D. Der Artikel 26 Absatz 1 der Richtlinie

Abweichend von Artikel 25 der Richtlinie sieht der Artikel 26 Absatz 1 der Richtlinie vor, dass personenbezogene Daten in Drittländer übermittelt werden dürfen, die kein angemessenes Schutzniveau gewährleisten, sofern einer der abschließend in den Buchstaben a) bis f) der Vorschrift aufgezählten Tatbestände vorliegt. Eine grenzüberschreitende Übermittlung ist danach zulässig, falls

a. der Betroffene zweifelsfrei eingewilligt hat,
b. sie zu der Erfüllung eines Vertrages zwischen dem Betroffenen und dem für die Verarbeitung Verantwortlichen oder zur Durchführung vorvertraglicher Maßnahmen auf Antrag des Betroffenen erforderlich ist,
c. sie zu dem Abschluss oder zur Erfüllung eines Vertrages erforderlich ist, der im Interesse des Betroffenen von dem für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder werden soll,
d. sie entweder zur Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist,
e. sie zur Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
f. sie aus einem öffentlichen Register erfolgt, sofern die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall vorliegen.

Diese Ausnahmen korrespondieren im Wesentlichen mit den Erlaubnistatbeständen der generellen Zulässigkeit einer Verarbeitung des Artikels 7 der Richtlinie, sind jedoch tendenziell enger gefasst und enthalten keine allgemeine Interessenabwägungsklausel im Sinne des Artikels 7f) der Richtlinie. Die strukturelle Übereinstimmung ist erforderlich, da die Übermittlung anderenfalls an den Zulässigkeitskriterien des Artikels 7 der Richtlinie scheitern würde. Eine völlige Kongruenz führte indessen dazu, dass ohne Rücksicht auf das Schutzniveau in dem Destinationsland für Übermittlungen in Drittländer dieselben Konditionen wie innerhalb der Europäischen Union gelten würden.

Die Tatbestände des Artikels 26 Absatz 1 der Richtlinie zeichnen sich dadurch aus, dass in den betreffenden Konstellationen entweder andere Rechtsgüter das Schutzinteresse des Betroffenen überwiegen oder nur

ein geringes Risiko für eine Verletzung der Privatsphäre des Betroffenen besteht, weil die Übermittlung entweder seinem erklärten Willen oder seinem mutmaßlichen Interesse entspricht.[592]

Allerdings endet der Schutz des Betroffenen infolge einer Übermittlung gemäß Artikel 26 Absatz 1 der Richtlinie an den mitgliedstaatlichen Grenzen, sodass die Ausnahmetatbestände unter der Berücksichtigung des Artikels 1 Absatz 1 der Richtlinie grundrechtskonform restriktiv auszulegen sind.[593] Ausweislich seines Wortlautes gilt der Artikel 26 Absatz 1 der Richtlinie darüber hinaus nur „vorbehaltlich entgegenstehender Regelungen für bestimmte Fälle im innerstaatlichen Recht". Die Mitgliedstaaten dürfen mithin einzelne Regelungsbereiche, zum Beispiel den Arbeitnehmer- oder Patientendatenschutz,[594] von der Anwendbarkeit der Ausnahmetatbestände ausnehmen.

I. Einwilligung

Gemäß dem mit Artikel 7a) der Richtlinie wortgleichen Artikel 26 Absatz 1a) ist eine Datenübermittlung in ein unsicheres Drittland zulässig, sofern der Betroffene „ohne jeden Zweifel" in die Übermittlung eingewilligt hat.

Als Einwilligung gilt gemäß der Legaldefinition des Artikels 2h) der Richtlinie „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden."

---

[592] *WP 12*, S. 26; *Abel*, BDSG, S. 76; Dammann/Simitis, EG-Datenschutzrichtlinie (-*Dammann*), Art. 26, Rn. 2; *Draf*, S. 106.

[593] *WP 12*, S. 26; vgl. aber *Wuermeling*, Handelshemmnis Datenschutz, S. 142, der die Auslegung der Richtlinie ausschließlich an ihren Zielen, also gemäß Artikel 100a EGV (neu: Artikel 95 EGV) an dem Ziel des Funktionierens des Binnenmarktes messen will und deswegen nur eine einheitliche Anwendung des Artikels 26 Absatz 1 der Richtlinie in den Mitgliedstaaten fordert. Dabei übersieht er jedoch, dass zwar der Anwendungsbereich der Richtlinie aus kompetenziellen Gründen nur von den im Gemeinschaftsvertrag festgelegten Zielen geprägt sein darf, die Auslegung des Gemeinschaftsrechts innerhalb seines Anwendungsbereichs aber gleichwohl gemäß dem Artikel 6 Absatz 2 EUV von den Grundrechten der mitgliedstaatlichen Verfassungen sowie der Europäischen Menschenrechtskonvention und von dem im Wege der richterlichen Rechtsfortbildung vom EuGH entwickelten Grundrechtskatalog sowie von der proklamierten Charta der Grundrechte der Europäischen Union beeinflusst wird.

[594] *WP 12*, S. 26.

Dieser Ausnahme liegt der Gedanke zugrunde, dass der Betroffene als Souverän seiner Daten sich freiwillig des von der Richtlinie 95/46/EG gewährleisteten Schutzniveaus begeben kann.[595]

Eine freie und bewusste Entscheidung über die Disposition der eigenen personenbezogenen Daten setzt als intensivste Ausdrucksform der informationellen Selbstbestimmung jedoch voraus, dass der Betroffene das konkrete Risiko einer Übermittlung abzuschätzen vermag. Mit Rücksicht auf die Artikel 10 und 11 der Richtlinie über die Informationspflicht und in Anlehnung an den Grundsatz der Beschränkung der Weiterübermittlung aus den Anlagen 2 und 3 der Standardvertragsklauseln im Rahmen einer Funktionsübertragung[596] muss der Betroffene daher mindestens über die Zwecke der Übermittlung, die Identität des für die Übermittlung Verantwortlichen, die Kategorien der Empfänger und Empfängerländer, sowie die Tatsache informiert sein, dass letztere bei einer Verarbeitung personenbezogener Informationen kein angemessenes Schutzniveau für die Privatsphäre des Einzelnen gewährleisten.

Die Einwilligung des Betroffenen gilt dementsprechend nur für einen konkreten Fall. Eine Blankoeinwilligung für pauschale, nicht näher definierte Verarbeitungen, etwa für eine Sammlung der Daten in einem Depot für zukünftige, noch völlig offene Zwecke ist sonach unwirksam.[597]

Ferner muss die Einwilligung frei von Zwang erfolgen. Generell angezweifelt wird die Freiwilligkeit der Einwilligung im Rahmen von Arbeitsverhältnissen aufgrund der sozialen Abhängigkeit des Betroffenen von seinem Arbeitgeber.[598] Insbesondere in diesem Zusammenhang ist also sehr genau zu prüfen, ob die Einwilligung des Betroffenen im Einzelfall wirklich Ausdruck seines freien Willens ist.[599]

---

[595] *Wuermeling*, Handelshemmnis Datenschutz, S. 143.

[596] *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 bzw. S. 31; vgl. dazu auch Gliederungspunkt E.I.3.a.(1).(b).aa. dieses Kapitels.

[597] *Däubler*, Rn. 328; *ders.*, CR 1999, S. 49, S. 51; *Klug*, BDSG, S. 130; *ders.*, RDV 2001, S. 266, S. 272; *ders.*, RDV 1999, S. 109, S. 113; *Koch*, S. 304; *Räther/Seitz*, MMR 2002, S. 425, S. 431; *Schaar*, Datenschutz im Internet, Rn. 583; *Wohlgemuth*, BB 1996, S. 690, S. 693.

[598] Bräutigam/Leupold (- *Büllesbach*), A.III.1., Rn. 62; *Kuner*, DuD 2002, S. 553, S. 554; *Schaar*, Datenschutz im Internet, Rn. 556; *ders.*, MMR 2001, S. 644; vgl. auch *WP 48*, S. 27 f. und S. 31.

[599] Ausführlich zu dieser Problematik *Däubler*, Rn. 331 ff.; *ders.*, CR 1999, S. 49, S. 52; *ders.* in: Tinnefeld/Philipps/Heil, S. 110, S. 122 f.; *Gola*, RDV 2002, S. 109, S. 110 ff.; *Klug*, BDSG, S. 130 f. Bedenken gegen die Zulässigkeit einer Einwilligung im Arbeitsverhältnis hegt auch *Wohlgemuth*, BB 1996, S. 690, S. 693; *ders.*, BB 1991, S. 340, S. 341. A. A. *Lambrich/Cahlik*, RDV 2002, S. 287, S. 292 ff., die diese Form des Arbeitnehmerdatenschutzes

Darüber hinaus muss der Betroffene der Übermittlung „ohne jeden Zweifel“ zustimmen, sodass jegliche Unsicherheit über das tatsächliche Vorliegen einer Einwilligung der Zulässigkeit der Übermittlung entgegensteht.[600]

In diesem Sinne findet auch eine Einwilligung durch schlüssiges Verhalten nur Berücksichtigung, sofern die betreffende Handlung eindeutig den Willen des Betroffenen dokumentiert.[601] Indessen ist eine ausdrückliche Zustimmung im Umkehrschluss zu Artikel 8 Absatz 2a) der Richtlinie, der eine solche für die Verarbeitung sensibler Daten verlangt, nicht erforderlich.[602]

II. Verträge und vorvertragliche Vertrauensverhältnisse

Die Ausnahmen des Artikels 26 Absatz 1b) und c) der Richtlinie für Übermittlungen mit dem Ziel der Vertragserfüllung beziehungsweise der Durchführung vorvertraglicher Vertrauensverhältnisse scheinen auf den ersten Blick beinahe sämtliche Übermittlungen und Kategorien von Übermittlungen in Drittländer zu erfassen. Allerdings begrenzen beide Tatbestände die Zulässigkeit der Übermittlung auf das Maß der Erforderlichkeit. Es dürfen folglich nur solche Daten weitergegeben werden, die zwingend notwendig sind, um den Vertrag zu erfüllen beziehungsweise das vorvertragliche Vertrauensverhältnis durchzuführen.

Eine Übermittlung im Sinne des mit dem Artikel 7b) der Richtlinie identischen Artikels 26 Absatz 1b) setzt entweder einen Vertrag oder eine Vertragsanbahnung zwischen dem für die Verarbeitung Verantwortlichen und dem Betroffenen voraus.

---

für ungerechtfertigt halten. Eine ausdrückliche Begrenzung der Zulässigkeit der Einwilligung im Arbeitsverhältnis scheint entsprechend der Diskussion über die geplante EU-Richtlinie zum Arbeitnehmerdatenschutz für die Zukunft jedoch wahrscheinlich, vgl. dazu die „Zweite Phase der Anhörung der Sozialpartner zum Schutz von personenbezogenen Daten von Arbeitnehmern“, S. 6, S. 7, S. 12 und S. 21 (abrufbar unter: http://europa.eu.int/comm/employment_social/labour_law/docs/secondstagecomsultdataprot_de.pdf).

[600] *WP 12*, S. 26.

[601] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 26, Rn. 5; *Draf*, S. 112 f.; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 26, Rn. 7; *Wuermeling*, Handelshemmnis Datenschutz, S. 143; wohl auch *Riemann*, CR 1997, S. 762, S. 765; a. A. *Brühann* in: Datenverkehr ohne Datenschutz?, S. 35, S. 44; *ders*., RDV 1996, S. 12, S. 15, der ohne Begründung einer konkludenten Einwilligung von vornherein die Zweifelsfreiheit abspricht.

[602] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 26, Rn. 5.

Die zweite Tatbestandsvariante erfordert zudem, dass die Übermittlung auf Antrag des Betroffenen erfolgt, sodass der für die Verarbeitung Verantwortliche nicht willkürlich, im Rahmen selbst initiierter vorvertraglicher Vertrauensverhältnisse personenbezogene Daten des Betroffenen in Drittländer übermitteln kann. In diesem Sinne zulässig ist etwa eine Übermittlung aufgrund eines nichtigen Vertrages oder im Rahmen von Verhandlungen über eine Kreditvergabe.[603]

Die Ausnahme des Artikels 26 Absatz 1c) der Richtlinie betrifft schließlich einen Vertrag, der im Interesse des Betroffenen zwischen dem für die Verarbeitung Verantwortlichen und einem Dritten geschlossen wurde oder werden soll. Dieser nicht in Artikel 7 der Richtlinie ausdrücklich niedergelegte Tatbestand gilt als Spezialfall der allgemeinen Interessenabwägungsklausel des Artikels 7f) der Richtlinie,[604] nach der eine Verarbeitung zur Verwirklichung eines berechtigten Interesses zulässig ist, „das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person (...) überwiegen."

Die Ausnahmetatbestände des Artikels 26 Absatz 1b) und c) der Richtlinie überschneiden sich zuweilen. So erfordert etwa ein Reisevertrag des Betroffenen mit einem Reisebüro die Übermittlung von personenbezogenen Daten an die jeweilige Fluggesellschaft sowie an das gebuchte Hotel. Zugleich werden die Daten aber auch zur Erfüllung der im Interesse des Betroffenen geschlossenen Verträge des Reisebüros mit der Fluggesellschaft beziehungsweise dem Hotel übermittelt.

Typische Sachverhalte für die Anwendbarkeit der Ausnahmetatbestände der Buchstaben b) und/oder c) des Artikels 26 Absatz 1 der Richtlinie sind etwa Datenübermittlungen im Rahmen von elektronischen Warenbestellungen, Geldüberweisungen oder sonstigen bargeldlosen Transaktionen, Kontoeröffnungen, Kranken- und Haftpflichtversicherungen sowie Übermittlungen von einem Händler an den Hersteller im Garantiefall.[605]

---

[603] *Schapper*, CR 1987, S. 86, S. 91.

[604] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 26, Rn. 7; *Draf*, S. 114; *Wuermeling*, Handelshemmnis Datenschutz, S. 147.

[605] *Abel*, BDSG, S. 77 f.; *Büllesbach*, RDV 2002, S. 55, S. 58; *ders.*, CR 2000, S. 544, S. 552; Grabitz/Hilf III (- *Brühann*), A 30, Art. 26, Rn. 7 f.; *Draf*, S. 108 und S. 113; *Geis*, NJW 1997, S. 288, S. 291; *Gola/Klug*, S. 68 f.; *Schapper*, CR 1987, S. 86, S. 91; Simitis u. a. (- *Simitis*), BDSG, § 4c, Rn. 17; *ders.*, CR 2000, S. 472, S. 473; *ders.* in: Datenverkehr ohne Datenschutz?, S. 177, S. 180; *Terwangne/Louveaux*, MMR 1998, S. 451, S. 457.

Zu differenzieren ist indessen bei der Frage, ob Artikel 26 Absatz 1b) der Richtlinie eine konzerninterne Übermittlung von Arbeitnehmerdaten in Drittländer zu legitimieren vermag. Hier kommt es entscheidend auf das Tatbestandsmerkmal der Erforderlichkeit an. Erforderlich zur Erfüllung des Arbeitsvertrages mit dem Betroffenen kann grundsätzlich nur eine Übermittlung sein, die einer globalen Aufstellung des Unternehmens und der infolgedessen notwendigen weltweiten Zusammenarbeit im Unternehmen immanent ist. Das trifft etwa auf die Weitergabe dienstlicher Kontaktdaten in einem globalen Directory oder auf die Übermittlung von Personaldaten an Vorgesetzte in dem jeweiligen Drittland zu, die diese Daten zur Ausübung ihrer Weisungsbefugnisse benötigen. In dem letzten Beispiel entfällt die Erforderlichkeit im Übrigen nicht deswegen, weil der Vorgesetzte nicht zwingend in dem Drittland ansässig sein müsste. Die Hierarchie eines globalen Konzerns weist mindestens an einer Stelle zwangsläufig eine Grenzüberschreitung auf. Insoweit kann der Einzelne nicht damit gegen eine Übermittlung protestieren, dass sein Vorgesetzter theoretisch auch von einem Standort in der Europäischen Union aus agieren könnte, da dadurch lediglich der Kreis der von der Datenübermittlung betroffenen Personen verschoben würde. Davon abgesehen ist kaum zu erwarten, dass das Unternehmen die Ansiedlung einer Grenzüberschreitung innerhalb der Hierarchie unter Datenschutzgesichtspunkten künstlich herbeiführt. Im Zweifel wird diese Entscheidung ausschließlich von Faktoren einer funktionsfähigen Organisation beeinflusst, die sich wiederum als essentiell für die Erfüllung der arbeitsvertraglichen Pflichten des Arbeitgebers darstellt.

Selten unmittelbar für die Erfüllung von Kunden- oder Arbeitsverträgen erforderlich ist demgegenüber eine Übermittlung an eine zentrale Datenbank oder an ein Rechenzentrum in einem Drittland. Ein solches Outsourcing dient zumeist lediglich einer effektiveren und beschleunigten Datenverarbeitung und ist nur in Ausnahmefällen einer globalen Zusammenarbeit des Konzerns immanent, weil etwa eine zentrale Verwaltung bestimmter Daten unumgänglich wäre.[606]

Weitere nicht von den Ausnahmetatbeständen erfasste Sachverhaltsvarianten wurden bereits an anderer Stelle dargestellt.[607]

[606] *Büllesbach*, RDV 2002, S. 55, S. 58; *Büllesbach/Höss-Löw*, DuD 2001, S. 135, S. 136.
[607] Vgl. dazu Gliederungspunkt A. dieses Kapitels.

III. Wichtige öffentliche Interessen und Gerichtsverfahren

Eine Übermittlung ist ferner zulässig, falls es zur Wahrung eines wichtigen öffentlichen Interesses oder zur Verwirklichung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist.

Teilweise wird infrage gestellt, dass sich der Zusatz „gesetzlich vorgeschrieben“ auch auf die aufgezählten Merkmale des wichtigen öffentlichen Interesses und die Verfügbarkeit der Daten im Rahmen eines Gerichtsverfahrens bezieht.[608]

Die deutsche Richtlinienversion ist insofern grammatikalisch tatsächlich nicht eindeutig formuliert. Demgegenüber lassen jedoch zum Beispiel die englische,[609] die französische[610] und die italienische[611] Fassung der Vorschrift keine andere Auslegung zu, da sie den Ausnahmetatbestand jeweils mit der Phrase „erforderlich oder gesetzlich vorgeschrieben“ in der jeweiligen Sprache einleiten.

Im Gegensatz zu dem korrespondierenden Artikel 7e) der Richtlinie lässt der Artikel 26 Absatz 1d) eine Übermittlung nicht zur Wahrung jeglichen öffentlichen Interesses zu. Vielmehr vermag nur ein wichtiges, also qualifiziertes öffentliches Interesse eine Datenübermittlung in ein Drittland zu rechtfertigen.[612]

Gemäß der Begründung des geänderten Vorschlags zur Richtlinie soll mit dieser Ausnahme die internationale Zusammenarbeit zum Beispiel bei der Bekämpfung der Geldwäsche oder im Rahmen der Überwachung der Finanzinstitute gestattet werden.[613] Erwägungsgrund (58) der Richtlinie nennt zudem beispielhaft den internationalen Datenaustausch zwischen Steuer- oder Zollverwaltungen und zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind.

---

[608] *Wuermeling*, Handelshemmnis Datenschutz, S. 148.

[609] Article 26, 1(d): the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims (…).

[610] Article 26, 1(d): le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d’un intérêt public important, ou pour la constatation, l’exercice ou la défense d’un droit en justice (…).

[611] Articolo 26, 1d): il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto per via giudiziaria, (…).

[612] Simitis u. a. (- *Simitis*), BDSG, § 4c, Rn. 19.

[613] *Begründung des geänderten Vorschlags*, abgedruckt in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 26, S. 283.

Ganz offensichtlich ist bei dieser Ausnahme also vorrangig an Datenübermittlungen an öffentliche Stellen gedacht. Unter besonderen Umständen scheint allerdings auch eine Übermittlung an einen privaten Verarbeiter gerechtfertigt.[614] So steht etwa gemäß Erwägungsgrund (34) ebenfalls die wissenschaftliche Forschung in einem wichtigen öffentlichen Interesse.

Der Schutz des Betroffenen muss im Wege einer allgemeinen Interessenabwägung ferner zurücktreten, falls die Übermittlung der personenbezogenen Daten zur Verwirklichung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist. Dabei differenziert die Regelung nicht danach, welche Rolle dem Betroffenen in dem Prozess zukommt. Eine Datenübermittlung ist also sowohl bei einer Beteiligung als Beklagter als auch als Zeuge zulässig.[615]

IV. Lebenswichtige Interessen des Betroffenen

Die Wahrung lebenswichtiger Interessen des Betroffenen vermag in Entsprechung zu Artikel 7d) der Richtlinie ebenfalls eine grenzüberschreitende Datenübermittlung zu legitimieren. Damit soll gemäß der Begründung des geänderten Vorschlags zur Richtlinie die Weitergabe medizinischer Daten in solchen Fällen ermöglicht werden, in denen der Betroffene seinen Willen nicht äußern kann.[616]

Der Ausnahmetatbestand des Artikels 26 Absatz 1e) der Richtlinie ist sonach auf jene Fälle beschränkt, in denen keine Einwilligung von dem Betroffenen eingeholt zu werden vermag.[617] Vereinzelt wird dieser Ansicht zwar unter Hinweis auf den Umkehrschluss zu Artikel 8 Absatz 2c) der Richtlinie widersprochen, der eine äquivalente Regelung für die Verarbeitung sensibler Daten vorsieht und deren tatbestandliche Erfüllung ausdrücklich davon abhängig macht, dass der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, eine Einwilligung zu erteilen.[618] Da die lebenswichtigen Interessen des Betroffenen jedoch zu dessen eigener und grundsätzlich freien Disposition stehen, darf sein

---

[614] *Wuermeling*, Handelshemmnis Datenschutz, S. 149 f.; vgl. auch *Ellger*, CR 1993, S. 2, S. 8; *Gola/Schomerus*, BDSG, § 4c, Rn. 5, die dies jedenfalls nicht ausschließen.

[615] Grabitz/Hilf III (- *Brühann*), A 30, Art. 26, Rn. 9.

[616] *Begründung des geänderten Vorschlags*, abgedruckt in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 26, S. 283.

[617] Für den inhaltlich entsprechenden § 4c Absatz 1 Satz 1 Nr. 5 BDSG: *Abel*, Praxishandbuch, 8/4.4.3, S. 7; *ders.*, BDSG, S. 78; Simitis u. a. (- *Simitis*), BDSG, § 4c, Rn. 22; *Begründung der Bundesregierung zum Entwurf des Bundesdatenschutzgesetzes*, BT-Drs. 14/4329 vom 13.10.2000, S. 34 f.

