion ihrer Details auf ihre reine Wirkungsweise eröffnete die Möglichkeit zu einer Modifikation ihres Aussagegehalts und ließe sonach Spielraum für eine positive Bewertung eines außereuropäischen Schutzniveaus, das nur noch sehr schemenhaft mit den Bestimmungen der Richtlinie korrespondierte. Als Bezugsgröße für eine Angemessenheitsprüfung wäre ein an der reinen Wirkungsweise der inhaltlichen Prinzipien ausgerichteter Maßstab daher zu pauschal.

Auch aus Erwägungen über eine praxisnahe und effektive Anwendung der Drittländerregelung muss die Bezugsgröße eindeutige und konkrete Hinweise auf die Modalitäten zur Umsetzung eines angemessenen Schutzniveaus liefern. Den Anwendern der Drittländerregelung, insbesondere also den für die Verarbeitung Verantwortlichen und jenen Drittländern, die eine Anpassung ihres Schutzniveaus anstreben, wäre mit einer generalisierenden Betrachtungsweise kaum geholfen. Um ihren Verpflichtungen aus den Vorschriften über den Drittländertransfer nachzukommen, bedürfen sie vernünftiger Anhaltspunkte für die Angemessenheitsprüfung. Unpräzise und komplizierte Vorgaben führten höchstens dazu, dass das Übermittlungsverbot nicht ordnungsgemäß

[358] Spätere Veröffentlichung in: *Schwartz/Reidenberg* (Autoren der Studie).
[359] Vgl. *Schwartz/Reidenberg*, S. 24 f., die von einer „Functional Similarity" sprechen und unter diesem Aspekt Regelungen danach untersuchen, ob sie zu dem gleichen Ziel führen wie die entsprechende Richtlinienbestimmung.
[360] *Schwartz/Reidenberg*, S. 13 ff. zzgl. des jeweiligen Aufbaus der Analysen zu den einzelnen Sektoren des US-Datenschutzrechts.

umgesetzt würde. Die gemäß der Begründung des Rates zum gemeinsamen Standpunkt der Richtlinie mittels der Artikel 25 und 26 der Richtlinie zu erreichende „Undurchlässigkeit“ des auf dem Binnenmarkt eingeführten Datenschutzsystems wäre auf diese Weise jedenfalls nicht zu erzielen.

Dagegen bemängelt *Wuermeling*, dass die Gliederung der inhaltlichen Anforderungen an ein angemessenes Schutzniveau keine entsprechende Gewichtung in dem Aufbau der Richtlinie fände.[361] Insbesondere sei es überzogen, den Zweckbindungsgrundsatz, also das strengste Element der datenschutzrechtlichen Reglementierung als zwingend zu betrachten.[362] Es reiche aus, die Zweckbindung im Rahmen einer Überprüfung der Rechtmäßigkeitsvoraussetzungen zu berücksichtigen. Zu diesen allgemeinen Rechtmäßigkeitsvoraussetzungen gehörten darüber hinaus die Drittländerregelung, ein Widerspruchsrecht, ein mit dem Artikel 3 der Richtlinie korrespondierender Anwendungsbereich sowie Erlaubnistatbestände im Sinne des Artikels 7 der Richtlinie.[363] Die Pflicht zur Information des Betroffenen sowie die Datenpflege seien entsprechend der Richtlinie zwar ebenfalls Rechtmäßigkeitvoraussetzungen, die jedoch als Schwerpunkte eines angemessenen Schutzniveaus gesondert analysiert werden müssten. Weiterhin sei das Datenschutzsystem des Drittlandes auf Verpflichtungen des Verantwortlichen zu technischen Schutzmaßnahmen zu überprüfen, sowie nach Kontrollmechanismen, einer Haftung und Sanktionen bei Verstößen zu untersuchen.

Bei dieser Kritik wird jedoch verkannt, dass die Art. 29-Gruppe keine eigentliche Gewichtung zwischen den einzelnen Schutzprinzipien vorgenommen hat. Vielmehr wurden die Essentialia der Richtlinie herausgefiltert und in einem Schutzzielkatalog generell unverzichtbarer Kernprinzipien zusammengefasst. Die Bedeutungsschwerpunkte sind zwar auf den ersten Blick insofern verschoben, als dass etwa der Zweckbindungsgrundsatz und die Datenqualität sowie die Datenverhältnismäßigkeit in der Richtlinie in einer einzigen Vorschrift zusammengefasst sind, während sie in dem Katalog der Art. 29-Gruppe jeweils gleichwertig beispielsweise neben das sich in der Richtlinie über zwei Artikel erstreckende Transparenzgebot gestellt werden. Wie bereits an anderer Stelle erläutert, besteht aber dennoch kein Zweifel daran, dass es sich sowohl bei dem Zweckbindungsgrundsatz als auch bei dem Gebot der Datenpflege um entscheidende und unverzichtbare Faktoren der

[361] *Wuermeling*, Handelshemmnis Datenschutz, S. 116.
[362] *Wuermeling*, Handelshemmnis Datenschutz, S. 114 f.
[363] *Wuermeling*, Handelshemmnis Datenschutz, S. 117 ff.

Rechtmäßigkeit einer Datenverarbeitung handelt.[364] Genau das bringt aber der von der Art. 29-Gruppe erstellte Katalog der Kernprinzipien für ein angemessenes Schutzniveau lediglich zum Ausdruck. Die spezifische Gewichtung der Grundsätze erfolgt indessen erst nach Maßgabe ihrer jeweiligen Relevanz in dem konkreten Einzelfall.

Sicherlich hätten die Rechtmäßigkeitsvoraussetzungen vollständig in einem entsprechend untergliederten Thesenpunkt zusammengefasst werden können. Da sie jedoch bei einer generellen Darstellung der wesentlichen Elemente der Richtlinie in jedem Fall vollständig anzuführen sind und ihnen ohne Kenntnis des konkreten Einzelfalls zunächst eine äquivalente Relevanz unterstellt werden muss, führte eine derartige Darstellung zu keinen nennenswerten Gewichtungsunterschieden. Im Gegenteil müsste einem zusammengefassten Rechtmäßigkeitskomplex sogar ein größeres Gewicht im Verhältnis zu den nachfolgenden Schutzprinzipien eingeräumt werden, da er mehrere Schwerpunkte zugleich in die Prüfung einbrächte.

Davon abgesehen ändert die fehlende Bezeichnung einzelner Prinzipien als Rechtmäßigkeitsvoraussetzungen nichts an ihrer tatsächlichen Eigenschaft als solche, da sie mit Blick auf die Richtlinie interpretiert werden müssen und dort diese Funktion einnehmen.

Wie an anderer Stelle bereits dargelegt,[365] ist indessen eine Bestimmung im Sinne des Artikels 7 der Richtlinie in dem Drittland entbehrlich. Sofern der Datenempfänger an den Übermittlungszweck gebunden ist, kommt es auf die einzelnen Erlaubnistatbestände einer Verarbeitung nicht mehr an. Insbesondere im Hinblick auf einen Datentransfer stellt sich der Zweckbindungsgrundsatz daher tatsächlich als das zentrale Element der Zulässigkeit einer Verarbeitung dar.

Die Frage nach dem Anwendungsbereich des Datenschutzrechts wird zwar von der Art. 29-Gruppe nicht ausdrücklich geklärt. Sie ist jedoch konkludent mitgeregelt, da die inhaltlichen Grundsätze nicht gewährleistet wären, sofern das Datenschutzrecht des Drittstaates auf die konkrete Verarbeitung keine Anwendung fände.

Da es also für die Beurteilung eines Schutzniveaus in erster Linie auf die Wirkung der bestehenden Datenschutzregeln ankommt und die Gewichtung der einzelnen Anforderungen nur im Hinblick auf die konkre-

[364] Vgl. Gliederungspunkt C.II.1.a. dieses Kapitels.
[365] Vgl. Gliederungspunkt C.II.1.a. dieses Kapitels.

te Datenübermittlung vorgenommen werden kann, stellt sich der von der Art. 29-Gruppe gefundene Konsens der Mitgliedstaaten über die Auslegung des Merkmals der Angemessenheit anhand von inhaltlichen und verfahrensrechtlichen Schutzzielen insgesamt als geeignete Bezugsgröße dar.

2. Die Umstände einer Datenübermittlung

Gemäß Artikel 25 Absatz 2 der Richtlinie ist das Schutzniveau in dem Drittland nicht im Rahmen eines pauschalen Ländervergleichs zu ermitteln, sondern unter Berücksichtigung aller Umstände zu beurteilen, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen.[366]

Die bei der Prüfung maßgeblichen Kriterien sind in Artikel 25 Absatz 2 der Richtlinie beispielhaft aufgezählt. Sie gliedern sich in zwei wesentliche Kategorien:

Zum einen sind bei der Beurteilung des Schutzniveaus die Art der Daten, die Zweckbestimmung und die Dauer der geplanten Verarbeitung sowie das Herkunfts- und das Endbestimmungsland zu berücksichtigen. Diese Umstände beschreiben den individuellen Charakter einer Übermittlung.

Zum anderen sind die in dem Drittland geltenden allgemeinen und sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen zu untersuchen. Hierbei geht es also um die Feststellung des in dem Drittland generell vorhandenen Datenschutzes.

a. Der Charakter der Übermittlung

Anhand des individuellen Charakters des jeweiligen Transfers ist das Risiko einer konkreten Gefahr von Rechtsverlusten für den Betroffenen zu ermitteln.[367]

(1) Die Art der Daten

Ein besonderes Schutzbedürfnis kann dabei aus der Art der Daten erwachsen. Das gilt insbesondere für sensible Daten im Sinne des Arti-

[366] Vgl. Gliederungspunkt C.I.1.b. dieses Kapitels.
[367] Grabitz/Hilf III (- *Brühann*), A 30, Art. 25, Rn. 12.

kels 8 Absatz 1 der Richtlinie.[368] Danach dürfen solche Informationen, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie (...) Daten über Gesundheit oder Sexualleben“ nur unter spezifischen Bedingungen verarbeitet werden. Dasselbe gilt gemäß Artikel 8 Absatz 5 der Richtlinie für Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen.

Zu differenzieren ist ferner zwischen Daten, die allein der Identifikation des Betroffenen dienen, und solchen über besondere persönliche Merkmale. Unterschiedliche Voraussetzungen an den Schutzmechanismus rechtfertigen schließlich auch Daten über die finanzielle Situation des Betroffenen und über seine beruflichen Aktivitäten.[369]

Bedeutend kann außerdem sein, inwieweit die Daten entsprechend ihrer Qualität und Quantität eine sichere Identifizierung[370] des Betroffenen ermöglichen.

Darüber hinaus gibt die Art der Daten regelmäßig nur im Kontext mit anderen Umständen Auskunft über die konkrete Risikolage.

(2) Die Zweckbestimmung

Auch die Zweckbestimmung wirkt sich auf den Charakter der Übermittlung aus. So ist der Betroffene zum Beispiel weniger schutzbedürftig, sofern der Transfer in seinem besonderen Interesse liegt, ohne dass ihm eine vorherige Einwilligung gemäß Artikel 26 Absatz 1a) der Richtlinie möglich gewesen wäre. Umgekehrt muss ein intensiverer Schutz bei Übermittlungen gelten, die mit den Interessen des Betroffenen kollidieren könnten, indem sie zum Beispiel ein erhöhtes Risiko eines finanziellen Verlustes, einer Gefahr für die persönliche Sicherheit oder einer Rufschädigung[371] in sich bergen.

Besondere Voraussetzungen gelten ferner für Übermittlungen zu journalistischen, künstlerischen oder literarischen Zwecken sowie zum Zwecke des Direktmarketings.

---

[368] Erwägungsgrund (60) der Richtlinie.
[369] *Europäische Kommission*, Evaluating the Adequacy, S. 29.
[370] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 10.
[371] *WP 4*, S. 4 f.

Von Belang ist darüber hinaus, ob es sich um einen eng umgrenzten oder um einen umfangreicheren Zweck handelt.[372]

(3) Die Dauer der geplanten Verarbeitung

In die Bewertung der geplanten Verarbeitung fließt überdies deren Dauer ein. Während eine langwierige Verarbeitung regelmäßig einen intensiveren Schutz gebietet, minimiert sich das Risiko einer Verletzung des Persönlichkeitsrechts regelmäßig bei einer kürzeren Nutzung der Daten.

Eine anlassbezogene Verwendung kann sogar die Ausübung der Betroffenenrechte zeitlich unmöglich machen, sodass hier die Forderung nach einem Berichtigungs- oder Löschungsanspruch bei der Bewertung des Schutzniveaus zu vernachlässigen wäre.

(4) Das Herkunfts- und das Endbestimmungsland

Schließlich vermögen das Herkunfts- und das Endbestimmungsland der Daten die Verarbeitung zu beeinflussen.

Das Herkunftsland spielt vor allem bei Verarbeitungen innerhalb der Europäischen Union eine Rolle. Lässt etwa ein außereuropäischer Verantwortlicher personenbezogene Daten, die nicht aus der Europäischen Union stammen, in einem Mitgliedstaat durch eine Niederlassung oder im Auftrag verarbeiten, können bei der Rückübermittlung derselben Daten nicht allzu hohe Ansprüche an das Schutzniveau in dem Drittland gestellt werden.

Zwar gilt für die Auftragsverarbeitung im Gemeinschaftsgebiet das jeweilige mitgliedstaatliche Datenschutzgesetz, da die für die Durchfuhr in Artikel 4 Absatz 1c) der Richtlinie vorgesehene Ausnahme vom Anwendungsbereich nicht auf die Auftragsverarbeitung übertragbar ist.[373] Indessen ist nicht ersichtlich, warum die Daten nach ihrer Rückkehr in ihr Herkunftsland einen erheblich höheren Schutz genießen sollten als ihnen ursprünglich in dem Drittland zugebilligt wurde.[374] Die Gegenmeinung argumentiert, dass die Richtlinie den Schutz der Privatsphäre nicht nur als Unionsbürgerrecht, sondern auch als Menschenrecht ver-

[372] *Abel*, BDSG, S. 66; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 10; *Draf*, S. 78.
[373] Vgl. dazu Gliederungspunkt B.II.2.b. des zweiten Kapitels.
[374] *Wuermeling*, Handelshemmnis Datenschutz, S. 109.

stehe.[375] Es geht hier jedoch nicht um die Frage der Nationalität oder des Wohnsitzes des Betroffenen, sondern um den Datenschutz, den der Betroffene bei einer Verarbeitung vernünftigerweise erwarten darf. Überlässt er seine Daten einem außereuropäischen Verantwortlichen, geht er nicht von der Beachtung eines Schutzniveaus aus, das angemessen im Verhältnis zu der Datenschutzrichtlinie ist.

Ferner wirkt sich die Berücksichtigung des Herkunftslandes bei außereuropäischen Geschäftsreisenden aus, die mit ihrem Notebook in die Europäische Union ein- und wieder ausreisen. Die bereits zum Zeitpunkt der Einreise auf dem Computer gespeicherten Daten sollten im Grunde ohne Hindernisse wieder exportiert werden dürfen.[376]

Der Hinweis auf die Berücksichtigung des Endbestimmungslandes zielt darauf ab, überzogene Anforderungen an das Datenschutzniveau von Transitländern bei einer bloßen Durchleitung zu vermeiden.[377] Da erst im Endbestimmungsland die eigentlich bezweckte Verarbeitung stattfinden wird, reicht in dem Transitland oft schon die Gewährleistung einer sicheren Durchfuhr aus.

(5) Sonstige Umstände

Die in Artikel 25 Absatz 2 der Richtlinie genannten Umstände sind nur „insbesondere“ zu beachten, sodass sich die Aufzählung nicht als abschließend versteht. Darüber hinaus können also auch andere Kriterien in die Angemessenheitsprüfung einfließen.

Berücksichtigung könnte etwa das Vorliegen des Erlaubnistatbestandes aus Artikel 7f) der Richtlinie finden. Danach sind Verarbeitungen zulässig, die zur Verwirklichung eines berechtigten Interesses erforderlich sind, „das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden“. Voraussetzung ist jedoch, dass „das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person“ nicht überwiegen.

Da diese allgemeine Interessenabwägung der einzige Erlaubnistatbestand des Artikels 7 der Richtlinie ist, der nicht ausdrücklich von dem Ausnahmenkatalog des Artikels 26 Absatz 1 der Richtlinie berücksich-

[375] So *Draf*, S. 79.
[376] *Wuermeling*, Handelshemmnis Datenschutz, S. 109.
[377] *Abel*, BDSG, S. 66; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 25, Rn. 16.

tigt wird, liegt eine Beachtung im Rahmen des Artikels 25 der Richtlinie nahe. Die Gewichtung der Bestimmung darf jedoch nicht die Entscheidung des Richtliniengebers gegen ihre Aufnahme in den Artikel 26 Absatz 1 der Richtlinie revidieren.[378]

Des Weiteren war es vor Erlass der Richtlinie aus der Sicht der schwedischen Kontrollbehörde für die Beurteilung des Schutzniveaus von Belang, dass es sich bei dem außereuropäischen Empfänger von Arbeitnehmerdaten um ein Unternehmen desselben Konzerns handelte.[379] Diese Praxis dürfte aber inzwischen überholt sein, da die Tatsache der Zugehörigkeit zu demselben Konzern noch keine Aussage über das Schutzniveau bei der empfangenden Stelle und in dem jeweiligen Drittland trifft.[380]

Eine Kommentierung zum deutschen Bundesdatenschutzgesetz geht sogar davon aus, dass einer lang andauernden Geschäftsbeziehung, in der es bisher nicht zu Datenmissbräuchen oder Datenunfällen gekommen sei, in der Praxis ein großes Gewicht bei der Beurteilung des Schutzniveaus zukomme.[381] Zu dieser Annahme verleitet insbesondere das deutsche Bundesdatenschutzgesetz, das entgegen dem Wortlaut der Richtlinie nicht explizit in dem Drittland ein angemessenes Schutzniveau verlangt, sondern nur bei der empfangenden Stelle. Richtlinienkonform ist das Bundesdatenschutzgesetz jedoch so zu verstehen, dass ein angemessenes Schutzniveau bei dem Datenempfänger stets ein angemessenes Schutzniveau in dem Drittland voraussetzt.[382] Geschäftsbeziehungen können danach ebenso wenig wie eine Konzernzugehörigkeit bei der Angemessenheitsprüfung berücksichtigt werden.

---

[378] *Wuermeling*, Handelshemmnis Datenschutz, S. 108 und S. 110 f.
[379] *Vassilaki*, 9 CLSR, S. 33, S. 35.
[380] A. A. offenbar, aber ohne Begründung: *Terwangne/Louveaux*, MMR 1998, S. 451, S. 456; *Wuermeling*, Handelshemmnis Datenschutz, S. 110.
[381] So *Schaffland/Wiltfang*, BDSG, 5001, § 4b, Rn. 4, u. § 4c, Rn. 1.
[382] *Moritz/Tinnefeld*, JurPC Web-Dok. 181/2003, Abs. 13; *Rittweger/Weiße*, CR 2003, S. 142, S. 146 f.; vgl. auch die *Begründung der Bundesregierung zum Entwurf des Bundesdatenschutzgesetzes*, BT-Drs. 14/4329 vom 13.10.2000, S. 29 und S. 34, gemäß der die Zulässigkeitsvoraussetzungen für eine Übermittlung in ein Drittland durch § 4b Absatz 2 Satz 2 BDSG im Vergleich zum alten BDSG um „das Erfordernis des angemessenen Datenschutzniveaus im Drittstaat“ ergänzt werden und „damit den Anforderungen des Artikels 25 Abs. 1 der Richtlinie“ genügt ist; *Hamburger DuD-Kommentierung*, DuD 2002, S. 5, S. 15 f.; *Räther/Seitz*, MMR 2002, S. 425 f. und S. 520, die bei der Feststellung des Datenschutzniveaus bei der empfangenden Stelle zunächst die Frage nach der Angemessenheit des Schutzniveaus in dem Empfängerland für wichtig halten. Die meisten Autoren übergehen diese Frage jedoch, indem sie ausschließlich auf die Merkmale eines angemessenen Schutzniveaus in dem Drittland eingehen.

b. Die in dem Drittland bestehenden Schutzmaßnahmen

Der zweite Teil der Aufzählung des Artikels 25 Absatz 2 der Richtlinie befasst sich mit den in dem Drittland bestehenden Schutzmaßnahmen, aus denen sich die geltenden inhaltlichen Grundsätze sowie das Maß und die Mittel der Verbindlichkeit[383] der materiellen Vorgaben erschließen. Das angemessene Schutzniveau kann sich danach aus den allgemeinen oder sektoriellen Rechtsnormen sowie den geltenden Standesregeln und Sicherheitsmaßnahmen ergeben.

(1) Allgemeine und sektorielle Rechtsnormen

In erster Linie leitet sich das Schutzniveau in dem Drittland aus den geltenden allgemeinen und sektoriellen Rechtsnormen ab.

Dabei kommt es nicht darauf an, dass die Vorschriften unmittelbar die Verarbeitung personenbezogener Daten regeln, solange sie ein angemessenes Schutzniveau im Einzelfall gewährleisten oder jedenfalls dazu beitragen. Sowohl der Wortlaut der Drittländerregelung als auch ihr Ziel eines undurchlässigen Datenschutzsystems auf dem Binnenmarkt lassen die Berücksichtigung sämtlicher, auch mittelbar datenschützend wirkender Bestimmungen zu.[384] In die Analyse einzubeziehen sind daher neben dem Verfassungsrecht und dem sonstigen öffentlichen Recht auch zivil- oder strafrechtliche Vorschriften.[385]

Voraussetzung ist allerdings, dass der Anwendungsbereich der jeweiligen Vorschriften eröffnet ist. Gerade der Betroffene als natürliche Person muss im Hinblick auf die konkret übermittelten personenbezogenen Daten vor Eingriffen in seine Privatsphäre, seine Grundrechte und Grundfreiheiten geschützt werden.[386] Handelt es sich zum Beispiel um Daten eines Betroffenen, der nicht Staatsbürger des betreffenden Drittlandes ist, müssen die Bestimmungen auch für die personenbezogenen Informationen ausländischer Personen gelten. Ausreichend wäre es allerdings schon, wenn als Reaktion auf die Richtlinie Vorschriften erlassen würden, die sich speziell mit dem Schutz der aus der Europäischen Union importierten Daten befassten.[387]

---

[383] *Simitis*, CR 2000, S. 472, S. 479.
[384] *Draf*, S. 96; *Terwangne/Louveaux*, MMR 1998, S. 451, S. 456; a. A. ohne maßgebliche Begründung Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 53 f.; Dammann/Simitis, EG-Datenschutzrichtlinie (- *ders.*), Einleitung, Rn. 30; *ders.*, NJW 1997, S. 281, S. 285.
[385] *Wuermeling*, Handelshemmnis Datenschutz, S. 124.
[386] *Bergmann*, S. 219 f.
[387] *Wuermeling*, Handelshemmnis Datenschutz, S. 124.

(2) Standesregeln

Die Angemessenheit des Schutzniveaus kann sich zudem aus so genannten Standesregeln ergeben.

Diesen im deutschen Rechtsgebrauch kaum geläufigen Begriff illustriert ein Blick auf die englische und die französische Richtlinienversion, die an derselben Stelle von „professional rules“ beziehungsweise „règles professionelles“ und demzufolge von den Regeln eines Berufsstandes sprechen. Die sich sonach ergebende Konkretisierung des Begriffs der Standesregel bestätigt auch die Begründung des geänderten Richtlinienvorschlags, gemäß der sich ein angemessenes Schutzniveau aus den „in den Verhaltenskodexen ausgedrückten berufsständischen Regeln“[388] ergeben könne.

Sofern der jeweilige Gesetzgeber des Drittlandes derartige Kodizes erlässt, wird es sich dabei regelmäßig um allgemeine oder sektorielle Rechtsnormen handeln. Die zusätzliche Erwähnung der Standesregeln in Artikel 25 Absatz 2 der Richtlinie nimmt also in erster Linie Bezug auf die außergesetzlichen Selbstregulierungsmaßnahmen der Wirtschaft.[389]

(a) Abgrenzung zu den Verhaltensregeln im Sinne des Artikels 27 der Richtlinie

In der Literatur wird teilweise unterstellt, dass es sich bei Standesregeln der Sache nach um Verhaltensregeln im Sinne des Artikels 27 der Richtlinie handele.[390] Diese Bestimmung sieht vor, dass „Berufsverbände und andere Vereinigungen, die andere Kategorien von für die Verarbeitung Verantwortlichen vertreten,“ Verhaltensregeln entwerfen können, „die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen“. Verhaltensregeln im Sinne des Artikels 27 der Richtlinie sind danach meist unverbindliche Selbstregulierungsmaßnahmen[391] von

[388] *Begründung des geänderten Vorschlags*, abgedruckt in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 25, S. 269.
[389] *WP 12*, S. 3 und S. 11; so bereits in *WP 7*, S. 2.
[390] So *Abel*, Praxishandbuch, 8/4.4.2, S. 15; *ders.*, BDSG, S. 67; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 25, Rn. 16; vgl. auch *Draf*, S. 81, der jedoch ohne Nennung eines gesetzlichen Hintergrundes von Verhaltensregeln spricht, und *Bergmann/Möhrle/Herb*, § 4b BDSG, Rn. 27, die meinen, dass Standesregeln den in Artikel 27 der Richtlinie angesprochenen Verhaltensregeln ähnlich wären.
[391] *Abel*, RDV 2003, S. 11; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 27, Rn. 1; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 27, Rn. 3 und 9.

Wirtschaftsverbänden, die in erster Linie einer Förderung der Umsetzung und Durchführung[392] der bestehenden gesetzlichen Datenschutzregeln dienen. Ihre Befolgung ist nur zwingend, soweit die Verhaltensregeln die Anforderungen des jeweiligen mitgliedstaatlichen Datenschutzgesetzes wiederholen.[393] Sie finden ihre Grundlage in einem bereits gesetzlich festgelegten angemessenen Schutzniveau und schaffen somit nicht eigenständig dessen Voraussetzungen.

Eine Gleichsetzung des Begriffs der Standesregel im Sinne des Artikels 25 Absatz 2 der Richtlinie mit jenem der Verhaltensregel aus Artikel 27 der Richtlinie hätte also zur Folge, dass eine Standesregel ebenfalls nicht selbstständig die Grundlage zur Gewährleistung eines angemessenen Schutzniveaus bilden, sondern lediglich ein Gesetz illustrieren könnte.

Diese Annahme scheint sich mit der im Schrifttum vereinzelt vertretenen Ansicht zu decken, dass ein angemessenes Schutzniveau zwingend gesetzlich verankerte Verarbeitungsmodalitäten voraussetze, da es anderenfalls an der notwendigen Verbindlichkeit der Regelungen fehle.[394] Zweifelhaft ist allerdings, ob der Artikel 25 Absatz 2 der Richtlinie dieser Ansicht folgt.

Gemäß dem Wortlaut des Artikels 25 Absatz 2 der Richtlinie soll das Schutzniveau in dem Drittland unter der Berücksichtigung *aller* Umstände ermittelt werden, die bei einer Datenübermittlung eine Rolle spielen. Es ist nicht ersichtlich, dass dabei nur an Schutzinstrumente mit einem gesetzlichen Hintergrund gedacht ist.[395] Vielmehr scheint es in erster Linie auf den in dem Drittland tatsächlich verwirklichten Datenschutz anzukommen.[396] Sofern Standesregeln und im Übrigen auch Sicherheitsmaßnahmen im Sinne des Artikels 25 Absatz 2 der Richtlinie tatsächlich auf allgemeinen oder sektoriellen Rechtsnormen basieren müssten, erwiese sich ihre zusätzliche Erwähnung außerdem als redundant.

---

[392] Erwägungsgrund (61) der Richtlinie.

[393] Vgl. Artikel 27 Absatz 2 der Richtlinie, der eine Vorlage der entworfenen Verhaltensregeln bei einer einzelstaatlichen Stelle zur Überprüfung der Konformität mit den mitgliedstaatlichen Datenschutzgesetzen vorsieht.

[394] So Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 55 ff.; *ders*., CR 2000, S. 472, S. 479; *Ellger*, CR 1993, S. 2, S. 9; *ders*., RabelsZ 60, S. 738, S. 750 f., der Standesregeln jedoch grundsätzlich für unverbindlich hält; vgl. auch Grabitz/Hilf III (- *Brühann*), A 30, Art. 25, Rn. 15, der Selbstregulierungssysteme nur befürwortet, sofern sie im Rahmen gesetzlicher Vorschriften operieren.

[395] *Poullet* in: UNESCO, S. 147, S. 167.

[396] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 25, Rn. 10.

Von der Möglichkeit der Gewährleistung eines angemessenen Schutzniveaus allein durch Standesregeln geht offenbar auch die Art. 29-Gruppe in ihrer Arbeitsunterlage WP 12 aus. Danach dürften Selbstregulierungsmaßnahmen lediglich dann als wirksamer Bestandteil eines angemessenen Schutzniveaus angesehen werden, sofern sie für ihre Mitglieder verbindlich seien.[397] Die Forderung nach einer Verbindlichkeit erweist sich nur als sinnvoll, sofern die Angemessenheit des Schutzniveaus nicht bereits durch ein Gesetz abgesichert ist. So können die Bindungswirkung der Regeln und ihre Durchsetzbarkeit durch ein unabhängiges Organ zum Beispiel auch auf vertraglichem Wege erzeugt werden und bedürfen somit nicht notwendigerweise einer gesetzlichen Verankerung.[398]

Standesregeln im Sinne des Artikels 25 Absatz 2 der Richtlinie verfolgen mithin einen anderen Zweck als die Verhaltensregeln im Sinne des Artikels 27 der Richtlinie.[399] Während letztere lediglich einer Förderung der Durchführung eines Datenschutzgesetzes zu dienen bestimmt sind, vermögen Standesregeln selbstständig ein angemessenen Datenschutzniveau herzustellen und somit eine gesetzliche Regelung zu ersetzen.

Zwar mag eine Schnittmenge zwischen beiden Regelungsformen existieren. Es liegt sogar nahe, dass Verhaltensregeln insgesamt dem Oberbegriff der Standesregel unterfallen. Für die vorliegende Erörterung der Umstände, die bei einer Datenübermittlung im Sinne des Artikels 25 der Richtlinie eine Rolle spielen, ist die Frage der Einordnung der Verhaltensregeln im Sinne des Artikels 27 der Richtlinie jedoch nicht von Belang, da sie sich nicht auf die Feststellung eines angemessenen Schutzniveaus in einem Drittland auszuwirken vermag.

(b) Die Umsetzung der Prinzipien eines angemessenen Schutzniveaus

Als Standesregeln werden gemeinhin Selbstkontrollkodizes der Wirtschaft verstanden, die vor allem in den USA als besonders attraktiv gelten[400].

---

[397] *WP 12*, S. 15; so bereits in *WP 7*, S. 6.
[398] Vgl. dazu Gliederungspunkt C.II.2.b.(2).(b). dieses Kapitels.
[399] Davon auch ausgehend *Heil*, DuD 2001, S. 129, Fn. 8; *Tinnefeld*, NJW 2001, S. 3078, S. 3081; *Wuermeling*, Handelshemmnis Datenschutz, S. 125.
[400] *Schwartz/Reidenberg*, S. 11; vgl. dazu insbesondere Gliederungspunkt C.III.1. dieses Kapitels.

Die Arbeitsunterlage WP 12 der Art. 29-Gruppe stellt daher in Kapitel 3[401] die wesentlichen Kriterien zur Beurteilung von Selbstregulierungssystemen, also solchen Datenschutzbestimmungen dar, „die auf eine Vielzahl von für die Verarbeitung Verantwortlichen in einer Berufsgruppe oder einem Wirtschaftsbereich Anwendung finden und deren Inhalt ursprünglich von Angehörigen des betreffenden Wirtschaftszweiges oder der betreffenden Berufsgruppe festgelegt wurde."[402]

Während sich der Vergleich des regelmäßig von einem repräsentativen Gremium herausgegebenen Selbstregulierungskodexes mit den inhaltlichen Anforderungen eines angemessenen Schutzniveaus[403] aufgrund der objektiven Vorgaben der Schutzprinzipien der Richtlinie recht einfach gestaltet, erweist sich die Beurteilung der Effektivität des Durchsetzungsmechanismus wegen ihrer wertenden Elemente als ausgesprochen komplex. Insbesondere muss eine Kompensation für die fehlende gesetzliche Verankerung der Bestimmungen vorgesehen sein.

Der folgende, von der Art. 29-Gruppe entwickelte Prüfungsaufbau zeigt deutlich, dass es zur Feststellung eines angemessenen Durchsetzungsmechanismus auch im Rahmen eines Selbstregulierungskodexes insbesondere auf die Transparenz zugunsten des Betroffenen und zugunsten eines unabhängigen Aufsichtsorgans ankommt sowie der Schaffung externer Durchsetzungsmechanismen in Form einer regulierten Selbstregulierung bedarf:

(I). Eine gute *Befolgungsrate* erschließe sich einerseits aus der Bekanntheit der Datenschutzregeln unter den Verbandsmitgliedern sowie aus den zur Sicherstellung der Transparenz des Kodexes für die Verbraucher ergriffenen Schritten, die unter anderem den Druck des Wettbewerbs erhöhten.

Andererseits leite sie sich aus der Existenz eines Systems der externen Kontrolle sowie aus der Androhung von Sanktionen für den Fall der Nichtbefolgung des Kodexes ab.

In diesem Sinne müsse zunächst untersucht werden, welche Maßnahmen des den Kodex herausgebenden Gremiums erforderlich seien, um die Bekanntheit der Regeln sicherzustellen, und ob die Verbandsmit-

[401] *WP 12*, S. 11 ff.; so bereits in *WP 7*, S. 2 ff.
[402] *WP 12*, S. 11; so bereits in *WP 7*, S. 2.
[403] Vgl. Gliederungspunkt C.II.1.a. und b. dieses Kapitels.

glieder entweder selbst oder durch eine externe Stelle Nachweise über die Umsetzung der Datenschutzregeln zu erbringen hätten.

Mit dieser Voraussetzung soll vor allem sichergestellt werden, dass sich die verarbeitenden Stellen ihrer Verpflichtungen aus dem Kodex stark bewusst sind und sich zu dessen Einhaltung verpflichtet fühlen.

Eine gute Befolgungsrate hinge zudem davon ab, ob die Einhaltung des Kodexes freiwillig sei oder ob der Kodex verbindlich für alle Mitglieder des betreffenden Verbandes gelte. Relevant sei ferner, ob das Gremium mutmaßliche Verstöße gegen den Kodex untersuche und welche disziplinarischen Maßnahmen ihm bei einem nachgewiesenen Verstoß zur Verfügung stünden.

Darüber hinaus komme es darauf an, ob die Befolgung der Datenschutzregeln gerichtlich durchsetzbar sei, entweder unmittelbar oder zum Beispiel aufgrund eines Gesetzes, das unfaire Handelspraktiken oder den unlauteren Wettbewerb ahnde.[404] Insbesondere sofern keine zwingende externe Kontrolle der verarbeitenden Stelle vorgesehen sei, müssten zudem für den Fall der Nichtbefolgung der Vorschriften abschreckende Strafmaßnahmen in Aussicht gestellt werden.[405]

(II). Als ebenfalls essentiell stelle sich ein transparentes *Beschwerdesystem* als Ausdruck der Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte dar.

Die Beschwerdestelle solle möglichst neutral und unabhängig sein, also nicht dem sich selbstregulierenden Verband angehören, und die erforderlichen Untersuchungsbefugnisse zur Prüfung jeder Beschwerde eines Betroffenen besitzen. Dieser Anforderung könne zum Beispiel mittels eines mit Vertretern von Verbrauchern und Wirtschaftsverbänden paritätisch zusammengesetzten Gremiums nachgekommen werden.

Von der Art. 29-Gruppe nicht eindeutig hervorgehoben wird indessen die Gewährleistung der Rechtsweggarantie, möglichst zu einer staatlichen Instanz. Im Interesse einer effektiven Gewährleistung der Betroffenenrechte und im Hinblick auf eine möglichst wirkungsvolle Kom-

[404] Vgl. dazu Gliederungspunkt III.2. dieses Kapitels über die Safe Harbor Privacy Principles.
[405] So auch *Europäisches Parlament*, Entschließung des Europäischen Parlaments zu dem Entwurf einer Entscheidung der Kommission über die Angemessenheit der US-Grundsätze des Sicheren Hafens und diesbezügliche häufig gestellte Fragen (FAQ), vorgelegt vom Handelsministerium der USA (C5-0280/2000 – 2000/2144(COS)) vom 5.7.2000, A5-0177/2000, ABl. C 121 vom 24.4.2001, S. 152, S. 154.

pensation einer fehlenden gesetzlichen Verankerung der Vorschriften sollte dieses Element bei der Bewertung des Schutzniveaus ebenfalls deutlich ins Gewicht fallen.

(III). Ein angemessenes *Entschädigungssystem* zeichne sich einerseits durch die Möglichkeit zur Durchsetzung einer Korrektur oder einer Rückgängigmachung des Schaden bringenden Verhaltens sowie andererseits durch einen Anspruch zur Kompensation sowohl materieller als auch immaterieller Schäden aus. Diese Ansprüche könnten zum Beispiel im Wege des öffentlichen Rechts, namentlich des Verbraucherschutzes sowie der Regeln zum unlauteren Wettbewerb geltend gemacht werden oder aber, indem ein Verstoß gegen den Kodex einem Vertragsverstoß gleichzusetzen sei.

(3) Sicherheitsmaßnahmen

Zu untersuchen sind ferner die Sicherheitsmaßnahmen in dem betreffenden Drittland, sodass auch den Aspekten der Datensicherheit bei der Beurteilung des Schutzniveaus ein hoher Stellenwert eingeräumt wird.

Unter Umständen können die getroffenen Sicherheitsvorkehrungen sogar den Ausschlag für die Bewertung des Schutzstandards geben. So liefern sie insbesondere bei einem reinen Transit durch ein Drittland bedeutende Anhaltspunkte, wenn nicht sogar das entscheidende Kriterium für die Zulässigkeit des Transfers.

(4) Sonstige Schutzinstrumente

Fraglich ist, ob auch weitere Schutzinstrumente die Bewertung des Schutzniveaus beeinflussen können.

(a) Individualvertrag

Es wird vertreten, dass eine vertragliche Vereinbarung zwischen dem Übermittler und dem Datenempfänger bei der Angemessenheitsprüfung ebenfalls nicht unbeachtlich sei.[406] Sie dürfe nur in ihrem Schutzgehalt nicht überbewertet werden.

[406] So *Wuermeling*, Handelshemmnis Datenschutz, S. 126 f.; vgl. auch *Gola/Schomerus*, BDSG, § 4b, Rn. 10, die dasselbe im Hinblick auf die von der Europäischen Kommission verabschiedeten Standardvertragsklauseln annehmen.

Damit wird im Grunde die bereits vor Erlass der Richtlinie 95/46/EG im Hinblick auf die Herstellung eines gleichwertigen Schutzniveaus in Drittländern jeweils national geführte Diskussion[407] über die Zulässigkeit einer Vertragslösung aufgegriffen, die zum Beispiel in Deutschland im Rahmen des § 28 Absatz 1 BDSG a. F. stattgefunden hat[408].

Da die Vertragslösung jedoch inzwischen aufgrund ihrer Normierung in Artikel 26 Absatz 2 der Richtlinie allgemein anerkannt ist, steht nur noch infrage, ob sie auch im Rahmen der Angemessenheitsprüfung im Sinne des Artikels 25 der Richtlinie Bedeutung erlangen kann.

Dafür spreche, dass das Fehlen ihrer Berücksichtigung in der Aufzählung des Artikels 25 Absatz 2 der Richtlinie im Grunde nur auf die mühsamere Kontrolle der Umsetzung einer vertraglichen Verpflichtung zurückgeführt werden könne. Ein externer, auf eine unbestimmte Anzahl von Sachverhalten anwendbarer Regulierungsmechanismus vermöge allgemein und von außen im Hinblick auf eine konkrete Übermittlung geprüft zu werden, während eine vertragliche Abmachung eine detaillierte Analyse der internen Strukturen eines bestimmten Verantwortlichen erfordere. Solche praktischen Erwägungen allein dürften aber nicht per se zu einer Ablehnung einer durch Verträge herbeigeführten Angemessenheit führen.[409]

Diese Argumentation übersieht jedoch zwei wesentliche Strukturelemente der Vorschriften über den Drittländertransfer.

Einerseits setzt die Zulässigkeit einer Übermittlung gemäß dem Wortlaut des Artikels 25 der Richtlinie ein angemessenes Schutzniveau in dem Drittland voraus, während ein Vertrag ausschließlich intern das Schutzniveau bei der empfangenden Stelle reguliert.

Bei dieser Formulierung handelt es sich weder um ein bloßes Versehen noch um eine Entscheidung zugunsten rein prüfungstaktischer Gesichtspunkte. Zu Recht sieht der Richtliniengeber ein angemessenes Schutzniveau nur gewährleistet bei einer Integration des außereuropäischen Verarbeiters in ein abstrakt-generell geregeltes Datenschutzsystem, das möglichst aus einer gesellschaftlichen Überzeugung hervorgegangen ist und dessen Funktionsfähigkeit mittels einer übergeordneten

[407] Vgl. dazu Gliederungspunkt E.I.1.b. dieses Kapitels.
[408] Z. B.: *Stein* in: Festschrift f. Rudolf, S. 513, S. 516 f.
[409] *Wuermeling*, Handelshemmnis Datenschutz, S. 127.

Kontrolle sowie durch den Wettbewerb der Verpflichteten untereinander gewährleistet ist.

Ferner erklärt die Gegenmeinung nicht, in welchem Verhältnis eine Vertragslösung im Rahmen von Artikel 25 Absatz 1 zu den genehmigungspflichtigen Übermittlungen des Artikels 26 Absatz 2 der Richtlinie stehen sollte und wie beide voneinander abzugrenzen wären.

Gemäß Artikel 26 Absatz 2 der Richtlinie kann ein Mitgliedstaat eine Übermittlung genehmigen, sofern der für die Verarbeitung Verantwortliche „ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet". Insbesondere ergeben sich derartige Garantien „aus entsprechenden Vertragsklauseln". Da die Garantien nur ausreichend sein können, wenn sie im Verhältnis zu den Prinzipien der Richtlinie noch einen verhältnismäßigen beziehungsweise angemessenen Schutz gewährleisten,[410] messen die Artikel 25 und 26 Absatz 2 der Richtlinie das Schutzniveau an demselben Richtwert.[411]

Könnte daher bereits eine individuelle Vertragslösung zu einem angemessenen Schutzniveau im Sinne des Artikels 25 der Richtlinie beitragen, käme der Artikel 26 Absatz 2 der Richtlinie im Grunde nie zur Anwendung. Infolgedessen drohte eine permanente Umgehung des Genehmigungserfordernisses und im Übrigen auch des der Europäischen Kommission und den anderen Mitgliedstaaten gemäß Artikel 26 Absatz 3 Satz 2 der Richtlinie gegen jene mitgliedstaatliche Genehmigung zustehenden Widerspruchsrechts.

Bei diesen Verfahrenselementen handelt es sich nicht etwa nur um rein formale Kriterien. Sinn und Zweck der auf europäischer Ebene mittels des Widerspruchsrechts kontrollierten Genehmigung ist die Vorweg-

---

[410] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 26, Rn. 14; *Draf*, S. 127; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 26, Rn. 23; *Ellger*, RabelsZ 60, S. 738, S. 756; *Giesen*, DuD 1996, S. 394, S. 395; *Kaspersen* in: *e*Directives, S. 119, S. 125; Bettinger/Leistner (- *Klein*), Teil 2 E, Rn. 33; *Räther/Seitz*, MMR 2002, S. 520, S. 521; *Schaar*, Datenschutz im Internet, Rn. 869; Simitis u. a. (- *Simitis*), BDSG, § 4c, Rn. 41; *WP 12*, S. 17; so bereits in *WP 9*, S. 4; *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 27, die sogar von „angemessenen" Garantien spricht; gleiche Wortwahl auch bei *Reimer*, DuD 2001, S. 498; a. A. offenbar *Abel*, BDSG, S. 81, der im Hinblick auf die dem Artikel 26 Absatz 2 der Richtlinie nachgebildete Vorschrift des § 4c Absatz 2 BDSG annimmt, dass die Garantien die Behandlung der Daten entsprechend dem Standard des BDSG sicherstellen müssen.

[411] *WP 4*, S. 2.

nahme einer unabhängigen Kontrolle, die den Übermittlungsverlauf im Wege einer administrativen Steuerung von Anfang an in „datenschutzkonforme Bahnen“ lenkt.[412] Ferner soll durch die Genehmigungskompetenz der Kontrollbehörde ein Ausgleich dafür geschaffen werden, dass der Betroffene nicht an der Vertragsgestaltung beteiligt ist und die Berücksichtigung seiner schutzwürdigen Interessen einzufordern vermag.

Anderenfalls könnte der Vertrag außerdem jederzeit privatautonom von den Übermittlungsparteien ohne Mitwirkung des Betroffenen geändert werden.[413] Da eine vertragliche Vereinbarung überdies selten eine Konkurrenz zwischen verpflichteten Stellen oder ein gesellschaftliches Datenschutzbewusstsein auslösen dürfte, stellt sich die Genehmigungspflicht für Übermittlungen und somit die Vergegenwärtigung der staatlichen Aufsicht für vertragliche Abmachungen bei nicht vorformulierten oder veröffentlichten Verträgen wie zum Beispiel Standardvertragsklauseln der Europäischen Kommission als wichtiger Indikator einer guten Befolgungsrate dar.

Der Hinweis der Gegenmeinung, dass eine Vertragslösung in ihrem Schutzgehalt nicht überbewertet werden dürfe, ist darüber hinaus sehr ungenau. Es wird nicht erläutert, ob ein Vertrag allein schon imstande ist, ein angemessenes Schutzniveau herbeizuführen, oder ob noch weitere Kriterien hinzukommen müssen.