[618] So *Wuermeling*, Handelshemmnis Datenschutz, S. 151.

Recht auf informationelle Selbstbestimmung nicht schlicht übergangen werden. Der Formulierung des Artikels 8 Absatz 2c) der Richtlinie kommt insoweit nur eine klarstellende Funktion zu und rechtfertigt keinen Umkehrschluss zu Artikel 26 Absatz 1e) der Richtlinie.[619]

Indessen kann die Frage, ob die personenbezogenen Daten des Betroffenen auch gegen dessen erklärten Willen übermittelt werden dürfen, nur im Rahmen eines konkreten Einzelfalls beantwortet werden. Unter der Berücksichtigung der Existentialität lebenswichtiger Interessen sind dabei die widerstreitenden Rechtsgüter des Betroffenen mit Blick auf etwaige staatliche Schutzpflichten miteinander abzuwägen.[620]

Infrage steht ferner, ob sich das Tatbestandsmerkmal der Lebenswichtigkeit auf die körperliche Integrität des Betroffenen reduziert oder ob ebenso andere existentiell bedeutsame Rechtsgüter von Belang sein können. Im Hinblick auf den mit Artikel 26 Absatz 1e) der Richtlinie wortgleichen Artikel 7d) führt Erwägungsgrund (31) aus, dass die Verarbeitung, also vorliegend die Übermittlung, dem Schutz eines „für das Leben der betroffenen Person wesentliche(n) Interesse(s)“ dienen muss. Sowohl diese Erläuterung als auch die englische und die französische Richtlinienversion, die von „vital interests“ beziehungsweise „l’intérêt vital“ sprechen, deuten auf einen über die gesundheitlichen Erfordernisse hinausgehenden Radius relevanter Interessen hin. Eine Begrenzung des Ausnahmetatbestandes auf Übermittlungen zur Erhaltung der körperlichen Integrität des Betroffenen ist sonach nicht zu begründen.[621]

Da es sich allerdings um ein „wesentliches Interesse“ des Betroffenen für sein Leben handeln muss, dürften Übermittlungen etwa aus finanziellen, eigentumsbezogenen oder familiären Gründen nur in Ausnahmefällen von dem Tatbestand des Artikels 26 Absatz 1e) der Richtlinie gedeckt sein.[622]

---

[619] *Draf*, S. 116.
[620] A. A. *Wuermeling*, Handelshemmnis Datenschutz, S. 152, der dafür plädiert, dass die informationelle Selbstbestimmung dem Betroffenen stets das Recht einräumt, eine Verarbeitung seiner Daten, die ausschließlich in seinem persönlichen Interesse steht, zu verhindern; so wohl auch *Abel*, BDSG, S. 79.
[621] *Wuermeling*, Handelshemmnis Datenschutz, S. 151; vgl. auch *Singleton*, 11 CL&P, S. 140, S. 142, die den inhaltsgleichen Tatbestand des Artikels 7d) der Richtlinie für sehr weitläufig und offen für Missbrauch hält; a. A. *Draf*, S. 115, der aus der Bezugnahme auf medizinische Daten in der Begründung des geänderten Richtlinienvorschlags schließt, dass nur das Rechtsgut „Leben“ geschützt sei.
[622] *WP 12*, S. 27.

V. Öffentliche Register

Die Zulässigkeit der Übermittlung von personenbezogenen Daten aus öffentlichen Registern soll verhindern, dass eine Einsichtnahme in ein Register, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, nur daran scheitert, dass der Einsichtsberechtigte seine Anfrage von einem Drittland aus stellt. Sofern also die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall vorliegen, dürfen personenbezogene Daten etwa aus Handelsregistern, Grundbüchern oder Schuldnerlisten in das außereuropäische Ausland übermittelt werden.[623]

Erwägungsgrund (58) der Richtlinie schränkt die Ausnahme jedoch insoweit ein, als dass nicht die Gesamtheit oder ganze Kategorien der in dem Register enthaltenen Daten übermittelt werden dürfen. Ist darüber hinaus ein Register ausschließlich zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, hat die Übermittlung nur auf Antrag dieser Personen oder nur dann zu erfolgen, wenn diese Personen die Adressaten der Übermittlung sind. Massenhafte Übermittlungen für kommerzielle Zwecke oder zur Erstellung von Persönlichkeitsprofilen scheiden dementsprechend aus.[624]

VI. Sonstige Ausnahmen: Die Betriebsvereinbarung

Einer Literaturmeinung zufolge vermöge auch eine Betriebsvereinbarung unabhängig von einer aufsichtsbehördlichen Genehmigung die Zulässigkeit eines Drittländertransfers zu begründen.[625] Das ergäbe sich einerseits aus Erwägungsgrund (9) der Richtlinie, dem gemäß den Mitgliedstaaten ein Spielraum im Rahmen der Durchführung der Richtlinie verbleibt, der von den Wirtschafts- und Sozialpartnern zur Verbesserung des durch die jeweiligen nationalen Rechtsvorschriften gewährleisteten Schutzes genutzt werden darf. Andererseits erlaube Erwägungsgrund (22) den Mitgliedstaaten eine Präzisierung und eine bereichsspezifische Gestaltung der Rechtmäßigkeitsvoraussetzungen einer Verarbeitung und somit auch der Übermittlungsvorschriften.

---

[623] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 26, Rn. 11.
[624] *WP 12*, S. 27.
[625] So *Eul/Godefroid*, RDV 1998, S. 185, S. 189.

Sofern eine Betriebsvereinbarung, etwa als andere Rechtsvorschrift im Sinne des § 4 Absatz 1 BDSG, die Ausnahmetatbestände des Artikels 26 Absatz 1 der Richtlinie inhaltlich präzisiert und die Zulässigkeit der erforderlichen Übermittlungen in diesem Rahmen für den konkreten Betrieb spezifiziert, kommt sie durchaus als Grundlage für eine grenzüberschreitende Datenübermittlung in Betracht. Sie verließe jedoch den von dem Harmonisierungsgedanken und dem Schutz der Grundrechte und Grundfreiheiten des Betroffenen, insbesondere seiner Privatsphäre gefassten Rahmen, sofern sie über die Tatbestände des Artikels 26 Absatz 1 der Richtlinie hinausginge.

Das ergibt sich einerseits aus dem Wortlaut der Erwägungsgründe (9) und (22), die sich ausdrücklich nur auf die Gestaltung der allgemeinen Bedingungen der Rechtmäßigkeit aus Kapitel II und nicht auf die Vorschriften über den Drittländertransfer aus Kapitel IV der Richtlinie beziehen. Im Interesse einer gewissen Undurchlässigkeit des europäischen Datenschutzsystems[626] sind letztere danach nur insoweit der einzelstaatlichen Ausgestaltung zugänglich, als dass sie eine ausdrückliche Ermächtigung zu einer Ausnahme enthalten. In diesem Sinne spricht Artikel 26 Absatz 1 der Richtlinie die Mitgliedstaaten zwar von der Verpflichtung frei, alle seine Tatbestände vollständig in nationales Recht umzusetzen. Das Hinzufügen weiterer Ausnahmen ist jedoch nicht vorgesehen.

Eine zusätzliche Abweichung von dem Übermittlungsverbot in Drittländer liefe auch dem Schutzbedürfnis des Betroffenen zuwider, das eine abschließende und restriktive Auslegung des Artikels 26 Absatz 1 der Richtlinie erfordert. Während außerdem der Erwägungsgrund (9) der Richtlinie die Mitgliedstaaten zu einer Verbesserung des nationalen Schutzniveaus bei ihrer Ausgestaltung der allgemeinen Rechtmäßigkeitsbedingungen anhielte, würde eine weitere Öffnungsklausel die Rechtsposition des Betroffenen bei einem Drittländertransfer im Widerspruch zu Artikel 1 Absatz 1 der Richtlinie erheblich schwächen. Eine Betriebsvereinbarung kann einen Drittländertransfer somit außerhalb der Tatbestände des Artikels 26 Absatz 1 der Richtlinie nicht legitimieren.

Zu überlegen ist indessen, ob die Betriebsvereinbarung eine Einwilligung des Betroffenen im Sinne des Artikels 26 Absatz 1a) der Richtlinie zu ersetzen vermag. Dem steht jedoch der individuelle Charakter

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

einer Einwilligung als Ausdruck des allgemeinen Persönlichkeitsrechts des Betroffenen entgegen. Danach muss der Betroffene als Souverän seiner Daten selbst entscheiden können, ob er seine personenbezogenen Informationen zur Disposition stellt. Die Einschränkung der freien Entscheidung des Arbeitnehmers durch die Betriebspartner widerspräche ferner dem § 75 Absatz 2 Betriebsverfassungsgesetz, der letztere mit dem Schutz und der Förderung der freien Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer betraut.

Da Betriebsvereinbarungen regelmäßig keine Geltung in außereuropäischen Unternehmensteilen entfalten, vermögen sie folglich auch darüber hinaus keine eigenständige Bedeutung im Rahmen der Vorschriften über den Drittländertransfer zu erlangen. [627]

[627] Davon auch ausgehend *o.V.*, RDV 2003, S. 102, S. 105.

E. Der Artikel 26 Absatz 2 der Richtlinie

Sofern weder das Schutzniveau in dem betreffenden Drittland den Erfordernissen der Angemessenheit im Sinne des Artikels 25 Absatz 2 der Richtlinie genügt noch einer der Ausnahmetatbestände des Artikels 26 Absatz 1 der Richtlinie vorliegt, räumt der Artikel 26 Absatz 2 der Richtlinie den Mitgliedstaaten die Möglichkeit zu einer Genehmigung einer Übermittlung oder einer Kategorie von Übermittlungen personenbezogener Daten ein. Voraussetzung ist allerdings, dass „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".

Der für die Verarbeitung Verantwortliche hat sich also in geeigneter Weise für eine Kompensation der fehlenden Elemente zu einem angemessenen Schutzniveau in dem betreffenden Drittland zu verbürgen. Dementsprechend müssen die darzubringenden Garantien im Hinblick auf die genehmigungsfähigen Übermittlungen ebenfalls einen angemessenen Schutz gewährleisten.[628]

Als Instrumente zur Bereitstellung angemessener Garantien nennt der Artikel 26 Absatz 2 der Richtlinie beispielhaft Vertragsklauseln, mit denen sich der Datenempfänger gegenüber dem Datenübermittler zur Einhaltung der Grundsätze eines angemessenen Schutzniveaus im Sinne der Richtlinie 95/46/EG verpflichtet.

Darüber hinaus kommen jedoch auch weitere Mittel in Betracht, von denen derzeit allerdings nur verbindliche Unternehmensrichtlinien, so genannte Codes of Conduct, als echte Alternative zur Vertragslösung diskutiert werden.

I. Die Vertragslösung

Gemäß Artikel 26 Absatz 2, 2. Halbsatz, der Richtlinie können sich die ausreichenden Garantien insbesondere aus Vertragsklauseln ergeben. Damit verweist der Richtliniengeber auf ein Instrument, das bereits im Vorfeld der Richtlinie 95/46/EG zum Export des nationalen Datenschutzstandards entwickelt worden war.

---

[628] *WP 12*, S. 17 f.; so bereits in *WP 9*, S. 4, und S. 12; vgl. auch Gliederungspunkt C.II.2.b.(4).(a). dieses Kapitels, m. w. N.

Die Mitgliedstaaten genehmigen zwar nicht den Vertrag an sich, sondern die auf seiner Grundlage stattfindenden Übermittlungen, sodass die zu erbringenden Garantien der verantwortlichen Stelle auf den konkreten Einzelfall abgestimmt sein müssen. Da der Ausgleich fehlender kodifizierter Datenschutzbestimmungen jedoch häufig eine ähnliche Vorgehensweise verlangt, lassen sich dennoch insgesamt die wesentlichen Charakteristika hinreichender Vertragsklauseln ausmachen.

Die diesen Voraussetzungen entsprechenden vertraglichen Garantien können entweder individuell ausgehandelt werden oder sich der seitens der Europäischen Kommission gemäß Artikel 26 Absatz 4 der Richtlinie für ausreichend befundenen Standardvertragsklauseln bedienen.

1. Die Zeit vor der Richtlinie 95/46/EG

Da die Gewährleistung datenschutzrechtlicher Garantien auf vertraglichem Wege in Europa kein Novum ist, vermögen sich die Vertragsentwürfe im Rahmen des Artikels 26 Absatz 2 und Absatz 4 der Richtlinie an einer gewissen praktischen Erfahrung einiger Mitgliedstaaten sowie an einer bereits im Vorfeld der Richtlinie 95/46/EG geführten Kontroverse über die Zulässigkeit von Vertragsklauseln im Rahmen des grenzüberschreitenden Datenverkehrs zu orientieren.

a. Vertragliche Ansätze im Vorfeld der Richtlinie

Schon vor Erlass der Richtlinie 95/46/EG waren insbesondere in Schweden, Österreich und Frankreich[629] privatrechtliche Vereinbarungen zwischen dem Datenübermittler und dem Datenempfänger zur Sicherung des nationalen Datenschutzniveaus bei einer Übermittlung personenbezogener Daten in Drittländer, zu denen seinerzeit mangels der innergemeinschaftlichen Harmonisierung des Datenschutzniveaus auch noch die übrigen Mitgliedstaaten zählten, durchaus üblich.

Während die beiden erstgenannten Länder sich derartiger Verträge vor allem bei der Vergabe von Auftragsverarbeitungen in das Ausland bedienten,[630] wurden in Frankreich privatautonome Vereinbarungen zur Herstellung eines angemessenen Schutzniveaus bei dem Datenempfänger seit den späten achtziger Jahren auch im Rahmen von Funktions-

[629] Vgl. dazu die Beispiele bei *Vassilaki*, 9 CLSR, S. 33 f.
[630] *Ellger*, RabelsZ 60, S. 738, S. 745.

übertragungen genutzt. So machte die französische Datenschutzbehörde (CNIL) zum Beispiel die Zulässigkeit einer konzerninternen Übermittlung von Mitarbeiterdaten im so genannten „Fiat"-Fall mangels einer Datenschutzgesetzgebung in Italien davon abhängig, dass sich die italienische Fiat-Konzernmutter gegenüber der übermittelnden französischen Tochter dazu verpflichtete, bei der Verarbeitung der übermittelten Daten die Grundsätze der Europaratskonvention Nr. 108 einzuhalten.[631]

Sich des aus diesen Vereinbarungen herauskristallisierenden allgemeinen Bedürfnisses nach einer Absicherung des jeweiligen nationalen Datenschutzniveaus im Rahmen grenzüberschreitender Datenübermittlungen gewahr, legte der Beratende Ausschuss des Europarates schließlich im Jahr 1992 unterstützend ein sich ebenfalls an die Schutzbestimmungen der Europaratskonvention Nr. 108 anlehnendes Mustervertragswerk für den internationalen Datenverkehr vor, das in einer gemeinsamen Studie des Europarates, der Europäischen Kommission und der Internationalen Handelskammer erarbeitet worden war.[632]

Auch in Deutschland fanden privatrechtliche Verträge zur Gewährleistung eines dem Bundesdatenschutzgesetz gleichwertigen Schutzstandards in Drittländern im Rahmen von grenzüberschreitenden Datenübermittlungen Anwendung.[633] Zwar reglementierte das frühere BDSG den Drittländertransfer privater Stellen nicht ausdrücklich. Es war jedoch allgemein anerkannt, dass eine Übermittlung in ein unsicheres Drittland den „schutzwürdigen Interessen" des Betroffenen im Sinne der Erlaubnistatbestände des § 28 Absatz 1 BDSG a. F. zuwiderliefe.

Als Hilfestellung für die infolgedessen verpflichteten Unternehmen hatte der so genannte „Düsseldorfer Kreis", ein informelles Gremium zum Austausch von Erfahrungen zwischen den deutschen Datenschutzbehörden und zur Koordination einer bundeseinheitlichen Rechtsanwendung,[634] im Jahr 1994 sogar eine „Checkliste"[635] für den erforderlichen Inhalt vertraglicher Bestimmungen herausgegeben.

---

[631] Décision 89-78 du 11 Juillet 1989, Dixième Rapport (1990), p. 32.
[632] *Europarat*, Mustervertrag zur Sicherstellung des gleichwertigen Datenschutzes im Zusammenhang mit grenzüberschreitendem Datenverkehr mit erläuterndem Memorandum vom Beratungsausschuss des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ETS 108) angenommen am 02. November 1992, abgedruckt in: CR 1993, S. 64.
[633] Vgl. dazu die Beispiele bei *Vassilaki*, 9 CLSR, S. 33, S. 35.
[634] *Bizer*, DuD 2003, S. 2.
[635] *Düsseldorfer Kreis*, DSB 1994, S. 10.

Das wohl prominenteste Beispiel für eine vertragliche Absicherung eines datenschutzrechtlichen Standards bei einer grenzüberschreitenden Datenübermittlung im Vorfeld der Umsetzung der Richtlinie 95/46/EG liefert indessen der unter der Anleitung des Berliner Datenschutzbeauftragten im Jahr 1996 zustande gekommene Vertrag zwischen der Deutschen Bahn AG und jenen Citibank-Unternehmen in Deutschland und in den USA, die an der Ausgabe aller mit einer Zahlungsfunktion ausgestatteten „BahnCard"-Varianten beteiligt sind.[636] In dieser für die Gestaltung von Verträgen im Rahmen des Artikels 26 Absatz 2 der Richtlinie wegweisenden Vereinbarung haben sich die Rechenzentren der Citibank in den USA, die mit der Herstellung der „BahnCard" und der dazu notwendigen Datenverarbeitung beauftragt sind, gegenüber den deutschen Stellen auf den Standard des Bundesdatenschutzgesetzes verpflichtet und einer diesem entsprechenden, seitens der US-amerikanischen Bankaufsichtsbehörden geduldeten Kontrolle durch den Berliner Datenschutzbeauftragten zugestimmt.

b. Die wesentliche Kritik an der Zulässigkeit einer Vertragslösung

Die Effektivität und somit auch die Zulässigkeit von Datenschutzverträgen zwischen dem Datenübermittler und dem Datenempfänger mit dem Ziel des Ausgleichs fehlender kodifizierter Datenschutzbestimmungen wurde allerdings von Anfang an stark angezweifelt.[637]

Ein Teil der Literatur lehnte die Vertragslösung gänzlich ab, da der Betroffene nicht Vertragspartei sei und daher nicht die Gestaltung und die Einhaltung der Vereinbarung beeinflussen könne.[638] Außerdem erweise sich eine wirksame Kontrolle als ungewiss, da die Befugnisse der Aufsichtsbehörden des exportierenden Staates an den nationalen Grenzen

---

[636] Die ausführliche Sachverhaltsdarstellung sowie die Vertragsklauseln sind auf der Website des *Berliner Datenschutzbeauftragten* abrufbar
(Sachverhalt: www.datenschutz-berlin.de/jahresbe/95/3a.htm;
Vertragsklauseln: www.datenschutz-berlin.de/doc/int/konf/18/intdp_de.htm).

[637] Vgl. zum Meinungsstand z. B. *Auernhammer*, § 28, Rn. 48 f.; Däubler/Klebe/Wedde (- *Däubler*), Einleitung, Rn. 200; *Ellger*, RabelsZ 60, S. 438, S. 745 ff., m. w. N.; *Ellger/Geis*, CR 1996, S. 574, S. 576; *Geis*, NJW 1997, S. 288 f.; *Knauth*, WM 1990, S. 209, S. 211; *Koch*, RDV 1991, S. 105, S. 111; *Lütkemeier*, DuD 1995, S. 597, S. 601; *Riemann*, CR 1997, S. 762 m. w. N.; *Schwartz*, 80 Iowa L. Rev., S. 471, S. 476 f.; *Ulbricht*, CR 1990, S. 602, S. 606 f.; Kilian/Heussen (- *Weichert*), Nr. 132, Rn. 122; *Wohlgemuth*, BB 1996, S. 690, S. 694; *ders.*, Rn. 260; *ders.*, BB 1991, S. 340, S. 342.

[638] So z. B. *Bergmann*, S. 220; *Ellger*, RDV 1991, S. 121, S. 133; *Reidenberg*, 80 Iowa L. Rev., S. 497, S. 546.

endeten.[639] Davon abgesehen sei der Destinationsstaat selbst nicht an die vertragliche Vereinbarung gebunden, sodass die Gefahr eines jederzeitigen hoheitlichen Zugriffs auf die übermittelten Daten bestünde.[640] Vereinzelt wurden auch völkerrechtliche Bedenken gegen die Vertragslösung geäußert, da dem Destinationsland letztlich mittels eines „vertraglichen Kunstgriffs“[641] die datenschutzrechtliche Kontrolle durch den exportierenden Staat aufgedrängt würde.

Angesichts der ausdrücklichen Aufnahme der Vertragslösung in die Richtlinie 95/46/EG haben sich diese Argumente im Hinblick auf die Frage einer generellen Zulässigkeit der Vertragslösung zwar erledigt. Die sich aus ihnen ergebenden Hinweise auf potentielle Schwächen einer privatautonomen Vereinbarung zur Sicherung eines angemessenen Datenschutzniveaus finden indessen Berücksichtigung bei der Feststellung der Angemessenheit im konkreten Einzelfall und prägen daher die wesentlichen Charakteristika ausreichender vertraglicher Garantien.

2. Die wesentlichen Charakteristika ausreichender vertraglicher Garantien

Die Hauptaufgabe der von dem für die Verarbeitung Verantwortlichen beigebrachten Garantien besteht darin, die jeweils fehlenden Elemente eines angemessenen Schutzniveaus auszugleichen. Der Vertrag muss also entsprechend den bereits dargestellten Kriterien der Angemessenheit[642] einerseits den Datenempfänger in dem Drittland auf die inhaltlichen Grundsätze eines angemessenen Schutzniveaus verpflichten und andererseits die Durchsetzung seiner Bestimmungen sicherstellen.

a. Die Gewährleistung der inhaltlichen Grundsätze

Die Gewährleistung der inhaltlichen Grundsätze bereitet insoweit keine Probleme, als dass die Prinzipien eines angemessenen Schutzniveaus lediglich in den Vertragstext aufgenommen werden müssen.