Eine vertragliche Vereinbarung vermag einen Drittländertransfer daher nur im Rahmen des Genehmigungstatbestandes des Artikels 26 Absatz 2 der Richtlinie zu legitimieren.[414] Die eigenmächtige Einflussnahme der einzelnen Übermittlungsparteien auf das Schutzniveau in dem Drittland durch einen Vertrag ist folglich ausgeschlossen.[415]

[412] Simitis u. a. (- *Simitis*), BDSG, § 4c, Rn. 2 und Rn. 30.
[413] *Ehmann*, CR 1991, S. 234, S. 235 f.
[414] Davon offenbar auch ausgehend *Ellger*, RabelsZ 60, S. 738, S. 743; *Hoeren/Queck*, S. 276; *Stein* in: Festschrift f. Rudolf, S. 513, S. 517, dort insb. Fn. 15; *WP 12*, S. 16 ff.; so bereits in *WP 4*, S. 2 und *WP 9*, S. 4. Ebenso im Hinblick auf das BDSG: Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 43; *ders*., CR 2000, S. 472, S. 480.
[415] *Ehmann*, CR 1991, S. 234, S. 236; *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 16; offenbar auch *Räther/Seitz*, MMR 2002, S. 425, S. 426; *Rittweger/Weiße*, CR 2003, S. 142, S. 148, allerdings für Unternehmensrichtlinien; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 30; *ders*., NJW 1997, S. 281, S. 285.

(b) Anwendbarkeit des mitgliedstaatlichen Datenschutzrechts

Berücksichtigung finden darf bei der Angemessenheitsprüfung demgegenüber die Anwendbarkeit eines mitgliedstaatlichen Datenschutzgesetzes in dem Drittland.[416]

Entsprechend dem Sitzprinzip ist das europäische Datenschutzrecht zum Beispiel auf die außereuropäischen Verarbeitungen eines in den Mitgliedstaaten ansässigen Verantwortlichen anzuwenden.[417] Das Risiko eines konkreten Transfers besteht hier also weniger in dem Schutzgehalt des anwendbaren Rechts, als in jenen dem außereuropäischen Staat zustehenden Zugriffsrechten, die über die Ausnahmetatbestände des Artikels 13 der Richtlinie hinausgehen.[418]

III. Die Angemessenheit des Schutzniveaus in den USA

Von einem regen Austausch personenbezogener Informationen begleitet sind die weltweit wichtigsten Handels- und Investitionsströme[419] zwischen der Europäischen Union und den USA. Vor diesem Hintergrund weckte das Datenschutzniveau in den USA im Hinblick auf die zu erwartenden Vorschriften zum Drittländertransfer bereits vor Erlass der Richtlinie 95/46/EG weltweit großes Interesse.[420]

Ein kurzer Überblick über das US-amerikanische Datenschutzsystem verdeutlicht rasch die auffälligen Unterschiede im Vergleich zu dem europäischen Datenschutzansatz.

Um den transatlantischen Handel durch Unsicherheiten der Privatwirtschaft im Hinblick auf die Angemessenheit des Schutzniveaus in den USA nicht dauerhaft zu gefährden, entwickelte das US-amerikanische Handelsministerium daher in Zusammenarbeit mit der Europäischen Kommission eine Kompromisslösung in Form der Safe Harbor Privacy

---

[416] *Wuermeling*, Handelshemmnis Datenschutz, S. 128, aber nur im Hinblick auf die Auftragsverarbeitung.
[417] Vgl. Gliederungspunkt B.I. des zweiten Kapitels.
[418] Vgl. Gliederungspunkt B.II.2.d des zweiten Kapitels.
[419] *Heil*, DuD 1999, S. 458.
[420] Stellvertretend für viele vgl. z. B. die Beiträge von *Cate*, 80 Iowa L. Rev., S. 431, S. 437 ff.; *Mei*, 25 L.P.Int'l.B., S. 305, S. 322 ff.; *Reidenberg*, 80 Iowa L. Rev., S. 497, S. 541 m. w. N.; *Wilske*, CR 1993, S. 297 ff.; *Wuermeling*, Handelshemmnis Datenschutz, S. 202 ff. Vgl. auch die von der Europäischen Kommission bei der Goethe Universität in Frankfurt a. M. in Auftrag gegebene Studie über das Datenschutzrecht der USA (veröffentlicht in: *Schwartz/Reidenberg*).

Principles, denen US-amerikanische Wirtschaftsunternehmen im Wege einer freiwilligen Selbstverpflichtung zur Herstellung eines angemessenen Schutzniveaus in ihrem Wirkungsbereich beitreten können.

1. Das US-amerikanische Datenschutzsystem

Die Richtlinie 95/46/EG bringt die gemeinsame Überzeugung der Mitgliedstaaten zum Ausdruck, dass es zu einer effektiven Gewährleistung der Privatsphäre, der Grundrechte sowie der Grundfreiheiten der Personen einer Normierung feststehender Schutzprinzipien in einem allgemeinen Datenschutzgesetz bedarf, das sich mit dem Schutz personenbezogener Informationen sowohl gegenüber dem Staat als auch gegenüber privaten Datenverarbeitern befasst.

Demgegenüber verfolgen die USA einen datenschutzrechtlichen Ansatz, der sich hauptsächlich mit dem Schutz der Bürger vor staatlichen Eingriffen in die informationelle Selbstbestimmung beschäftigt. Der Datenverkehr zwischen den Bürgern untereinander wird hingegen nur in einzelnen Bereichen geregelt. Diese sektorspezifischen Bestimmungen gelten zwar teils landeseinheitlich auf Bundesebene,[421] teils aber auch nur in einzelnen Bundesstaaten. Weder auf föderaler noch auf einzelstaatlicher Ebene existiert indessen ein allgemeines Datenschutzgesetz.[422]

Ergänzt wird das „komplexe Gefüge“[423] aus sektoralen Vorschriften von einer Selbstregulierung der Wirtschaft. Die Selbstkontrolle stellt sich in den USA generell als zentrales Regulativ des Handels dar, sodass der Gesetzgeber auch im Bereich des Datenschutzes weitestgehend auf den Druck des Wettbewerbs vertraut[424]. In der Praxis sind daher bei vielen Unternehmen so genannte Privacy Codes oder Privacy Policies durchaus üblich,[425] die sich jedoch meistens nur an den OECD-Leitlinien orientieren[426], unverbindlich sind und einen effektiven

[421] Vgl. dazu die ausführliche Aufzählung der Datenschutzgesetzgebungen auf föderaler Ebene: *U.S. Chamber of Commerce*, S. 43 ff.
[422] *Wilske*, CR 1993, S. 297, S. 299 und S. 304.
[423] *WP 15*, S. 2.
[424] Z. B. *Garstka*, DVBl. 1998, S. 981, S. 982; *Jacob* in: Datenverkehr ohne Datenschutz?, S. 25, S. 28.
[425] Vgl. dazu die Hilfestellungen im Handbuch der *U.S. Chamber of Commerce* für den Entwurf einer Privacy Policy für Websites.
[426] *Wellbery* in: Datenverkehr ohne Datenschutz?, S. 167, S. 172; *Wuermeling*, Handelshemmnis Datenschutz, S. 187.

Durchsetzungsmechanismus im Wege einer unabhängigen Kontrolle vermissen lassen.[427]

a. Das „Right to Privacy“

Der Schutz personenbezogener Informationen wird in den USA als Aspekt des bereits im Jahre 1890 erstmals von *Warren* und *Brandeis* im Harvard Law Review[428] definierten „Right to Privacy“ verstanden. Der Begriff „Privacy“ beschreibt die Unverletzlichkeit der Intimsphäre, die Entscheidungsautonomie des Individuums sowie die Selbstbestimmung des Einzelnen bei der Veröffentlichung seiner personenbezogenen Informationen.[429] In diesem Sinne ist das „Right to Privacy“ vergleichbar mit dem allgemeinen Persönlichkeitsrecht der europäischen Rechtsordnungen, betont jedoch noch stärker den Gesichtspunkt der autonomen Selbstbestimmung des Individuums.[430]

Das „Right to Privacy“ ist weder in der US-amerikanischen Verfassung noch in der Bill of Rights ausdrücklich niedergelegt. Auch hat das U.S. Supreme Court bislang keine dem Volkszählungsurteil des Bundesverfassungsgerichts[431] vergleichbare Grundsatzentscheidung über ein Grundrecht auf informationelle Selbstbestimmung getroffen.[432] Dennoch wird das „Right to Privacy“ inzwischen aus verschiedenen Vorschriften der Bill of Rights, insbesondere aus dem vierten Zusatzartikel[433] der Verfassung hergeleitet[434] und ist nunmehr auch als Common Law Right anerkannt.[435]

---

[427] *Heil*, DuD 2001, S. 129, S. 130.
[428] *Warren/Brandeis*, 4 Harvard L. Rev., S. 193 ff.
[429] *Bennett*, S. 12 ff., der jedoch im Hinblick auf die Regulierung der Verarbeitung personenbezogener Daten den Terminus „data protection“ bevorzugt.
[430] *Grimm/Roßnagel*, DuD 2000, S. 446, S. 447; *Westin*, S. 346.
[431] *BVerfGE* 65, S. 1.
[432] *Cate*, 80 Iowa L. Rev., S. 431, S. 437 f.; *Gellman* in: Governance of Global Networks, S. 71, S. 72. In der Entscheidung Whalen v. Roe stellte das U.S. Supreme allerdings fest, dass eine staatliche Datensammlung jedenfalls dann verfassungsmäßig ist, sofern ihr ein hinreichend Daten schützendes Gesetz zugrunde liegt (Whalen v. Roe, 429 U.S. 589 (1977).
[433] Fourth Amendment: „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.“
[434] *Bennett*, S. 199; *Grimm/Roßnagel*, DuD 2000, S. 446; Schwartz/Reidenberg (- *Schwartz*), S. 30; vgl. insbesondere auch *Westin*, S. 330 ff., der das „Right to Privacy“ aus verschiedenen Zusatzartikeln der Verfassung herleitet und im Übrigen auf S. 348 darauf hinweist, dass Warren und Brandeis bei ihrer Definition des „Right to Privacy“ in erster Linie den Eingriff privater Stellen vor Augen hatten. Im Fall Katz v. United States entschied das U.S. Supreme Court erstmals, dass auch ein nicht physisches Eindringen in die Privatsphäre des Individuums eine Verletzung des von dem Fourth Amendment gewährleisteten Schutzes darstellen kann (Katz v. United States, 389 U.S. 347 (1967)).

b. Der Schutz vor staatlichen Eingriffen

Einen grundsätzlichen Schutz vor staatlichen Eingriffen in das „Right to Privacy“ bietet gemäß den vorstehenden Erläuterungen das US-amerikanische Verfassungsrecht.

Anlass zu einer detaillierteren Regelung des Umgangs der Bundesverwaltung mit den personenbezogenen Informationen der Bürger bot schließlich Anfang der sechziger Jahre eine Diskussion über die Verfassungsmäßigkeit der Einrichtung einer staatlichen Datenbank zur Sammlung sämtlicher Daten über alle US-amerikanischen Staatsbürger.[436] Dem infolgedessen verabschiedeten Privacy Act of 1974[437] folgten im Laufe der Zeit äquivalente Gesetzgebungen in fast allen US-Bundesstaaten. Über die von dem Privacy Act gewährleisteten Ansprüche hinausgehende Zugangsrechte zu den von der Verwaltung gespeicherten Informationen sind ferner in dem Freedom of Information Act[438] vorgesehen. Diese generellen Bestimmungen für den staatlichen Umgang mit personenbezogenen Daten werden zudem von einigen Spezialgesetzgebungen flankiert.[439]

Als großes Defizit dieser Regulierung galt aus europäischer Sicht jedoch lange das Fehlen einer effizienten und unabhängigen Kontrolle.[440] So wurden erst im Jahre 1998 die Bundesbehörden zur Festlegung eines Verantwortlichen für die Umsetzung der Vorschriften angewiesen.[441]

Mögen diese Datenschutzbestimmungen sonach inzwischen im Einzelfall einen angemessenen Schutzstandard hinsichtlich der Datenverarbeitungen der öffentlichen Verwaltungen vorweisen, so schützen sie jedoch lediglich die Daten von US-amerikanischen Staatsbürgern.[442]

Aus diesem Grund haben sich die USA nach langwierigen Verhandlungen mit Vertretern der Europäischen Kommission gegenüber der Euro-

---

[435] *Grimm/Roßnagel*, DuD 2000, S. 446, S. 447; *Wilske*, CR 1993, S. 297, S. 304.
[436] *Garstka*, DVBl. 1998, S. 981, S. 982.
[437] Privacy Act of 1974, 5 U.S.C. § 552a.
[438] 5 U.S.C. § 552.
[439] Vgl. dazu ebenfalls die ausführliche Aufzählung der Datenschutzgesetzgebungen auf föderaler Ebene: *U.S. Chamber of Commerce*, S. 43 ff.
[440] *Bennett*, S. 198 f.
[441] *Garstka*, DVBl. 1998, S. 981, dort Fn. 14.
[442] *WP 66*, S. 6, dort insb. Fn. 16; z. B. Privacy Act of 1974, 5 U.S.C. Sec. 552a (a) (2): “the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence“.

päischen Gemeinschaft zur Einhaltung bestimmter[443], von der Europäischen Kommission für angemessen im Sinne des Artikels 25 Absatz 1 der Richtlinie befundenen Datenschutzgrundsätzen bei der Verarbeitung von personenbezogenen Informationen der Passagiere und Besatzungsmitglieder von Flügen in das Hoheitsgebiet der USA verpflichtet.[444] Anlässlich der Ereignisse des 11. September 2001 sind alle Fluggesellschaften seit einiger Zeit dazu verpflichtet, diese Daten an das Bureau of Customs and Border Protection des United States Department of Homeland Security zu übermitteln, indem sie ihm einen elektronischen Zugriff auf ihre Reservierungssysteme gestatten.[445]

Einschränkungen im Hinblick auf den Schutz vor staatlichen Eingriffen hat das „Right to Privacy" aufgrund des ebenfalls anlässlich der Ereignisse des 11. September 2001 erlassenen USA „Patriot Act"[446] vom 26. Oktober 2001 erfahren.[447] Danach stehen den US-amerikanischen Strafverfolgungsbehörden extensive Ermittlungsbefugnisse zur Prävention und Verfolgung terroristischer Straftaten zu. Als datenschutzrechtlich äußerst bedenklich erweisen sich dabei insbesondere die umfangreichen Zugangsrechte und Ermächtigungen zur Überwachung und Aufzeichnung der Telekommunikation und der elektronischen Kommunikation via Internet.[448]

---

[443] So wurden insbesondere eine Bindung an bestimmte Zwecke der Verarbeitung, eine Pflicht zur Unterrichtung der Betroffenen, Löschfristen, ein Recht auf Auskunft und Berichtigung, ein Verzicht auf die Verarbeitung sensibler Daten im Sinne des Artikels 8 Absatz 1 der Richtlinie, ein Durchsetzungsmechanismus sowie technische und organisatorische Sicherheitsmaßnahmen insbesondere hinsichtlich der Zugriffsberechtigungen auf die Reservierungssysteme der Fluggesellschaften, der Sicherheit der Computersysteme des Bureau of Customs and Border Protection und der Schulung von dessen Mitarbeitern festgelegt.

[444] Abkommen zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security vom 28. Mai 2004; *Europäische Kommission*, Entscheidung der Kommission vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden (2004/535/EG), ABl. EG Nr. L 235 vom 06.07.2004, S. 11; die Verhandlungen begleitend: *WP 66*, *WP 78* und *WP 87* einschließlich des bereits von dem United States Bureau of Customs and Border Protection und der United States Transportation Security Administration vorgelegten Entwurfs zur Gewährleistung eines angemessenen Schutzniveaus vom 22.5.2003 (Annex zu WP 78).

[445] Grundlage dieser Verpflichtung sind Vorschriften des „Aviation and Transportation Security Act" vom 19.11.2001 und des „Enhanced Border Security and Visa Entry Reform Act 2002" vom 14.5.2002.

[446] Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot) Act of 2001, P.L. 107-56 (H.R. 2975/H.R. 3162).

[447] Gute Übersicht zu den dadurch geänderten Gesetzen bei *Blokzyl*, S. 3 ff.

[448] Ausführlich dazu: *Band/Kennedy*, CRi 2002, S. 1 ff.

Zwar ist die Geltungsdauer des „Patriot Act“ auf vier Jahre begrenzt, sofern der Kongress die Zeitbeschränkung bis dahin nicht revidiert hat (Sunset Klausel). Allerdings sind schon jetzt erste Bestrebungen zur Aufhebung der Befristung zu beobachten,[449] sodass die erhebliche Beeinträchtigung des „Right to Privacy“ dauerhaft bei der Bewertung des US-amerikanischen Datenschutzniveaus zu berücksichtigen sein dürfte.

c. Gesetzlich normierter Datenschutz gegenüber privaten Datenverarbeitern

Der Schutz personenbezogener Informationen gegenüber privaten Datenverarbeitern wird in den USA ausschließlich bereichsspezifisch[450] von Gesetzen reglementiert.

Dieser sektorale Ansatz geht historisch auf die ausgeprägte liberalstaatliche Regulierungsphilosophie der USA zurück.[451] Traditionell befasst sich das US-amerikanische Verfassungsrecht ausschließlich mit den Abwehr- und den Zugangsrechten des Bürgers gegenüber dem Staat.[452] Die grundrechtlichen Garantien der Bill of Rights entfalten im Allgemeinen weder eine Drittwirkung[453] noch begründen sie staatliche Schutzpflichten hinsichtlich der Eingriffe durch private Stellen.[454] Im Gegenteil zeichnen sich die verfassungsrechtlich garantierten Freiheitsrechte der Bürger und im Übrigen auch parallel dazu das sich entsprechend seiner richterrechtlichen Rechtstradition gebildete System des Common Law unter anderem dadurch aus, dass der Staat sich bei der Regulierung privatrechtlicher Beziehungen weitestgehend zurückhält.[455]

In diesem Sinne ist die gesetzliche Normierung des Datenschutzes gegenüber Privaten vor allem von dem mit dem „Right to Privacy“ kon-

---

[449] *o.V.*, Presseportal vom 10.4.2003.
[450] Z. B. Gesetze zum Schutz medizinischer Daten, sowie zum Finanz-, Telekommunikations- oder Arbeitnehmerdatenschutz.
[451] *Wuermeling*, Handelshemmnis Datenschutz, S. 177.
[452] *Schwartz/Reidenberg*, S. 6.
[453] *Grimm/Roßnagel*, DuD 2000, S. 446, S. 447; Schwartz/Reidenberg (- *Schwartz*), S. 31 und S. 32; *Wilske*, CR 1993, S. 297, S. 299 und S. 304; *Wuermeling*, Handelshemmnis Datenschutz, S. 179. In Kalifornien wurde dem in der dortigen Landesverfassung verankerten „Right to Privacy“ jedoch im Urteil Porten v. University of San Francisco teilweise ein Drittschutz im Arbeitgeber-Arbeitnehmer-Verhältnis zuerkannt (Porten v. University of San Francisco, 64 Cal.App.3d 825 (1976)).
[454] Schwartz/Reidenberg (- *Schwartz*), S. 31.
[455] *Büllesbach*, RDV 2002, S. 55, S. 59; *Schwartz/Reidenberg*, S. 6; *Wellbery* in: Datenverkehr ohne Datenschutz?, S. 167, S. 170 f.; *Westin*, S. 330; zu dieser Wirkung des Common Law: *Ellger*, S. 86; *Miedbrodt*, Freundesgabe Büllesbach, S. 273, S. 279.

kurrierenden ersten Zusatzartikel[456] der US-amerikanischen Verfassung geprägt,[457] der unter anderem die Presse- und die Kommunikationsfreiheit, also mithin auch einen freien und transparenten Informationsfluss gewährleistet.[458] Dem sich daraus ergebenden konstitutionellen Abwehrrecht gegenüber staatlichen Eingriffen wird aufgrund des Fehlens einer verfassungsrechtlichen Pflicht zum Schutz des Bürgers vor Eingriffen privater Stellen in sein „Right to Privacy" generell eine dem Datenschutz übergeordnete Bedeutung beigemessen. Diese grundsätzliche Gewichtung legitimiert regelmäßig nur eine partielle Beeinträchtigung der Informationsfreiheit zugunsten des „Right to Privacy", die sich stets auf eine Reglementierung der Datenverarbeitung in einzelnen, eng umrissenen[459] und als besonders risikoreich für den Eintritt einer Verletzung des „Right to Privacy" betrachteten Bereichen beschränkt.[460]

Die scheinbare Fülle sektorieller Vorschriften auf föderaler Ebene sollte daher nicht über das fragmentarische Gesamtbild des privatrechtlichen Datenschutzes in den USA hinwegtäuschen, das nach allgemeiner Ansicht nicht den Erfordernissen des Artikels 25 der Richtlinie 95/46/EG genügt.[461] Eine andere Beurteilung rechtfertigt sich bisher auch nicht für einzelne Regelungssparten.[462] Ausnahmslos sind in allen Bereichen die fast unbegrenzte Zulässigkeit der dauerhaften Einrichtung von Datensammlungen, die fehlende Regelung von Verarbeitungsmodalitäten, die Möglichkeit einer Nutzung der Daten zu Sekun-

[456] „Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

[457] Vgl. *Grainger* in: UNESCO, S. 71, S. 83 f., der die Debatten um das „First Amendment Problem" bei der Regulierung des Internets wiedergibt.

[458] Durch die Gewährleistung einer passiven Kommunikationsfreiheit garantiert der erste Zusatzartikel auf der anderen Seite auch das „Right to Privacy", *Wellbery* in: Datenverkehr ohne Datenschutz?, S. 167, S. 170; *Westin*, S. 330 f. und S. 342.

[459] *Reidenberg*, 80 Iowa L. Rev., S. 497, S. 541.

[460] *Grimm/Roßnagel*, DuD 2000, S. 446, S. 447; *Schwartz/Reidenberg*, S. 7, ebenda (- *Reidenberg*), S. 215.

[461] Z. B. *WP 19*, S. 3; so bereits in *WP 15*, S. 3; Bräutigam/Leupold (- *Büllesbach*), A.III.1., Rn. 93; *Büllesbach/Höss-Löw*, DuD 2001, S. 135, S. 136; *Däubler*, RDV 1998, S. 96, S. 98; *Eul/Godefroid*, RDV 1998, S. 185, S. 189; *Gellman* in: Governance of Global Networks, S. 71, S. 79; Hamann/Weidert (- *Hamann*), S. 43; *Räther/Seitz*, MMR 2002, S. 425, S. 427; *Riemann*, CR 1997, S. 762, S. 763 f.; *Schaar*, Datenschutz im Internet, Rn. 872; *Seffer*, ITRB 2002, S. 66, S. 67.

[462] Im Ergebnis die sich ausführlich einzelnen Sektoren (Telecommunications, Financial Services, Direct Marketing, Employment) widmende Studie von Schwartz/Reidenberg (- *Reidenberg*), S. 219 ff.; so auch *Wilske*, CR 1993, S. 297, S. 299 ff.; *Wuermeling*, Handelshemmnis Datenschutz, S. 190 ff.; vgl. auch die Fallstudie von *Raab/Bennett/Gellman/Waters*.

därzwecken sowie das Fehlen einer unabhängigen Kontrolle zu beanstanden.[463]

Dennoch äußern sowohl das US-Handelsministerium als auch das US-Finanzministerium im Hinblick auf die noch ausstehenden Verhandlungen mit der Europäischen Kommission über die Gewährleistung eines angemessenen Schutzniveaus auf dem Finanzsektor nach wie vor ihre Hoffnungen auf eine positive Bewertung der in diesem Bereich bereits existierenden zahlreichen Reglementierungen[464] zum Datenschutz.[465]

Bereits während der Verhandlungen über die Safe Harbor Privacy Principles versprach sich das US-Handelsministerium die Feststellung eines angemessenen Schutzniveaus hinsichtlich des Fair Credit Reporting Act of 1970[466] (FCRA).[467] Das Gesetz reglementiert die Weitergabe und Offenlegung von Bankauskünften durch Kreditauskunfteien und fordert die Vertraulichkeit, die Korrektheit, die Relevanz und eine Nutzung der gesammelten Daten in einer angemessenen Art und Weise.[468]

Zu Recht hat die Europäische Kommission jedoch zu erkennen gegeben, dass sie nicht von der Angemessenheit des FCRA überzeugt ist.[469] Zum einen sind die Erlaubnistatbestände[470] für eine Weitergabe von Kreditauskünften vor dem Hintergrund des häufig sensiblen Inhalts der Angaben viel zu weit gefasst. Des Weiteren billigt das Gesetz dem Betroffenen zwar einen Auskunfts-[471] sowie einen verfahrensrechtlich abgesicherten Berichtigungsanspruch[472] zu. Die Ausübung dieser Rechte

[463] Schwartz/Reidenberg (- *Reidenberg*), S. 380 und S. 391 f.; *ders*., 80 Iowa L. Rev., S. 497, S. 544 f.; *Wilske*, CR 1993, S. 297, S. 307.
[464] Datenschutzrechtliche Regelungen in diesem Bereich sehen auf Bundesebene insbesondere folgende Gesetze vor: der Fair Credit Reporting Act of 1970, der Fair Credit Billing Act of 1974 (15 U.S.C. § 1666), der Equal Credit Opportunity Act of 1974 (15 U.S.C. § 1691 et seq.), der Fair Dept Collection Practices Act of 1977 (15 U.S.C. § 1692 et seq.), der Electronic Funds Transfer Act of 1978 (15 U.S.C. § 1693, 1693m) sowie der Financial Modernization Act 1999 (Gramm-Leach-Bliley Act).
[465] So in dem gemeinsamen Brief der beiden Ministerien an die Generaldirektion Binnenmarkt vom 23.3.2001: www.export.gov/safeharbor/March%2023%20Joint%20Letter.htm; hoffnungsvoll auch *Swire/Litan*, S. 32; *McCullagh*, WiredNews, 9.5.2000.
[466] 15 U.S.C. § 1681 et seq. (dem entspricht die in der „Safe Harbor"-Entscheidung in Bezug genommene, von der Federal Trade Commission anders paragraphierte Version (§§ 601 – 626) des Fair Credit Reporting Act: www.ftc.gov/os/statutes/fcra.htm#609).
[467] *Anhang IV* - B - der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 37, dort insb. Fn. 16; *WP 27*, S. 14.
[468] 15 U.S.C. § 1681.
[469] *Anhang IV* - B - der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 37.
[470] 15 U.S.C. § 1681b.
[471] 15 U.S.C. § 1681g.
[472] 15 U.S.C. § 1681i.

ist dem Betroffenen jedoch aufgrund einer fehlenden Informationspflicht über die Erhebung der Daten nur schwer möglich. Kritisiert wird außerdem das Fehlen des Erfordernisses einer Einwilligung in die Sammlung und Offenlegung der personenbezogenen Informationen.[473]

Mängel weist ferner der Durchsetzungsmechanismus auf. Zwar werden fahrlässige und vorsätzliche Verstöße[474] gegen den FCRA sanktioniert. Auch stehen der Federal Trade Commission Befugnisse zur Durchsetzung der Verpflichtungen aus dem FCRA zu.[475] Ein effektiver Kontrollmechanismus ist allerdings nicht ersichtlich.

Nicht zuletzt aber wegen des aufgrund des „Patriot Act“ neu eingefügten 15 U.S.C. § 1681v., der Strafverfolgungsbehörden zur Bekämpfung terroristischer Straftaten ein quasi autonomes Zugangsrecht zu allen Informationen gewährt, die eine Kreditauskunftei über einen Betroffenen gesammelt hat, sollte von der Feststellung eines angemessenen Schutzniveaus abgesehen werden. Das empfiehlt sich umso mehr, als dass die Wahrnehmung dieses Zugangsrechts vor jedermann, also auch vor dem Betroffenen selbst geheim zu halten ist.

Da die genannten Defizite in der jüngsten Änderung des FCRA vom 4.12.2003[476] keine Berücksichtigung finden, ist wohl auch in absehbarer Zukunft nicht an die Feststellung eines angemessenen Schutzniveaus bei Kreditauskunfteien zu denken.

Neben dem FCRA enthält auf dem Finanzsektor darüber hinaus nur noch der Financial Modernization Act 1999[477] (FMA) nach europäischen Maßstäben verhältnismäßig ausführliche Datenschutzregelungen.

Der FMA verpflichtet die US-amerikanischen Finanzinstitute zur Gewährleistung eines Vertraulichkeitsschutzes für personenbezogene Informationen ihrer Kunden sowie zu Maßnahmen der Datensicherheit.[478]

---

[473] So *Mei*, 25 L.P.Int'l.B., S. 305, S. 327.
[474] 15 U.S.C. § 1681o und § 1681p.
[475] 15 U.S.C. § 1681s.
[476] Abrufbar unter: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2622enr.txt.pdf (vgl. auch den der Änderung zugrunde liegenden Antrag des US-Finanzministeriums vom 30.6.2003: www.ustreas.gov/press/releases/reports/js5152.doc, zusammengefasst und erläutert von der Federal Trade Commission unter: www.ftc.gov/os/2003/07/fcratest.html).
[477] 15 U.S.C. § 6801 et seq. (Gramm-Leach-Bliley Act).
[478] 15 U.S.C. § 6801.

Dennoch weist auch dieses Gesetz Mängel auf. Um dem Betroffenen einen Widerspruch gegen einzelne Übermittlungen seiner Daten an Dritte zu ermöglichen, ist zwar die Zulässigkeit einer Datenweitergabe durch eine regelmäßige Information des Betroffenen über die Art der erhobenen Daten sowie die Kategorien von Datenempfängern bedingt.[479] Einem angemessenen Schutzniveau widersprechen dürften allerdings die zahlreichen Ausnahmen zu diesen Grundsätzen der Informationspflicht und der „opt-out"-Wahlmöglichkeit. Die beiden Prinzipien sind zum Beispiel nicht zu berücksichtigen bei Weitergaben an Stellen, die mit dem jeweiligen Finanzinstitut verbunden sind.[480] Ihre Beachtung entfällt ferner bei einer Übermittlung an eine Kreditauskunftei im Sinne des FCRA,[481] sodass sich schon aufgrund dieser Durchlässigkeit des Schutzsystems zugunsten des kein angemessenes Schutzniveau vermittelnden FCRA die Feststellung einer Angemessenheit verbietet.

Davon abgesehen bestehen weder ein Auskunfts- noch ein Berichtigungsanspruch. Die Durchführung seiner Vorschriften überträgt der FMA zwar den jeweils zuständigen staatlichen Stellen.[482] Ein individuelles Beschwerdeverfahren ist demgegenüber nicht vorgesehen, sodass die Feststellung eines angemessenen Schutzniveaus auch daran scheitern sollte.

Da selbst diese im Vergleich zu anderen Sparten noch recht umfangreichen Reglementierungen auf dem Finanzsektor nicht den Anforderungen des Artikels 25 Absatz 1 der Richtlinie genügen, scheint auf föderaler Ebene derzeit kein Gesetz ersichtlich, für dessen Anwendungsbereich insgesamt ein angemessenes Schutzniveau festgestellt werden könnte.

Auch auf einzelstaatlicher Ebene stellt sich die Situation nicht wesentlich anders dar. Wenngleich die Verfassungen einiger Bundesstaaten ausdrücklich ein „Right to Privacy" vorsehen,[483] ist bislang kein Gesetz bekannt, das europäischen Maßstäben entsprechen würde.

---

[479] 15 U.S.C. § 6802 und 6803 (b).
[480] 15 U.S.C. § 6802 (a).
[481] 15 U.S.C. § 6802 (e) (6) (A).
[482] 15 U.S.C. § 6804, 6805: vgl. z. B. für die in die Zuständigkeit der Federal Trade Commission fallenden Institute: www.ftc.gov/privacy/privacyinitiatives/financial_rule.html, mit weiteren Links.
[483] Alaska, Arizona, Kalifornien, Florida, Hawaii, Illinois, Louisiana, Montana, New York, Pennsylvania, South Carolina und Washington.

Das bedeutet zwar nicht, dass sich im Rahmen einer konkreten Datenübermittlung nicht doch einmal ein angemessenes Schutzniveau aus US-amerikanischen Datenschutzbestimmungen ergeben könnte. Voraussetzung dafür wäre jedoch, dass der jeweilige Datenempfänger bei der konkret vorgesehenen oder möglichen Verarbeitung der spezifischen Daten an angemessene Schutzgarantien gebunden ist. Im Hinblick auf die aufgezeigten Defizite der nationalen Datenschutzgesetze dürfte es sich jedoch dabei eher um einen Ausnahmefall handeln.

d. Das Deliktsrecht des Common Law

In die Bewertung des Schutzniveaus einfließen kann ferner das von den einzelstaatlichen Gerichten ausgestaltete Deliktsrecht, das in der zweiten Bearbeitung des Restatement, Sachgebiet „Unerlaubte Handlungen“, (Restatement (Second) of Law – Torts) durch das American Law Institute zusammengefasst wurde.

Bei einer Verletzung des „Right to Privacy“ können danach vier verschiedene Anspruchsgrundlagen einen Schadensersatz auslösen: „intrusion upon seclusion“[484] (Verletzung der Intimsphäre), „misappropriation of name or likeness for commercial purposes“[485] (unbefugter Namens- oder Bildgebrauch durch Dritte für eigene Zwecke oder zum eigenen Nutzen), „public disclosure of private facts“[486] (Veröffentlichung privater Sachverhalte) sowie „false light publicity“[487] (irreführende Darstellung in der Öffentlichkeit).[488]

Ein Missbrauch im Sinne dieser Tatbestände hinsichtlich der aus den Mitgliedstaaten übermittelten Daten sollte allerdings einen Ausnahmefall bilden. Dem Deliktsrecht kommt bei der Beurteilung des Datenschutzniveaus in den USA daher grundsätzlich nur eine untergeordnete Bedeutung zu.

2. Die „Safe Harbor“-Entscheidung der Europäischen Kommission

Angesichts dieser erheblichen Divergenzen zwischen dem europäischen und dem US-amerikanischen Datenschutzansatz brachte die so genann-

[484] Restatement, § 652B.
[485] Restatement, § 652C.
[486] Restatement, § 652D.
[487] Restatement, § 652E.
[488] Ausführlich zu den einzelnen Tatbeständen *Wilske*, CR 1993, S. 297, S. 304 f.; *Wuermeling*, Handelshemmnis Datenschutz, S. 185 ff.; ebenso der *Anhang IV* - A- der „Safe Harbor“-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 32 ff.

te „Safe Harbor"-Entscheidung der Europäischen Kommission vom 26. Juli 2000[489] erstmals Entspannung in die Debatte über die Frage, wann von einem angemessenen Schutzniveau im Sinne des Artikels 25 Absatz 2 der Richtlinie[490] im Hinblick auf Datenübermittlungen in die USA ausgegangen werden darf.[491]

In der Literatur wurde gar von einem „Meilenstein" auf dem Weg zu einer weltweiten Absicherung des europäischen Datenschutzstandards gesprochen, da die Entscheidung Maßstäbe für zukünftige Datenschutzverträge gesetzt habe.[492] Nicht zu leugnen ist jedenfalls, dass die Entscheidung der Europäischen Kommission die Gefahr einer handelshemmenden Wirkung des Datenschutzes auf internationaler Ebene deutlich entschärft hat und der Kooperation zwischen den US-amerikanischen und den europäischen Verhandlungspartnern eine gewisse Vorbildfunktion im Hinblick auf künftige Regelungen, insbesondere hinsichtlich der erforderlichen datenschutzrechtlichen Regulierungen des Internets zukommt.

Gemäß dem Artikel 1 Absatz 1 der „Safe Harbor"-Entscheidung geht die Europäische Kommission unter der Berücksichtigung der Anhänge III bis VI[493] der Entscheidung davon aus, dass die in Anhang I der Entscheidung beigefügten, von dem US-Handelsministerium herausgegebenen Safe Harbor Privacy Principles[494] ein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 der Richtlinie für personenbezogene Daten gewährleisten, die aus der Europäischen Union an eine in den USA niedergelassene Organisation übermittelt werden. Voraussetzung ist allerdings, dass die Principles gemäß den ebenfalls vom US-Handelsministerium herausgegebenen und in Anhang II der Entschei-

[489] *Europäische Kommission*, Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (2000/520/EG), ABl. EG Nr. L 215 vom 25.08.2000, S. 7.

[490] Artikel 1 Absatz 1 der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 8; a. A. *Koenig/Röder*, CR 2000, S. 668, S. 675, die die Safe Harbor Privacy Principles ohne nähere Begründung dem Artikel 26 Absatz 2 der Richtlinie zuordnen; so auch *Hoeren*, S. 270.

[491] Vgl. z. B. Bericht von *McCullagh*, WiredNews, 9.5.2000.

[492] So *Heymann*, CRi 2000, S. 70, S. 71.

[493] Die *Anhänge III bis VI* enthalten folgende, vom US-Handelsministerium veröffentlichte Dokumente: „Grundsätze des sicheren Hafens: Überblick über die Möglichkeiten der Durchsetzung" (Anhang III); ein Memorandum über Entschädigungen für die Verletzung der Privatsphäre und ausdrückliche Ermächtigungen gemäß dem US-Recht (Anhang IV); ein Schreiben der Federal Trade Commission (Anhang V) und ein Schreiben des US-Verkehrsministeriums (Anhang VI).

[494] Auch abgedruckt in: *U.S. Department of Commerce*, DuD 2000, S. 480.

dung dargestellten Frequently Asked Questions (FAQ) umgesetzt werden. Dieses Angemessenheitsurteil bezieht sich auf alle unter die Richtlinie 95/46/EG fallenden Tätigkeiten.

Entsprechend dieser Feststellung der Europäischen Kommission im Sinne des Artikels 25 Absatz 6 der Richtlinie ist also eine Datenübermittlung aus den Mitgliedstaaten in die USA grundsätzlich gemäß Artikel 25 Absatz 1 der Richtlinie zulässig, sofern der US-amerikanische Datenempfänger dem „sicheren Hafen" angehört. Die Entscheidung betont zudem die eigentliche Selbstverständlichkeit[495], dass die Safe Harbor Privacy Principles nicht die Anwendbarkeit des jeweiligen mitgliedstaatlichen Datenschutzgesetzes gemäß Artikel 4 Absatz 1 der Richtlinie ersetzen, sofern ein US-amerikanischer Verantwortlicher unmittelbar in der Europäischen Union Daten erhebt oder verwendet.[496]

a. System der freiwilligen Selbstregulierung

Bei den Safe Harbor Privacy Principles einschließlich der FAQ handelt es sich um ein System der freiwilligen Selbstregulierung. Es obliegt daher der freien Entscheidung eines US-amerikanischen Datenverarbeiters, ob er sich auf die Einhaltung der bindenden Datenschutzprinzipien verpflichten möchte.

Die Methodik der Safe Harbor Privacy Principles entspricht dem Regulierungsmechanismus datenschutzrechtlicher Selbstkontrollkodizes der Wirtschaft, die gemäß der Arbeitsunterlage WP 12 der Art. 29-Gruppe[497] als Standesregeln im Sinne des Artikels 25 Absatz 2 der Richtlinie in die Bewertung des Datenschutzniveaus eines Drittlandes einfließen können.

Zwar wurden die Safe Harbor Privacy Principles nicht von einem Berufsstand oder einem Wirtschaftsverband entwickelt, sondern von dem selbst keine Durchsetzungsfunktionen wahrnehmenden US-Handelsministerium gewissermaßen als Referenzrahmen[498] für eine den

---

[495] Vgl. dazu Gliederungspunkt B. des zweiten Kapitels.

[496] Artikel 2 der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 9. Nicht nachvollziehbar daher *Gola/Klug*, S. 44 f., die bei der Frage der Anwendbarkeit des BDSG auf verantwortliche Stellen, die in Deutschland vom Drittland aus Daten erheben, verarbeiten oder nutzen, offenbar berücksichtigen wollen, ob das betreffende Drittland über ein angemessenes Schutzniveau verfügt.

[497] *WP 12*, S. 11 ff.; so bereits in *WP 7*, S. 2 ff.

[498] *Klug*, RDV 1999, S. 109, S. 112; vgl. auch *Franzen*, DB 2001, S. 1867, S. 1869, der von einem „selbstregulierte(n) Rechtsrahmen" spricht.

Anforderungen des Artikels 25 Absatz 2 der Richtlinie genügende Selbstregulierung herausgegeben. Da jedoch nur solche Datenverarbeiter von den Vorteilen des „sicheren Hafens“ zu profitieren vermögen, die sich freiwillig der Regulierungsbefugnis einer unabhängigen Stelle unterwerfen, unterscheidet sich die Funktionsweise der von den Safe Harbor Privacy Principles gestalteten Selbstregulierung nicht von jener eines herkömmlichen[499] Standeskodexes.[500]

b. Qualifizierung für den „sicheren Hafen“

Ein für die Verarbeitung Verantwortlicher, der personenbezogene Daten aus der Europäischen Union in die USA übermittelt, darf von einem angemessenen Schutzniveau im Sinne des Artikels 25 Absatz 2 der Richtlinie bei dem Datenempfänger ausgehen, sofern sich dieser für den „sicheren Hafen“ qualifiziert hat. Die Voraussetzungen dieser Qualifikation sind in Artikel 1 Absatz 2 und Absatz 3 der „Safe Harbor“-Entscheidung niedergelegt.

(1) Die Selbstverpflichtung zur Befolgung der Safe Harbor Privacy Principles

Gemäß Artikel 1 Absatz 2a) der „Safe Harbor“-Entscheidung muss sich der US-amerikanische Datenempfänger eindeutig und öffentlich zur Einhaltung der Safe Harbor Privacy Principles verpflichten, die bei ihm gemäß den FAQ umgesetzt wurden. Zwar hat der US-amerikanische Verarbeiter dabei nicht nachzuweisen, dass er die Grundsätze des „sicheren Hafens“ tatsächlich befolgt. Mit der Verpflichtungserklärung bestätigt er jedoch konstitutiv, dass er die Safe Harbor Privacy Principles in seinem Wirkungskreis implementiert hat und sie entsprechend ihrem Anwendungsbereich einhalten wird.

(a) Qualifikationskonzepte

Als Grundlage zur Implementierung der Safe Harbor Privacy Principles kommen gemäß dem Anhang I der „Safe Harbor“-Entscheidung[501] verschiedene Qualifikationskonzepte in Betracht.

---

[499] Vgl. dazu Gliederungspunkt C.II.2.b.(2). dieses Kapitels.

[500] A. A. offenbar Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 71, der die Safe Harbor Privacy Principles aufgrund der Selbstverpflichtung mit den Übermittlungsregelungen nach Artikel 26 Absatz 2 der Richtlinie vergleicht. Dabei übersieht er jedoch, dass Artikel 26 Absatz 2 der Richtlinie Garantien seitens der für die Übermittlung verantwortlichen Stelle voraussetzt.

[501] *Anhang I* der „Safe Harbor“-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 10.

So kann sich die verarbeitende Stelle beispielsweise einem von und für die Privatwirtschaft entworfenen, die Principles berücksichtigenden Datenschutzprogramm anschließen. Viele der derzeit geläufigen Programme sind allerdings für das Internet konzipiert[502] und erweisen sich daher nur für Datenverarbeitungen in diesem Rahmen als geeignet.

Alternativ hat der Datenverarbeiter die Möglichkeit, eigene Maßnahmen zur Umsetzung der Safe Harbor Privacy Principles zu entwickeln. Diese Option dürfte insbesondere für jene Unternehmen interessant sein, die bereits vor Erlass der „Safe Harbor"-Entscheidung eine firmeneigene, für alle Mitarbeiter verbindliche „Privacy Policy" besaßen, die sie lediglich um die Anforderungen des „sicheren Hafens" ergänzen müssen.

Schließlich vermögen solche Organisationen vom „sicheren Hafen" zu profitieren, welche Gesetzen, Regulierungs-, Verwaltungs- oder anderen Rechtsvorschriften unterliegen, die einen hinreichenden Schutz personenbezogener Daten gewährleisten. Aufgrund der fragmentarischen Datenschutzgesetzgebung in den USA wird diese Form der Qualifizierung aber wohl nur im Einzelfall möglich sein.

(b) Der Anwendungsbereich der Safe Harbor Privacy Principles

Die verarbeitende Stelle ist dazu verpflichtet, die Safe Harbor Privacy Principles auf alle personenbezogenen Daten anzuwenden, die ihr während ihrer Teilnahme am „sicheren Hafen" aus der Europäischen Union übermittelt werden. Diese Bindung besteht auch nach dem Verlassen des „sicheren Hafens" fort.[503]

Sie erweist sich insbesondere als problematisch, sofern ein „Safe Harbor"-Unternehmen aufgrund einer Fusion oder einer Übernahme seinen Status als selbstständige Einheit verliert und die übernehmende beziehungsweise aus der Fusion hervorgehende Einheit die Safe Harbor Privacy Principles bei ihren Datenverarbeitungen nicht zu respektieren beabsichtigt.

Die *FAQ 6* begegnet dieser Unwägbarkeit mit einer vorherigen Anzeigepflicht einer derartigen Fusion gegenüber dem US-

[502] Z. B. von TRUSTe und BBBOnLine.
[503] *Anhang II* (FAQ 6) der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 16.

Handelsministerium. Erklärt sich die neue Einheit nicht ausdrücklich zu einer Übernahme der „Safe Harbor"-Verpflichtungen bereit, sind alle aus der Europäischen Union im Rahmen des „sicheren Hafens" empfangenen Datenbestände unverzüglich zu löschen.[504]

Ausnahmsweise kann die Anwendung der Safe Harbor Privacy Principles allerdings beschränkt werden. So ist eine Außerachtlassung der Grundsätze zulässig, falls es sich aus Erfordernissen der nationalen Sicherheit, des Staatsinteresses oder staatlicher Vollzugs- und Vollstreckungsmaßnahmen[505] als notwendig erweist.

Auch Gesetze, staatliche Verordnungen oder das Fallrecht erlauben eine Abweichung, sofern und soweit sie entweder ausdrücklich dazu ermächtigen oder ihre Befolgung in einem unlösbaren Konflikt mit den Principles stehen würde. Die verarbeitende Stelle hat in Wahrnehmung einer derartigen Ausnahme jedoch nachzuweisen, dass sie die Anforderungen der Principles nur in dem Umfang vernachlässigt, als es in dem von der Ermächtigung zum Ausdruck gebrachten, übergeordneten berechtigten Interesse geboten ist. Ferner soll sie möglichst darlegen, welche dieser Ausnahmen regelmäßig bei ihren Verarbeitungen vorkommen.