Zu beachten ist allerdings, dass es im Rahmen einer nur vertraglichen Abmachung an einem Gesetz oder einem anderweitigen Kodex fehlt,

---

[639] So z. B. *Bergmann*, S. 220; *Ehmann*, CR 1991, S. 234, S. 235; *Geis*, NJW 1997, S. 288, S. 289; *Koch*, S. 335; *Lütkemeier*, DuD 1995, S. 597, S. 601.
[640] So z. B. *Ellger/Geis*, CR 1996, S. 574, S. 576; *Simitis*, CR 1991, S. 161, S. 177; *ders.*, RDV 1990, S. 3, S. 12; *Wohlgemuth*, BB 1992, S. 281, S. 284.
[641] *Ehmann*, CR 1991, S. 234, S. 235; *Ulbricht*, CR 1990, S. 602, S. 607.
[642] Vgl. Gliederungspunkt C.II.1. dieses Kapitels.

der die Art und Weise vorgibt, in welcher die jeweiligen Bestimmungen durchzuführen sind. Die Vielfalt der sich daraus möglicherweise ergebenden Interpretationsmöglichkeiten der Vertragsklauseln sowie der damit einhergehende Verarbeitungsspielraum des Datenempfängers können zuweilen dem Interesse der Rechtssicherheit des Betroffenen zuwiderlaufen.[643] Deshalb ist die Anwendung der allgemein formulierten Verarbeitungsgrundsätze detailliert zu spezifizieren,[644] indem zum Beispiel die Verarbeitungszwecke oder die zu verarbeitenden Datenkategorien konkret benannt werden. Auch können sich eine exakte Begrenzung der Speicherzeit oder eine genaue Beschreibung der Sicherheitsmaßnahmen als erforderlich erweisen.[645]

Dagegen ist nicht zu befürchten, dass sich die fehlende Beteiligung des Betroffenen an der Gestaltung des Vertrages negativ auszuwirken vermag. Zwar ist es dem Betroffenen unter diesen Umständen nicht möglich, die Berücksichtigung seiner schutzwürdigen Interessen einzufordern. Ein wesentlicher Nachteil sollte sich daraus jedoch nicht ergeben, da einerseits das Kriterium der Angemessenheit den Vertragsparteien keinen Beurteilungsspielraum zuerkennt und andererseits der jeweilige Mitgliedstaat die tatsächliche Angemessenheit der gebotenen Garantien im Rahmen des Genehmigungsverfahrens der Übermittlung vollständig zu überprüfen hat. Aus denselben Erwägungen ist im Übrigen auch keine einseitige Modifikation der Vertragsklauseln zulasten des Betroffenen durch die Vertragsparteien zu besorgen.

b. Das Verfahren der Durchsetzung

Die eigentliche Herausforderung einer vertraglichen Lösung besteht indessen in der Gestaltung eines effektiven Durchsetzungsmechanismus.

Zum einen gilt es einen Ausgleich dafür zu schaffen, dass der Betroffene selbst nicht Vertragspartei ist und ihm daher nicht automatisch ein Anspruch auf Durchsetzung seiner sich aus dem Vertrag ergebenden Rechte zusteht. Zum anderen ist dem Umstand Rechnung zu tragen, dass der Datenempfänger in dem Drittland in kein allgemeines Datenschutzsystem eingebunden ist, dessen Aufsicht und Durchsetzung einer allen Teilnehmern beziehungsweise Adressaten der materiellen Bestimmungen übergeordneten Stelle obliegt.[646]

[643] *WP 12*, S. 18; so bereits in *WP 9*, S. 7.
[644] *WP 12*, S. 18; so bereits in *WP 9*, S. 6.
[645] *WP 12*, S. 18; *WP 9*, S. 6.
[646] *WP 12*, S. 19; so bereits in *WP 9*, S. 6.

Fraglich ist daher, wie eine privatautonome Vereinbarung eine gute Befolgungsrate, die Unterstützung des Betroffenen bei der Wahrnehmung seiner Rechte sowie ein angemessenes Entschädigungsverfahren garantieren kann.

(1) Befolgungsrate

Eine gute Befolgungsrate von Vertragsklauseln ermittelt sich entsprechend den bisherigen Erläuterungen[647] hauptsächlich aus ihrer Bekanntheit bei den Beteiligten, aus der Verbindlichkeit eines regelmäßigen externen Kontrollverfahrens sowie aus der Androhung abschreckender Strafmaßnahmen.

Die Bekanntheit der vertraglichen Bestimmungen bei den Übermittlungsparteien ist bereits durch die freiwillige Verpflichtung im Rahmen des Vertragsabschlusses indiziert. Mit dem Ziel einer Anpassung der internen Arbeitsprozesse sollte sich der Datenimporteur außerdem zu einer Unterrichtung und Instruktion seiner Mitarbeiter verpflichten. Je nach Art und Dauer der Auswirkungen eines Übermittlungsvertrages auf die internen Vorgänge können die zu treffenden Maßnahmen zwischen gezielten Einzelanweisungen und allgemeinen Schulungen variieren.

Die Transparenz gegenüber dem Betroffenen ist bereits durch die Informationspflicht gewahrt. Darüber hinaus vermag sie mittels einer Veröffentlichung der Vertragsbestimmungen gefördert zu werden.

Eine wirkungsvolle externe Kontrolle ist gewährleistet, indem der Datenempfänger verbindlich die Durchführung eines Audits durch ein zuständiges Gremium oder ein spezialisiertes Wirtschaftsprüfungsunternehmen[648] verspricht.[649] Ebenfalls denkbar wäre, dass dem Datenübermittler selbst die Gelegenheit zu einer regelmäßigen Kontrolle der Datenverarbeitungseinrichtungen des Datenempfängers eingeräumt wird.[650]

---

[647] Vgl. dazu die Gliederungspunkte C.II.1.c. und C.II.2.b.(2).(b). dieses Kapitels.
[648] *WP 12*, S. 21; so bereits in *WP 9*, S. 10; *Draf*, S. 142. So für die Zukunft im „BahnCard"-Fall vereinbart – allerdings dort in Vertretung für den zuständigen Berliner Datenschutzbeauftragten.
[649] *Reidenberg*, 80 Iowa L. Rev., S. 497, S. 548; *Simitis*, CR 2000, S. 472, S. 481; *ders*. in: Datenverkehr ohne Datenschutz?, S. 177, S. 216.
[650] *Giesen*, DuD 1996, S. 394, S. 396.

Eine Selbstkontrolle vermag indessen nur zu genügen, sofern die Parteien für den Fall eines Vertragsverstoßes abschreckende Sanktionen androhen. Die Effektivität von Strafmaßnahmen, etwa einer Vertragsstrafe,[651] erweist sich allerdings auf vertraglicher Ebene als äußerst ungewiss, da ihre Durchsetzung von der Bereitschaft des Datenübermittlers zum Tätigwerden abhängt. Dessen ungeachtet könnte sich der Datenübermittler zur Forcierung einer ordnungsgemäßen Durchführung der Vereinbarung angehalten fühlen, sofern er mit einer gesamtschuldnerischen Haftung für Verstöße des Datenempfängers belastet würde.[652]

Über die rein vertragliche Haftung hinaus sind bei der Bewertung der Befolgungsrate ebenfalls jene Instrumente zu berücksichtigen, welche die Rechtsordnung des jeweiligen Empfängerstaates bereitstellt. So ist im Hinblick auf die USA zum Beispiel auf die Befugnisse der Federal Trade Commission gemäß dem Abschnitt 5 des Federal Trade Commission Act hinzuweisen.[653] Ferner vermag die Option zur Erhebung einer Schadensersatzklage im Rahmen des Common Law (Restatement (Second) – Torts), zum Beispiel wegen einer Falschdarstellung gegenüber dem Datenübermittler, den Druck zur Befolgung des Vertrages zu erhöhen.[654]

(2) Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte

Die Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte erweist sich in zweierlei Hinsicht als problematisch. Einerseits ist der Betroffene nicht Vertragspartei, sodass er nicht zwangsläufig seine vertraglich zugesicherten Rechte auch durchzusetzen vermag. Andererseits steht ihm unter Umständen keine unabhängige Beschwerdeinstanz zur Verfügung, da die Befugnisse der mitgliedstaatlichen Kontrollbehörden entsprechend dem völkerrechtlichen Prinzip der Staatensouveränität an den jeweiligen Staatsgrenzen enden.

---

[651] Z. B. noch in der „Checkliste“ des *Düsseldorfer Kreises*, DSB 1994, S. 10, S. 11.
[652] Vgl. z. B. *Napier*, RDV 1990, S. 209, S. 217, der den Datenübermittler mithilfe einer unmittelbaren Haftung zum Garanten für die Einhaltung der Vorschriften durch den Datenempfänger machen will.
[653] Vgl. dazu Gliederungspunkt C.III.2.c.(7).(a).cc. dieses Kapitels.
[654] Vgl. dazu die Gliederungspunkte C.III.1.d. und C.III.2.c.(7).(b).cc. dieses Kapitels.

(a) Die Rechte des Betroffenen

Der Betroffene ist grundsätzlich nur dann zur Geltendmachung seiner Rechte imstande, wenn diese ebenfalls in dem Vertrag zwischen dem Datenübermittler und dem Datenempfänger niedergelegt sind. Allerdings schreiben einige Rechtsordnungen eine strikte Bindung an den Grundsatz der Relativität eines Vertragsverhältnisses vor und lassen sonach keine vertragliche Begründung von Rechten Dritter zu.[655] Der Betroffene könnte also je nach geltendem Vertragsrecht daran gehindert sein, seine vertraglich festgelegten Ansprüche auf dem Rechtsweg einzufordern.

Für die Feststellung ausreichender Garantien kommt es demnach ganz wesentlich darauf an, welches Recht auf den Vertrag anzuwenden ist. Im Zweifel wird es sich dabei um das Recht desjenigen Mitgliedstaates handeln, in dem der Datenübermittler ansässig ist.

Da seit geraumer Zeit alle Mitgliedstaaten die Rechtsfigur des Vertrages zugunsten Dritter kennen,[656] tauchen diesbezügliche Probleme inzwischen nur noch auf, sofern das Recht des Destinationsstaates die vertragliche Begründung von Rechten Dritter ausschließt und eine große Wahrscheinlichkeit dafür besteht, dass die Gerichte dieses Staates aufgrund des dort geltenden Internationalen Privatrechts das eigene Vertragsrecht für vorrangig halten. In solchen Fällen sind die im Rahmen eines angemessenen Schutzniveaus vorausgesetzten Rechte des Betroffenen mithin anderweitig zu garantieren.

In Betracht kommt zum Beispiel ein Belassen der Verantwortlichkeit für die Verarbeitung bei dem in der Europäischen Union ansässigen Datenübermittler.[657] Das jeweilige mitgliedstaatliche Datenschutzgesetz bliebe folglich entsprechend dem Artikel 4 Absatz 1 der Richtlinie anwendbar, sodass der Betroffene auf dieser gesetzlichen Grundlage den Datenübermittler ebenfalls für die Verstöße des Datenempfängers gegen die einschlägigen Datenschutzbestimmungen zur Rechenschaft ziehen könnte.

---

[655] Insbesondere die vom Common Law geprägten Rechtsordnungen orientieren sich an der „privity of contract"-Doktrin, mit Ausnahme u. a. von Großbritannien, das inzwischen den Contracts (Rights of Third Parties) Act 1999, 1999 Chapter c.31, erlassen hat, und den USA, die einen „Third Party Beneficiary Claim" kennen.

[656] *WP 74*, S. 12, Fn. 12; vgl. aber *WP 12*, S. 19, und bereits *WP 9*, S. 7, die noch nicht von dieser Voraussetzung ausgehen konnten.

[657] *WP 12*, S. 19 f.; so bereits in *WP 9*, S. 7.

Das setzt jedoch im Einzelfall voraus, dass der in der Europäischen Union niedergelassene Datenübermittler entsprechend der Legaldefinition des „für die Verarbeitung Verantwortliche(n)“ in Artikel 2d) der Richtlinie weiterhin über die Zwecke und die Mittel der Verarbeitung zu entscheiden befugt ist. Eine derartig einschränkende Bindung des Datenempfängers an die von dem Datenübermittler festgelegten Verarbeitungsmodalitäten dürfte wohl nur im Rahmen einer Auftragsverarbeitung infrage kommen.

Der Erwerb der Daten für eigene Zwecke ist indessen regelmäßig mit einem Verantwortungsübergang auf den Datenempfänger verbunden. Da das Recht des Exportstaates sonach auf die in dem Drittland durchgeführten Verarbeitungen keine Anwendung mehr findet, müssen hier andere Mechanismen zur Stärkung der Position des Betroffenen geschaffen werden. Die dafür zur Verfügung stehenden Mittel scheinen jedoch eher begrenzt.

So ist im Grunde nur an eine von einem Weitergabeverbot gestützte absolute Bindung des Datenempfängers an den Übermittlungszweck zu denken, und zwar über das Maß der bloßen Unvereinbarkeit mit diesem Zweck hinaus. Eine derartige Konstruktion würde indessen nicht über die fehlende Möglichkeit des Betroffenen zur Durchsetzung seiner Rechte hinweghelfen.

Sofern also die tatsächliche Durchsetzung der vertraglich begründeten Rechte Dritter nicht zu gewährleisten ist, sollte sich die Zulässigkeit einer auf vertraglichen Garantien basierenden grenzüberschreitenden Datenübermittlung in unsichere Drittländer auf die Auftragsverarbeitung beschränken.[658]

Eine Datenübermittlung in die USA dürfte indessen derartige Probleme nicht aufwerfen, da der Betroffene selbst bei Anwendbarkeit des US-Rechts auf den Vertrag zwischen den Übermittlungsparteien seine ver-

[658] Vgl. *Ellger*, RabelsZ 60, S. 738, S. 766 f., der die Zulässigkeit der Vertragslösung allerdings auch deswegen auf die Auftragsverarbeitung beschränken will, weil nur dann auch der Datenübermittler ein Interesse an einer Beachtung der Datenschutzbestimmungen durch den Datenempfänger habe und diese durchsetzen werde; *ders.*, CR 1993, S. 2, S. 10; dem folgend *Draf*, S. 143.

traglich begründeten Rechte im Wege eines „Third Party Beneficiary Claim“ gerichtlich geltend machen könnte.[659]

(b) Unabhängige Beschwerdestelle

Unsicher ist ferner die Gewährleistung eines effektiven Beschwerdeverfahrens,[660] da die mitgliedstaatlichen Kontrollbefugnisse jenseits der eigenen Staatsgrenzen keine Wirkung entfalten. Existiert zudem keine anderweitige völkerrechtliche Grundlage für Eingriffe der mitgliedstaatlichen Kontrollbehörden, etwa in Form eines Verwaltungsabkommens oder der Einwilligung des Destinationsstaates,[661] und ist auch der Datenempfänger in seinem Sitzland keinem System unabhängiger Aufsicht unterworfen, besteht für den Betroffenen im Grunde keine Möglichkeit, um sich mit einer Eingabe an eine unabhängige, mit Ermittlungsbefugnissen gegenüber dem Datenverarbeiter ausgestatteten Stelle zu wenden.

Die im Rahmen einer Vertragslösung offerierten Garantien können infolgedessen nur unter der Bedingung für ausreichend erachtet werden, dass sich der Datenempfänger entweder unmittelbar in dem Übermittlungsvertrag oder mittels einer direkten Verpflichtungserklärung gegenüber der jeweiligen mitgliedstaatlichen Kontrollbehörde zur Hinnahme aufsichtsbehördlicher Eingriffe sowohl durch die Behörde selbst als auch durch von dieser beauftragten, akkreditierte Auditoren[662] verpflichtet.[663]

Um einer Umgehung des völkerrechtlichen Prinzips der Staatensouveränität durch privatrechtliche Absprachen vorzubeugen,[664] sollte sich

---

[659] Vgl. aber *Däubler* in: Datenverkehr ohne Datenschutz?, S. 71, S. 86; *ders.*, CR 1999, S. 49, S. 55, der davon ausgeht, dass sich ein außereuropäisches Gericht möglicherweise an den gesamten Vertrag nicht gebunden fühlen könnte.

[660] Vgl. zu den Voraussetzungen eines effektiven Beschwerdeverfahrens Gliederungspunkt C.II.1.c. dieses Kapitels.

[661] *Däubler* in: Datenverkehr ohne Datenschutz?, S. 71, S. 83; *ders.*, CR 1999, S. 49, S. 54; Simitis u. a. (- *Simitis*), BDSG, § 4c, Rn. 44. Vgl. auch den „BahnCard“-Fall, in dem der Berliner Datenschutzbeauftragte bei der Gestaltung des Vertrages mit den US-amerikanischen Bankaufsichtsbehörden zusammengearbeitet hat (vgl. Gliederungspunkt E.I.1.a. dieses Kapitels).

[662] *Draf*, S. 142 f.

[663] *WP 12*, S. 21 f.; so bereits in *WP 9*, S. 9; *Simitis*, CR 2000, S. 472, S. 481; *ders.* in: Datenverkehr ohne Datenschutz?, S. 177, S. 215.

[664] *Däubler*, CR 1999, S. 49, S. 54; *ders.*, RDV 1998, S. 96, S. 98; *Ehmann*, CR 1991, S. 234, S. 235; *Ellger*, RabelsZ 60, S. 738, S. 762; *Giesen*, DuD 1996, S. 394, S. 396; *Simitis*, CR 2000, S. 472, S. 481; *ders.* in: Datenverkehr ohne Datenschutz?, S. 177, S. 215 f.; *ders.*, RDV 1990, S. 3, S. 12; *Ulbricht*, CR 1990, S. 602, S. 606 ff.

der Datenempfänger jedoch vorher des Einverständnisses der Staatshoheit seines Sitzlandes in seine Unterwerfung unter die Befugnisse der mitgliedstaatlichen Datenschutzaufsicht versichern.[665]

Alternativ könnten die Parteien auch einen unabhängigen Schiedsrichter in den Vertragsbestimmungen benennen, dem neben seiner Entscheidungsbefugnisse auch Ermittlungen bei Verdacht eines Vertragsverstoßes erlaubt sein müssten.[666]

Darüber hinaus scheint eine Verpflichtung der Parteien zu einer unbedingten Schlichtung für den Fall erforderlich, dass der Betroffene die ordnungsgemäße Erfüllung des Vertrages anzweifelt.[667] Diese Aufgabe könnte zum Beispiel von einer bereits existierenden, unabhängigen Schiedsstelle oder, mit Blick auf die Rechtsweggarantie des Artikels 22 der Richtlinie, von einem mitgliedstaatlichen Gericht wahrgenommen werden.

(3) Entschädigung des Betroffenen

Die Gewährleistung von Entschädigungen für den Betroffenen hängt ebenfalls von der Möglichkeit zur Begründung seiner Rechte in dem Vertrag zwischen den Übermittlungsparteien ab.

Um darüber hinaus die tatsächliche Erfüllung eines Anspruchs zu gewährleisten, sollte sich der Datenübermittler möglichst unmittelbar gegenüber dem Betroffenen vertraglich zur Haftung für solche Schäden und Notfälle verpflichten, die infolge eines Verstoßes des Datenempfängers gegen die Kernprinzipien des Datenschutzes entstehen.[668] Der Datenübermittler wäre dadurch zwar mit dem Risiko der Durchsetzung seiner Regressansprüche gegenüber dem Datenempfänger belastet. Andererseits obliegt es aber seiner privatautonomen Entscheidung, sich einen besonders zuverlässigen Vertragspartner auszuwählen. Eine diesbezügliche Sorgfalt würde sich sogar im Zweifel auch positiv auf die Befolgungsrate der Vertragsklauseln auswirken.

---

[665] Diese Bedenken wurden von der Art. 29-Gruppe ausweislich ihrer Arbeitsdokumente (*WP 12*, S. 21 f.; so bereits in *WP 9*, S. 9) bei ihrem diesbezüglichen Vorschlag offensichtlich nicht in Betracht gezogen.

[666] *Napier*, RDV 1990, S. 209, S. 218.

[667] *Napier*, RDV 1990, S. 209, S. 217; *WP 12*, S. 20; so bereits in *WP 9*, S. 8.

[668] *WP 12*, S. 20; so bereits in *WP 9*, S. 8; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 26, Rn. 19, und *Reidenberg*, 80 Iowa L. Rev., S. 497, S. 547.

(4) Eingriffsbefugnisse des Destinationsstaates

Bei der Bewertung der von dem für die Verarbeitung Verantwortlichen angebotenen Garantien zur Durchsetzung der Vertragsklauseln darf indessen nicht außer Acht gelassen werden, dass der Destinationsstaat selbst nicht an die vertragliche Vereinbarung gebunden ist, sodass möglicherweise die Gefahr eines jederzeitigen hoheitlichen Zugriffs auf die übermittelten Daten besteht[669] oder der Datenempfänger regulär zur Bekanntgabe beispielsweise bestimmter Arbeitnehmerdaten an staatliche Stellen gesetzlich verpflichtet ist.

Sofern solche hoheitlichen Befugnisse zur Einsichtnahme in die Datenbestände des Empfängers über die in einer demokratischen Gesellschaft aus Gründen der öffentlichen Sicherheit erforderlichen, in Artikel 13 der Richtlinie benannten Fälle hinausgehen, vermag eine vertragliche Vereinbarung ein angemessenes Schutzniveau per se nicht sicherzustellen.[670]

3. Die Standardvertragsklauseln

Da sowohl die Gestaltung ausreichender Vertragsklauseln für einen einzelnen Verantwortlichen als auch die Beurteilung ihrer Angemessenheit für die mitgliedstaatlichen Kontrollbehörden eine große Herausforderung[671] darstellen, ist die Europäische Kommission gemäß Artikel 26 Absatz 4 der Richtlinie im Wege des Verfahrens nach Artikel 31 Absatz 2 der Richtlinie zu der abstrakten Feststellung befugt, dass bestimmte Standardvertragsklauseln ausreichende Garantien im Sinne des Artikels 26 Absatz 2 der Richtlinie bieten.

Zwei erste Entscheidungen in diesem Sinne hat die Europäische Kommission bereits im Jahr 2001 getroffen. In der ersten vom 15. Juni 2001[672] befindet sie über einen Angemessenheitsstandard für Vertragsklauseln im Hinblick auf Datenübermittlungen mit der Folge einer Funktionsübertragung, während sich die zweite Entscheidung vom 27.

---

[669] Vgl. aber *Däubler* in: Datenverkehr ohne Datenschutz?, S. 71, S. 85; *ders.*, CR 1999, S. 49, S. 54, der derartige Vorkommnisse für unwahrscheinlich hält.

[670] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 26, Rn. 16; *Ellger*, RabelsZ 60, S. 738, S. 762 f.; *WP 12*, S. 22 f.; so bereits in *WP 9*, S. 10 f.

[671] *Wedler*, RDV 1999, S. 251, S. 254.

[672] *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.

Dezember 2001[673] mit einer entsprechenden Feststellung für Vertragsklauseln im Rahmen einer Auftragsvergabe in das außereuropäische Ausland befasst.

a. Standardvertragsklauseln im Rahmen einer Funktionsübertragung

Gemäß Artikel 1 der Entscheidung der Europäischen Kommission vom 15. Juni 2001 gelten die der Entscheidung im Anhang beigefügten Standardvertragsklauseln bezogen auf eine grenzüberschreitende Datenübermittlung mit der Folge einer Verantwortungsübertragung[674] auf den Datenempfänger „als ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte im Sinne von Artikel 26 Absatz 2 der Richtlinie 95/46/EG."

Die nachfolgende Analyse zeigt einerseits, inwieweit die in den Standardvertragsklauseln festgelegten Verarbeitungsmodalitäten mit den inhaltlichen Grundsätzen eines angemessenen Schutzniveaus korrespondieren. Andererseits wird die Gestaltung des Durchsetzungsmechanismus genauer betrachtet.

(1) Die Berücksichtigung der inhaltlichen Anforderungen ausreichender Garantien

Die inhaltlichen Grundsätze der von den Standardvertragsklauseln vorgesehenen Garantien sind in den Klauseln 2, 4b), c) und d) sowie 5b), c) und e) des Standardvertrages festgehalten, wobei die Klausel 4 sich insgesamt mit den Pflichten des Datenexporteurs beschäftigt, während die Klausel 5 die Pflichten des Datenimporteurs regelt.

Dabei gilt als „Datenexporteur" gemäß der Klausel 1b) der Standardvertragsklauseln „der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt". Als „Datenimporteur" bezeichnen die Standardvertragsklauseln gemäß der Klausel 1c) dagegen denjenigen „für die Verarbeitung Verantwortliche(n), der sich bereit erklärt, vom Datenexporteur personenbezogene Daten für die Verarbeitung gemäß den Bestimmungen dieser Vertragsklauseln entgegenzu-

[673] *Entscheidung der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (2002/16/EG),* ABl. EG Nr. L 6 vom 10.1.2002, S. 52.
[674] Vgl. dazu die Definitionen in Artikel 3 d) und e) der Entscheidung vom 15. Juni 2001.

nehmen und der nicht an ein System eines Drittlandes gebunden ist, das angemessenen Schutz gewährleistet.“

Die darüber hinaus von den Standardvertragsklauseln verwendeten Begriffe erschließen sich gemäß der Klausel 1a) der Standardvertragsklauseln aus den entsprechenden Definitionen der Richtlinie 95/46/EG.

(a) Die Konkretisierung des Verarbeitungsinhalts

Im Interesse der Rechtssicherheit[675] für den Betroffenen sieht die Klausel 2 der Standardvertragsklauseln vor, dass die Übermittlungsparteien die Einzelheiten der Übermittlung in der Anlage 1 der Standardvertragsklauseln konkret formulieren.

Dabei sind zum einen der Datenexporteur sowie der Datenimporteur einschließlich ihrer für die Übermittlung relevanten Tätigkeiten zu benennen. Des Weiteren sollen die übermittelten Datenkategorien, die Übermittlungszwecke, die Kategorien von Betroffenen, der Aufbewahrungszeitraum sowie die Kategorien von Empfängern näher bestimmt werden, an welche die Daten durch den Datenimporteur weitergegeben werden dürfen.

Im Übrigen bleibt es den Mitgliedstaaten ausweislich des der Anlage 1 in Klammern beigefügten Zusatzes sowie gemäß dem Erwägungsgrund (9) der Entscheidung der Europäischen Kommission vom 15. Juni 2001 unbenommen, dieser Liste weitere Aspekte verbindlich hinzuzufügen.

(b) Die inhaltlichen Datenschutzgrundsätze

Die von dem Datenimporteur zu beachtenden inhaltlichen Grundsätze eines angemessenen Datenschutzniveaus sind in der Klausel 5b) festgehalten. Darüber hinaus präzisieren die Klauseln 4b), c) und d) sowie 5c) und e) die Grundsätze der Information und des Auskunftsrechts des Betroffenen.

aa. Die Verarbeitungsgrundsätze

Gemäß der Klausel 5b) der Standardvertragsklauseln können die Vertragsparteien die inhaltlichen Datenschutzgrundsätze, die der Datenim-

[675] Vgl. dazu Gliederungspunkt E.I.2.a. dieses Kapitels.

porteur bei der Verarbeitung der übermittelten Daten beachten muss, aus drei alternativen Quellen rekrutieren.

Als Grundsatz gilt dabei die Verpflichtung des Datenimporteurs, die Verarbeitung an jenen verbindlichen Datenschutzgrundsätzen auszurichten, die dem Vertrag in der Anlage 2 beigefügt sind. Stattdessen dürfen die Parteien jedoch auch vereinbaren, dass der Importeur die Daten in Übereinstimmung mit den jeweiligen, in dem Vertrag im Einzelnen aufzuführenden mitgliedstaatlichen Datenschutzgesetzen verarbeitet. Darüber hinaus besteht die Option zur vertraglichen Übernahme jener in dem Sitzland des Datenimporteurs geltenden Datenschutzbestimmungen, denen die Europäische Kommission bereits gemäß Artikel 25 Absatz 6 der Richtlinie die Erfüllung der Angemessenheitskriterien bescheinigt hat, sofern der Datenimporteur nicht zu dem Adressatenkreis dieser Bestimmungen gehört und letztere ihrem Inhalt entsprechend auf die Übermittlung anwendbar sind.

Entscheiden sich die Übermittlungsparteien für eine der beiden letztgenannten Varianten, sind zusätzlich die verbindlichen Datenschutzgrundsätze der Anlage 3 der Standardvertragsklauseln zu beachten.

(I). Die *Anlage 2* der Standardvertragsklauseln korrespondiert mit Ausnahme der Formulierungen des Zweckbindungsgrundsatzes und des Grundsatzes der beschränkten Weitergabe an Dritte vollständig mit den von der Art. 29-Gruppe in der Arbeitsunterlage WP 12 entwickelten Grundsätzen eines inhaltlich angemessenen Datenschutzniveaus.[676]

Der Zweckbindungsgrundsatz zieht indessen sogar einen engeren Rahmen, als es die Arbeitsunterlage vorsieht. Während letztere nur solche Verwendungen der Daten verbietet, die mit dem Verarbeitungszweck unvereinbar sind, dürfen die Daten im Rahmen der Standardvertragsklauseln lediglich zielgerichtet zu den spezifischen, in der Anlage 1 durch die Vertragsparteien bezeichneten Zwecken verarbeitet werden.

Demgegenüber hat sich die Kommission bei der Gestaltung des Grundsatzes der Weitergabe in unsichere Drittländer an dem nur wenig überzeugenden Vorbild der Safe Harbor Privacy Principles orientiert.[677] Danach erfordert eine Bekanntgabe der Daten an Dritte lediglich die Beachtung der Grundsätze der Informationspflicht und der Wahlmöglichkeit. Sofern es dabei um besondere Kategorien von Daten, also insbe-

[676] Vgl. Gliederungspunkte C.II.1.a. und b. dieses Kapitels.
[677] Vgl. Gliederungspunkte C.III.2.c.(3). dieses Kapitels.

sondere sensible Daten geht, setzt die Weitergabe zwar eine Zustimmung („opt-in“) des Betroffenen voraus. In allen übrigen Fällen ist die Bekanntgabe der Daten jedoch ausschließlich durch die Einräumung eines Widerspruchsrechts bedingt.

Es bleibt allerdings zu hoffen, dass die erweiterte Aufklärungspflicht über die Zwecke der Weiterübermittlung, die Identität des in der Gemeinschaft ansässigen Datenexporteurs, die Kategorien weiterer Empfänger der Daten und Empfängerländer sowie den Umstand, dass die Daten in ein unsicheres Drittland übermittelt werden, einem unreflektierten Schweigen des Betroffenen weitestgehend vorzubeugen geeignet ist. Die Verpflichtung der Vertragsparteien, bereits zum Zeitpunkt des Vertragsabschlusses in der Anlage 1 die zulässigen Kategorien von weiteren Empfängern festzulegen, vermag aufgrund der unbegrenzten Eingabemöglichkeiten für sich betrachtet die mit den weitreichenden Weitergabemöglichkeiten verbundenen Gefahren für den Betroffenen jedenfalls kaum zu entschärfen.[678]

Vorzugswürdig im Interesse eines hohen Schutzniveaus erscheint daher die zweite Variante des Weitergabegrundsatzes. Danach müssen die Vertragsparteien die Grundsätze der Informationspflicht und der Wahlmöglichkeit nicht beachten, sofern sie den Empfänger der weiter übermittelten Daten mit den Verpflichtungen eines Datenimporteurs in ihren Übermittlungsvertrag aufnehmen. Infolgedessen wären die Daten auch nach der Weiterübermittlung durch ausreichende Garantien geschützt.

(II). Die *Anlage 3* der Standardvertragsklauseln verlangt von dem Datenimporteur die Beachtung der in gleicher Weise wie in der Anlage 2 geregelten Grundsätze der Zweckbindung und der Beschränkung der Weiterübermittlung. Darüber hinaus ist die Gewährleistung der Rechte auf Zugriff, Berichtigung, Löschung und Widerspruch des Betroffenen in Übereinstimmung mit der Arbeitsunterlage WP 12 vorgesehen.

Diese ausdrückliche Bezugnahme mag trotz der Anwendbarkeit entweder eines mitgliedstaatlichen Datenschutzgesetzes oder der den oben genannten Merkmalen entsprechenden Bestimmungen aus dem Sitzland des Datenimporteurs auf die besondere Gestaltung dieser Grundsätze im Rahmen der Standardvertragsklauseln zurückzuführen sein.

[678] Die Art. 29-Gruppe hatte sich sogar für ein Weiterübermittlungsverbot ausgesprochen, vgl. *WP 38*, S. 5.

Wie bereits erläutert, sind die Grundsätze der Zweckbindung und der Beschränkung der Weitergabe in unsichere Länder in einer teilweise speziell auf die Bedürfnisse der Vertragslösung abgestimmten Art und Weise geregelt,[679] sodass ein Äquivalent in der darüber hinaus anzuwendenden Rechtsquelle nicht zu erwarten ist.

Die Formulierung der Rechte des Betroffenen schließlich bezieht sich unter anderem explizit auf einen Verstoß gegen die beiden erstgenannten Grundsätze. Ohne die ausdrückliche Aufnahme dieses Grundsatzes in die Anlage 3 wäre der Betroffene teilweise schutzlos, sofern die von den gewählten Datenschutzbestimmungen vorgesehenen Rechte nicht zu einem Vorgehen gegen eine Verletzung der besonderen Merkmale der beiden anderen Prinzipien berechtigen würden.

Ein Rückgriff auf die mitgliedstaatlichen Datenschutzgesetze zur inhaltlichen Gestaltung des Vertrages scheint insbesondere angebracht, sofern das Recht des betreffenden Mitgliedstaates generell Besonderheiten bei der Übermittlung von Daten zu den seitens der Übermittlungsparteien geplanten Zwecken vorsieht oder bestimmte Kategorien von Daten in besonderer Weise schützt.[680] In Anlehnung an die FAQ 9 der Safe Harbor Privacy Principles ist dabei etwa an die Spezialregelungen einiger Mitgliedstaaten für die Übermittlung von Arbeitnehmerdaten zu denken. Je nach Komplexität der geregelten Materie kann sich die Übernahme der mitgliedstaatlichen Gesetzestexte in solchen Fällen unter Umständen als einzig praktikable Möglichkeit zur Gewährleistung eines effektiven Datenschutzes darstellen.

Über die dritte Variante der Herleitung verbindlicher Datenschutzgrundsätze können derzeit nur die Safe Harbor Privacy Principles in die Vertragsklauseln einfließen. Dieser Weg empfiehlt sich im Grunde für alle Datenschutzverträge mit solchen US-Unternehmen, die sich entweder grundsätzlich nicht oder nur partiell auf die Grundsätze des „sicheren Hafens“ verpflichten möchten, sowie mit jenen Datenimporteuren, die nicht der Aufsicht der Federal Trade Commission oder des US-Verkehrsministeriums unterliegen und sonach auch nicht von der Entscheidung über die Angemessenheit der Principles seitens der Europäischen Kommission erfasst sind.

[679] Vgl. dazu auch Gliederungspunkt E.I.2.b.(2).(a) dieses Kapitels.
[680] Vgl. dazu auch Erwägungsgrund (6) der Entscheidung vom 15. Juni 2001.

bb. Erhöhung der Transparenz

Die Klauseln 4b), c) und d) sowie 5c) und e) der Standardvertragsklauseln schreiben den Übermittlungsparteien Pflichten zur Erhöhung der Transparenz der Verarbeitung vor.

Sofern die Übermittlung an den Datenimporteur besondere Kategorien von Daten einbezieht, hat der Datenexporteur gemäß der Klausel 4b) den Betroffenen vorher davon in Kenntnis zu setzen, dass seine Daten in ein unsicheres Drittland transferiert werden. Diese Klausel trägt der besonderen Schutzbedürftigkeit sensibler Daten Rechnung, die kein Zuwarten auf eine etwaige Nachfrage des Betroffenen über den Umgang mit seinen Daten erlaubt. Zwar steht dem Betroffenen gegen die Übermittlung kein Widerspruch zu. Die Information über den Drittländertransfer versetzt ihn jedoch überhaupt erst in die Lage, die Geltendmachung seiner Rechte zu erwägen. So kann der Betroffene gemäß der Klausel 4c) von dem Datenexporteur beziehungsweise gemäß der Klausel 5e) von dem Datenimporteur umgehend eine Kopie des Übermittlungsvertrages anfordern und den Datenimporteur zudem nach einer Anlaufstelle für Beschwerden fragen.

Teilweise wird kritisiert, dass neben dem Datenexporteur auch der Datenimporteur eine Kopie des Vertrages zur Verfügung stellen muss, da der Betroffene regelmäßig auf einfacherem Wege Kontakt zu dem Datenexporteur herstellen können werde.[681] Allerdings mag es auch Ausnahmen geben, etwa wenn sich der Betroffene in dem Sitzland des Datenimporteurs aufhält oder sich ohnehin bei diesem nach einer Beschwerdestelle erkundigen möchte. In solchen Fällen könnte die Anfrage bei dem Datenexporteur unter Umständen zu einer deutlich größeren Belastung des Betroffenen führen. Davon abgesehen sollte die Klausel 5e) den Datenimporteur kaum je übermäßig belasten, da der Betroffene mit seinem Anliegen dennoch in der Regel auf den Datenexporteur zurückkommen wird.

Die Klauseln 4d) und 5c) der Standardvertragsklauseln sehen schließlich vor, dass der Betroffene Auskunft über die von dem Datenimporteur vorgenommene Verarbeitung seiner personenbezogenen Daten sowohl von dem Datenimporteur als auch, im Hinblick auf die Prämisse eines leichten Zugangs, von dem Datenexporteur verlangen darf. Um

[681] So *US-Handelsministerium*, abrufbar unter: www.export.gov/safeharbor/DOCStaff_Comments.htm; dem folgend: *Räther/Seitz*, MMR 2002, S. 520, S. 524.

den sonach erforderlichen Informationsfluss zwischen beiden Übermittlungsparteien zu gewährleisten, ist der Datenimporteur gemäß der Klausel 5c) darüber hinaus zu einer unverzüglichen und genauen Bearbeitung der Anfragen des Datenexporteurs verpflichtet.

(2) Die Durchsetzung der Vertragsklauseln

Für die Durchsetzung der inhaltlichen Datenschutzgrundsätze sind die Klauseln 3, 4d), 5a), c) und d), 6 bis 8 sowie 10 relevant. Entsprechend dem bisherigen Prüfungsschema werden sie im Folgenden in Bezug auf eine gute Befolgungsrate, eine effektive Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte sowie die Gewährleistung einer angemessenen Entschädigung des Betroffenen bei Verstößen untersucht.

(a) Befolgungsrate

Eine gute Befolgungsrate ist stets im Wege einer hohen Transparenz für alle Beteiligten sowie mithilfe einer externen Kontrolle und der Androhung abschreckender Sanktionen zu erzielen.

Während die Transparenz der Verarbeitung zugunsten des Betroffenen einerseits mit den bereits dargestellten Informationspflichten und andererseits mit dem Angebot einer Kopie der Vertragsklauseln sichergestellt wird, ist eine Bekanntgabe der Vertragsbestimmungen gegenüber den Mitarbeitern des Datenimporteurs nicht vorgeschrieben. Die Standardvertragsklauseln verlassen sich also ganz offensichtlich darauf, dass der Datenimporteur diese Maßnahmen zwangsläufig treffen muss, um seinen Vertrag ordnungsgemäß zu erfüllen. Damit stehen die Klauseln allerdings im Widerspruch zu den diesbezüglich ausgehandelten Details hinsichtlich der internen Umsetzung der Safe Harbor Privacy Principles.[682]

Eine externe Kontrolle des Datenimporteurs ist in der Klausel 5d) der Standardvertragsklauseln vorgesehen. Danach muss der Datenimporteur auf Verlangen des Datenexporteurs eine Kontrolle seiner für die Verarbeitung notwendigen Datenverarbeitungseinrichtungen dulden, die entweder durch den Datenexporteur selbst oder durch ein von diesem ausgewähltes Prüfgremium durchgeführt wird, dessen Mitglieder unabhängig sind und über die erforderlichen Qualifikationen verfügen.

[682] Vgl. dazu Gliederungspunkt C.III.2.c.(7).(a).bb. dieses Kapitels.

Das Eigeninteresse des Datenexporteurs an der tatsächlichen Vornahme einer solchen Kontrolle ergibt sich in erster Linie aus einer in der Klausel 6 festgelegten gesamtschuldnerischen Schadensersatzhaftung der beiden Übermittlungsparteien für ihre gegenseitigen Verstöße.

Auf eine vertragliche Androhung von Sanktionen wurde indessen vollständig verzichtet. Da die Durchsetzung der im Grunde einzig möglichen Option einer Vertragsstrafe von dem freien Entschluss des Datenexporteurs abhinge, wäre sie der Befolgungsrate aber ohnehin nur sehr bedingt zuträglich gewesen.

(b) Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte

Die Unterstützung des Betroffenen bei der Durchsetzung seiner Rechte setzt einerseits deren rechtsgültige Begründung in dem Übermittlungsvertrag und andererseits die Einrichtung eines effektiven Beschwerdeverfahrens voraus.

aa. Die Rechte des Betroffenen

Die Klausel 3 der Standardvertragsklauseln sieht vor, dass der Betroffene alle Maßnahmen und Rechte aus den ihn begünstigenden, im Einzelnen aufgezählten Klauseln des Übermittlungsvertrages als Drittbegünstigter geltend machen kann. Allein die Durchführung einer Kontrolle bei dem Datenimporteur durch den Datenexporteur im Sinne der Klausel 5d) sowie die Zusammenarbeit der Übermittlungsparteien mit den Kontrollbehörden gemäß der Klausel 8 vermag er nicht zu erzwingen.

Bei der Geltendmachung seiner Rechte darf sich der Betroffene von einer Vereinigung oder einer sonstigen Einrichtung, also zum Beispiel einem Verbraucherschutzverband,[683] vertreten lassen.

Die Rechte des Betroffenen werden sonach unmittelbar in dem betreffenden Übermittlungsvertrag begründet. Da gemäß der Klausel 10 auf den Vertrag das Recht desjenigen Mitgliedstaates anwendbar ist, in dem der Datenexporteur seinen Sitz hat, und auch der Gerichtsstand gemäß der Klausel 7 - 1b) - in eben diesem Mitgliedstaat als vereinbart

[683] *Räther/Seitz*, MMR 2002, S. 520, S. 523.

gilt, kommt es für die gerichtliche Geltendmachung der Klausel nicht mehr darauf an, ob die Rechtsordnung des Drittlandes eine vertragliche Begründung von Rechten Dritter zulässt.[684]

bb. Das Beschwerdeverfahren

Das Beschwerdeverfahren ist hauptsächlich in der Klausel 7 der Standardvertragsklauseln geregelt, der grundsätzlich drei verschiedene Optionen zur Streitbeilegung vorsieht, sofern ein Konflikt zwischen dem sich auf die Drittbegünstigtenklausel berufenden Betroffenen und einer Übermittlungspartei nicht einvernehmlich gelöst zu werden vermag.
Danach darf der Betroffene die Klärung des Disputs entweder einem von einer unabhängigen Person oder gegebenenfalls der Kontrollstelle durchgeführten Schlichtungsverfahren überlassen oder einem Gericht desjenigen Mitgliedstaates antragen, in dem der Datenexporteur ansässig ist. Alternativ[685] kann die Streitigkeit nach Absprache zwischen dem Betroffenen und der relevanten Übermittlungspartei auch einem Schiedsgericht unterbreitet werden, sofern in dem Sitzland der betreffenden Partei das New Yorker Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche vom 10.6.1958 ratifiziert wurde. Letzteres bietet sich insbesondere an, sofern die Anerkennung und die Vollstreckung des Urteils eines mitgliedstaatlichen Gerichts in dem Sitzland des Datenimporteurs als ungewiss gilt.

Ob allerdings diese theoretische Wahlmöglichkeit in der Praxis tatsächlich ein Äquivalent findet, hängt entsprechend dem Erwägungsgrund (21) der Entscheidung der Kommission über die Standardvertragsklauseln von der Existenz zuverlässiger und anerkannter Schlichtungs- und Schiedsgerichtssysteme ab.

Unbeschadet der Geltendmachung seiner vertraglichen Ansprüche aus der Drittbegünstigtenklausel steht es dem Betroffenen gemäß der Klausel 7 Absatz 3 offen, zusätzliche Rechtsbehelfe entsprechend seinen weiteren materiellen Ansprüchen oder Verfahrensrechten aus anderen Bestimmungen des nationalen oder internationalen Rechts einzulegen. Die vertragliche Gewährleistung der Drittbegünstigung entbindet die Übermittlungsparteien sonach nicht von ihrer Haftung aus außerver-

[684] Vgl. dazu die Erläuterungen unter Gliederungspunkt E.I.2.b.(2).(a). dieses Kapitels.
[685] Vgl. mangels eines eindeutigen Wortlauts in der Klausel 7 dazu den Erwägungsgrund (21) der Entscheidung vom 15. Juni 2001.

traglichen Rechtsgrundlagen wie zum Beispiel einem Schadensersatzanspruch aus unerlaubter Handlung.[686]

Dieses offensichtlich effektive Streitbeilegungssystem garantiert dem Betroffenen mit hoher Wahrscheinlichkeit eine zuverlässige Durchsetzung seiner Rechte. Allerdings unterstützt es ihn nicht bei der oftmals kaum von ihm allein zu bewältigenden Verifikation des Bestehens seiner Ansprüche.