Die Ausnahme der ausdrücklichen rechtlichen Ermächtigung gab der Art. 29-Gruppe Anlass zu der Sorge, dass sich auf diese Weise Ausnahmen von den Safe Harbor Privacy Principles rechtfertigen ließen, die über die Ausnahmetatbestände der Richtlinie hinausgingen.[506] Das US-Handelsministerium beschwichtigte jedoch, da es regelmäßig entweder an einer zur Erfüllung des Tatbestandes einer solchen Ermächtigung erforderlichen expliziten Autorisierung fehle oder die Abweichung von den Principles sich ohnehin bereits aus einem staatlichen Interesse legitimiere.[507]

---

[504] Vgl. dazu auch die Erläuterungen des US-Handelsministeriums zum US-amerikanischen Fusionsrecht in *Anhang IV* - C - der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 38.

[505] Vgl. die englische Originalversion des vom US-Handelsministerium herausgegebenen *Anhangs I* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 10, die von „public interest" und „law enforcement requirements" spricht. Die deutsche Übersetzung, nach welcher „dem öffentlichen Interesse" und der „Durchführung von Gesetzen Rechnung getragen werden" soll, ist hier etwas undeutlich.

[506] *WP 32*, S. 5.

[507] Vgl. die beispielhaften Belege des US-Handelsministeriums in *Anhang IV* - B - der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 35 ff.

Des Weiteren darf der US-amerikanische Datenverarbeiter in einem jeweils vergleichbaren Kontext auf die in der Richtlinie 95/46/EG und die in dem nationalen Recht des jeweiligen Mitgliedstaates ausdrücklich vorgesehenen Ausnahmen zurückgreifen. Zu denken ist hier etwa an die nicht ohnehin bereits erwähnten Tatbestände des Artikels 13 der Richtlinie sowie an den Empfang von Daten im Rahmen von Übermittlungen aus der Europäischen Union auf der Grundlage des Artikels 26 Absatz 1 der Richtlinie.

In Einklang mit Artikel 9 der Richtlinie,[508] der unter anderem Ausnahmen für Verarbeitungen zu journalistischen Zwecken vorsieht, stellt schließlich die *FAQ 2* klar, dass ein Konflikt zwischen der Anwendung der Safe Harbor Privacy Principles und der Gewährleistung der im ersten Zusatzartikel der US-amerikanischen Verfassung verankerten Pressefreiheit stets zugunsten der letzteren zu lösen sei.[509]

(2) Der Geltungsbereich der Safe Harbor Privacy Principles

Die Möglichkeit der Teilnahme am „sicheren Hafen“ steht gemäß Artikel 1 Absatz 2b) in Verbindung mit Anhang VII der „Safe Harbor“-Entscheidung bislang nur solchen Organisationen offen, die den gesetzlichen Befugnissen der Federal Trade Commission (FTC) oder des US-Verkehrsministeriums und somit jeweils der Aufsicht einer staatlichen Einrichtung unterliegen, die unfaire und irreführende Geschäftspraktiken verfolgt, zu denen auch ein Verstoß gegen die proklamierte eigene Datenschutzpolitik gehört.

Die Rechtsbefugnisse der FTC ergeben sich aus dem Abschnitt 5 des Federal Trade Commission Act (FTC Act)[510] und betreffen unfaire und irreführende Praktiken und Handlungen in und mit Bezug auf den gesamten Handel. Ausgenommen von der Zuständigkeit der FTC sind allerdings Banken, Spar- und Darlehenskassen, Kreditgenossenschaften, Telekommunikationsunternehmen, bundesstaatübergreifend tätige Transportunternehmen, Luftverkehrsgesellschaften, Verlader und Lagerbetriebe sowie Vieh- und Fleischhändler beziehungsweise Fleischwarenproduzenten.[511] Soweit das Versicherungsgeschäft von den ein-

[508] So wohl *WP 21*, S. 4.
[509] Vgl. dazu Gliederungspunkt C.III.1.c. dieses Kapitels.
[510] 15 U.S.C. § 41 et seq.
[511] 15 U.S.C. § 45 (a) (2); vgl. auch *Anhang III* sowie *Anhang VII* der „Safe Harbor“-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 26 ff. und S. 47, die diese Gruppen ausdrücklich von dem Anwendungsbereich der „Safe Harbor“-Entscheidung ausschließen.

zelnen Bundesstaaten reguliert wird,[512] fällt es ebenfalls nicht in den Zuständigkeitsbereich der FTC.

Das US-Verkehrsministerium verfolgt auf der Grundlage des 49 U.S.C. 41712 unlautere und irreführende Praktiken von Luftverkehrsgesellschaften bei dem Verkauf von Flugtickets.

Darüber hinaus ist der Geltungsbereich des „sicheren Hafens“ gemäß Erwägungsgrund (6) der „Safe Harbor“-Entscheidung auf solche Datenverarbeitungen beschränkt, zu deren Regulierung die FTC oder das US-Verkehrsministerium sachlich befugt sind. Obschon ein US-amerikanischer Datenempfänger also grundsätzlich der Zuständigkeit der FTC oder des US-Verkehrsministeriums unterliegt, vermag er sich nur im Hinblick auf solche Verarbeitungen für den „sicheren Hafen“ zu qualifizieren, die Tätigkeiten im Bereich des Handels oder der Luftfahrt betreffen. Die Feststellung eines angemessenen Schutzniveaus gilt daher zum Beispiel nicht für Verarbeitungen ohne einen gewerblichen Hintergrund, wie etwa Tätigkeiten im Rahmen der Mittelbeschaffung zu wohltätigen Zwecken[513].

(3) Die Selbstzertifizierung

Die genannten Voraussetzungen des Artikels 1 Absatz 2 gelten gemäß Artikel 1 Absatz 3 der „Safe Harbor“-Entscheidung als erfüllt, sobald der US-amerikanische Datenverarbeiter dem US-Handelsministerium die öffentliche Bekanntgabe seiner Verpflichtung nach Artikel 1 Absatz 2a) sowie die Identität der für ihn zuständigen staatlichen Einrichtung gemäß Artikel 1 Absatz 2b) mitgeteilt hat.

Das Prozedere dieser so genannten Selbstzertifizierung ist in der *FAQ 6* dargestellt. Danach muss der den Safe Harbor Privacy Principles beitretende Datenverarbeiter dem US-Handelsministerium unter anderem schriftlich die Tätigkeit beschreiben, in deren Zusammenhang er die aus der Europäischen Union importierten personenbezogenen Daten verarbeitet. Die darüber hinaus darzubringende Erläuterung seiner Datenschutzgrundsätze soll mindestens den Ort beinhalten, an dem die Datenschutzbedingungen öffentlich ausgelegt sind, sowie den Termin, zu welchem sie umgesetzt wurden.

[512] Vgl. McCarran-Ferguson Act: 15 U.S.C. § 1011 et seq., insb. § 1012 (a), der die Regulierungskompetenz für das Versicherungsgeschäft den Bundesstaaten zuweist.
[513] *Anhang III* der „Safe Harbor“-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 27, sowie *Anhang V* (S. 39 ff.) und *Anhang VI* (S. 45 f.).

Weiterhin ist der für Beschwerden, Auskunftsersuchen und ähnliche Angelegenheiten im Sinne der Principles zuständige Ansprechpartner zu benennen sowie das unabhängige Schiedsverfahren und/oder das Datenschutzprogramm zu bezeichnen, an dem die Organisation zur Umsetzung des Durchsetzungsgrundsatzes teilnimmt. Die verarbeitende Stelle muss außerdem anzeigen, ob sie ein internes oder ein externes Kontrollverfahren durchführt. Möchte sie auch manuelle Datenbestände sowie Personaldaten empfangen, hat sie darauf ebenfalls ausdrücklich hinzuweisen.[514]

Das US-Handelsministerium veröffentlicht diese Informationen auf seiner Website in der eigens dafür eingerichteten „Safe Harbor"-Liste[515], die regelmäßig aktualisiert wird. Erneuert eine Organisation ihr Selbstzertifizierungsschreiben nicht mindestens einmal im Jahr, wird sie von der Liste gestrichen und verliert infolgedessen ihren Status als „sicherer Hafen".

c. Der Inhalt der Safe Harbor Privacy Principles

Gemäß der „Safe Harbor"-Entscheidung der Europäischen Kommission ist ein angemessenes Schutzniveau hinsichtlich einer Datenübermittlung in die USA gewährleistet, sofern der US-amerikanische Datenempfänger die Grundsätze des „sicheren Hafens" unter der Berücksichtigung der FAQ umgesetzt hat.

Die FAQ erläutern die Safe Harbor Privacy Principles und gestalten sie verbindlich aus. Das ist insofern ungewöhnlich, als dass Frequently Asked Questions normalerweise unverbindlich sind und lediglich ein Regelwerk oder ein Verfahren zu seiner besseren Verständlichkeit in einem besonders leicht zugänglichen Frage-Antwort-Stil illustrieren.[516]

Ursächlich für die Deklaration der FAQ zu verbindlichen Auslegungsmaximen mag einerseits eine Stellungnahme der Art. 29-Gruppe[517] sein, nach der ein Selbstregulierungskodex nur dann ein angemessenes Schutzniveau gewährleiste, sofern er in einer allgemein verständlichen Sprache formuliert sei und konkrete Beispiele zur Veranschaulichung

---

[514] *Anhang I* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 10 f.
[515] Abrufbar unter: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
[516] *Räther/Seitz*, MMR 2002, S. 425, S. 428, dort insb. Fn. 22.
[517] *WP 12*, S. 12; so bereits in *WP 7*, S. 3.

seiner Bestimmungen enthalte. Andererseits überbrückt die Verbindlichkeit der FAQ aus europäischer Sicht die wesentlichen Unwägbarkeiten bei der Durchführung der Safe Harbor Privacy Principles,[518] deren Auslegung grundsätzlich nach US-Recht erfolgen soll[519].

In diesem Sinne werden die sieben Safe Harbor Privacy Principles nachfolgend unter Einbezug der fünfzehn FAQ vorgestellt und in ihren wesentlichen Aussagen unter Berücksichtigung der Voraussetzungen eines angemessenen Schutzniveaus analysiert.

(1) Notice – Informationspflicht

Gemäß der Informationspflicht hat der US-amerikanische Datenempfänger den Betroffenen über den Zweck zu informieren, für den die personenbezogenen Daten erhoben und verwendet werden, sowie darüber aufzuklären, wie er bei eventuellen Nachfragen und Beschwerden kontaktiert werden kann. Ferner muss der Betroffene erfahren, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege ihm zur Verfügung stehen, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Informationen sind möglichst zum Zeitpunkt der Erhebung zu erteilen, jedoch spätestens, bevor der US-amerikanische Verarbeiter die Daten zu anderen Zwecken verwendet als zu denen, für welche die Daten ursprünglich erhoben oder verarbeitet wurden, oder bevor die verarbeitende Stelle die Daten erstmalig an einen Dritten weitergibt.

Mit der Informationspflicht greifen die Safe Harbor Privacy Principles umfassend den von der Art. 29-Gruppe in der Arbeitsunterlage WP 12 postulierten Grundsatz der Transparenz auf.[520] Über die Forderungen der Datenschutzgruppe hinaus schreiben sie, wenngleich auch etwas großzügiger als die Artikel 10 und 11 der Richtlinie, sogar den Zeitpunkt für die Information des Betroffenen vor.[521]

(2) Choice – Wahlmöglichkeit

[518] Dennoch befürchten *Verbiest/Wéry*, Rn. 898, dass das Fehlen der meisten Definitionen aus der Richtlinie zu Abweichungen von fundamentalen Grundsätzen führen könnte.
[519] *Anhang I* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 11.
[520] Vgl. dazu Gliederungspunkt C.II.1.a. dieses Kapitels.
[521] Vgl. aber *Räther/Seitz*, MMR 2002, S. 425, S. 429 f., die den Grundsatz der Informationspflicht wegen des Fehlens einer bereits zum Zeitpunkt der Erhebung zwingenden Informationspflicht kritisieren.

Entsprechend dem Grundsatz der Wahlmöglichkeit steht dem Betroffenen generell ein Widerspruchsrecht gegen die Weitergabe der Daten an Dritte sowie gegen die Verarbeitung zu Sekundärzwecken zu.[522] Die Ausübung dieses so genannten „opt-out"-Wahlrechts muss dem Betroffenen durch leicht erkennbare und verständliche sowie leicht zugängliche und kostengünstige Verfahren möglich sein.

Eine ausdrückliche Zustimmung („opt-in") des Betroffenen benötigt die US-amerikanische Stelle indessen für eine Weitergabe oder Zweckänderung der Verarbeitung sensibler Daten. Die Sensibilität der Daten erschließt sich dabei aus einer Aufzählung der in Artikel 8 Absatz 1 der Richtlinie genannten Merkmale sowie daraus, dass der europäische Datenübermittler die Daten ausdrücklich als sensibel bezeichnet. Ausnahmen von dem Zustimmungserfordernis sind nur in den von der *FAQ 1* genannten Fällen zulässig, die mit den Ausnahmetatbeständen des Artikels 8 Absatz 2 und Absatz 3 der Richtlinie korrespondieren und somit im Verhältnis zu der Richtlinie 95/46/EG keine Minderung des Datenschutzniveaus herbeiführen.

Während die „opt-in"-Wahlmöglichkeit demnach für die Verarbeitung sensibler Daten weitestgehend mit den Bestimmungen der Richtlinie 95/46/EG übereinstimmende Zulässigkeitsbedingungen schafft, bewirkt die „opt-out"-Wahlmöglichkeit für die Verwendung der nicht sensiblen personenbezogenen Daten eine Aufweichung des Zweckbindungsgrundsatzes[523].

Zwar ist die Verwendung der Daten zu Sekundärzwecken, die nicht mit dem Ursprungs- oder dem nachträglich genehmigten Zweck vereinbar sind, durch eine Informationspflicht und die Möglichkeit eines Widerspruchs des Betroffenen beschränkt. Da die Zulässigkeit der Verarbeitung in den USA jedoch insgesamt keiner Zweckbegrenzung im Sinne des Artikels 7 der Richtlinie unterliegt und das Merkmal der bloßen Vereinbarkeit mit dem Ursprungszweck einer relativ weiten Auslegung zugänglich ist, scheint die Hürde zu einer Verwendungsfreigabe, die

[522] Gemäß der vom US-Handelsministerium verfassten englischen Originalversion des *Anhangs I* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 11. Die deutsche Übersetzung erweckt den Eindruck, als sei nur die (erste) Abweichung von dem Erhebungszweck widerspruchsfähig.

[523] *WP 19*, S. 7; so bereits in *WP 15*, S. 4, und *WP 27*, S. 8; Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 73; *ders.*, CR 2000, S. 472, S. 476; *ders.* in: Sokol, S. 5, S. 37, der generell und insbesondere im Hinblick auf die „Safe Harbor"-Verhandlungen bemängelt, dass die Einwilligung zur Aushebelung der Datenschutzgrundsätze, vor allem der Zweckbindung benutzt werde; *Räther/Seitz*, MMR 2002, S. 425, S. 430; *Verbiest/Wéry*, Rn. 899.

bereits durch ein unreflektiertes Schweigen des Betroffenen ausgelöst zu werden vermag, und somit unter Umständen auch zu einer Umgehung der mitgliedstaatlichen Datenschutzgesetze recht niedrig angesiedelt.

Insbesondere vor dem Hintergrund, dass die Zweckbindung als eines der Kernprinzipien des Datenschutzes erachtet wird,[524] rechtfertigt sich die Annahme eines angemessenen Schutzniveaus daher allenfalls noch aus dem Umstand, dass die Verarbeitung der Daten entsprechend dem Wortlaut der Wahlmöglichkeit grundsätzlich nur zu einem bestimmten Zweck erfolgen darf. Auf diese Weise verbietet sich zumindest die Speicherung der personenbezogenen Informationen in Datenbanken auf Vorrat für zukünftige, noch nicht festgelegte Zwecke.[525]

Letzteres bestätigt auch die *FAQ 12*, der gemäß der Grundsatz der Wahlmöglichkeit gewährleisten solle, dass personenbezogene Daten in einer Weise genutzt und weitergegeben würden, die mit den Erwartungen und Entscheidungen des Betroffenen und sonach mit den diesem bekannten Zwecken übereinstimmten.

Unter der Berücksichtigung dieser Prämisse räumt die FAQ 12 der verarbeitenden Stelle einen gewissen Spielraum zur Regulierung der Ausübung des Widerspruchsrechts ein. Eine angemessene Präklusionsfrist für den grundsätzlich unbefristet möglichen Widerspruch sei zum Beispiel legitim, sofern sich dies zur effektiven Berücksichtigung des Widerspruchs als notwendig erweise. Außerdem darf die verarbeitende Stelle Informationen anfordern, um die Identität der widersprechenden Person zu bestätigen. Dieses Prozedere mag zwar auf den ersten Blick einem „leicht zugängliche(n) (...) Verfahren“ entgegenstehen, erscheint jedoch im Hinblick auf die Feststellung der Widerspruchsberechtigung auch im Interesse des Betroffenen geboten.

Darüber hinaus erweckt die FAQ 12 den Eindruck, als denke das US-Handelsministerium bei der Verarbeitung zu Sekundärzwecken in erster Linie an das Direktmarketing, da lediglich in diesem Zusammenhang auf die Ausübung des Widerspruchsrechts eingegangen wird. Die Formulierungen fokussieren jedoch zu sehr den Einzelfall, um daraus eine Limitierung zulässiger Sekundärzwecke herzuleiten oder gar auf eine

[524] Vgl. dazu Gliederungspunkt C.II.1.a. dieses Kapitels.
[525] So sind etwa zu nicht näher konkretisierten Zwecken eingerichtete Data Warehouses verboten, in denen mithilfe des Data Mining nach noch nicht erkannten Zusammenhängen zwischen einzelnen personenbezogenen Informationen geforscht werden kann.

Beschränkung des Widerspruchsrechts auf den Zweck des Direktmarketings zu schließen. So könne sich die verarbeitende Stelle beispielsweise einem in den USA recht üblichen zentralen Widerspruchsprogramm anschließen, bei dem sich Verbraucher eintragen lassen, die keine kommerzielle Werbung erhalten möchten. Ferner müsse sich der Betroffene erst gegen wiederholte Werbemaßnahmen wenden können, falls der verarbeitenden Stelle die Einräumung des Widerspruchsrechts vor einer ersten Direktwerbung unmöglich sei.

Letzteres widerspricht eindeutig dem Artikel 14b) der Richtlinie, gemäß dem der Betroffene unbedingt vor einer ersten Direktwerbung informiert werden soll. Im Übrigen ist diese Ausnahme auch insofern interessant, als dass die Voraussetzungen jener Unmöglichkeit nicht näher definiert werden. Dem Einfallsreichtum der verarbeitenden Stelle sind daher kaum Grenzen gesetzt, um wenigstens einmal auf sich aufmerksam zu machen.[526] Eine unangemessene Beeinträchtigung der Privatsphäre des Betroffenen ist davon jedoch nicht zu erwarten, sodass diese Ausnahme die Beurteilung des Schutzniveaus insgesamt nicht allzu sehr beeinflussen sollte.

Mit den Modalitäten der Wahlmöglichkeit bei der Verarbeitung von Personaldaten, die im Rahmen eines Beschäftigungsverhältnisses in der Europäischen Union erhoben und anschließend in die USA übermittelt werden, beschäftigt sich schließlich die *FAQ 9*.

So dürfen dem Betroffenen gemäß der FAQ 9, Frage/Antwort 2 (F/A 2), aus der Ausübung seines Widerspruchs- beziehungsweise Zustimmungsverweigerungsrechts keine beruflichen Nachteile erwachsen oder Sanktionen drohen. Ferner besteht eine absolute Bindung an den Übermittlungszweck, sofern der Mitgliedstaat, aus dem die Daten übermittelt wurden, mittels einer abstrakt-generellen Regelung die Nutzung von Personaldaten zu Sekundärzwecken ausgeschlossen hat. Damit ist eine Zweckbindung wenigstens im Arbeitnehmerdatenschutz jedenfalls partiell gewährleistet. Darüber hinaus hält die F/A 2 die verarbeitende Stelle allgemein dazu an, möglichst weit auf die Datenschutzbedürfnisse des Arbeitnehmers einzugehen. Falls es der konkrete Verarbeitungszweck zulasse, solle beispielsweise auf Wunsch der Zugriff auf bestimmte Daten limitiert sowie eine Anonymisierung oder Pseudonymisierung der Daten veranlasst werden.

[526] Vgl. auch *Räther/Seitz*, MMR 2002, S. 425, S. 430, die prognostizieren, dass diese Ausnahme in der Praxis den Regelfall bilden werde.

Demgegenüber ist eine Befreiung der verarbeitenden Stelle sowohl von der Wahlmöglichkeit als auch von der Informationspflicht vorgesehen, sofern und soweit sich dies im Zusammenhang mit Beförderungen, Ernennungen und ähnlichen Personalentscheidungen zur Wahrung der legitimen Interessen der verarbeitenden Stelle als erforderlich erweist. Diese Ausnahme steht in Einklang mit Artikel 13 Absatz 1g) der Richtlinie und beeinträchtigt das von den Safe Harbor Privacy Principles gewährleistete Schutzniveau daher in keiner unangemessenen Weise.

(3) Onward Transfer - Weitergabe

Der Grundsatz der Weitergabe bekräftigt, dass eine Übermittlung der Daten durch den US-amerikanischen Datenverarbeiter an weitere Dritte die Einhaltung der Grundsätze der Informationspflicht und der Wahlmöglichkeit voraussetzt.[527] Darüber hinaus unterliegt die Weitergabe jedoch keinen weiteren Beschränkungen. Die verarbeitende Stelle darf also die personenbezogenen Daten des Betroffenen sowohl in unsichere Drittländer weitergeben als auch an solche Dritte in den USA, die selbst nicht über ein angemessenes Schutzniveau verfügen.

Zwar entspricht die „opt-in"-Wahlmöglichkeit für die Übermittlung sensibler Daten der Ausnahme einer Einwilligung des Betroffenen im Sinne des Artikels 26 Absatz 1a) der Richtlinie. Die bloße Widerspruchsmöglichkeit in allen übrigen Fällen, die über die Ausnahmetatbestände des Artikels 26 der Richtlinie hinausgehen, vermag jedoch kaum der herausragenden Bedeutung[528] der Beschränkung einer Weitergabe an Dritte für die Undurchlässigkeit[529] des europäischen Datenschutzsystems Rechnung zu tragen.[530] Diese Aufweichung der Drittländerregelung steht eindeutig der Angemessenheit des von den Safe Harbor Privacy Principles gewährleisteten Schutzniveaus entgegen.[531]

---

[527] Ein Missverständnis liegt daher bei *Schaar*, Datenschutz im Internet, Rn. 877, vor, der meint, dass die Zulässigkeit der Weitergabe die Beachtung der Grundsätze der Informationspflicht und der Wahlmöglichkeit durch den Datenempfänger voraussetze.

[528] Dazu Gliederungspunkt C.II.1.a. dieses Kapitels.

[529] *Begründung des Rates zum gemeinsamen Standpunkt*, ABl. EG Nr. C 93 vom 13.4.1995, S. 19, S. 20.

[530] Erstaunlicherweise ist der Grundsatz der Weiterübermittlung in der Entscheidung der Europäischen Kommission hinsichtlich Standardvertragsklauseln identisch gestaltet (*Entscheidung der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (2001/497/EG)*, ABl. EG Nr. L 181 vom 4.7.2001, S. 19, S. 30 und S. 31 (Anlagen 2 und 3)). Dagegen wendet sich allerdings auch das *WP 38*, S. 5.

[531] Wohl auch *WP 32*, S. 7, das sich allerdings noch auf den Entwurf der Safe Harbor Privacy Principles vom 28.4.2000 bezieht, in dem offensichtlich noch alternativ zur Ausübung der Wahlmöglichkeit u. a. eine vertragliche Verpflichtung des Dritten gegenüber der verarbeiten-

Für die Datenübermittlung an Dritte im Rahmen eines Auftragsverhältnisses sieht der Grundsatz der Weitergabe sogar eine Ausnahme von den Grundsätzen der Informationspflicht und der Wahlmöglichkeit vor, da die Daten hier nicht den Einflussbereich der weitergebenden Stelle verlassen. Allerdings setzt eine derartige Übermittlung voraus, dass der Auftragnehmer entweder selbst dem „sicheren Hafen“ angehört, den Schutzbestimmungen der Richtlinie unterliegt, von einer anderen Feststellung über ein angemessenes Schutzniveau erfasst ist oder sich vertraglich zur Einhaltung mindestens der Grundsätze des „sicheren Hafens“ gegenüber der weitergebenden Stelle verpflichtet hat. Auf diese Weise wird die verantwortliche Stelle daran gehindert, sich der Geltung der Safe Harbor Privacy Principles zu entziehen, indem sie die Verarbeitung der geschützten Daten an eine andere Stelle delegiert.

Die Effektivität dieses Umgehungshindernisses wird jedoch zum einen dadurch relativiert, dass eine vertragliche Vereinbarung mit dem Auftragsverarbeiter eigentlich nur dann eine ausreichende Garantie darstellt, sofern die ihr zugrunde liegende Übermittlung gemäß dem Artikel 26 Absatz 2 der Richtlinie genehmigt wurde.[532] Zum anderen ist zu bemängeln, dass die weitergebende Stelle lediglich für solche Verstöße des Auftragnehmers haften soll, von denen sie wusste oder wissen konnte und dennoch keine geeigneten Gegenmaßnahmen getroffen hat. Im Gegensatz zu Artikel 23 Absatz 1 der Richtlinie, der eine Gefährdungshaftung zulasten der verantwortlichen Stelle vorsieht, obliegt dem Betroffenen daher mangels Beweislastumkehr auch nach dem hier geltenden US-Recht[533] der oftmals kaum zu erbringende Nachweis des gegnerischen Verschuldens.

(4) Security - Sicherheit

---

den Stelle auf die Grundsätze des „sicheren Hafens“ vorgesehen war (so jedenfalls noch im Entwurf vom 17.3.2000, abrufbar unter: www.export.gov/safeharbor/sh_historicaldocuments.html).

[532] Vgl. dazu Gliederungspunkt C.II.2.b.(4).(a). dieses Kapitels.

[533] Vgl. dazu die Federal Rules Of Evidence, Art. III. Rule 301. Presumptions in General Civil Actions and Proceedings: „In all civil actions and proceedings not otherwise provided for by Act of Congress or by these rules, a presumption imposes on the party against whom it is directed the burden of going forward with evidence to rebut or meet the presumption, but does not shift to such party the burden of proof in the sense of the risk of nonpersuasion, which remains throughout the trial upon the party on whom it was originally cast.“ Die jeweiligen Vorschriften der einzelnen Bundesstaaten entsprechen diesem Grundsatz der Federal Rules Of Evidence (vgl. http://www.law.cornell.edu/rules/fre/overview.html).

Entsprechend dem Grundsatz der Sicherheit muss der US-amerikanische Datenempfänger angemessene Maßnahmen treffen, um die Daten vor Verlust, Missbrauch, Zerstörung sowie vor unbefugten Zugriffen, Weitergaben und Änderungen zu schützen. Die Bestimmung entspricht inhaltlich den Voraussetzungen des Artikels 17 Absatz 1 der Richtlinie über die Datensicherheit und ist daher unproblematisch.

(5) Data Integrity - Datenintegrität

Der Grundsatz der Datenintegrität gewährleistet eine mit den von der Art. 29-Gruppe aufgestellten Voraussetzungen eines angemessenen Schutzniveaus konforme Datenpflege. Zum einen müssen die Daten in Übereinstimmung mit dem Zweckbindungsgrundsatz für den beabsichtigten Verwendungszweck erheblich sein. Zum anderen hat die verarbeitende Stelle zu gewährleisten, dass die Informationen hinreichend zuverlässig, genau, vollständig und aktuell sind.

(6) Access - Auskunftsrecht

Das Auskunftsrecht gewährt dem Betroffenen einen Anspruch auf Zugang, Berichtigung und Löschung der Daten. Die verarbeitende Stelle muss jedoch nicht erfüllen, sofern dadurch entweder die Rechte anderer Personen verletzt würden oder die Belastung und die Kosten für die Gewährung des Zugangs in dem konkreten Fall in einem Missverhältnis zu den sich aus der Verweigerung der Auskunft ergebenden Nachteilen für den Betroffenen stünden.

Diese letzte Ausnahme geht im Grunde über die von Artikel 13 der Richtlinie genannten Ausnahmen zum Auskunftsanspruch des Artikels 12 der Richtlinie und den seitens der Art. 29-Gruppe aufgestellten, für ein angemessenes Schutzniveau wesentlichen Zugangserfordernissen hinaus.[534] Selbst der Artikel 13 Absatz 1g) der Richtlinie, der notwendige Beschränkungen zugunsten der Rechte und Freiheiten anderer Personen und somit auch der verarbeitenden Stelle vorsieht,[535] wird überdehnt, sofern gemäß der *FAQ 8* bereits ein unverhältnismäßiger Ar-

[534] Vgl. auch *Räther/Seitz*, MMR 2002, S. 425, S. 430, die das Auskunftsrecht dadurch erheblich eingeschränkt sehen; allerdings schlägt das *WP 19*, S. 9, diese Formulierung mit Blick auf die offenbar für die Festlegung der inhaltlichen Grundsätze als Diskussionsgrundlage gewählten OECD-Leitlinien (*WP 27*, S. 3, und bereits in *WP 15*, S. 4) selbst vor; vgl. auch *Brühann*, DuD 1998, S. 700, S. 701, der ebenfalls die OECD-Leitlinien als Verhandlungsbasis der inhaltlichen Grundsätze betrachtet.

[535] *Gounalakis/Mand*, CR 1997, S. 497, S. 498; *Weber*, DuD 1995, S. 658, S. 702.

beitsaufwand sogar eine vollständige Auskunftsverweigerung zu rechtfertigen vermag.

Augenscheinlich eröffnet das Erfordernis der Verhältnismäßigkeit und Zumutbarkeit der Belastung mit einem Auskunftsanspruch außerdem ein breites Spektrum an Umgehungsmöglichkeiten des Zugangsrechts. Zu besorgen könnte etwa ein Missbrauch dergestalt sein, dass die verarbeitende Stelle sich nicht nur bei einer tatsächlichen Unverhältnismäßigkeit auf ihr Verweigerungsrecht beruft, sondern durch eine komplizierte interne Kompetenzverteilung und die Einrichtung eines mehrstufigen Entscheidungsverfahrens eine regelmäßig unzumutbare Situation absichtlich herbeiführt.

Indessen stellt jedoch die F/A 1 der FAQ 8 ausdrücklich klar, dass ein Auskunftsrecht wegen „seines grundlegenden Charakters“ nicht „ohne Not“ beschränkt werden dürfe. Das belegen auch die in der FAQ 8 aufgeführten Beispielsfälle, gemäß denen es in der Praxis, insbesondere unter der Berücksichtigung der schnellen und kostengünstigen Verfügbarkeit von Daten im Rahmen der elektronischen Datenverarbeitung und des Unternehmensinteresses, den jederzeitigen Zugriff auf die Daten zur Erfüllung der eigenen Verarbeitungszwecke zu gewährleisten,[536] so gut wie nie zu einer tatsächlichen Unverhältnismäßigkeit der Erfüllung des Auskunftsbegehrens kommen dürfte.

So muss gemäß der F/A 1 die Auskunft stets erteilt werden, sofern die personenbezogenen Daten leicht zugänglich sind und kostengünstig zur Verfügung gestellt werden können. Ferner ist der verarbeitenden Stelle ein hoher Kosten- oder Arbeitsaufwand regelmäßig zumutbar, falls die Daten als sensibel eingestuft sind und/oder die Grundlage für eine Entscheidung von großer Tragweite[537] für den Betroffenen bilden.

Hinderlich soll zudem in der Regel nicht sein, dass die angeforderten Daten mit anderen, besonders schutzbedürftigen Informationen, zum Beispiel vertraulichen Geschäftsdaten im Sinne der F/A 2, untrennbar verbunden sind. Nur sofern und soweit letztere bei der Offenlegung nicht unkenntlich gemacht werden könnten, rechtfertige sich eine damit begründete Auskunftsverweigerung.

[536] *Räther/Seitz*, MMR 2002, S. 425, S. 430.
[537] Z. B. eine Entscheidung über einen Arbeitsplatz oder eine Kreditvergabe.

Aus Kostengründen darf die verarbeitende Stelle den Anspruch gemäß der F/A 6 nicht abweisen, sofern der Betroffene die Ausgaben für die Offenlegung der Daten zu übernehmen bereit ist.

Darüber hinaus trägt die F/A 1 der verarbeitenden Stelle auf, die Erfüllung eines inhaltlich zu unspezifischen Auskunftsbegehrens dadurch zu ermöglichen, dass sie den Hintergrund des Antrags erforscht, „um die Gründe für die Anfrage besser zu verstehen und die gewünschten Daten zu ermitteln."

Schließlich darf sich der US-amerikanische Verarbeiter entsprechend der *FAQ 9* (F/A 3) nicht auf einen unverhältnismäßig hohen Aufwand berufen, sofern er Personaldaten aus der Europäischen Union in den USA verarbeitet und der europäische Arbeitgeber kraft Gesetzes dazu verpflichtet ist, den Zugang zu diesen Daten zu gewährleisten.

Zu diesen die Ausnahme der Unverhältnismäßigkeit und Unzumutbarkeit erheblich einschränkenden Vorwegnahmen des Abwägungsergebnisses zugunsten eines Auskunftsrechts des Betroffenen kommt hinzu, dass die verarbeitende Stelle eine Auskunftsverweigerung gemäß der F/A 5 der FAQ 8 konkret begründen muss und dem Betroffenen eine Kontaktstelle für weitere Fragen zu nennen hat. Nicht zuletzt wegen dieses bürokratischen Aufwandes und erst recht aufgrund der von der verarbeitenden Stelle zu tragenden Beweislast für das Vorliegen einer Ausnahme sollte eigentlich kein ernst zu nehmender Anreiz zu einer Ausnutzung oder zu einem Missbrauch des Auskunftsverweigerungsrechts existieren.

Bei der Formulierung des Auskunftsgrundsatzes fällt des Weiteren auf, dass dem Betroffenen nur dann ein Recht auf Löschung zusteht, wenn seine Daten falsch sind, nicht aber, sofern sie in einer gegen die Safe Harbor Privacy Principles verstoßenden Art und Weise verarbeitet werden. Obgleich während der Verhandlungen über die Safe Harbor Privacy Principles mehrfach auf diesen Mangel hingewiesen wurde,[538] dürfen bis heute nur die Beschwerdestelle gemäß der FAQ 11 beziehungsweise das europäische Data Protection Panel im Rahmen der FAQ 5 eine derartige Löschung verlangen.

Von diesen Abweichungen abgesehen weist die Gestaltung des Auskunftsanspruchs im Verhältnis zu der Richtlinie 95/46/EG keine weite-

[538] *WP 32*, S. 6; so bereits in *WP 19*, S. 9, *WP 23*, S. 4, und *WP 27*, S. 9.

ren Besonderheiten auf. Während die F/A 5 der FAQ 8 weitere, mit den Tatbeständen des Artikels 13 der Richtlinie grundsätzlich korrespondierende Ausnahmen zum Auskunftsrecht aufzählt, erläutern die F/A 9, 10 und 11 der FAQ 8 in Übereinstimmung mit Artikel 12a) der Richtlinie, dass die verarbeitende Stelle dem Betroffenen die gewünschten Auskünfte in angemessenen Abständen sowie ohne übermäßige Verzögerung innerhalb einer angemessenen Frist zu erteilen hat. Um einer Auskunftserschleichung vorzubeugen, kann auch hier der zweifelsfreie Nachweis der Identität des Betroffenen verlangt werden. Ferner darf die verarbeitende Stelle gemäß der F/A 6 in Einklang mit Artikel 12a) der Richtlinie eine Gebühr für die Erteilung der Auskunft erheben.

(7) Enforcement - Durchsetzung

Der Grundsatz der Durchsetzung schreibt in Übereinstimmung mit den von der Art. 29-Gruppe in der Arbeitsunterlage WP 12[539] entwickelten Voraussetzungen eines angemessenen Selbstregulierungsmechanismus vor,[540] dass der US-amerikanische Datenempfänger Verfahren schaffen muss, welche die Einhaltung der Safe Harbor Privacy Principles gewährleisten, Behelfe für den Betroffenen vorsehen sowie der verarbeitenden Stelle Sanktionen androhen.

Die Effektivität der von den Safe Harbor Privacy Principles zur Umsetzung dieses Grundsatzes vorgesehenen Instrumente wird allerdings überwiegend angezweifelt.

[539] *WP 12*, S. 12 ff.; so bereits in *WP 7*, S. 3 ff.
[540] Vgl. dazu Gliederungspunkt C.II.2.b.(2).(b). dieses Kapitels.

(a) Die Gestaltung des Durchsetzungsmechanismus

Der Durchsetzungsmechanismus muss sich gemäß den Safe Harbor Privacy Principles mindestens auszeichnen durch

a) leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren, nach denen die Beschwerden der Betroffenen behandelt werden und nach denen Schadensersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen,
b) Kontrollmaßnahmen zur Prüfung, ob die Bescheinigungen und Behauptungen der verarbeitenden Stelle über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden,
c) Verpflichtungen zum Beheben von Problemen, die daraus resultieren, dass die verarbeitende Stelle sich entgegen ihrer eigenen Erklärung nicht an die Grundsätze des „sicheren Hafens“ gehalten hat, sowie die Androhung hinreichend strenger Sanktionen, welche die Befolgung der Grundsätze sicherstellen.

Mit der Umsetzung der Verpflichtungen aus a) und c) befassen sich die *FAQ 11* und die *FAQ 5*, während sich die *FAQ 7* mit den internen Kontrollmaßnahmen gemäß dem Buchstaben b) beschäftigt.

aa. Die Zusammenarbeit mit einer unabhängigen Beschwerdestelle

Den Anforderungen aus a) und c) kommt die verarbeitende Stelle nach, indem sie mit einer unabhängigen Beschwerdestelle zusammenarbeitet.

(I). Dazu kann sie sich beispielsweise gemäß der *FAQ 11* einem von einer unabhängigen privaten Selbstregulierungsstelle entwickelten und durchgeführten Datenschutzprogramm anschließen, in das die Safe Harbor Privacy Principles einschließlich des darin vorgesehenen Durchsetzungsmechanismus integriert sind.[541]

Die tatsächliche Übereinstimmung des offerierten Programms mit den Anforderungen der Safe Harbor Privacy Principles hat die verarbeitende Stelle allerdings in eigener Verantwortung zu verifizieren. Dabei

[541] Als Beispiele nennt das *US-Handelsministerium* auf seiner Website BBBOnLine, TRUSTe, AICPA, WebTrust, die Direct Marketing Association, das Entertainment Software Rating Board, JAMS und die American Arbitration Association (AAA) (http://www.export.gov/safeharbor/helpful_hints.html).

vermag sie zum Beispiel die erforderliche Unabhängigkeit des Selbstregulierungsorgans an dessen transparenter Besetzung und Finanzierung sowie an dessen nachweisbarer einschlägiger Erfahrung zu erkennen.

Behauptet ein privates Selbstregulierungsorgan zu Unrecht, dass es über ein Programm im Sinne des Durchsetzungsgrundsatzes der Safe Harbor Privacy Principles verfüge, kann diese falsche Darstellung im Übrigen gemäß dem Abschnitt 5 des FTC Act geahndet werden.[542]

Das Beschwerdeverfahren des Selbstregulierungsorgans muss für den Betroffenen einfach zugänglich, finanziell erschwinglich und mithilfe umfassender, leicht erhältlicher Informationen über seinen Ablauf gut zu überblicken sein.

Abgesehen von einer offensichtlichen Unbegründetheit oder einer fehlenden Ernsthaftigkeit des Anliegens hat die Selbstregulierungsstelle jeder von einer Einzelperson vorgetragenen Rüge nachzugehen. Sie darf den Zugang zu dem Verfahren allerdings durch die Formulierung von Zulässigkeitsvoraussetzungen begrenzen, die sich jedoch als transparent und berechtigt erweisen müssen und nicht zu einer Lockerung der grundsätzlich bestehenden Pflicht zu einer Prüfung aller berechtigten Beschwerden führen dürfen.

Die von der Selbstregulierungsstelle für den Fall eines Verstoßes gegen die Safe Harbor Privacy Principles angekündigten Maßnahmen sollen darauf gerichtet sein, dass die verarbeitende Stelle die Auswirkungen des Verstoßes so weit wie möglich korrigiert oder rückgängig macht, bei ihren zukünftigen Verarbeitungen die Grundsätze beachtet und, soweit erforderlich, die Verarbeitung der Daten des Beschwerdeführers vollständig einstellt.

Des Weiteren müssen zur Ahndung einer Verletzung der Principles ausreichend strenge Strafsanktionen in Aussicht gestellt werden, um eine gute Befolgungsrate zu gewährleisten. In Betracht kommen je nach Schwere des Verstoßes zum Beispiel dessen öffentliche Bekanntmachung, die Anordnung einer Datenlöschung, Untersagungsanordnun-

[542] Vgl. *Anhang V* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 43.

gen[543] sowie der vorübergehende oder dauernde Ausschluss von der Zuständigkeit der Selbstregulierungsstelle.

Ferner hat das Datenschutzprogramm der Selbstregulierungsstelle die Möglichkeit einer Anordnung von angemessenen Entschädigungen zugunsten all jener Personen vorzusehen, denen aus dem jeweiligen Verstoß ein Schaden entstanden ist.

Missachtet die verarbeitende Stelle den Erlass einer solchen Maßnahme, ist die Selbstregulierungsstelle dazu verpflichtet[544], entweder die Gerichte anzurufen oder die FTC beziehungsweise das US-Verkehrsministerium zu unterrichten. Ferner hat sie das US-Handelsministerium im Hinblick auf die Korrektur der „Safe Harbor"-Liste zu benachrichtigen.

(II). Alternativ zu einer Teilnahme an einem derartigen Selbstregulierungsprogramm kann sich die verarbeitende Stelle zur Erfüllung der Durchsetzungsgrundsätze aus a) und c) zu einer Kooperation mit den Datenschutzbehörden in der Europäischen Union entschließen. Gemäß der *FAQ 5* wird diese Aufgabe nicht direkt von den einzelnen mitgliedstaatlichen Datenschutzbehörden wahrgenommen, sondern im Interesse einer einheitlichen Entscheidungspraxis von einem informellen, aus ihren Vertretern zusammengesetzten Gremium, dem Data Protection Panel,[545] durchgeführt.

Die Zusammenarbeit mit dem europäischen Panel zeichnet sich durch Information und Beratung aus, indem das Panel die verarbeitende Stelle bei der Behandlung ungeklärter Beschwerden von Einzelpersonen über den Umgang mit personenbezogenen Daten gegen Entrichtung einer Jahresgebühr anleitet. Um die Effektivität der Kooperation zu garantieren, muss die verarbeitende Stelle zuvor ausdrücklich ihre Bereitschaft anzeigen, sich an die Empfehlungen des Panels zu halten und ihm deren jeweilige Umsetzung schriftlich zu bestätigen.

---

[543] Vgl. dazu die vom US-Handelsministerium verfasste englische Originalversion des *Anhangs II* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 22 (FAQ 11).
[544] Das übersehen *Räther/Seitz*, MMR 2002, S. 425, S. 430, die eine unsichere Abstimmung zwischen den Selbstregulierungsstellen und der FTC monieren. Der vorletzte Entwurf der FAQ sah tatsächlich noch vor, dass die Selbstregulierungsstellen die FTC nur informieren „sollen". Die endgültige Version spricht jedoch von „müssen".
[545] SECUREIDA: Data Protection Panel: http://forum.europa.eu.int/Public/irc/secureida/safeharbor/home.

Die Einleitung eines derartigen Beratungsverfahrens erfolgt entweder durch eine Anfrage der verarbeitenden Stelle oder aufgrund einer unmittelbaren Beschwerde eines Betroffenen. Beiden Parteien soll vor der Erteilung der Empfehlung eine hinreichende Gelegenheit zur Stellungnahme und zu einer Vorlage von Beweisen gegeben werden, wobei für die Auslegung der Safe Harbor Privacy Principles ausnahmsweise nicht das US-Recht gilt[546].

Falls das Panel im Ergebnis tatsächlich einen Verstoß gegen die Safe Harbor Privacy Principles feststellt, darf es angemessene Abhilfemaßnahmen und Schadenskompensationen anregen und insbesondere auch eine Entschädigungszahlung an den Betroffenen anordnen.[547]

Kommt der US-amerikanische Datenverarbeiter einer Empfehlung des Panels nicht binnen einer Frist von 25 Tagen nach und liefert er auch keine befriedigende Erklärung für die Verspätung, wird das Panel ihn entweder darauf hinweisen, dass es die Angelegenheit an die FTC beziehungsweise das US-Verkehrsministerium weiterleiten wird, oder dass es zu dem Schluss gelangt ist, dass der Kooperationsvertrag mit dem Panel gebrochen wurde und daher für hinfällig erklärt werden müsse. In dem letzteren Fall informiert das Panel zudem das US-Handelsministerium über seine Feststellung, um eine Änderung der „Safe Harbor"-Liste herbeizuführen.

Die Option zu einer Regulierung des Datenschutzes über das europäische Panel erfährt ausweislich der „Safe Harbor"-Liste in der Praxis großen Zuspruch.[548] Bestätigt werden kann daher nicht die zunächst nahe liegende Vermutung, dass sich die meisten US-Unternehmen nicht auf eine Kooperation mit europäischen Behörden einlassen würden.

Die Freiwilligkeit dieser augenscheinlichen Kooperationsbereitschaft sollte allerdings auch nicht überbewertet werden angesichts der Ver-

---

[546] *Anhang I* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 11.

[547] So die vom US-Handelsministerium verfasste englische Originalversion des *Anhangs II* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 14 (FAQ 5). Gemäß der irreführenden deutschen Übersetzung soll das Panel der verarbeitenden Stelle zu „Rechtsmitteln" für den Betroffenen raten können.