Für die Übernahme dieser Aufgabe scheint eine weitere unabhängige Instanz erforderlich, die mit den entsprechenden Untersuchungsbefugnissen ausgestattet ist.

Die mitgliedstaatlichen Kontrollbehörden vermögen dieses Defizit jedenfalls kaum auszugleichen, da ihnen der Übermittlungsvertrag nur sehr begrenzte Eingriffsbefugnisse zugesteht.[687] Mit Ausnahme der Verpflichtung des Datenimporteurs aus der Klausel 5c), alle Feststellungen der Kontrollbehörde im Hinblick auf die Verarbeitung der übermittelten Daten zu respektieren, überschneiden sich die erlaubten Maßnahmen der Kontrollbehörden vollständig mit einzelnen Rechten des Betroffenen. So müssen die Übermittlungsparteien gemäß der Klausel 8 auf Verlangen der Kontrollstelle beziehungsweise aus Erfordernissen des nationalen Rechts eine Kopie des Übermittlungsvertrages bei der Kontrollstelle hinterlegen und ihr gemäß den Klauseln 4d) beziehungsweise 5c) Anfragen bezüglich der von dem Datenimporteur durchgeführten Verarbeitungen zeitgerecht beantworten.

Eine Befugnis zur effektiven Einsichtnahme in die Verarbeitung des Datenimporteurs ist indessen nicht vorgesehen. Anderenfalls stünde allerdings auch ein unzulässiger Eingriff in die Staatensouveränität des Destinationsstaates über den Umweg eines privatrechtlichen Vertrages zu befürchten. Bereits die Kooperationspflicht mit den mitgliedstaatlichen Kontrollbehörde scheint in dieser Hinsicht nicht ganz unbedenklich. Eine Duldung des Destinationsstaates dergestalt, dass die Kontrollstelle ihre Befugnisse auch gerichtlich durchzusetzen vermag, muss jedenfalls in Bezug auf die meisten Drittstaaten als äußerst unwahrscheinlich betrachtet werden.

---

[686] Vgl. aber *Räther/Seitz*, MMR 2002, S. 520, S. 525, die aufgrund der Klausel 7 Absatz 3 unverständlicherweise eine doppelte Inanspruchnahme der Übermittlungsparteien wähnen.
[687] Simitis (- *Simitis* u. a.), BDSG, § 4c, Rn. 50.

In den USA indessen könnte die effektive Gewährleistung der vertraglich festgelegten Kontrollbefugnisse tatsächlich gelingen. Das US-Handelsministerium wurde bereits während der Entwurfsphase der Standardvertragsklauseln regelmäßig über den Stand der Entwicklungen informiert und äußerte trotz seiner insgesamt steten Kritik keine Bedenken gegen die Klauseln über die Zusammenarbeit mit den europäischen Kontrollbehörden.[688] Die Standardvertragsklauseln im Rahmen einer Funktionsübertragung sind sogar über die Website des US-Handelsministeriums abrufbar. Dementsprechend ist wohl von einer Bewilligung beziehungsweise Duldung der Maßnahmen der Kontrollbehörden entsprechend den Standardvertragsklauseln auf dem Hoheitsgebiet der USA auszugehen.

(c) Entschädigung des Betroffenen

Die Entschädigung des Betroffenen ist schließlich in der Klausel 6 der Standardvertragsklauseln geregelt. In Anlehnung an Artikel 23 Absatz 1 der Richtlinie 95/46/EG ist der Betroffene danach berechtigt, von den Übermittlungsparteien Ersatz für solche Schäden zu fordern, die er infolge einer Verletzung der vom Anwendungsbereich der Drittbegünstigtenklausel erfassten Bestimmungen erleidet.

Die Übermittlungsparteien haften gesamtschuldnerisch und sind sonach entsprechend der dem Artikel 23 Absatz 2 nachgebildeten Möglichkeit zum Entlastungsbeweis nur dann von ihrer Haftung befreit, falls sie nachweisen können, dass keine von ihnen für die Verletzung der Datenschutzbestimmungen verantwortlich ist. Darüber hinaus sieht die Klausel 6 eine aufgrund ihrer Irrelevanz für den Betroffenen nur fakultativ in den Vertrag aufzunehmende Bestimmung über den Regress der beiden Übermittlungsparteien vor.

Die gesamtschuldnerische Haftung der beiden Parteien stellt sicher, dass die Ansprüche des Betroffenen nicht daran scheitern, dass letzterer trotz einer offensichtlichen Verletzung der Vertragsklauseln keiner Partei die tatsächliche Verantwortung nachzuweisen vermag.[689] Außerdem stellt sich eine Vollstreckung innerhalb der Europäischen Union für den Betroffenen regelmäßig als deutlich einfacher dar als in dem betreffenden Drittland. Soweit sich also insgesamt ein Verstoß gegen die Bestimmungen des Vertrages beweisen lässt, bietet das Entschädigungs-

[688] Die Stellungnahmen des *US-Handelsministeriums* sind abrufbar unter: www.export.gov/safeharbor/sh_modelcontract.html.
[689] *Räther/Seitz*, MMR 2002, S. 520, S. 524.

system der Standardvertragsklauseln eine effektive Gewährleistung von Schadensersatz.

Die Sorge einiger außereuropäischer Datenverarbeiter, sie könnten für Verletzungen des Datenexporteurs im Vorfeld der Übermittlung in Anspruch genommen werden,[690] erweist sich indessen als unbegründet. Zwar wird der Datenexporteur in der Klausel 4a) darauf hingewiesen, dass ihn die Zulässigkeit des Transfers aufgrund der Standardvertragsklauseln nicht von einer Rechtmäßigkeit der Übermittlung gemäß den übrigen mitgliedstaatlichen Datenschutzbestimmungen entbindet. Diese Klausel ist jedoch nicht in die vertragliche Drittbegünstigung und somit auch nicht in die gesamtschuldnerische Mithaftung des Datenimporteurs eingeschlossen.[691]

(d) Eingriffsbefugnisse des Destinationsstaates

Der Datenimporteur hat gemäß der Klausel 5a) der Standardvertragsklauseln zu untersuchen, ob er hoheitlichen Eingriffsbefugnissen seines Sitzstaates unterworfen ist, die ihm die Erfüllung seiner Vertragspflichten insoweit unmöglich machen, als dass sie über die Ausnahmen des in der Anlage 2 eigens zitierten Artikels 13 der Richtlinie 95/46/EG hinausgehen. Die zuständige Kontrollstelle sowie der Datenexporteur sind darüber hinaus über solche Gesetzesänderungen zu informieren, die sich voraussichtlich sehr nachteilig auf die Gewährleistung der vertraglichen Garantien auszuwirken vermögen. Der Datenexporteur ist infolge einer solchen Entwicklung zur Aussetzung der Übermittlungen befugt und darf von dem Übermittlungsvertrag zurücktreten.

Setzt der Datenexporteur den Drittländertransfer dennoch fort, dürfen die mitgliedstaatlichen Kontrollbehörden gemäß Artikel 4 Absatz 1a) der Entscheidung der Europäischen Kommission vom 15. Juni 2001 ihre Befugnisse zur Unterbindung der Übermittlungen ausüben.

(3) Die sonstigen Vertragsklauseln

Die Klauseln 9 und 11 des Vertrages befassen sich schließlich mit der Kündigung sowie der Änderung des Vertrages.

---

[690] So z. B. das *US-Handelsministerium*, abrufbar unter: www.export.gov/safeharbor/DOCStaff_Comments.htm; dem folgend *Räther/Seitz*, MMR 2002, S. 520, S. 524.

[691] Erwägungsgrund (20) der Entscheidung vom 15. Juni 2001.

Während die Klausel 9 die Übermittlungsparteien dazu verpflichtet, nach einer Kündigung des Vertrages die übermittelten Daten auch weiterhin entsprechend den Vertragsbestimmungen zu verarbeiten, verbietet die Klausel 11 den Parteien eine Änderung des Wortlautes der Vertragsklauseln.

Von dieser Modifikationssperre nicht erfasst sind allerdings jene geschäftsbezogenen, den Standardvertragsklauseln nicht widersprechenden Bestimmungen, welche die Vertragsparteien entsprechend dem Erwägungsgrund (5) der Entscheidung der Europäischen Kommission vom 15. Juni 2001 zusätzlich in den Vertrag aufgenommen haben.

(4) Ergebnis

Im Ergebnis ist es der Europäischen Kommission tatsächlich weitestgehend gelungen, die eingangs erwähnten Bedenken[692] gegen die Zulässigkeit eines Vertrages zur Gewährleistung ausreichender Garantien im Rahmen einer Funktionsübertragung auszuräumen. Allerdings weist der Kontrollmechanismus nach wie vor erhebliche Schwächen auf, die jedoch aufgrund des völkerrechtlichen Prinzips der Staatensouveränität kaum zu beseitigen sein werden.

Wie bereits die „Safe Harbor“-Entscheidung weist daher auch die Entscheidung der Kommission vom 15. Juni 2001 die mitgliedstaatlichen Datenschutzbehörden in Artikel 4 darauf hin, dass sie die Übermittlung von Daten unterbinden dürfen, sofern der Datenimporteur gegen die Vertragsbestimmungen verstößt oder eine hohe Wahrscheinlichkeit für einen solchen Verstoß besteht und dem Betroffenen bei einer Fortsetzung der Übermittlungen ein irreparabler Schaden entstehen würde.

In Artikel 5 schließlich kündigt die Europäische Kommission an, dass sie die Durchführung ihrer Entscheidung drei Jahre nach ihrer Bekanntgabe an die Mitgliedstaaten, also im Jahr 2004 bewerten wird.

b. Die Standardvertragsklauseln für Datenübermittlungen an Auftragsverarbeiter

In Anbetracht des Bedürfnisses nach Flexibilität des internationalen Handels entwickelte die Europäische Kommission schließlich in ihrer Entscheidung vom 27. Dezember 2001 ebenfalls mithilfe von Standard-

[692] Vgl. Gliederungspunkt E.I.1.b. dieses Kapitels.

vertragsklauseln ausreichende Garantien im Sinne des Artikels 26 Absatz 2 der Richtlinie 95/46/EG hinsichtlich grenzüberschreitender Datenübermittlungen an Auftragsverarbeiter.

Im Gegensatz zu einer Datenübermittlung im Rahmen einer Funktionsübertragung kommt es bei einer Auftragsverarbeitung nicht zu einem Verantwortungsübergang auf den Datenimporteur, bei welchem es sich gemäß der Klausel 1c) der Standardvertragsklauseln um jenen „Auftragsverarbeiter (handelt), der sich bereit erklärt, vom Datenexporteur personenbezogene Daten zur Verarbeitung gemäß den Bestimmungen dieser Vertragsklauseln entgegenzunehmen, und der nicht an ein System eines Drittlandes gebunden ist, das angemessenen Schutz gewährleistet“.

Da die Verantwortung sonach bei dem in der Europäischen Union ansässigen Datenexporteur verbleibt, entscheidet allein dieser gemäß Artikel 2d) der Richtlinie 95/46/EG über die Zwecke und die Mittel der von dem Datenimporteur durchzuführenden Verarbeitung.

Mangels eines eigenen Entscheidungsspielraums ist also der Datenimporteur lediglich auf die technischen und organisatorischen Sicherheitsmaßnahmen im Sinne des Artikels 17 der Richtlinie 95/46/EG sowie auf einen den Anweisungen des Datenexporteurs entsprechenden Vollzug der Verarbeitung zu verpflichten, der sich entsprechend dem in den Klauseln 4a) in Verbindung mit der Klausel 1d) der Standardvertragsklauseln wiedergegebenen Sitzprinzip nach dem jeweiligen mitgliedstaatlichen Datenschutzgesetz richtet.

Die für die nachfolgenden Ausführungen zum Inhalt und zur Durchsetzung der Vertragsklauseln erforderlichen Definitionen der Klausel 1 der Standardvertragsklauseln entsprechen jenen der Richtlinie 95/46/EG beziehungsweise den Begriffsbestimmungen der Standardvertragsklauseln im Rahmen einer Funktionsübertragung[693], auf deren Darstellung insoweit verwiesen wird.

Die Vertragsklauseln unterliegen im Übrigen gemäß der Klausel 10 einem Modifikationsverbot.

[693] Vgl. Gliederungspunkt E.I.3.a.(1). dieses Kapitels.

(1) Die Berücksichtigung der inhaltlichen Anforderungen ausreichender Garantien

Die inhaltlichen Grundsätze der von den Standardvertragsklauseln beigebrachten Garantien ergeben sich aus den Klauseln 2, 4a) bis f) und h) sowie 5a), c), d) und g) der Standardvertragsklauseln, wobei sich wiederum die Klausel 4 mit den Pflichten des Datenexporteurs und die Klausel 5 mit jenen des Datenimporteurs beschäftigen.

(a) Die Konkretisierung des Verarbeitungsinhalts

Der Inhalt des Vertrages ist gemäß der Klausel 2 in der Anlage 1 zu konkretisieren. Die abgefragten Rubriken stimmen im Wesentlichen mit jenen aus der äquivalenten Anlage der Standardvertragsklauseln im Rahmen einer Funktionsübertragung überein.[694] Allerdings sollen die Übermittlungsparteien anstelle der entbehrlichen Spezifizierung des Übermittlungszwecks, der vorliegend allein in der Auftragsverarbeitung besteht, die durchzuführenden Verarbeitungsmaßnahmen festhalten. Verzichtbar sind mangels einer autonomen Entscheidungsbefugnis des Datenimporteurs indessen Angaben zum Aufbewahrungszeitraum sowie über zulässige Empfänger einer Weiterübermittlung.

(b) Die inhaltlichen Datenschutzgrundsätze

Die inhaltlichen Datenschutzgrundsätze für die seitens des Datenimporteurs durchgeführte Auftragsverarbeitung ergeben sich gemäß dem Sitzprinzip grundsätzlich aus dem Datenschutzgesetz desjenigen Mitgliedstaates, in dem der für die Verarbeitung verantwortliche Datenexporteur ansässig ist.

Als Ausnahme dazu richtet sich allerdings die Anwendbarkeit der Vorschriften über die zu treffenden technischen und organisatorischen Sicherheitsvorkehrungen gemäß Artikel 17 Absatz 3 der Richtlinie im Rahmen einer Auftragsverarbeitung nach dem Sitz des Auftragsverarbeiters. Da in Bezug auf die Datensicherheit bei einem Drittländertransfer sonach kein mitgliedstaatliches Datenschutzgesetz Anwendung findet, ist der Auftragsverarbeiter gesondert auf den diesbezüglichen Grundsatz zu verpflichten.

[694] Vgl. dazu Gliederungspunkt E.I.3.a.(1).(a). dieses Kapitels.

aa. Die Bindung an ein mitgliedstaatliches Datenschutzgesetz

Gemäß der Klausel 4a) der Standardvertragsklauseln garantiert der Datenexporteur, dass sowohl die Übermittlung der Daten als auch ihre anschließende Verarbeitung in dem Drittland entsprechend den einschlägigen Bestimmungen des für ihn verbindlichen mitgliedstaatlichen Datenschutzgesetzes durchgeführt werden. Ferner hat der Datenexporteur den Datenimporteur gemäß der Klausel 4b) anzuweisen, die übermittelten Daten nur in seinem Auftrag und in Übereinstimmung mit dem anwendbaren mitgliedstaatlichen Datenschutzgesetz sowie den Klauseln des Übermittlungsvertrages zu verarbeiten.

Im Gegenzug verpflichtet sich der Datenimporteur gemäß der Klausel 5a), diesen Pflichten nachzukommen und den Datenexporteur unverzüglich zu benachrichtigen, sofern er dies nicht einhalten kann. Der Datenexporteur darf sodann die Datenübermittlungen aussetzen sowie von dem Vertrag zurücktreten.

Die genannten Klauseln dienen im Grunde nur der Schaffung einer nach Artikel 17 Absatz 3 der Richtlinie für jede Auftragsverarbeitung erforderlichen Rechtsgrundlage[695] und beinhalten keine spezifischen Besonderheiten hinsichtlich eines Drittländertransfers.

bb. Der Grundsatz der Datensicherheit

Die Klauseln 4c) bis e) sowie 5c) und d) befassen sich mit der Gewährleistung technischer und organisatorischer Sicherheitsmaßnahmen.

Gemäß der Klausel 4c) garantiert der Datenexporteur, dass der Datenimporteur die in der Anlage 2 von den Vertragsparteien im Einzelnen dargelegten Sicherheitsmaßnahmen bietet, die gemäß der Klausel 4d) den Anforderungen des Artikels 17 Absatz 1 der Richtlinie und des jeweils anzuwendenden mitgliedstaatlichen Datenschutzgesetzes genügen müssen. Ferner verpflichtet sich der Datenexporteur gemäß der Klausel 4e), dass er für die Einhaltung dieser Sicherheitsmaßnahmen Sorge trägt, während der Datenimporteur gemäß der Klausel 5c) versichert, dass er die vereinbarten Sicherheitsmaßnahmen auch tatsächlich ergriffen hat. Darüber hinaus verspricht der Datenimporteur, dass er den Datenexporteur gemäß den Klauseln 5d)i) und ii) unverzüglich über jeden zufälligen oder unberechtigten Zugang zu den Datenbeständen beziehungsweise über jede rechtlich bindende Aufforderung einer Vollstre-

[695] Erwägungsgrund (7) der Entscheidung vom 27.12.2001.

ckungsbehörde zur Weitergabe der Daten informieren wird, sofern ihm dies nicht aus Gründen der Vertraulichkeit verboten ist.

Die eingangs erwähnte Anwendungslücke der mitgliedstaatlichen Datenschutzgesetze wird also geschlossen, indem sich die entsprechende Richtlinienbestimmung zur Datensicherheit vollständig in dem Vertragstext wiederfindet und das mitgliedstaatliche Datenschutzgesetz, das in dem Sitzland des Datenexporteurs gilt, bei der Spezifizierung der Maßnahmen in der Anlage 2 zu beachten ist.

cc. Erhöhung der Transparenz

Die Erhöhung der Transparenz der Verarbeitung wird von den Klauseln 4f) und h) sowie 5g) im Wege derselben Auskunfts- und Informationspflichten erreicht wie bei den entsprechenden Standardvertragsklauseln im Rahmen einer Funktionsübertragung.[696]

Mit Rücksicht auf die Betriebsgeheimnisse des Datenimporteurs müssen die Parteien dem Betroffenen allerdings keine Kopie der Anlage 2 überlassen. Stattdessen kann der Betroffene jedoch eine kurze Beschreibung der Sicherheitsmaßnahmen verlangen.

Ferner steht dem Betroffenen kein vertragliches Auskunftsrecht über die von dem Datenimporteur durchgeführte Verarbeitung zu, da er sich gemäß seinem äquivalenten Anspruch aus dem anzuwendenden mitgliedstaatlichen Datenschutzgesetz unmittelbar an den verantwortlichen Datenexporteur wenden kann. Das bestätigt auch die Klausel 5d)iii), die dem Datenimporteur eine Pflicht zur unverzüglichen Information des Datenexporteurs über etwaige Anfragen betroffener Personen auferlegt und ihm, sofern er nicht anderweitig dazu berechtigt ist, eine Erteilung der gewünschten Auskunft verbietet.

(2) Die Durchsetzung der Vertragsklauseln

Die Durchsetzung der Vertragsklauseln wird von den Klauseln 3, 4g), 5b), e) und f) sowie 6 bis 8 geregelt.

Hinsichtlich der Feststellung einer guten Befolgungsrate und der Eingriffsbefugnisse des Destinationsstaates wird wegen der identischen Bestimmungen im Vergleich zu den Standardvertragsklauseln im Rah-

[696] Vgl. Gliederungspunkt E.I.3.a.(1).(b).bb. dieses Kapitels.

men von Funktionsübertragungen auf die dortigen Erläuterungen verwiesen.[697] Indessen weisen das System zur Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte und das Verfahren zu seiner Entschädigung einige Unterschiede dazu auf.

(a) Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte

Die Effektivität des Beschwerdesystems hängt einerseits von den Merkmalen der Drittbegünstigtenklausel ab sowie andererseits von einem effektiven Schieds- und Kontrollmechanismus.

aa. Die Rechte des Betroffenen

Die Klausel 3 begründet im Wege der Drittbegünstigung vertragliche Rechte des Betroffenen, die ihn sowohl zu einem Vorgehen gegen den Datenexporteur als auch gegen den Datenimporteur wegen dessen eigener Verstöße berechtigen, sofern sich der Datenexporteur tatsächlich aufgelöst hat oder rechtlich nicht mehr besteht.

Der Betroffene soll also neben den Verletzungen des anzuwendenden mitgliedstaatlichen Datenschutzgesetzes auch Verstöße gegen die einzelnen Vertragsklauseln geltend machen können. Das stärkt seine Position vor allem gegenüber dem Datenimporteur, da ein Auftragsverarbeiter normalerweise keiner direkten Haftung gegenüber dem Betroffenen unterliegt.

Die Klausel 3 wird daher wegen ihres angeblich über das innergemeinschaftliche Schutzniveau hinausgehenden Ansatzes kritisiert.[698] Diese Ansicht verkennt jedoch, dass der Betroffene ohne diese Regelung infolge einer Auflösung des Datenexporteurs jeglicher Möglichkeit der Einflussnahme auf die Verarbeitung seiner personenbezogenen Informationen enthoben wäre. Die Daten stünden aufgrund der Erlöschung des Auftragsverhältnisses zur freien Verfügung des Datenimporteurs. Obgleich dieser gemäß der Klausel 11 nach der Erbringung der Dienstleistung an den Datenexporteur zur Rückübermittlung beziehungsweise zur Zerstörung der Daten gehalten ist, wäre jedoch niemand mehr dazu in der Lage, diese Verpflichtung tatsächlich durchzusetzen.

[697] Vgl. Gliederungspunkt E.I.3.a.(2).(a). und (d).dieses Kapitels.
[698] Vgl. dazu den Kommentar der *ICC*, S. 2 f., die betont, dass die Standardvertragsklauseln nicht über die Regelung der Auftragsverarbeitung in der Richtlinie 95/46/EG hinausgehen sollten und daher u. a. die Drittbegünstigtenklausel überflüssig sei; so wohl auch *EICTA*, S. 3 f.