[548] Vgl. dazu die entsprechenden Einträge in der „Safe Harbor"-Liste, abrufbar unter: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list. Im November 2003 hatten 73 % der „Safe Harbor"-Unternehmen eine Zusammenarbeit mit dem Panel zertifiziert (Quelle: *Europäische Kommission*, Commission Staff Working Document vom 20.10.2004, The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC (2004) 1323, S. 11).

pflichtung zu einer Zusammenarbeit entweder mit einer mitgliedstaatlichen Datenschutzbehörde oder, sofern diese einer Kooperation nicht zustimmt, mit dem europäischen Panel, um sich für den „sicheren Hafen“ hinsichtlich des Empfangs von Personaldaten zu qualifizieren, die im Rahmen eines in der Europäischen Union bestehenden Beschäftigungsverhältnisses des Betroffenen in die USA übermittelt werden[549]. Da für ein solches Arbeitsverhältnis stets insgesamt das Recht desjenigen Mitgliedstaates anwendbar bleibt, in dem der betroffene Arbeitnehmer beschäftigt ist, soll sich letzterer nämlich gemäß der *FAQ 9* (F/A 4), sofern er mit dem Ergebnis einer Beschwerde gegen den US-amerikanischen Datenverarbeiter vor einer gemäß den Safe Harbor Privacy Principles eingerichteten internen oder externen Kontrollinstanz nicht zufrieden ist, im Interesse eines reibungslosen Zusammenspiels der sich überschneidenden Bestimmungen des Arbeitsrechts, der Tarifverträge und des Datenschutzrechts an die jeweils zuständigen Behörden in der Europäischen Union wenden.

(III). Eine dritte Variante zur Erfüllung der Durchsetzungsgrundsätze aus a) und c) ergibt sich gemäß der FAQ 11 schließlich aus der Möglichkeit, sich einem gesetzlich oder durch Rechtsverordnung vorgesehenen Kontrollorgan zu unterwerfen, das Beschwerden von Einzelpersonen nachgeht und Streitigkeiten schlichtet.

Bislang ist allerdings nicht ersichtlich, dass einem gesetzlich legitimierten Kontrollorgan diese Aufgabe übertragen wurde. Einen Hinweis auf eine derartige staatliche Einrichtung liefern im Unterschied zu den ausführlichen Angaben über die bereits vorgestellten Alternativen jedenfalls weder die FAQ noch die Website des US-Handelsministeriums[550], die US-amerikanische Unternehmen bei der Umsetzung der Safe Harbor Privacy Principles ausführlich anleitet.

(IV). Die vorstehend wiedergegebene Aufzählung der unabhängigen Kontrollstellen versteht sich gemäß der FAQ 11 zwar nicht als abschließend. Eine weitere Regulierungsform im Sinne der Buchstaben a) und c) zur Gewährleistung einer effektiven Durchsetzung der Safe Harbor Privacy Principles scheint jedoch derzeit nicht vorstellbar.

---

[549] *Anhang II* der „Safe Harbor“-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 15 (FAQ 6).

[550] http://www.export.gov/safeharbor/helpful_hints.html und http://www.export.gov/safeharbor/sh_workbook.html.

bb. Die internen Kontrollmaßnahmen

Die *FAQ 7* gibt der verarbeitenden Stelle Auskunft darüber, wie sie die tatsächliche Umsetzung ihrer eigenen Datenschutzpolitik im Sinne des Buchstabens b) überprüfen soll. Danach können die internen Strukturen sowohl durch eine eigene, von der verarbeitenden Stelle selbst vorgenommene Bewertung als auch mittels einer externen Begutachtung durch einen Dritten kontrolliert werden.

Das jeweils gewählte Kontrollverfahren sollte mindestens einmal im Jahr stattfinden und durch eine von einem leitenden Angestellten oder einem Bevollmächtigten der verarbeitenden Stelle unterschriebene Durchführungserklärung dokumentiert werden, für die im Falle einer externen Kontrolle zusätzlich die jeweilige Prüfungsstelle zeichnungsberechtigt ist. Diese Erklärung soll auf Verlangen des Betroffenen sowie im Rahmen einer Untersuchung oder einer Beschwerde zur Verfügung stehen.

Eine von der verarbeitenden Stelle selbst durchgeführte Kontrolle richtet sich nach einer relativ ausführlichen Auflistung einzelner Indikatoren für eine tatsächliche und effektive Umsetzung der Safe Harbor Privacy Principles. Kann die verarbeitende Stelle alle genannten Voraussetzungen bei sich feststellen, darf sie von einer effektiven Gewährleistung eines Datenschutzes im Sinne der Safe Harbor Privacy Principles in ihrem Verantwortungsbereich ausgehen.

Im Einzelnen hat das Ergebnis einer internen Untersuchung darauf hinzudeuten, dass die von der verarbeitenden Stelle veröffentlichten Datenschutzbedingungen sachgerecht, umfassend, an auffälliger Stelle bekannt gemacht, vollständig umgesetzt und für jedermann zugänglich sind. Ferner muss sich ergeben, dass die Bestimmungen tatsächlich den Safe Harbor Privacy Principles entsprechen, dass die Mitarbeiter der verarbeitenden Stelle zur Umsetzung der Datenschutzregeln und hinsichtlich der Verfolgung von Verstößen geschult werden, dass die Betroffenen über interne Beschwerdeverfahren oder solche bei unabhängigen Schiedsstellen informiert sind und dass interne Verfahren zu einer regelmäßigen sowie objektiven Überprüfung der Befolgung der Datenschutzvorschriften existieren.

Ihre Aufzeichnungen über diese Kontrollen soll die verarbeitende Stelle für etwaige Beschwerdeverfahren oder Untersuchungen von Verstößen gegen die Datenschutzbestimmungen aufbewahren.

Eine externe Kontrolle ist dagegen nicht an detailliert vorgegebene Prüfungspunkte gebunden. Gemäß der FAQ 7 hat sie zwar nachzuweisen, dass die Datenschutzbedingungen der verarbeitenden Stelle den Safe Harbor Privacy Principles entsprechen, dass die Vorschriften eingehalten werden und dass die Betroffenen über die potentiellen Beschwerdewege informiert sind. Selbst überlassen ist dem externen Kontrollorgan indessen, auf welche Weise es seine Feststellungen treffen möchte. In Betracht kommen zum Beispiel Buchprüfungen, Zufallskontrollen, der Einsatz von Lockvögeln sowie die Inanspruchnahme jedweder technischer Hilfsmittel.

Ausweislich der „Safe Harbor"-Liste[551] wird die Option zu einer externen Kontrolle in der Praxis nur sehr vereinzelt und in der Regel auch nur insoweit wahrgenommen, als dass neben einer Selbstkontrolle die eigenen Kunden unter bestimmten Umständen die Möglichkeit zu einem Audit erhalten. Den Ausschlag für diesen einheitlichen Trend zugunsten einer Selbstkontrolle mag einerseits ein mangelhaftes Angebot an Anbietern eines externen Kontrollverfahrens geben. Der entscheidende Grund dürfte aber wohl in dem Umstand zu suchen sein, dass die Unternehmen freiwillig nur ungern Einblick in ihre Interna gewähren.

Als Konsequenz wächst insbesondere bei internationalen Unternehmen im Hinblick auf die Gewährleistung einer regelmäßigen internen Überwachung des Datenschutzes die Popularität des Einsatzes eines so genannten „Data Security Officer" (DSO), dessen Betätigungsfeld bei der verarbeitenden Stelle den Funktionen des von der Richtlinie 95/46/EG vorgesehenen Datenschutzbeauftragten ähnelt.[552] Anders als dieser übt der DSO seine Rechte und Pflichten allerdings nicht in gesetzlich garantierter Unabhängigkeit aus, sodass seine bloße Existenz in einem Unternehmen nur wenig Auskunft über die tatsächliche Effektivität des internen Kontrollmechanismus zu geben imstande ist.

Obliegt dem DSO indessen die Datenschutzkoordination in einem Unternehmensteil eines in der Europäischen Union niedergelassenen Konzerns quasi weisungsgebunden als „verlängerter Arm" eines gemäß der Richtlinie 95/46/EG gesetzlich legitimierten Datenschutzbeauftragten, vermag er durchaus ein starkes Datenschutzbewusstsein und einen effektiven internen Kontrollmechanismus des Unternehmens zu indizieren.

[551] Abrufbar unter: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
[552] Vgl. Art. 18 Absatz 2, 2. Spiegelstrich, der Richtlinie.

cc. Die Rolle der FTC und des US-Verkehrsministeriums

Wenngleich die Umsetzung der Safe Harbor Privacy Principles in der Praxis weitestgehend im Rahmen der in den Buchstaben a) bis c) des Durchsetzungsgrundsatzes festgelegten Selbstregulierung erfolgen soll, kommt diesem Verfahren insgesamt jedoch nur eine ergänzende Funktion zu. Sowohl Verstöße gegen die Principles selbst als auch jeder Verstoß gegen die Kooperationsvereinbarung mit dem europäischen Data Protection Panel sind aufgrund der Zuwiderhandlung gegen die öffentlich verkündete eigene Datenschutzpolitik verfolgbar als unlautere und irreführende Geschäftspraktik im Sinne des Abschnittes 5 des FTC Act[553] beziehungsweise gemäß 49 U.S.C. 41712.

Stellt die FTC einen derartigen Verstoß fest, darf sie eine behördliche Anordnung zur Unterlassung der beanstandeten Praxis aussprechen oder vor einem Bezirksgericht klagen.[554] Gibt letzteres der Klage statt, kann sogar ein Bundesgericht eine Untersagung der unlauteren Geschäftspraktik verfügen.

Jeden Verstoß gegen die eigene behördliche Anordnung darf die FTC mit einer Geldstrafe bis zu einer Höhe von USD 10.000,- ahnden, wobei jeder Tag eines fortgesetzten Verstoßes einen weiteren Verstoß darstellt.[555] Die Missachtung der gerichtlichen Anordnung ermächtigt die FTC neben ihrer Befugnis zu einem zivilgerichtlichen Vorgehen sogar zur Einleitung strafgerichtlicher Schritte.

Hat die FTC bereits die Unterlassung einer unfairen und irreführenden Handlung angeordnet oder geht es in dem betreffenden Fall um eine weit verbreitete ebensolche Geschäftspraktik, ist die FTC zur Veröffentlichung einer entsprechenden Verwaltungsvorschrift ermächtigt.[556] Jeder vorsätzliche Verstoß gegen eine derartige Regelung wird ebenfalls mit jeweils einer Geldstrafe in Höhe von USD 10.000,- geahndet.[557] Die Durchsetzung dieser Sanktionen erfolgt entweder durch das US-Justizministerium oder durch die FTC selbst.[558]

---

[553] 15 U.S.C. § 41, et seq.
[554] 15 U.S.C. § 45 (b) und § 53 (b).
[555] Gemäß der aktuellen Fassung des 15 U.S.C. § 45 (l); vgl. aber den *Anhang III* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 26, der von USD 11.000,- spricht, im Gegensatz zu der Website des US-Handelsministeriums (www.export.gov/safeharbor/sh_overview.html), die sogar auf eine Strafe i. H. v. USD 12.000,- hinweist.
[556] 15 U.S.C. § 57a.
[557] 15 U.S.C. § 57a (d) (3) in Verbindung mit § 45.
[558] 15 U.S.C. § 56.

Bei einem bewussten Verstoß gegen eine Unterlassungsanordnung vermag die FTC außerdem vor Gericht Schadensersatz für geschädigte Verbraucher zu erwirken.[559]

Das US-Verkehrsministerium spricht aufgrund äquivalenter Verstöße von Luftverkehrsgesellschaften gemäß 49 U.S.C. 41712 Unterlassungsanordnungen aus, die zivilgerichtlichen Schritten offen stehen. Wiederholte Verletzungen des 49 U.S.C. 41712 können in gravierenden Fällen unter Umständen sogar zur Annahme des Fehlens der Betriebstauglichkeit und sonach zu dem Entzug der wirtschaftlichen Betriebsgenehmigung der Luftfahrtgesellschaft führen.[560] Im Gegensatz zu der FTC ist das US-Verkehrsministerium allerdings nicht zu der Erwirkung eines Schadensersatzes für geschädigte Verbraucher befugt.

Beide Organe werden sowohl aufgrund eigener Untersuchungen als auch auf eine Verbraucherbeschwerde hin tätig. Insbesondere die FTC hat sich außerdem dazu verpflichtet, vorrangig jene Fälle einer Missachtung der Principles zu behandeln, welche die Selbstregulierungsstellen oder das europäische Data Protection Panel an sie verweisen.[561]

Über die jeweils von ihnen unternommenen Schritte haben die beiden staatlichen Kontrollstellen das US-Handelsministerium zu unterrichten, um eine Anpassung der „Safe Harbor"-Liste zu veranlassen.

dd. Der Verlust des Status des „sicheren Hafens"

Sofern die verarbeitende Stelle gegen eine Anordnung der FTC oder eines anderen staatlichen Kontrollorgans verstößt oder einer endgültigen Entscheidung eines staatlichen Kontrollorgans oder eines Selbstregulierungsorgans nicht zu folgen bereit ist, verliert sie den Status des „sicheren Hafens". Dieselbe Rechtsfolge tritt ein, falls ein solches Organ feststellt, dass sich das Versprechen der verarbeitenden Stelle zur Einhaltung der Grundsätze des „sicheren Hafens" aufgrund regelmäßiger Verstöße als unglaubwürdig erwiesen hat.

---

[559] 15 U.S.C. § 57b.
[560] *Anhang VI* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 45 f.
[561] *Anhang II* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 22 (FAQ 11), i. V. m. *Anhang V* auf S. 40.

Über diese Vorgänge hat die verarbeitende Stelle das US-Handelsministerium mit dem Ziel der Korrektur der „Safe Harbor"-Liste unverzüglich in Kenntnis zu setzen. Eine Unterlassung der Mitteilung kann wie im Übrigen auch jede andere unzutreffende Bekanntgabe an das US-Handelsministerium gemäß dem False Statements Act[562] strafrechtlich verfolgt werden.

Sofern statt der verarbeitenden Stelle das jeweilige Selbstregulierungsorgan oder ein staatliches Kontrollorgan die fortgesetzte Missachtung der Grundsätze mitteilen, wird die verarbeitende Stelle 30 Tage vor einer Bekanntmachung in der „Safe Harbor"-Liste darüber informiert. Bisher ist in dem Verzeichnis jedoch noch bei keinem Unternehmen der Verlust des „Compliance Status" vermerkt.

(b) Kritische Würdigung

Auf den ersten Blick scheint dieses vielschichtige Verfahren alle Voraussetzungen[563] für eine effektive Durchführung eines Selbstregulierungskodexes zu erfüllen. Dennoch wird die Umsetzung des Grundsatzes der Durchsetzung im Rahmen der Safe Harbor Privacy Principles teilweise heftig kritisiert.[564] Die Gestaltung des Durchsetzungsmechanismus ist daher im Folgenden anhand der von der Art. 29-Gruppe aufgestellten Kriterien einer guten Befolgungsrate, eines wirkungsvollen Beschwerdeverfahrens und eines angemessenen Entschädigungssystems zu untersuchen.

aa. Befolgungsrate

Eine gute Befolgungsrate eines Selbstregulierungskodexes ergibt sich aus seiner Bekanntheit bei seinen Teilnehmern und aus seiner Transparenz gegenüber den Betroffenen. Ferner indizieren die Existenz einer externen Kontrolle sowie abschreckende Sanktionen die Einhaltung der inhaltlichen Grundsätze.

---

[562] 18 U.S.C. § 1001.

[563] Vgl. Gliederungspunkt C.II.2.b.(2).(b). dieses Kapitels.

[564] *Europäisches Parlament*, Entschließung des Europäischen Parlaments zu dem Entwurf einer Entscheidung der Kommission über die Angemessenheit der US-Grundsätze des Sicheren Hafens und diesbezügliche häufig gestellte Fragen (FAQ), vorgelegt vom Handelsministerium der USA (C5-0280/2000 – 2000/2144(COS)) vom 5.7.2000, A5-0177/2000, ABl. C 121 vom 24.4.2001, S. 152, S. 155; *WP 32*, S. 7 f.; *Klug*, BDSG, S. 133; *ders.*, RDV 2000, S. 212, S. 216; *Räther/Seitz*, MMR 2002, S. 425, S. 430.

Die Tatsache der Bekanntheit der Safe Harbor Privacy Principles bei ihren Teilnehmern ergibt sich bereits aus dem Umstand der freiwilligen Qualifikation und der jährlich gegenüber dem US-Handelsministerium zu erneuernden Selbstzertifizierung. Auch die Transparenz gegenüber den Betroffenen ist weitestgehend durch den Grundsatz der Informationspflicht und die Veröffentlichung der im Rahmen der Selbstzertifizierung an das US-Handelsministerium mitgeteilten Angaben in der „Safe Harbor"-Liste gewährleistet.

Eine externe Kontrolle ist indessen nicht garantiert. Zwar fordert der Grundsatz der Durchsetzung in Buchstabe b) regelmäßige Kontrollmaßnahmen, deren jährliche Durchführung mittels einer Erklärung zu dokumentieren ist. Die meisten Unternehmen führen diese Überwachung jedoch ausweislich der „Safe Harbor"-Liste in eigener Regie durch.

Das Fehlen einer Verpflichtung zu einer externen Kontrolle könnte indessen durch abschreckende Strafmaßnahmen kompensiert sein.[565] Aber auch diesbezüglich bieten die Safe Harbor Privacy Principles eine in ihrer Wirkungsweise nach europäischen Maßstäben nicht in jeder Hinsicht überzeugende Lösung an.

So sind weder die Selbstregulierungsorgane noch das europäische Data Protection Panel dazu befugt, ihre Maßnahmen gegenüber der verarbeitenden Stelle effektiv durchzusetzen. Es bleibt abzuwarten, inwieweit die Möglichkeit der privaten Selbstregulierungsorgane zur Anrufung der Gerichte diesem Defizit im Einzelfall abzuhelfen geeignet ist.

Ernst zu nehmen und in diesem Sinne auch nicht zu unterschätzen ist allerdings der möglicherweise von Wettbewerbsnachteilen begleitete Imageverlust infolge einer öffentlichen Bekanntmachung des Verstoßes oder infolge eines Ausschlusses von der Zuständigkeit der Selbstregulierungsstelle. Ähnlich zu wirken vermag auch der Entzug des Status des „sicheren Hafens" anlässlich der Mitteilung eines Verstoßes an das US-Handelsministerium.

Die seitens der FTC mögliche Verhängung einer Geldstrafe in Höhe von USD 10.000,- sollte indessen die wenigsten Unternehmen übermäßig belasten, sodass auch im Rahmen der Befugnisse der FTC allein die

[565] Vgl. Gliederungspunkt C.II.2.b.(2).(b). dieses Kapitels.

öffentliche Anprangerung einer Verletzung der eigenen Datenschutzpolitik eine wirklich effektive Sanktion darzustellen scheint.

Weitestgehend hypothetischer Natur sein dürfte demgegenüber der grundsätzlich abschreckende Entzug der Betriebserlaubnis durch das US-Verkehrsministerium, da die hierfür erforderlichen wiederholten Verletzungen der eigenen Datenschutzpolitik sich kaum je als derart gravierend erweisen werden, dass sie die Annahme des Fehlens einer Betriebstauglichkeit der Luftfahrtgesellschaft zu rechtfertigen vermögen.

Die abschreckende Wirkung einer Geldstrafe und/oder einer Haftstrafe von bis zu fünf Jahren bei einer Verletzung des False Statements Act aufgrund falscher Angaben gegenüber dem US-Handelsministerium wird schließlich durch die selten nachzuweisende Voraussetzung des direkten Vorsatzes relativiert.

bb. Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte

Gemäß dem Buchstaben a) des Durchsetzungsgrundsatzes unterstützen die Safe Harbor Privacy Principles den Betroffenen bei der Geltendmachung seiner Rechte, indem sie ein leicht zugängliches und kostengünstiges Beschwerdeverfahren bieten, das allerdings hauptsächlich vor privaten Selbstregulierungsorganen stattfindet.

Mag man diesen Organen die notwendige Unabhängigkeit und Neutralität noch zuerkennen, so fehlen ihnen doch regelmäßig die Befugnisse zu einer effektiven Untersuchung der Beschwerde und zur Durchsetzung der Rechte des Betroffenen. Dem von den Safe Harbor Privacy Principles gewährleisteten Beschwerdeverfahren könnte es sonach an einer wirkungsvollen Unterstützung des Betroffenen bei der Durchsetzung seiner Rechte mangeln.

Zwar steht es jedem Betroffenen im Rahmen der Safe Harbor Privacy Principles grundsätzlich frei, sich mit seinen Anliegen an die FTC oder an das US-Verkehrsministerium zu wenden. Auch sind die privaten Selbstregulierungsorgane dazu verpflichtet, Fälle der Missachtung ihrer eigenen Entscheidungen bei einem Verzicht auf gerichtliche Schritte an

die beiden staatlichen Kontrollinstanzen weiterzuleiten.[566] Im Widerspruch zu einer effektiven Hilfe bei einer Untersuchung von Verletzungen gegenüber dem Betroffenen liegt jedoch die tatsächliche Prüfung einer eingereichten Beschwerde durch die FTC oder das US-Verkehrsministerium in deren freien Ermessen über das Vorliegen eines begründeten Verdachts für einen Datenmissbrauch.

Zudem reguliert die FTC nach eigener Aussage keine individuellen Verbraucherstreitigkeiten, sondern ermittelt nur, ob sich die verarbeitende Stelle typischerweise unangemessen verhält.[567] Jenes auf Präzedenzfälle reduzierte Einschreiten resultiert aus dem staatlichen Auftrag der FTC, der nicht in dem Schutz des Einzelnen, etwa vor unzulässigen Eingriffen in die Privatsphäre besteht, sondern die Gewährleistung eines fairen Handels[568] beinhaltet.