Ein äquivalenter Sachverhalt innerhalb der Europäischen Union hätte zwar ebenfalls einen Verantwortungsübergang auf den Auftragsverarbeiter zur Konsequenz. Der Betroffene könnte seine Rechte jedoch infolgedessen auf der Grundlage der auf die Verarbeitungen des neuen Verantwortlichen anzuwendenden mitgliedstaatlichen Datenschutzbestimmungen geltend machen.

bb. Das Beschwerdeverfahren

Während der Betroffene gegen den Datenexporteur mithilfe der in dem jeweiligen mitgliedstaatlichen Datenschutzgesetz vorgesehenen Rechtsbehelfe vorzugehen vermag, ist das Streitbeilegungsverfahren mit dem Datenimporteur gemäß der Klausel 7 in gleicher Weise geregelt wie in der entsprechenden Vorschrift der Standardvertragsklauseln im Rahmen von Funktionsübertragungen.[699]

Im Gegensatz zu jenen Standardvertragsklauseln gestehen die Standardvertragsklauseln für Auftragsverarbeitungen den Kontrollbehörden jedoch deutlich intensivere Eingriffsbefugnisse zu. So dürfen die mitgliedstaatlichen Datenschutzbehörden neben ihrem Anspruch auf eine Kopie des Vertrages aus der Klausel 8 Absatz 1 gemäß der Klausel 8 Absatz 2 unter denselben Bedingungen Kontrollen bei dem Datenimporteur durchführen wie bei dem Datenexporteur.

Gemäß der Klausel 5e) hat der Datenimporteur zudem die Feststellungen der Kontrollbehörde im Hinblick auf die übermittelten Daten zu respektieren. Auf diese Weise soll verhindert werden, dass der Datenexporteur seine Datenverarbeitung absichtlich einer Aufsicht der mitgliedstaatlichen Kontrollbehörden entzieht. Die tatsächliche Umsetzung dieser umfassenden Aufsichtsbefugnisse hängt allerdings stark davon ab, ob der Destinationsstaat hoheitliche Kontrollen anderer Staaten auf seinem Territorium dulden wird.[700]

(b) Entschädigung des Betroffenen

Als Verantwortlicher der Verarbeitung haftet der Datenexporteur gemäß der Klausel 6 Absatz 1 grundsätzlich allein für alle Schäden des

[699] Vgl. dazu Gliederungspunkt E.I.3.a.(2).(b).bb. dieses Kapitels.
[700] Diese Bedenken teilt die Art. 29-Gruppe offenbar nicht, vgl. *WP 47*, S. 6.

Betroffenen, die dieser infolge eines Verstoßes gegen die von der Drittbegünstigtenklausel umfassten Bestimmungen erleidet.

Allerdings kommt der Datenimporteur gemäß der Klausel 6 Absatz 2 unmittelbar für die von ihm selbst verursachten Schäden des Betroffenen auf, sofern der Datenexporteur sich tatsächlich aufgelöst hat, rechtlich nicht mehr besteht oder zahlungsunfähig geworden ist.

Da eine gesamtschuldnerische Haftung der Übermittlungsparteien nicht vorgesehen ist, vermag der Betroffene also seine Ansprüche gegen den Datenexporteur ebenfalls nur bis zu dem Eintritt einer solchen Bedingung geltend zu machen. Dieser Haftungserlass zugunsten des Datenimporteurs rechtfertigt sich allerdings aus seiner fehlenden Verantwortlichkeit für die Verarbeitung.[701]

(3) Ergebnis

Wie bereits für die Standardvertragsklauseln im Rahmen einer Funktionsübertragung festgestellt, gelingt es auch den Vertragsklauseln für die Auftragsverarbeitung, dem Betroffenen einen weitreichenden Schutz seiner Privatsphäre zu gewährleisten. Die Befugnisse der mitgliedstaatlichen Datenschutzbehörden gegenüber dem Datenimporteur wurden im Vergleich zu der ersten Entscheidung der Kommission sogar ausgebaut.

Eine Unterbindung der Übermittlung ist den Kontrollbehörden gemäß Artikel 4 der Entscheidung vom 27. Dezember 2001 gleichwohl zu denselben Konditionen möglich wie im Rahmen der Entscheidung vom 15. Juni 2001.[702] Auch hat sich die Kommission wiederum in Artikel 5 eine Überprüfung der Durchführung ihrer Entscheidung nach einer Laufzeit von drei Jahren vorbehalten.

Da die beiden Entscheidungen über Standardvertragsklauseln noch recht jung sind, reichen die bisherigen Erfahrungen mit ihrer Durchsetzung in der Praxis nicht über die Phase des Vertragsabschlusses hinaus. Es bleibt daher abzuwarten, ob und wie sich die Vertragsklauseln dauerhaft bewähren werden.

[701] *Räther/Seitz*, MMR 2002, S. 520, S. 525.
[702] Vgl. dazu Gliederungspunkt E.I.3.a.(4). dieses Kapitels.

4. Die Genehmigung durch den Mitgliedstaat

Eine grenzüberschreitende Datenübermittlung im Sinne des Artikels 26 Absatz 2 der Richtlinie ist nur auf der Grundlage einer Genehmigung durch den betreffenden Mitgliedstaat zulässig. Eine solche Genehmigung „kann", muss aber nicht erteilt werden, sofern der Datenübermittler ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet. Der Datenübermittler hat also keinen Anspruch auf Erteilung der Genehmigung, sondern nur auf eine ermessensfehlerfreie Bescheidung seines Antrages.[703]

Die Behörde beurteilt die Angemessenheit der dargebotenen Garantien anhand einer ausführlichen Beschreibung der spezifischen Umstände der betreffenden Übermittlung oder Kategorien von Übermittlungen, die dem Antrag beizufügen ist. Zu den erforderlichen Informationen zählen in Anlehnung an die gemäß Artikel 25 Absatz 2 der Richtlinie bei der Beurteilung des Schutzniveaus eines Drittlandes zu berücksichtigenden Umstände in jedem Fall die Art der Daten, die Dauer ihrer Verarbeitung, der Übermittlungszweck, das Destinationsland sowie der Empfänger und die Tätigkeiten, in deren Rahmen die Übermittlung erfolgen soll.

Dabei prüft die Behörde grundsätzlich nicht die Zulässigkeit der Übermittlung nach dem jeweiligen mitgliedstaatlichen Datenschutzgesetz, sondern lediglich die Angemessenheit der angebotenen Garantien. Eine zusätzliche Kontrolle der weiteren Übermittlungsvoraussetzungen ist aber im Rahmen der allgemeinen Datenschutzaufsicht möglich. Stellt die Datenschutzbehörde bei dieser Gelegenheit die Unzulässigkeit der Übermittlung fest, erübrigt sich allerdings auch der Genehmigungsantrag, da kein Anspruch auf eine Genehmigung einer rechtswidrigen Übermittlung besteht.[704]

Über die von ihnen erteilten Genehmigungen informieren die Mitgliedstaaten gemäß Artikel 26 Absatz 3 der Richtlinie die Europäische Kommission und die übrigen Mitgliedstaaten, welche der Genehmigung

[703] *Räther/Seitz*, MMR 2002, S. 520, S. 521; *Rittweger/Weiße*, CR 2003, S. 142, S. 143 ff.; missverständlich *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 18, die offenbar von einer Erteilungspflicht ausgeht.
[704] *Innenministerium Baden-Württemberg*, Hinweise Nr. 40, RDV 2002, S. 148, S. 152 f.

widersprechen dürfen. Über die Begründetheit eines etwaigen Widerspruchs entscheidet die Europäische Kommission nach dem Verfahren des Artikels 31 Absatz 2 der Richtlinie. Im Interesse einer Harmonisierung der Genehmigungspraxis treffen die Mitgliedstaaten die infolgedessen gebotenen Maßnahmen. Im Falle einer negativen Feststellung obliegt dem genehmigenden Mitgliedstaat also die Rücknahme seiner positiven Bescheidung,[705] die sich allerdings nicht rückwirkend auf die Zulässigkeit der bereits auf der Grundlage der Genehmigung erfolgten Übermittlungen auswirkt.

Nicht ganz einheitlich wird die Frage beantwortet, ob eine Übermittlung unter Verwendung der Standardvertragsklauseln ebenfalls einer Genehmigung durch die Mitgliedstaaten bedarf.

Gemäß Artikel 26 Absatz 4 der Richtlinie sollen die Mitgliedstaaten infolge einer Entscheidung der Kommission über Standardvertragsklauseln die „gebotenen Maßnahmen“ treffen. Demgemäß sind die beiden bisherigen Entscheidungen der Kommission im Sinne des Artikels 249 Absatz 4 EGV als sekundäres Gemeinschaftsrecht entsprechend ihren Artikeln 7 an die Mitgliedstaaten gerichtet und müssen von diesen zur Anwendung gebracht werden. Bei der Auswahl der Maßnahmen ist vor allem das Effizienzgebot zu beachten, weshalb die Mitgliedstaaten eine auf der Grundlage von Standardvertragsklauseln stattfindende Übermittlung nicht mehr mit der Begründung behindern dürfen, dass der Datenübermittler keine ausreichenden Garantien im Sinne des Artikels 26 Absatz 2 der Richtlinie biete[706].

Fraglich ist also, ob eine Genehmigung, die ohnehin nicht verweigert werden darf, gewissermaßen aus Gründen eines ordnungsgemäßen Verwaltungsverfahrens dennoch zu beantragen ist.

Dafür spricht, dass die Aufsichtsbehörden auf diese Weise von der Übermittlung erfahren und bei der Gelegenheit auch gleichzeitig die weiteren Zulässigkeitsvoraussetzungen der Übermittlung untersuchen können. Allerdings räumen auch die Artikel 25 und 26 Absatz 1 der Richtlinie den Aufsichtsbehörden keinen besonderen Anlass zur Ausübung ihrer Kontrollbefugnisse ein.

---

[705] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 26, Rn. 27.

[706] *Klug*, BDSG, S. 133; *Metzger*, CR 2002, S. 395; *Räther/Seitz*, MMR 2002, S. 520, S. 522; *Reimer*, DuD 2002, S. 185; *ders*., DuD 2001, S. 498; *Schaar*, Datenschutz im Internet, Rn. 871; a. A. Simitis u. a. (- *Simitis*), BDSG, § 4c, Rn. 52 f., der von einer umfassenden Prüfungsbefugnis im konkreten Einzelfall ausgeht, die auch eine Genehmigungsverweigerung zur Folge haben könne.

Gegen das Erfordernis eines Genehmigungsverfahrens spricht ferner der Wortlaut des Artikels 26 Absatz 4 der Richtlinie, der nicht auf die Genehmigungspflicht aus Artikel 26 Absatz 2 der Richtlinie verweist, sondern lediglich auf das Merkmal der ausreichenden Garantien. Auch der Sinn und Zweck einer Flexibilisierung des grenzüberschreitenden Datenverkehrs legt nahe, dass es sich bei dem Artikel 26 Absatz 4 der Richtlinie um eine Ermächtigungsnorm für die Europäische Kommission zur Schaffung weiterer Erlaubnistatbestände für grenzüberschreitende Datenübermittlungen handelt. Die gebotenen Maßnahmen der Mitgliedstaaten können folglich nur darin bestehen, die Standardvertragsklauseln von der in ihren nationalen Gesetzen vorgeschriebenen Genehmigungspflicht für Übermittlungen auszunehmen.[707]

Zulässig bleibt indessen eine Meldepflicht gegenüber den mitgliedstaatlichen Kontrollbehörden[708] sowie die Ausübung der Kontrollbefugnisse im Rahmen des jeweiligen Artikels 4 der Entscheidungen der Kommission über die Standardvertragsklauseln.

II. Code of Conduct

In den Mitgliedstaaten und bei der Europäischen Kommission besteht inzwischen größtenteils Einigkeit darüber, dass auch verbindliche Unternehmensrichtlinien, so genannte Codes of Conduct, ausreichende Garantien im Sinne des Artikels 26 Absatz 2 der Richtlinie gewährleisten können.[709]

---

[707] Davon auch ausgehend *Innenministerium Baden-Württemberg*, Hinweise Nr. 40, RDV 2002, S. 148, S. 153 und dem seit April 2002 folgend der „*Düsseldorfer Kreis*“ (gemäß *Räther/Seitz*, MMR 2002, S. 520, S. 522); *Brühann*, DuD 2002, S. 359, S. 362; *Klug*, BDSG, S. 135; *Rittweger/Weiße*, CR 2003, S. 142, S. 149; *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 20; gegenteiliger Auffassung offenbar *Europäische Kommission*, Schreiben an die Mitgliedstaaten vom 21.8.2003 (Mitteilungen der Mitgliedstaaten nach Artikel 26 Absatz 3 der Richtlinie und Austausch bewährter Verfahren), S. 2 f.; ebenso *Abel*, Praxishandbuch, 8/4.4.3, S. 17; *ders.*, BDSG, S. 89; *Bergmann/Möhrle/Herb*, § 4c BDSG, Rn. 23; Kaminski u. a. (- *Blömer/Moos*) 2. Kap. D, Rn. 59; *Büllesbach*, RDV 2002, S. 55, S. 60; *Draf*, S. 124; *Ellger*, RabelsZ 60, S. 738, S. 760; *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5; S. 18; *Wuermeling*, Handelshemmnis Datenschutz, S. 165.

[708] *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 20.

[709] *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 27; *WP 74*, S. 4 ff.; *Änderungsvorschläge zur RL 95/46/EG* von Österreich, Finnland, Schweden und Großbritannien, (Explanatory Note, September 2002, abrufbar unter: www.lcd.gov.uk/ccpd/dpdamend.htm), Rn. 28; *Büllesbach*, Data Protection Conference, Brüssel 2002, S. 7; *Pradelles*, ebenda, S. 3; *Strack*, ebenda, S. 4. Der § 4c Absatz 2 BDSG erwähnt die Möglichkeit zur Nutzung von Unternehmensrichtlinien sogar ausdrücklich.

Für multinationale Konzerne erweist es sich wegen ihrer weltweit angelegten, komplexen Strukturen auf lange Sicht als höchst unpraktikabel, konzerninterne Datenübermittlungen in Drittländer jeweils auf der Grundlage einzelner Übermittlungsverträge im Sinne des Artikels 26 Absatz 2 der Richtlinie durchzuführen. Die konzernweite Implementierung eines Codes of Conduct ermöglicht indessen, dauerhaft ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen bei Verarbeitungen von personenbezogenen Daten weltweit in allen Konzernteilen zu bieten.

Schon seit längerem versuchen daher verschiedene multinationale Konzerne, einen konzerninternen Code of Conduct zu entwickeln, der im Hinblick auf die Anforderungen der Richtlinie 95/46/EG ausreichende Garantien bietet und die Besonderheiten der jeweiligen mitgliedstaatlichen Datenschutzgesetze berücksichtigt.[710] Ebenso wie bei der Gestaltung von Vertragsklauseln zeigen sich dabei als größte Herausforderungen die verbindliche Begründung von Rechten des Betroffenen sowie die Gestaltung einer Haftungs- und Kontrollregelung.[711]

Darüber hinaus stehen insbesondere solche Konzerne, die Niederlassungen in verschiedenen Mitgliedstaaten unterhalten, vor dem Problem, dass sie von allen Mitgliedstaaten eine Genehmigung einholen müssen, von deren Hoheitsgebiet Konzernteile personenbezogene Daten in Drittländer übermitteln. Aufgrund der national unterschiedlich geprägten Genehmigungspraxis und der sogar generell ablehnenden Haltung einiger Mitgliedstaaten gegenüber Codes of Conduct scheint es zudem fast unmöglich, in absehbarer Zeit ein allseitig akzeptiertes Konzept vorzulegen.

Im Übrigen ist es erst Ende letzten Jahres einem Konzern, namentlich der *DaimlerChrysler AG,*[712] gelungen, überhaupt von einem Mitgliedstaat, nämlich aus Deutschland, eine Genehmigung für Übermittlungen

[710] Z. B. Bosch, DaimlerChrysler, General Electrics, Hewlett Packard, Intel, Shell, Siemens und Unilever.
[711] *Innenministerium Baden-Württemberg*, Hinweise Nr. 40, RDV 2002, S. 148, S. 153, das daher zu einer Übernahme der entsprechenden Vorschriften der Standardvertragsklauseln rät.
[712] Abrufbar unter dem Link „Verhaltensregeln“ auf der Website: www.daimlerchrysler.com/dccom/0,,0-5-56921-49-56934-1-0-0-0-0-0-36-10736-0-0-0-0-0-0-0,00.html; abgedruckt in: *Berliner Datenschutzbeauftragter*, S. 38.

auf der Grundlage eines Codes of Conduct zu erhalten.[713] Die Genehmigung liegt derzeit der Kommission und den übrigen Mitgliedstaaten gemäß Artikel 26 Absatz 3 der Richtlinie zur Kenntnisnahme vor.

Angesichts dieser die einzelstaatliche Ebene übersteigenden Dimension nahm sich inzwischen auch die Europäische Kommission der Materie an und forderte die Art. 29-Gruppe zu einer Auseinandersetzung mit der Rolle verbindlicher unternehmensinterner Vorschriften bei der Gewährleistung ausreichender Garantien im Sinne des Artikels 26 Absatz 2 der Richtlinie auf.[714] Die ersten, im Arbeitsdokument WP 74 vom 3.6.2003 veröffentlichten wegweisenden Empfehlungen der Datenschutzgruppe wurden in der nachfolgenden Darstellung über die Merkmale des Inhalts und des Durchsetzungsmechanismus eines den Voraussetzungen des Artikels 26 Absatz 2 der Richtlinie entsprechenden Codes of Conduct berücksichtigt.

1. Die Gewährleistung der inhaltlichen Grundsätze ausreichender Garantien

Verbindliche Unternehmensrichtlinien zeichnen sich dadurch aus, dass sie einheitlich in einem gesamten Unternehmen beziehungsweise Konzern gelten.[715] Im Gegensatz zu Vertragsklauseln im Rahmen von Funktionsübertragungen müssen sie daher nicht nur ein angemessenes Schutzniveau bei der Verarbeitung in dem Drittland bieten, sondern auch hinsichtlich der Datenverwendungen innerhalb der Europäischen Union die Bestimmungen der Richtlinie 95/46/EG beziehungsweise der mitgliedstaatlichen Datenschutzgesetze berücksichtigen.

Bereits die inhaltliche Gestaltung von Vorschriften, die alle mitgliedstaatlichen Datenschutzgesetze vereinen, erweist sich aber geradezu als unmöglich, da die Mitgliedstaaten gemäß Artikel 5 der Richtlinie nach

---

[713] Zeitgleich wurde die Konformität eines Musters für Unternehmensrichtlinien des *Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV)* gemäß § 38a BDSG, der den Artikel 27 der Richtlinie in nationales Recht umsetzt, festgestellt; vgl. dazu *Berliner Datenschutzbeauftragter*, S. 49 ff. Inzwischen wurden auch General Electrics Datenübermittlungen auf der Grundlage eines Code of Conduct genehmigt.

[714] *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 27.

[715] Roßnagel (- *Büllesbach*), 7.1, Rn. 101; *Gackenholz*, DuD 2000, S. 727, S. 730 f.; Simitis u. a. (- *Simitis*), § 4c, Rn. 59; *Räther/Seitz*, MMR 2002, S. 520, S. 527, die auch einen Mindeststandard genügen lassen, den die einzelnen Unternehmensteile je nach Bedarf verschärfen bzw. anpassen dürften. Ein „einheitliche(r) Standard im Unternehmensverbund" ist auch das Ziel des Entwurfs eines „CoC"-Mustertexts der *Südwestmetall* für seine Mitglieder, RDV 2002, S. 262, S. 263.

Maßgabe der entsprechenden Richtlinienbestimmungen, abgesehen von den Vorschriften über den Drittländertransfer, selbstständig die Voraussetzungen näher bestimmen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

Sofern ein Konzern also Niederlassungen in verschiedenen Mitgliedstaaten unterhält, scheint es sinnvoll, die Vorschriften entweder ausschließlich an der Richtlinie 95/46/EG oder alternativ an jenem mitgliedstaatlichen Datenschutzgesetz zu orientieren, in dem die europäische Zentrale des Konzerns ansässig ist.[716] Die Niederlassungen in den übrigen Mitgliedstaaten müssten sodann angewiesen werden, die zusätzlichen Anforderungen ihrer nationalen Gesetze jeweils in einem speziellen Anhang zu formulieren.

Ein weiteres Problem taucht auf, sofern eine mitgliedstaatliche Niederlassung in einem außereuropäischen Konzernteil personenbezogene Daten verarbeiten lässt, ohne dass ihre Verantwortung auf die Stelle in dem Drittland übergeht. Gemäß Artikel 4 Absatz 1 der Richtlinie findet auf diese Verarbeitung das Recht desjenigen Mitgliedstaates Anwendung, in dem die für die Verarbeitung verantwortliche Niederlassung ansässig ist. Es bedarf also einer weiteren Bestimmung in dem Code of Conduct darüber, dass die Daten im Rahmen eines solchen Auftragsverhältnisses ausschließlich gemäß den Anweisungen der mitgliedstaatlichen Niederlassung verarbeitet werden dürfen, die wiederum auf der Grundlage des jeweiligen mitgliedstaatlichen Datenschutzgesetzes ergehen.

Darüber hinaus ist die Weiterübermittlung von aus der Europäischen Union importierten Daten durch außereuropäische Konzernteile an unternehmensfremde Stellen zu regeln, da sich die Vorschriften zum Drittländertransfer lediglich auf die grenzüberschreitende Datenübermittlung aus einem Mitgliedstaat in Drittländer beziehen. Hier bietet sich die Formulierung der ersten Variante des Weitergabegrundsatzes aus den Anlagen 2 und 3 der Standardvertragsklauseln im Rahmen von Funktionsübertragungen an.[717] Zwar bestehen nach wie vor Bedenken

[716] Der Code of Conduct der *DaimlerChrysler AG* ist zum Beispiel am deutschen BDSG ausgerichtet.

[717] Nicht ganz eindeutig dazu *WP 74*, S. 9, in dem nicht klar wird, ob eine Weitergabe von einem außereuropäischen Konzernteil an einen Dritten nur auf der Grundlage von Standardvertragsklauseln erfolgen darf und die Übermittlung des Dritten an weitere Empfänger dem Grundsatz der Weitergabe unterliegt oder ob sich bereits der Transfer durch die außereuropäische Zentrale an den Dritten nur an dem Weitergabegrundsatz der Standardvertragsklauseln orientieren soll; vgl. dazu auch dort Fn. 18 auf S. 17, die eher für die erste Variante spricht;

gegen die bloße Widerspruchsmöglichkeit bei einer Weitergabe nicht sensibler Daten. Es ergäbe aber wenig Sinn, einen strengeren Maßstab an die Verarbeitungen solcher Unternehmen anzulegen, die ihre Garantien mittels eines Codes of Conduct beibringen, als an solche, die stattdessen auf die Standardvertragsklauseln zurückgreifen.[718]

Die Art. 29-Gruppe spricht sich außerdem für eine Übernahme der Drittbegünstigtenklausel zugunsten des Betroffenen aus den Standardvertragsklauseln im Rahmen einer Funktionsübertragung aus, die dem Betroffenen zusätzliche Rechte im Hinblick auf die Verarbeitung seiner aus einem Mitgliedstaat übermittelten Daten in einem außereuropäischen Konzernteil einräumt.[719] Die in Bezug auf die Gestaltung der inhaltlichen Grundsätze relevanten Auskunfts- und Informationspflichten wurden bereits an anderer Stelle dargestellt.[720]

Wie ebenfalls im Rahmen der Standardvertragsklauseln erörtert, sind die Verarbeitungsvorschriften im Hinblick auf die Arbeitsabläufe und die interne Struktur des Unternehmens zu konkretisieren, um auch Mitarbeitern in solchen Ländern, die über keine ausgeprägte Datenschutzstruktur und –kultur verfügen, Anhaltspunkte für eine datenschutzgerechte Gestaltung ihrer Arbeitsprozesse zu liefern.[721]

2. Die Durchsetzungsmechanismen eines Codes of Conduct

Die größte Herausforderung bei der Implementierung eines Codes of Conduct stellt seine konzernweite Durchsetzung dar. Teils kann dabei zwar auf die in den Standardvertragsklauseln entwickelten Mechanismen zurückgegriffen werden, teils erfordern der enge Zusammenschluss der Übermittlungsparteien sowie die umfassende und dauerhafte Umsetzung des Codes in allen Arbeitsprozessen im Vergleich zu dem meist nur partiellen Einfluss der Standardvertragsklauseln auf die internen Verfahren andere Maßnahmen der Durchsetzung.

---

vgl. aber auch *Retzer/Rich/Wugmeister*, CRi 2003, S. 129, S. 132, die offensichtlich annehmen, dass das WP 74 die Weitergabe an Dritte außerhalb des Konzerns bereits unter Beachtung des Weitergabegrundsatzes der Standardvertragsklauseln zulassen will.

[718] Vgl. aber den Vorschlag für allgemeine Bestimmungen eines Code of Conduct bei *Gackenholz*, DuD 2000, S. 727, S. 732, der eine den Artikeln 25 und 26 entsprechende Regelung für den gesamten Konzern vorsieht.

[719] *WP 74*, S. 12 f.

[720] Vgl. oben Gliederungspunkt E.I.3.a.(1).(b).bb. dieses Kapitels.

[721] *WP 74*, S. 14 f.

Nach dem bewährten Prüfungsschema soll nachfolgend ermittelt werden, auf welche Weise eine gute Befolgungsrate, eine effektive Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte sowie ein zuverlässiges Entschädigungssystem zu gewährleisten sind.

a. Befolgungsrate

Eine gute Befolgungsrate setzt zum einen die interne Bekanntheit des Codes und eine entsprechende Bereitschaft zu seiner Einhaltung voraus sowie eine hinreichende Information des Betroffenen über seine Existenz. Als unabdingbar gilt ferner eine regelmäßige Kontrolle, die in ihrer Wirkung als Druckmittel von Straf- beziehungsweise Disziplinarmaßnahmen unterstützt werden sollte.

Die Sicherstellung der internen Bekanntheit eines Codes of Conduct erfordert eine Mitteilung sowohl an alle Konzernteile als auch individuell an alle Mitarbeiter,[722] denen die Umsetzung des Codes of Conduct als Unternehmensziel vermittelt werden sollte.[723] Darüber hinaus scheint eine zielgerichtete konzerninterne Organisationsstruktur[724] des Datenschutzes und der Datensicherheit in der Form eines Netzwerkes von auf allen Konzernebenen angesiedelten Mitarbeitern notwendig, die sowohl eine Kontroll- als auch eine beratende Funktion wahrnehmen und der Weisung eines kraft Gesetzes unabhängigen Konzerndatenschutzbeauftragten unterliegen.[725]

Eine Verpflichtung der Konzernteile zur Umsetzung des Codes könnte sich dabei je nach Form des Zusammenschlusses etwa aus einer für alle Konzernteile verbindlichen Zentralanweisung der Konzernmutter oder aus internen Verträgen ergeben, beides möglichst gestützt durch die Annahme des Codes vom Vorstand des Mutterunternehmens. Dabei ist nachdrücklich auf die Verbindlichkeit der Bestimmungen und ihre obligatorische Anwendbarkeit aufgrund der Vorschriften zum Drittländertransfer der mitgliedstaatlichen Datenschutzgesetze hinzuweisen.

---

[722] *Räther/Seitz*, MMR 2002, S. 520, S. 527.

[723] *Gackenholz*, DuD 2000, S. 727, S. 731; vgl. auch den Code of Conduct der *DaimlerChrysler AG* für Kunden- und Lieferantendaten, S. 7 (abrufbar unter dem Link „Verhaltensregeln“ auf der Website: www.daimlerchrysler.com/dccom/0,,0-5-56921-49-56934-1-0-0-0-0-0-36-10736-0-0-0-0-0-0-0,00.html), der Datenschutz und Datensicherheit als Unternehmensziele definiert; auch veröffentlicht von dem *Berliner Datenschutzbeauftragten*, S. 38.

[724] *Gackenholz*, DuD 2000, S. 727, S. 731.

[725] Vgl. dazu auch die Darstellung des dem Konzerndatenschutzbeauftragten unterstehenden weltweiten Netzwerkes von Mitarbeitern in den Bereichen Datenschutz und Informationssicherheit der Bosch-Gruppe: *Bijok/Triedwindt*, DuD 2003, S. 207, S. 208; zur vergleichbaren Situation bei DaimlerChrysler: *Büllesbach*, RDV 2000, S. 1, S. 3 f.

Im Interesse der Einhaltung der Vorschriften und einer effektiven Durchsetzung der Rechte des Betroffenen sollte jener in der Europäischen Union ansässige, an ein mitgliedstaatliches Datenschutzgesetz gebundene Konzernteil für die konzernweite Umsetzung verantwortlich sein, der die Garantien gegenüber der Datenschutzbehörde bietet.

Dessen ungeachtet ist die tatsächliche Vollziehung eines Codes of Conduct im Konzernalltag nur gewährleistet, sofern die einzelnen Mitarbeiter ein ausgeprägtes Datenschutzbewusstsein entwickeln und sich zur Anwendung der Datenschutzbestimmungen verpflichtet fühlen.

Ein solches Pflichtgefühl vermag insbesondere durch ausdrückliche Verantwortungszuweisungen auf allen Ebenen gefördert zu werden.[726] So schreibt die derzeitige, mit den inhaltlichen Grundsätzen der Richtlinie 95/46/EG korrespondierende Zentralweisung „Datenschutz und Persönlichkeitsrecht“ der *Bosch-Gruppe* zum Beispiel vor, dass Vorgesetzte für die Einhaltung und Umsetzung der Zentralanweisung in ihrem Bereich verantwortlich sind und ihre Mitarbeiter dementsprechend regelmäßig über ihre Rechte und Pflichten im Umgang mit personenbezogenen Daten unterrichten und ausbilden müssen. Die einzelnen Mitarbeiter werden von der Zentralanweisung auf ihre entsprechende Verantwortlichkeit im Rahmen ihrer Aufgabenstellung hingewiesen.

Die Wirkung dieser Verantwortungszuweisung bleibt jedoch beschränkt, sofern die Mitarbeiter nicht die notwendigen Informationen zur Umsetzung eines effektiven Datenschutzes an die Hand bekommen.

Die Bestimmungen müssen daher an einem allen Mitarbeitern zugänglichen und auffälligen Ort publik gemacht, verstanden und allgemein angewandt werden.

Als geeigneter Ort der Veröffentlichung kommt in erster Linie das unternehmenseigene Intranet in Betracht sowie anlässlich der Einführung des Codes im Unternehmen die Ausgabe eines Handbuchs oder einer Broschüre. Für die schnelle und zuverlässige Bekanntgabe etwaiger Aktualisierungen eignen sich insbesondere E-Mail-Rundschreiben.

---

[726] *Schrecker* in: Datenverkehr ohne Datenschutz?, S. 157, S. 165; vgl. dazu auch den Entwurf der *Südwestmetall*, RDV 2002, S. 262, S. 265, Rn. 9.1 und 9.2.2., der allerdings die Verantwortung so detailliert aufteilt, dass die Gefahr einer Abschiebung der Verantwortlichkeit auf eine jeweils andere Ebene besonders hoch scheint.

Darüber hinaus sind kontinuierliche, obligatorische Schulungen anzubieten,[727] die sich in ihrer Ausrichtung und Intensität je nach Aufgabengebiet der jeweiligen Mitarbeiter staffeln können. Die Teilnahme sollte nicht nur jenen Mitarbeitern offen stehen, die regelmäßig personenbezogene Daten verarbeiten, sondern auch solchen, die nur gelegentlich mit Daten in Kontakt kommen. Für Niederlassungen in jenen Drittstaaten, die über keine oder eine nur sehr eingeschränkte Datenschutzstruktur verfügen, empfehlen sich neben diesen Spezialfortbildungen zusätzlich allgemeine Datenschutzschulungen für alle in der Verwaltung tätigen Beschäftigten.

Für die Risikoanalyse im konkreten Einzelfall bieten sich außerdem Checklisten an, anhand derer zum Beispiel Führungskräfte den Sicherheitsstandard in ihrer Abteilung selbstständig und nach Bedarf zu ermitteln vermögen.[728]

Die Durchsetzung des Codes of Conduct vermag ferner durch die Androhung von Disziplinarmaßnahmen in Form von arbeitsrechtlichen Konsequenzen gefördert zu werden.[729]

Die Transparenz gegenüber dem Betroffenen ist in jedem Fall gewahrt, sofern die in der Drittbegünstigtenklausel der Standardvertragsklauseln im Rahmen einer Funktionsübertragung genannten Informations- und Auskunftspflichten zusätzlich in den Text der Unternehmensrichtlinie aufgenommen werden. Eine Bekanntgabe der Vorschriften auf der Website des Unternehmens im Internet würde dem Betroffenen zudem den Zugang zu den Bestimmungen erheblich erleichtern.[730]

Des Weiteren ist eine regelmäßige Kontrolle der Durchführung eines Codes of Conduct zu garantieren, die in Anlehnung an die FAQ 7 der Safe Harbor Privacy Principles entweder im Wege der Selbstüberwachung oder der Beauftragung externer Auditoren erledigt werden kann. Hinsichtlich der Durchführung eines Audits wird daher auf die entsprechenden Erläuterungen zu den Safe Harbor Privacy Principles verwiesen.[731]

---

[727] *Räther/Seitz*, MMR 2002, S. 520, S. 528.
[728] *Bijok/Triedwindt*, DuD 2003, S. 207, S. 209.
[729] So z. B. der Code of Conduct der *DaimlerChrysler AG* für Kunden- und Lieferantendaten, S. 15 (abrufbar unter dem Link „Verhaltensregeln“ auf der Website: www.daimlerchrysler.com/dccom/0,,0-5-56921-49-56934-1-0-0-0-0-0-36-10736-0-0-0-0-0-0-0,00.html); auch veröffentlicht von dem *Berliner Datenschutzbeauftragten*, S. 38, S. 46.
[730] *Büllesbach/Höss-Löw*, DuD 2001, S. 135, S. 138.
[731] Vgl. dazu Gliederungspunkt C.III.2.c.(7).(a).bb. dieses Kapitels.

Die Art. 29-Gruppe verlangt zudem eine Berichterstattung über das Audit an den Aufsichtsrat des Mutterkonzerns. Ebenfalls soll die zuständige mitgliedstaatliche Datenschutzbehörde eine Kopie des Durchführungsberichts entweder auf Anforderung oder bei der Gelegenheit einer Bekanntgabe von Aktualisierungen des Codes erhalten. Sei der Bericht nicht verfügbar oder gelange die Datenschutzbehörde zu der Auffassung, dass die für eine Aufrechterhaltung der Genehmigung erforderlichen Angaben nicht enthalten seien, so müsse sie darüber hinaus dazu befugt sein, selbst ein Audit zu initiieren. Sofern die bereits mehrfach angesprochenen völkerrechtlichen Bedenken auszuräumen sind, ist auf diese Weise jedenfalls eine effektive Kontrolle sichergestellt.

Indessen scheint die Androhung von Strafmaßnahmen gegen einzelne Konzernteile in einem Code of Conduct ähnlich wie im Rahmen der Vertragslösung kaum effektiv realisierbar, da sie auf eine konzerneigene Durchsetzung angewiesen wäre.

Eine sanktionierende Wirkung kommt allerdings der Möglichkeit der Datenschutzbehörde zur Aufhebung oder Aussetzung der Genehmigung zu, die sowohl der Europäischen Kommission als auch den übrigen Mitgliedstaaten berichtet wird und sogar veröffentlicht werden kann.

Darüber hinaus ist auf die wettbewerbsrechtlichen Eingriffsbefugnisse des Destinationsstaates, in Bezug auf die USA also der Federal Trade Commission, bei einem Verstoß von Unternehmen gegen die eigene Datenschutzpolitik zu hoffen.[732]

b. Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte

Die Unterstützung des Betroffenen bei der Geltendmachung seiner Rechte setzt voraus, dass diese verbindlich in dem Code of Conduct begründet werden. Ferner muss dem Betroffenen ein effektives Beschwerdeverfahren zur Verfügung stehen.

[732] Vgl. dazu ausführlich die Gliederungspunkte C.III.2.b.(2). und C.III.2.c.(7).(a).cc. dieses Kapitels.

(1) Die Rechte des Betroffenen

Die Rechte des Betroffenen, deren Umfang gemäß dem Arbeitsdokument WP 74 der Art. 29-Gruppe demjenigen von den Standardvertragsklauseln im Rahmen einer Funktionsübertragung vorausgesetzten entsprechen sollte, sind in Form einer Drittbegünstigtenklausel unmittelbar in dem Code of Conduct niederzulegen.[733]

Da jedoch unternehmensinterne Richtlinien grundsätzlich keine direkte Verbindlichkeit nach außen entfalten, müssen andere Wege zur Durchsetzbarkeit der Rechte des Betroffenen gefunden werden. Die einfachste Methode scheint dabei eine einseitige Verpflichtungserklärung des Konzerns mit Schutzwirkung zugunsten Dritter gegenüber der zuständigen Datenschutzbehörde zu sein. Eine solche Verpflichtung geht der Konzern im Grunde schon bei der Beantragung der Genehmigung aufschiebend bedingt durch deren tatsächliche Erteilung ein.[734]

Nicht alle mitgliedstaatlichen Rechtsordnungen sehen indessen eindeutig die Möglichkeit zur Begründung von Rechten Dritter in einseitigen Verpflichtungserklärungen vor.[735] In solchen Fällen müsste die für die Umsetzung des Codes of Conduct verantwortliche Niederlassung mit den einzelnen Konzernteilen Verträge mit Schutzwirkung zugunsten Dritter über die Verbindlichkeit der Unternehmensrichtlinien abschließen.[736] Diese Gestaltungsform stellt allerdings letztlich nichts anderes als eine Variante der Vertragslösung dar.[737]

(2) Das Beschwerdeverfahren

Ein effektives Beschwerdeverfahren setzt zunächst voraus, dass dem Betroffenen neben einem konzerninternen Ansprechpartner auch eine mit entsprechenden Untersuchungsbefugnissen ausgestattete, unabhängige Beschwerdestelle zur Verfügung steht.

---

[733] *WP 74*, S. 12 f.
[734] A. A. offenbar Simitis (- *Simitis*), § 4c, Rn. 60, der die verpflichtende Wirkung als Vorbedingung für die Überprüfung durch die Aufsichtsbehörde betrachtet.
[735] *WP 74*, S. 11 ff.
[736] *WP 74*, S. 13; vgl. aber *Büllesbach/Höss-Löw*, DuD 2001, S. 135, S. 137, die darauf hinweisen, dass insbesondere im anglo-amerikanischen Recht Formvorschriften oder andere Anforderungen zu beachten seien, die einen Vertragsabschluss deutlich erschweren würden.
[737] Simitis (- *Simitis*), § 4c, Rn. 55.

Wie bereits bei der Vertragslösung kommen für diese Aufgabe im Grunde nur die mitgliedstaatlichen Datenschutzbehörden in Betracht. In Anlehnung an die Regelung der Standardvertragsklauseln im Rahmen einer Funktionsübertragung scheint eine Kooperationsverpflichtung sinnvoll, mit der die außereuropäischen Konzernteile verbindlich zusagen, dass sie alle Feststellungen der Behörde hinsichtlich der Verarbeitung der aus der Europäischen Union übermittelten Daten respektieren werden.[738] Unterstützt zu werden vermag die Kontrollbehörde durch einen Konzerndatenschutzbeauftragten, der in gesetzlich legitimierter Unabhängigkeit mithilfe eines weltweiten, seiner Weisung unterliegenden Mitarbeiterstabes für eine ordnungsgemäße Durchführung des Codes of Conduct sorgt.[739]

Indessen hält es die Art. 29-Gruppe offenbar für unabdingbar, dass die Kontrollbehörden ihre Prüfungsbefugnisse in gleicher Weise bei den außereuropäischen Konzernteilen ausüben dürfen wie in den europäischen Niederlassungen.[740] Diese Vorstellung, die der Klausel 8 Absatz 2 der Standardvertragsklauseln zur Auftragsverarbeitung entspricht, scheint insoweit sinnvoll, als dass in der konzerninternen Organisation oftmals eine zentralisierte Erledigung bestimmter Aufgaben vorgesehen ist. So verarbeiten beispielsweise außereuropäische Rechenzentren Personal- und Kundendaten quasi auf Anweisung anderer Niederlassungen. In diesen Konstellationen des Outsourcings scheint die Festlegung einer Untersuchungsbefugnis im Wege eines Audits durch die Datenschutzbehörden notwendig, da der Konzern anderenfalls geneigt sein könnte, seine Verarbeitungen durch eine bewusste Auslagerung der betreffenden Bereiche absichtlich der Datenschutzaufsicht europäischer Behörden zu entziehen.

Bei Datenübermittlungen mit der Folge eines Verantwortungsübergangs scheint die Forderung der Art. 29-Gruppe indessen überzogen. Wie bereits bei der Frage nach einer Regelung der Weitergabe von Daten durch den außereuropäischen Konzernteil argumentiert, besteht kein Grund für eine schärfere Kontrolle jener Unternehmen, die sich eines Codes of Conduct bedienen, im Vergleich zu solchen, die ausschließlich mit der Vertragslösung operieren. Es sollte daher den Konzernen wenigstens erlaubt sein, die Zulassung der Kontrollbefugnisse der Datenschutzbehörden zu differenzieren je nachdem, ob es bei der betref-

[738] Niedergelegt in Klausel 5c) der entsprechenden Standardvertragsklauseln.
[739] Roßnagel (- *Büllesbach*), 7.1, Rn. 102.
[740] *WP 74*, S. 17 f.

fenden Übermittlung zu einem Verantwortungsübergang kommt oder nicht.

Der Rechtsweg zur Durchsetzung seiner Rechte ist dem Betroffenen möglichst vor einem mitgliedstaatlichen Gericht zu eröffnen. Die außereuropäischen Konzernteile müssen also entweder den Gerichtsstand der für die konzerninterne Durchsetzung des Codes of Conduct verantwortlichen Niederlassung oder jenes Unternehmensteils akzeptieren, der ihnen jeweils die Daten übermittelt hat.[741] In Anlehnung an die Klausel 7 beider Standardverträge wäre es zudem begrüßenswert, dem Betroffenen alternativ eine Schlichtung oder ein Schiedsgerichtsverfahren zur Auswahl zu stellen.[742]

c. Entschädigung des Betroffenen

Die aus einem Verstoß gegen den Code of Conduct erwachsenden Entschädigungsansprüche sollte der Betroffene indessen vollständig gegen eine Niederlassung in der Europäischen Union geltend machen dürfen, da nur auf diese Weise die tatsächliche Erfüllung und insbesondere die Vollstreckung eines zusprechenden Urteils eines mitgliedstaatlichen Gerichts zuverlässig zu gewährleisten ist.[743] Infolgedessen erhöht sich auch zugleich der Druck auf die haftende Niederlassung, den Code of Conduct wirklich gegenüber allen Konzernteilen effektiv durchzusetzen.

Um die Zahlungsfähigkeit des haftenden Konzernteils sicherzustellen, verlangt die Art. 29-Gruppe einen Nachweis darüber, dass er über die entsprechenden Mittel zur Gewährleistung des Schadensersatzes verfügt beziehungsweise eine diesbezügliche Haftpflichtversicherung abgeschlossen hat.[744]

Entsprechend der Entlastungsklausel des Artikels 23 Absatz 2 der Richtlinie sollte der Konzernteil jedoch von der Haftung befreit werden, sofern er im Einzelfall nachzuweisen vermag, dass der betreffende außereuropäische Konzernteil nicht für den Umstand verantwortlich ist, der zum Schadenseintritt geführt hat.

---

[741] *WP 74*, S. 20.
[742] Vgl. dazu insbesondere Gliederungspunkt E.I.3.a.(2).(b).bb. dieses Kapitels.
[743] Vgl. *Däubler* in: Datenverkehr ohne Datenschutz?, S. 71, S. 86; *ders.*, CR 1999, S. 49, S. 55, der bei einer konzerninternen Vertragslösung mit einer Vertragsstrafe für die innereuropäische Niederlassung dasselbe Ergebnis erzielen will.
[744] *WP 74*, S. 19.

d. Eingriffsbefugnisse des Destinationsstaates

Entsprechend den Ausführungen zur Vertragslösung sind auch im Rahmen der Gewährleistung ausreichender Garantien mithilfe eines Codes of Conduct die außereuropäischen Konzernteile dazu anzuhalten, ihre gesetzlichen Verpflichtungen gegenüber ihrem Sitzstaat auf eine Konformität mit den Tatbeständen des Artikels 13 der Richtlinie zu überprüfen.[745]

Im Falle einer negativen Feststellung muss der betreffende Konzernteil zu einer Mitteilung an die in der Europäischen Union ansässige, für die Durchführung des Codes of Conduct verantwortliche Niederlassung verpflichtet sein. Eine Befreiung von dieser Pflicht ist nur für den Fall vorzusehen, dass dem betreffenden Konzernteil die Offenlegung eines staatlichen Zugriffs durch eine Vollstreckungsbehörde aufgrund einer Vertraulichkeitsverpflichtung verboten ist.