Dieser kompetenzielle Wertungsunterschied hindert gemäß der Arbeitsunterlage WP 12 der Artikel 29-Gruppe[569] zwar grundsätzlich nicht die Feststellung eines angemessenen Schutzniveaus, sofern dennoch ein wirkungsvolles Beschwerdesystem etabliert ist. Auch macht die FTC ausweislich einer Auflistung von unzähligen Fällen ihres bisherigen Einschreitens[570] in diesem Sinne offensichtlich einen regen Gebrauch von ihren Befugnissen. Jedoch betrafen in der Vergangenheit insgesamt nur 21 Fälle der FTC Ermittlungen wegen unlauterer Geschäftspraktiken hinsichtlich einer Verletzung der Privatsphäre, von denen lediglich 12 Verfahren[571], darunter kein Verstoß gegen die Safe Harbor Privacy Principles, mit dem Erlass einer Untersagungsverfügung durch die FTC beziehungsweise durch ein seitens der FTC angerufenes Gericht endeten.[572] Dementsprechend hat die Europäische Kommission in ihrem ersten Bericht über die Umsetzung der „Safe Harbor"- Entscheidung die FTC zu einem verstärkten Handeln gegen „Safe Harbor"-Verstöße, insbesondere zu einem Vorgehen gegen sämtliche Unternehmen aufgefor-

[566] Die FAQ 11 des vorletzten Entwurfs der „Safe Harbor"-Entscheidung sah noch vor, dass die Selbstregulierungsorgane die FTC nur unterrichten „sollen" und nicht wie in der endgültigen Entscheidung unterrichten „müssen". Diese Änderung geht auf eine Stellungnahme der Art. 29-Gruppe (*WP 32*, S. 7) zurück. Insoweit erweist sich die Kritik an der unsicheren Abstimmung zwischen den unabhängigen Stellen und der FTC bei *Räther/Seitz*, MMR 2002, S. 425, S. 430, als unbegründet.
[567] *Anhang V* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 42.
[568] Auf diesen Unterschied weisen insbesondere *Verbiest/Wéry*, Rn. 902, hin.
[569] *WP 12*, S. 15; so bereits in *WP 7*, S. 4 f.; vgl. dazu insgesamt Gliederungspunkt C.II.2.b.(2).(b). dieses Kapitels.
[570] Abrufbar unter: www.ftc.gov/os/caselist/index.htm (Fälle ab Juni 1996).
[571] 2004 (bis Oktober): 2 Fälle; 2003: 3 Fälle; 2002: 2 Fälle; 2000: 3 Fälle; 1999: 2 Fälle.
[572] Vgl. die Auflistung unter: www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

dert, die entgegen ihrer Selbstverpflichtung ihre Teilnahme am „sicheren Hafen“ nicht in ihren Geschäftsbedingungen veröffentlicht haben.[573]

Zudem ist auch die Gewährleistung der Rechtsweggarantie äußerst zweifelhaft, da es nur schwer vorstellbar erscheint, dass sich die im Falle eines Verstoßes ausschließlich zuständigen US-amerikanischen Gerichte im Rahmen einer Klage des Betroffenen an den Selbstregulierungsmechanismus der Safe Harbor Privacy Principles gebunden fühlen werden.

Von einer Gewährleistung eines nach europäischen Maßstäben effektiven Beschwerdeverfahrens vermag sonach kaum gesprochen zu werden.

cc. Entschädigungssystem

Die Entschädigung des Betroffenen erfolgt gemäß dem Buchstaben a) des Durchsetzungsgrundsatzes ebenfalls in erster Linie über die privaten Selbstregulierungsorgane, denen es auch hierfür an einer Vollstreckungsbefugnis mangelt.

Zwar vermag auch die FTC im Gegensatz zu dem US-Verkehrsministerium unter bestimmten Umständen gemäß 15 U.S.C. § 57b Schadensersatz für Verbraucher zu erwirken. Dieses Verfahren ist jedoch nicht auf einen Schadensausgleich in einem Einzelfall gerichtet, sondern soll vielmehr im Wege einer allgemeinen Ahndung einer anhaltenden unlauteren Geschäftspraktik allen geschädigten Verbrauchern kompensatorisch Befriedigung verschaffen.

Der Grundsatz der Durchsetzung gewährleistet somit kein wirkungsvolles, von der Kooperationsbereitschaft der verarbeitenden Stelle unabhängiges Entschädigungsverfahren.

Indessen weist das US-Handelsministerium in Anhang IV der „Safe Harbor“-Entscheidung auf die zusätzliche Möglichkeit zu einer Schadensersatzklage im Rahmen des Common Law hin.

Sowohl der Betroffene als auch der europäische Datenübermittler könnten zum Beispiel ein US-amerikanisches Unternehmen wegen arglisti-

[573] *Europäische Kommission*, Commission Staff Working Document vom 20.10.2004, The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC (2004) 1323, S. 10.

ger oder fahrlässiger Falschdarstellung[574] verklagen, wenn dieses wider besseres Wissen vorgibt beziehungsweise entgegen seiner Sorgfaltspflichten fälschlicherweise erklärt hat, dass es die Safe Harbor Privacy Principles befolge, und dem Betroffenen beziehungsweise dem Datenübermittler aus dem Vertrauen auf diese Angaben ein finanzieller Verlust entstanden ist.[575] Der ersatzfähige Schaden beläuft sich im Falle einer Arglist auf die tatsächlichen Mehraufwendungen sowie den Verlust des kommerziellen Nutzens einer geschäftlichen Transaktion, während die fahrlässige Begehungsweise immerhin noch zu dem Ersatz der Mehraufwendungen führt.

Da im Grunde jede Datenübermittlung in die USA auf das Vertrauen in die behauptete Teilnahme des Datenempfängers am „sicheren Hafen" zurückzuführen ist, sollte die übermittelnde Stelle tatsächlich häufiger im Rahmen ihres überwiegend wirtschaftlich motivierten Datenumgangs einen Ersatz der genannten Schäden auf diese Weise geltend machen können.

Zweifelhaft ist allerdings, ob auch der aufgrund der Verletzung seiner Privatsphäre eigentlich zu entschädigende Betroffene von der Möglichkeit dieser Klage profitiert. Zwar sind Schäden infolge einer Abwertung der Kreditwürdigkeit oder des Verpassens einer potentiellen Gehaltserhöhung beziehungsweise der finanzielle Verlust infolge einer Entlassung aus einem Arbeitsverhältnis durchaus vorstellbar. Regelmäßig dürfte es jedoch an dem erforderlichen tatbestandlichen Kausalzusammenhang fehlen.

Obschon sich daher die Möglichkeit zu einer Schadensersatzklage wegen Falschdarstellung auf die Bewertung des Entschädigungssystems nur unwesentlich auszuwirken vermag, ist sie jedoch im Hinblick auf ihre gezielte Nutzbarkeit für die übermittelnde Stelle als Druckmittel im Rahmen der Feststellung einer guten Befolgungsrate nicht unerheblich.

Weiterhin legt das US-Handelsministerium in Anhang IV der „Safe Harbor"-Entscheidung dar, inwieweit sich die bereits vorgestellten, aus dem „Right to Privacy" ergebenden deliktischen Ansprüche des Common Law[576] zugunsten des Betroffenen auswirken können.[577] Es bleibt

[574] Restatement (Second) of the Law – Torts § 525 et seq. bzw. § 552 et seq.
[575] Eingehend dazu die Erläuterungen des US-Handelsministeriums in *Anhang IV* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 31.
[576] Vgl. dazu Gliederungspunkt C.III.1.d. dieses Kapitels.

jedoch abzuwarten, ob die derzeit noch nicht abzusehende gerichtliche Entscheidungspraxis tatsächlich eine Durchsetzung der Safe Harbor Privacy Principles zu fördern imstande ist.[578] Aufgrund des für beklagte Unternehmen recht unangenehm ausgestalteten US-Prozessrechts[579] sollte die grundsätzliche Möglichkeit zu einer Schadensersatzklage allerdings als Druckmittel zur freiwilligen Zahlung von Entschädigungen nicht unterschätzt werden.[580]

dd. Ergebnis

Die eingangs erwähnte Kritik an der Effektivität der Durchsetzung der Safe Harbor Privacy Principles erweist sich folglich als überaus berechtigt. Mag man den in Aussicht gestellten Sanktionen letztlich aufgrund des Drucks des Wettbewerbs und der Drohung von Schadenersatzklagen bei einem Verstoß gegen die Safe Harbor Privacy Principles noch eine angemessene Garantiefunktion zuerkennen, so erfüllen doch weder das Beschwerdeverfahren noch das Entschädigungssystem für sich betrachtet die Kriterien für das Vorliegen eines angemessenen Schutzniveaus.

Dementsprechend verwundert es auch nicht, dass der Artikel 3 der „Safe Harbor"-Entscheidung die mitgliedstaatlichen Datenschutzbehörden nachdrücklich auf ihre im Einzelfall trotz der Feststellung eines angemessenen Schutzniveaus durch die Europäische Kommission bestehen-

---

[577] *Anhang IV* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 32 ff.

[578] So wohl auch *WP 32*, S. 8.

[579] Von Unternehmen besonders gefürchtet sind vor allem vier Prinzipien: **1**. das Prinzip der *Punitive Damages*, das dem Geschädigten einer vorsätzlichen Rechtsverletzung auch einen immateriellen Strafschadensersatz in Form eines Schmerzensgeldes, oftmals in Millionenhöhe, als Genugtuung für den erlittenen Schaden sowie als Prävention vor einer Wiederholung zubilligt; **2**. das Prinzip des *Pretrial Discovery*, nach dem von dem Prozessgegner alle für die Prozessführung eventuell relevanten (internen) Informationen bereits vor der Hauptverhandlung angefordert werden dürfen und dem daher eine große Gefahr einer Ausforschung von Betriebsgeheimnissen und der Unternehmenspraxis innewohnt; **3**. die so genannte *Class Action*, die eine Klage in einem Präzedenzprozess zulässt, dessen Urteil für alle gleichartigen Fälle gilt, in denen die Betroffenen über die Klage informiert wurden und ihre Teilnahme nicht ausgeschlossen haben; **4**. das Prinzip der *Contigent Fee*, nach welcher der Verlierer die Kosten des Prozessgegners nicht trägt und sich die Anwaltsgebühr an dem Erfolg der Klage bemisst, also regelmäßig prozentual an der erstrittenen Summe, sodass der Anwalt des Klägers aus dieser Summe befriedigt werden kann – während das Verfahren für den Kläger also beinahe risikolos ist, muss das beklagte Unternehmen stets seine Anwaltskosten aufbringen. Ausführlich zum US-Prozessrecht: *Schack*, dort insb. S. 8 f., S. 44 ff., S. 79 ff. und Fn. 284; vgl. außerdem die Erläuterungen des US-Handelsministeriums zum US-Prozessrecht in *Anhang IV* der „Safe Harbor"-Entscheidung, ABl. EG Nr. L 215 vom 25.08.2000, S. 7, S. 33 f.

[580] Vgl. z. B. *Spies*, MMR 2002, S. 641, S. 642, der darauf verweist, dass viele Unternehmen die Teilnahme am „sicheren Hafen" scheuten, weil sie die Haftungsrisiken fürchteten.

den Befugnisse zur Unterbindung einer Übermittlung in ein Drittland hinweist.

So darf gemäß Artikel 3 Absatz 1a) der „Safe Harbor“-Entscheidung die Aussetzung einer Datenübermittlung an ein „Safe Harbor“-Unternehmen veranlasst werden, sofern entweder die FTC beziehungsweise das US-Verkehrsministerium oder eine unabhängige Selbstregulierungsinstanz im Sinne des Buchstabens a) des Durchsetzungsgrundsatzes eine Verletzung der Grundsätze des „sicheren Hafens“ bei dem betreffenden Datenempfänger festgestellt haben. Dasselbe gilt gemäß Artikel 3 Absatz 1b), falls eine Verletzung der Principles sehr wahrscheinlich ist und Grund zu der Annahme besteht, dass die jeweilige Durchsetzungsinstanz nicht rechtzeitig angemessen reagieren wird, die fortgesetzte Datenübermittlung für den Betroffenen das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde und die zuständige mitgliedstaatliche Behörde den US-amerikanischen Datenverarbeiter zuvor in angemessener Weise unterrichtet und ihm Gelegenheit zu einer Stellungnahme gegeben hat.

Im Interesse einer abgestimmten Vorgehensweise sollen die Mitgliedstaaten die Europäische Kommission gemäß Artikel 3 Absatz 2 der „Safe Harbor“-Entscheidung unverzüglich über ihre in diesem Sinne getroffenen Maßnahmen informieren. Darüber hinaus ist gemäß Absatz 3 ein Informationsaustausch zwischen den Mitgliedstaaten und der Kommission über solche Fälle vorgesehen, bei denen die Maßnahmen der für die Einhaltung der entsprechend den FAQ umgesetzten Principles in den USA verantwortlichen Einrichtungen nicht ausreichen, um die Befolgung der Principles zu gewährleisten.

Ergibt sich gemäß Absatz 4 aus den nach den Absätzen 1 bis 3 des Artikels 3 der „Safe Harbor“-Entscheidung gesammelten Angaben, dass eine für die Umsetzung der Principles in den USA verantwortliche Stelle ihrer Aufgabe nicht wirkungsvoll nachkommt, so informiert die Kommission das US-Handelsministerium und schlägt gemäß dem Verfahren nach Artikel 31 der Richtlinie entsprechende Maßnahmen hinsichtlich einer Aufhebung, Aussetzung oder Beschränkung des Geltungsbereichs der „Safe Harbor“-Entscheidung vor.

Die „Safe Harbor“-Entscheidung steht sonach im Grunde unter dem ständigen Vorbehalt einer effektiven Durchsetzung der Principles.

(8) Sonstige FAQ

Die weiteren FAQ gehen auf Spezialfälle hinsichtlich der Art der Daten oder des Zwecks der Verarbeitung ein.

So klärt die *FAQ 10* darüber auf, dass eine unter der Verantwortlichkeit eines europäischen Auftraggebers durchgeführte Auftragsverarbeitung in den USA trotz der Teilnahme am „sicheren Hafen" des Auftragnehmers und des sonach gewährleisteten angemessenen Schutzniveaus bei dem Empfänger den Abschluss eines zusätzlichen Vertrages erfordert, in dem der Auftraggeber im Rahmen seiner Verantwortlichkeit gemäß dem aufgrund des Sitzprinzips für die Verarbeitung geltenden mitgliedstaatlichen Datenschutzgesetz die Mittel und Zwecke der Verarbeitung festlegt.[581]

Die *FAQ 3* stellt klar, dass die Safe Harbor Privacy Principles, ebenso wie die Richtlinie selbst, keine hilfsweise Haftung von Internetdiensteanbietern, Telekommunikationsunternehmen und ähnlichen Organisationen kennt, die Daten im Namen anderer Stellen, welche gegen die für sie geltenden Bestimmungen verstoßen, lediglich weiterleiten und dabei weder die Mittel noch die Zwecke der Verarbeitung bestimmen.

Die *FAQ 4* sieht Ausnahmen von der Anwendung der Grundsätze der Informationspflicht, der Wahlmöglichkeit und des Auskunftsrechts für bestimmte Datenverarbeitungen von Investmentbanken und Wirtschaftsprüfern vor, während die *FAQ 13* auf die Vorteile der Qualifizierung für den „sicheren Hafen" bei dem regelmäßigen Empfang von Flugreservierungs- und anderen Reisedaten verweist. Die *FAQ 14* gibt ausführlich Auskunft über einzelne Anwendungsmodalitäten bei der Verarbeitung von personenbezogenen Daten für Zwecke der medizinischen und pharmazeutischen Forschung.

Schließlich ist noch auf die umfangreichen Ausnahmen von der Anwendbarkeit der Safe Harbor Privacy Principles gemäß der *FAQ 15* und der *FAQ 8* (F/A 7 und 8) für die Verarbeitung von Daten aus öffentlichen Registern und öffentlich zugänglichen Quellen hinzuweisen, die zu Recht bereits während der Verhandlungen über die Safe Harbor Privacy Principles konsequent kritisiert wurden. Zwar sind die erstgenannten Daten von der Ausnahmeregelung des Artikels 26f) der Richtlinie erfasst, sodass ihre Übermittlung aus der Europäischen Union in ein

[581] Vgl. dazu Gliederungspunkt B.I. des zweiten Kapitels.

Drittland ohnehin nicht an das Vorliegen eines angemessenen Schutzniveaus gebunden ist. Eine derartige Ausnahme für Daten aus anderen öffentlich zugänglichen Quellen rechtfertigt sich allerdings nicht, da aus der Öffentlichkeit einer Information nicht zwangsläufig auf ihre Richtigkeit und die Rechtmäßigkeit ihrer Verarbeitung geschlossen werden kann.[582]

d. Gesamtbetrachtung

Entsprechend den vorangehenden Erläuterungen bleiben die Safe Harbor Privacy Principles teilweise deutlich hinter den Anforderungen an ein angemessenes Schutzniveau im Sinne des Artikels 25 der Richtlinie 95/46/EG zurück.[583] Erhebliche Mängel weisen dabei insbesondere die Umsetzung des Zweckbindungsgrundsatzes, des Grundsatzes der bedingten Weitergabe an Drittländer sowie die Gestaltung des Grundsatzes der Durchsetzung auf.

Trotz dieser aus europäischer Sicht infolgedessen mit der „Safe Harbor"-Entscheidung getroffenen erheblichen Zugeständnisse an die US-amerikanische Seite verweigern die meisten Unternehmen in den USA die Teilnahme am „sicheren Hafen" aufgrund des nach ihren Maßstäben zu hohen Haftungsrisikos.[584] Ferner sähen die Principles unangemessen schwere Auflagen vor, die sich durch eine absolute Inkompatibilität mit den praktischen Gegebenheiten im Unternehmensalltag auszeichneten.[585]

Tatsächlich stellt sich eine unterschiedliche Behandlung von den aus den Mitgliedstaaten importierten Daten und den aus den USA beziehungsweise anderen Herkunftsländern stammenden personenbezogenen Informationen sowohl technisch als auch gesellschaftspolitisch als große Herausforderung für viele US-Unternehmen dar.

So ist die Trennung der Datenbestände im Rahmen einer zentralen Datenverarbeitung generell mit einem erheblichen Kosten-, Arbeits- und

---

[582] *WP 32*, S. 5; so bereits in *WP 15*, S. 4, in *WP 23*, S. 4, und in *WP 27*, S. 6 und S. 10.

[583] A. A. offenbar *Gerhold/Heil*, DuD 2001, S. 377, S. 378, die trotz der Schwächen annehmen, dass die Unionsbürger aufgrund der Safe Harbor Privacy Principles auf einen vorschriftsmäßigen Schutz ihrer Daten vertrauen dürften; so auch *Heil*, DuD 2000, S. 444; *Heymann*, CRi 2000, S. 70 ff.; *Reimer*, DuD 2000, S. 493; *ders.*, DuD 2000, S. 309.

[584] *Spies*, MMR 2002, S. 641, S. 642; vgl. auch *Karstedt-Meierrieks*, DuD 2001, S. 287, S. 288, die bemerkt, dass sich US-amerikanische Unternehmen von dem bürokratischen Aufwand der Principles abgeschreckt fühlten.

[585] *o.V.*, DuD 2001, S. 305; *o.V.*, MMR 5/2001, S. VII.

Organisationsaufwand verbunden. Oftmals erweist sich auch schon die Lokalisierung der Datenquelle als problematisch.

Einer nach Herkunftsländern differenzierenden Datenschutzpolitik haftet zudem unweigerlich der Verdacht eines diskriminierenden Geschäftsgebarens an. „Safe Harbor"-Unternehmen stehen mithin zwangsläufig vor der Frage, wie sie ohne den Verlust ihres guten Rufes in der US-amerikanischen Gesellschaft rechtfertigen sollen, warum sie scheinbar die Privatsphäre von Unionsbürgern für schützenswerter halten als jene von US-Bürgern.[586]

Aus diesen Erwägungen sehen sich viele US-amerikanische Unternehmen für den Fall ihrer Teilnahme am „sicheren Hafen" dazu gezwungen, das im Grunde europäische Datenschutzkonzept auf ihre gesamte Datenverarbeitung anzuwenden.

Naturgemäß führt dieser aus europäischer Sicht begrüßenswerte Nebeneffekt in den USA eher zu einer Abwehrhaltung. So haben bis Oktober 2004 seit der Einrichtung der „Safe Harbor"-Liste im November 2000 lediglich rund 600 Unternehmen ihren Beitritt zum „sicheren Hafen" veröffentlicht. Positiv stimmen mag zwar, dass die Zahl damit im Vergleich zu dem Vorjahreswert erneut um gut 50% gestiegen ist. Das sollte jedoch nicht darüber hinwegtäuschen, dass sie noch immer in keinem vernünftigen Verhältnis zu den wohl mehreren tausend tatsächlichen Empfängern von personenbezogenen Daten aus der Europäischen Union steht.

Hinzu kommt, dass gemäß den ersten Berichten der Europäischen Kommission über die Umsetzung der „Safe Harbor"-Entscheidung nicht einmal alle der am „sicheren Hafen" teilnehmenden Unternehmen die Principles auch tatsächlich in ihren Datenschutzrichtlinien vollständig umgesetzt haben.[587] Zu demselben Ergebnis gelangte die Europäische Kommission auch im Hinblick auf die Datenschutzprogramme der pri-

[586] *Schwartz*, 52 Vanderbilt L. Rev., S. 1609, S. 1700.

[587] *Europäische Kommission*, Commission Staff Working Document vom 20.10.2004, The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC (2004) 1323, S. 6 ff.; *dies*. so bereits im 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 vom 13.2.2002, SEK(2002) 196, S. 2 f. und S. 9 ff.

vaten Selbstregulierungsstellen im Sinne des Buchstabens a) des Durchsetzungsgrundsatzes.[588] Darüber hinaus lasse für alle beteiligten Stellen insgesamt die Transparenz der Anwendung der Safe Harbor Privacy Principles zu wünschen übrig.[589]

Der mit den Safe Harbor Privacy Principles angeblich gefundene Kompromiss stellt sonach im Ergebnis weder die europäische noch die US-amerikanische Seite wirklich zufrieden und bedarf daher jedenfalls hinsichtlich seiner Umsetzung einer Nachbesserung.

Besondere Aufmerksamkeit sollte dabei aus europäischer Sicht vor allem dem Umstand gewidmet werden, dass ein Datenschutzkonzept, ob gesetzlich festgeschrieben oder in Form einer Selbstregulierung, nur dann aufgehen kann, wenn auch die von den Regelungen betroffenen Parteien an seiner praktischen Umsetzung interessiert sind. Der hierfür erforderliche Druck des Wettbewerbs wird jedoch nicht nur über eine Konkurrenz der besseren Datenschutzpolitik auf horizontaler Ebene zwischen den einzelnen Unternehmen erzeugt, sondern in erster Linie von dem Auswahlverhalten der Kunden bestimmt. Ausweislich einer im Jahr 2002 durchgeführten Online-Umfrage der Europäischen Kommission bei Unternehmen und Verbrauchern besteht aber gerade bei letzteren noch ein erheblicher Aufklärungsbedarf und die Notwendigkeit einer Sensibilisierung für datenschutzrechtliche Belange.[590]

Unterstützend bemüht sich im Übrigen das US-Handelsministerium, die Einhaltung der europäischen Datenschutzgrundsätze und die Voraussetzungen der Teilnahme am „Safe Harbor“-Programm in kostenlosen Workshops für US-amerikanische Unternehmen zu vermitteln.[591]

Bei der Ausgestaltung der Safe Harbor Privacy Principles dürften sich indessen weitere Zugeständnisse seitens der europäischen Verhandlungspartner schon aus Gründen der Glaubwürdigkeit verbieten – haftet doch bereits der aktuellen Fassung aus der Sicht vieler Datenschützer

---

[588] *Europäische Kommission* vom 20.10.2004 (vgl. vorherige Fn.), S. 11, und *Europäische Kommission* vom 13.2.2002 (vgl. vorherige Fn.), S. 11.

[589] So auch *WP 62*, S. 3 f.; vgl. auch die stete Kritik des *TACD* an der mangelhaften Umsetzung der Principles, zuletzt im Oktober 2002.

[590] Abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/lawreport/consultation_en.htm; vgl. auch die Zusammenfassung der Ergebnisse: *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 10.

[591] Siehe Angebot unter http://www.export.gov/safeharbor/index.html und dort insbesondere http://www.export.gov/safeharbor/Chicago_Workshop_Flier.pdf.

der Charakter eines Scheingeschäfts zur Sicherung des freien Datenflusses im Rahmen des transatlantischen Handels an.