Die informierte Niederlassung soll infolge einer solchen Mitteilung gemäß der Art. 29-Gruppe zunächst eine „verantwortliche Entscheidung“ treffen und schließlich das weitere Vorgehen mit der Datenschutzbehörde abstimmen müssen.[746] Anstelle einer freien Entscheidungsfindung scheint es jedoch im Hinblick auf das Schutzbedürfnis des Betroffenen angemessener, die mitgliedstaatliche Niederlassung unmittelbar zu einem sofortigen Übermittlungsstopp zu verpflichten.

3. Variationen eines Codes of Conduct

Ein Code of Conduct sollte generell einheitlich im gesamten Konzern implementiert werden. Je nach Konkretisierung der einzelnen Arbeitsprozesse scheint es aber durchaus sinnvoll, verschiedene Codes of Conduct für unterschiedliche Regelungsbereiche zu entwerfen.

So hat sich die *DaimlerChrysler AG* zum Beispiel für eine Aufteilung ihrer Codes of Conduct zwischen Kunden- und Lieferantendaten auf der einen Seite und Mitarbeiterdaten auf der anderen Seite entschieden. Auf diese Weise konnte gezielter auf die spezifischen, die jeweiligen Daten betreffenden unternehmensinternen Abläufe sowie auf arbeitsrechtliche Besonderheiten im Hinblick auf die Verarbeitung von Mitarbeiterdaten eingegangen werden.

[745] Vgl. dazu die Gliederungspunkte E.I.2.b.(4). und E.I.3.a.(2).(d). dieses Kapitels.
[746] *WP 74*, S. 14.

Alternativ besteht auch die Möglichkeit zu einer Gliederung des Codes in einen allgemeinen und verschiedene besondere Teile,[747] die ebenfalls detailliert auf die Bedürfnisse der konkreten Verarbeitungsbereiche einzugehen vermögen, ohne dass alle Mitarbeiter mit dem gesamten Code vertraut sein müssten.

4. Das Genehmigungsverfahren

Für die Genehmigung der auf der Grundlage des Codes of Conduct geplanten Übermittlungen gelten grundsätzlich dieselben Bedingungen wie im Rahmen der Vertragslösung.[748]

Besonderheiten sollen allerdings hinsichtlich der Zulässigkeit von Änderungen des Codes bestehen. Ferner scheint eine Vereinfachung des Genehmigungsverfahrens für solche Konzerne erforderlich, die einer Genehmigung ihrer auf der Grundlage des Codes durchgeführten Übermittlungen aus verschiedenen Mitgliedstaaten bedürfen.

a. Änderungen des Codes of Conduct

Angesichts der sich stetig wandelnden Strukturen und Verfahrensweisen eines Unternehmens befürwortet die Art. 29-Gruppe unter bestimmten Voraussetzungen die durchaus sinnvolle Möglichkeit zu einer Anpassung des Codes of Conduct an geänderte Arbeitsprozesse oder ein neues Umfeld, ohne dass erneut eine Genehmigung beantragt werden müsse.[749]

Dabei dürfe es sich zwar hinsichtlich der Datenschutzbestimmungen des Codes nicht um signifikante Modifikationen, also etwa Änderungen der Datenschutzgrundsätze, der Verarbeitungszwecke, der Kategorien von Betroffenen oder der zu verarbeitenden Datenkategorien handeln. Indessen sei aber zum Beispiel eine Ausdehnung des Geltungsbereichs des Codes auf einen neuen Unternehmensteil zulässig, sobald dieser die Bestimmungen in seinem Wirkungsbereich implementiert habe.

Die Aktualisierungen müssten einschließlich einer Liste aller von dem Code of Conduct betroffenen Unternehmensteile aufgezeichnet werden, sodass dem Betroffenen oder einer zuständigen Datenschutzbehörde auf

---

[747] Bräutigam/Leupold (- *Büllesbach*), A.III.1., Rn. 110; *Büllesbach/Höss-Löw*, DuD 2001, S. 135, S. 138; *Gackenholz*, DuD 2000, S. 727, S. 731; *Räther/Seitz*, MMR 2002, S. 520, S. 527.
[748] Vgl. dazu Gliederungspunkt E.I.4. dieses Kapitels.
[749] *WP 74*, S. 15 f.

Antrag die erforderlichen Auskünfte erteilt werden könnten. Einmal jährlich habe der Konzern zudem unaufgefordert die Modifikationen mit einer kurzen Begründung den genehmigenden Datenschutzbehörden mitzuteilen.

b. Vereinfachung des Genehmigungsverfahrens im Hinblick auf eine europaweite Implementierung des Codes of Conduct

Bislang nicht gelöst ist die Frage nach einer Vereinfachung des Genehmigungsverfahrens für europaweit niedergelassene Konzerne, die einer Genehmigung aus allen Mitgliedstaaten bedürfen, von deren Hoheitsgebiet sie Daten in ein Drittland versenden.

Entsprechend dem völkerrechtlichen Prinzip der Staatensouveränität, nach dem kein Staat ohne seine Zustimmung die Vornahme von fremden Hoheitsakten auf seinem Gebiet dulden muss,[750] vermag grundsätzlich kein Mitgliedstaat eine Genehmigung für alle anderen Mitgliedstaaten zu erteilen. Ausnahmsweise kann jedoch eine völkerrechtliche Grundlage existieren, die eine gebietsübergreifende Genehmigung ermöglicht.

Eine solche Regelung könnte sich zum Beispiel unmittelbar aus dem Gemeinschaftsrecht ergeben, da im Anwendungsbereich der Gemeinschaftsverträge nach allgemeiner Ansicht das Völkerrecht verdrängt wird.[751] So enthält zum Beispiel die Richtlinie 77/780/EWG vom 15.12.1989[752] Bestimmungen, die den mitgliedstaatlichen Bankaufsichtsbehörden die Zuständigkeit für die Aufsicht über die gesamte Tätigkeit einer in ihrem Hoheitsgebiet ansässigen Bank einschließlich aller unselbstständigen Zweigstellen im gesamten Gemeinschaftsgebiet zusprechen.[753]

Eine derartige gemeinschaftsrechtliche Bestimmung könnte sich vorliegend allein aus der Richtlinie 95/46/EG selbst ergeben. Von der Frage abgesehen, ob eine Konzentration des Genehmigungsverfahrens in diesem konkreten Fall für das Funktionieren des Binnenmarktes erforderlich ist und sonach von der Ermächtigungsgrundlage der Richtlinie 95/46/EG, dem Artikel 100a EGV (neu: Artikel 95 EGV), gedeckt wä-

[750] *Groß*, JZ 1994, S. 596, S. 599.
[751] *Groß*, JZ 1994, S. 596, S. 600.
[752] ABl. EG L 386 vom 30.12.1989, S. 1.
[753] Ausführlich dazu *Groß*, JZ 1994, S. 596 ff.

re, ist dem Wortlaut der Richtlinie 95/46/EG die Option einer solchen Handhabung der Genehmigungspraxis allerdings nicht zu entnehmen.

Zwar sieht Artikel 26 Absatz 3 der Richtlinie eine Unterrichtungspflicht des genehmigenden Mitgliedstaates über die erteilte Genehmigung gegenüber der Kommission und den anderen Mitgliedstaaten vor. Aus einer verstrichenen Chance der weiteren Mitgliedstaaten zu einem Widerspruch gegen die Genehmigung kann jedoch nicht ohne weiteres gefolgert werden, dass diese die Geltung der Genehmigung auch für Verarbeitungen auf ihrem eigenen Hoheitsgebiet als verbindlich akzeptieren.

Sinn und Zweck des Widerspruchsrechts ist vielmehr die Schaffung eines einheitlichen Beurteilungsmaßstabes der Genehmigungsfähigkeit von Übermittlungen.[754] Es soll verhindert werden, dass einzelne Mitgliedstaaten mit einer großzügigen Genehmigungspraxis die Grenzen der Europäischen Union aufweichen und somit die Grundrechte der Betroffenen in allen Mitgliedstaaten gefährden.

Indessen scheint es zwar widersprüchlich, sofern ein Mitgliedstaat die Genehmigung eines anderen Mitgliedstaates im Rahmen des Artikels 26 Absatz 3 der Richtlinie hinnimmt und anschließend den Antrag derselben verantwortlichen Stelle für gleichartige Übermittlungen auf der Grundlage identischer Garantien für sein eigenes Hoheitsgebiet zurückweist. Auch sollte es im Rahmen einer harmonisierten Gesetzeslage und unter Berücksichtigung der einheitlichen Bezugsgröße für die Bewertung eines angemessenen Schutzniveaus, namentlich der Richtlinie 95/46/EG selbst,[755] eigentlich zu keiner unterschiedlichen Auffassung über die Angemessenheit kommen. Allerdings ist das Verfahren des Artikels 26 Absatz 3 der Richtlinie bislang nicht in einer Weise ausgestaltet, die den weiteren Mitgliedstaaten eine realistische Überprüfung des in dem Herkunftsmitgliedstaat gestellten Antrags ermöglichen würde. So enthält die vorgesehene Unterrichtungspflicht keine Vorgaben über die zu erteilenden Informationen,[756] sodass die anderen

[754] Roßnagel (- *Brühann*), 2.4, Rn. 53; Grabitz/Hilf III (- *ders.*), A 30, Art. 26, Rn. 14; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 26, Rn. 21; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 26, Rn. 28; *Ellger*, RabelsZ 60, S. 738, S. 759 f.; *Geis*, NJW 1997, S. 288, S. 291.
[755] Vgl. Gliederungspunkt C.I.1.a. dieses Kapitels.
[756] Vgl. dazu die *Änderungsvorschläge zur RL 95/46/EG* von Österreich, Finnland, Schweden und Großbritannien (Explanatory Note, September 2002, abrufbar unter: www.lcd.gov.uk/ccpd/dpdamend.htm), Rn. 32, die daher eine Präzisierung der zu liefernden Informationen fordern. Vgl. aber Dammann/Simitis (- *Dammann*), EG-Datenschutzrichtlinie, Art. 26, Rn. 23; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 26, Rn. 29, nach deren Auf-

Mitgliedstaaten unter Umständen gar nicht dazu in der Lage sind, sich ein umfassendes Bild von dem zu beurteilenden Sachverhalt zu machen.

Zudem darf die verarbeitende Stelle sofort von der Genehmigung Gebrauch machen und muss nicht das eventuelle Widerspruchsverfahren der Europäischen Kommission nach Artikel 31 Absatz 2 der Richtlinie abwarten.[757] Die verarbeitende Stelle könnte also bereits vor der Unterrichtung der übrigen Mitgliedstaaten von deren Hoheitsgebiet auf der Grundlage der Genehmigung personenbezogene Daten in Drittländer übermitteln.

Im Interesse einer Förderung der Bereitschaft multinationaler Konzerne zur Implementierung einer konzernweiten, den Anforderungen der Richtlinie 95/46/EG entsprechenden Datenschutzstruktur scheint es jedoch geboten, dieser Rechtslage Abhilfe zu schaffen.

Die Art. 29-Gruppe empfiehlt daher ein koordiniertes Genehmigungsverfahren der Mitgliedstaaten mit der Folge einer einheitlichen Genehmigung auf der Grundlage der Sätze 2 und 3 des Artikels 28 Absatz 6 der Richtlinie, nach denen die mitgliedstaatlichen Kontrollstellen einander um die Ausübung ihrer Befugnisse ersuchen dürfen und auf die notwendige gegenseitige Zusammenarbeit verpflichtet werden.[758] Der Mitgliedstaat der Antragstellung würde sodann auf die Erteilung einer Genehmigung durch alle übrigen betroffenen Mitgliedstaaten hinwirken, ohne dass der Betroffene jeweils einen neuen Antrag in diesen Mitgliedstaaten stellen müsste.

Es bleibt abzuwarten, wie ein solches Koordinationsverfahren aussehen wird. Möglich wäre einerseits, dass der Mitgliedstaat der Antragstellung den Antrag vollständig an die übrigen Mitgliedstaaten weiterleitet, um ihn dort von der jeweils zuständigen Behörde prüfen zu lassen. Gelangte einer der Mitgliedstaaten zu dem Ergebnis, dass der Antragsteller keine ausreichenden Garantien im Sinne des Artikels 26 Absatz 2 der Richtlinie bietet, wäre die Datenschutzbehörde des Herkunftsstaates gegenüber dem Antragsteller zur Ablehnung der Genehmigung beziehungsweise zu einer Aufforderung zur Nachbesserung verpflichtet. Ergäbe sich dagegen aus der Sicht aller Mitgliedstaaten eine Konformität

---

fassung bereits die aktuelle Richtlinienfassung zu einer umfassenden Unterrichtung verpflichte.

[757] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 26, Rn. 32.

[758] *WP 74*, S. 21.

der Garantien mit der Richtlinie 95/46/EG, müssten sie den Herkunftsstaat entsprechend ihrer Kooperationsverpflichtung gemäß Artikel 28 Absatz 6 der Richtlinie zu einer Erteilung der Genehmigung ermächtigen. Zur Vereinfachung dieses Prozedere wäre auch die Einrichtung eines Datenschutzforums der mitgliedstaatlichen Kontrollbehörden, vergleichbar etwa mit dem „Düsseldorfer Kreis“ der deutschen Datenschutzbehörden, denkbar.[759]

Alternativ könnten die Mitgliedstaaten auch im Wege eines Verwaltungsabkommens beschließen, dass sie die nach Maßgabe des nationalen Rechts des Herkunftsstaates erteilte Genehmigung, möglicherweise nach umfassender Information und unter Einräumung eines vorherigen Widerspruchsrechts, auch im Hinblick auf solche Niederlassungen eines Konzerns als verbindlich anerkennen, die in ihren eigenen Zuständigkeitsbereich fallen. Um eine Umgehung des Verwaltungsverfahrens besonders strenger Mitgliedstaaten zu vermeiden, sollte der Antragsteller allerdings zur Antragstellung in dem Mitgliedstaat seiner europäischen Zentrale gezwungen sein.

Dieses zunächst praktikabler anmutende Verfahren erweist sich jedoch nur dann als wirklich vorteilhafter als die erste Lösung, sofern die von der Genehmigung betroffenen Mitgliedstaaten zugleich auf die Ausübung ihres Widerspruchsrechts gemäß Artikel 26 Absatz 3 der Richtlinie verzichten. Anderenfalls könnten sie nachträglich ein Verfahren nach Artikel 31 Absatz 2 der Richtlinie anstrengen und somit im Falle einer negativen Feststellung der Europäischen Kommission dem genehmigenden Mitgliedstaat nachträglich die Pflicht zu einer Rücknahme der von ihnen selbst anerkannten Genehmigung aufbürden. Die Übermittlungen des Antragstellers wären sodann zwar zeitweise legalisiert gewesen. Da die konzerninterne Implementierung eines Codes of Conduct jedoch auf Dauer angelegt ist, dürfte dieses Risiko ebenso wenig in dem Interesse des betreffenden Konzerns liegen. Die darüber hinaus bei jeder Genehmigung bestehende Gefahr eines Widerspruchs der nicht betroffenen Mitgliedstaaten ist demgegenüber vergleichsweise gering.

Es bleibt also abzuwarten, inwieweit die Mitgliedstaaten in Zukunft dazu bereit sein werden, auf ihre Hoheitsbefugnisse zugunsten eines flexiblen Genehmigungsverfahrens zu verzichten.

[759] Vgl. auch *Rittweger/Weiße*, CR 2003, S. 142, S. 148 f., die sich allerdings für die Einrichtung einer Genehmigungsstelle auf europäischer Ebene aussprechen.

Eine Entscheidung der Europäischen Kommission über die Gewährleistung ausreichender Garantien durch Standardunternehmensrichtlinien muss indessen, jedenfalls sofern die Verbindlichkeit des Codes of Conduct nicht mithilfe von Verträgen, sondern durch eine einseitige Verpflichtungserklärung hergestellt wird, an dem Wortlaut des Artikels 26 Absatz 4 der Richtlinie scheitern, der ausschließlich Standardvertragsklauseln zulässt. Den Vorschlag[760] einiger Mitgliedstaaten zu einer diesbezüglichen Richtlinienänderung hat die Kommission bereits abgelehnt.[761]

III. Weitere Instrumente zur Gewährleistung angemessener Garantien

Abgesehen von Variationen und Kombinationen der Standardvertragsklauseln und der Codes of Conduct sind darüber hinaus derzeit keine alternativen Instrumente zur Gewährleistung ausreichender Garantien erkennbar. Vereinzelt wird zwar darauf hingewiesen, dass sich außereuropäische Datenverarbeiter auch Verhaltensregeln[762] im Sinne des Artikels 27 der Richtlinie anschließen könnten.[763] Diese Form der Selbstregulierung verfolgt jedoch regelmäßig einen anderen Zweck als die Garantien im Sinne des Artikels 26 Absatz 2 der Richtlinie.

Während Verhaltensregeln auf den mitgliedstaatlichen Datenschutzgesetzen basieren und deren Geltung für ihre Mitglieder auch voraussetzen,[764] müssen die Garantien zur Gewährleistung eines angemessenen Datenschutzniveaus im Rahmen eines Drittländertransfers eine datenschutzrechtliche Grundlage für den Verarbeiter in dem Drittland gerade erst schaffen. Die Unterwerfung eines außereuropäischen Verarbeiters unter eine Verhaltensregel im Sinne des Artikels 27 der Richtlinie setzte also voraus, dass dieser sich ebenfalls einem mitgliedstaatlichen Datenschutzgesetz beugte. Von völkerrechtlichen Bedenken im Hinblick auf die Eingriffsbefugnisse der Kontrollbehörden abgesehen wäre aber allein das schon ausreichend, um ein angemessenes Schutzniveau zu gewährleisten. Verhaltensregeln im Sinne des Artikels 27 der Richtlinie

---

[760] *Änderungsvorschläge zur RL 95/46/EG* von Österreich, Finnland, Schweden und Großbritannien, (Explanatory Note, September 2002, abrufbar unter: www.lcd.gov.uk/ccpd/dpdamend.htm), Rn. 28.

[761] *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 8.

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

[763] *Abel*, Praxishandbuch, 8/4.4.3, S. 11; *ders.*, BDSG, S. 82 f.; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 26, Rn. 19; *Swire/Litan*, S. 37.

[764] Vgl. z. B. den FEDMA Code, S. 2, abrufbar unter: http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77-annex_de.pdf.

eignen sich demnach grundsätzlich nicht als Instrumente im Sinne des Artikels 26 Absatz 2 der Richtlinie.[765]

Allerdings können Wirtschaftsverbände im Wege einer speziellen, sich ausdrücklich auf den Drittländertransfer beziehenden Verhaltensregel im Sinne des Artikels 27 der Richtlinie ihren Mitgliedern mithilfe von Musterklauseln Vorgaben machen, wie eine weltweit, von den einzelnen Mitgliedern jedoch insbesondere in ihren außereuropäischen Zweigstellen noch selbstständig zu implementierende Unternehmensrichtlinie aussehen könnte. Für einen solchen Entwurf des *Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV)* hat bereits der Berliner Datenschutzbeauftragte gemäß der den Artikel 27 der Richtlinie umsetzenden Vorschrift des § 38a BDSG eine Vereinbarkeit mit dem geltenden Datenschutzrecht festgestellt.[766] Der Arbeitgeberverband *Südwestmetall* strebt derzeit eine äquivalente Feststellung in Baden-Württemberg an.[767]

IV. Ausblick

Der Artikel 26 Absatz 2 der Richtlinie scheint im Ergebnis seiner Aufgabe, der Erleichterung des internationalen Datenverkehrs, gerecht zu werden. Dennoch steht die Ausarbeitung ausreichender Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte mit Ausnahme der ersten Entscheidungen über Standardvertragsklauseln noch am Anfang ihrer Entwicklung.

Die Europäische Kommission kündigte daher in ihrem ersten Bericht über die Durchführung der Richtlinie eine verstärkte Nutzung ihrer Entscheidungsbefugnis nach Artikel 26 Absatz 4 der Richtlinie an. Dabei will sie insbesondere Vorlagen von Wirtschaftsvertretern wie zum Beispiel der International Chamber of Commerce und anderen Unternehmensverbänden berücksichtigen.[768]

---

[765] Insoweit irreführend die Annahme von *Moritz/Tinnefeld*, JurPC Web-Dok. 181/2003, Abs. 7, dass es sich bei einem Code of Conduct um eine „Variante der von der EG-Datenschutzrichtlinie (Art. 27) sowie vom BDSG (§ 38a) übernommenen Verhaltensregeln" handele.

[766] Abgedruckt in: *Berliner Datenschutzbeauftragter*, S. 49 ff.

[767] Entwurf abgedruckt in RDV 2002, S. 262.

[768] *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 27. Im September 2003 haben verschiedene Wirtschaftsverbände (ICC, The EU Committee of the American Chamber of Commerce in Belgium, FEDMA, JBCE, ICRT, EICTA, CBI) daraufhin gemeinsam einen Entwurf für weitere Standardvertragsklauseln vorgelegt, abrufbar unter:

Eine Annahme von Vertragsentwürfen aus der Wirtschaft dürfte zudem der weltweiten Akzeptanz des europäischen Datenschutzniveaus zuträglich sein. Unter diesem Gesichtspunkt gebietet sich aber vor allem eine weiterhin intensive Unterstützung der Einführung von Codes of Conduct bei multinationalen Konzernen. Der Einfluss eines weltweiten Datenschutzexports durch einen Global Player sowohl auf Konkurrenzunternehmen als auch auf Zuliefererbetriebe ist in seiner Wirkungskraft von nicht zu unterschätzender Bedeutung für die Förderung der Globalisierung eines angemessenen Datenschutzniveaus.

www.iccwbo.org/home/e_business/word_documents/Model%20contract%20Sept%202003%20FINAL.pdf. Die Klauseln stimmen weitgehend mit den Regelungen der Standardvertragsklauseln im Rahmen einer Funktionsübertragung überein. Indessen bemängelt die Art. 29-Gruppe in *WP 84*, dass die Kooperationsverpflichtung des Datenimporteurs mit den europäischen Aufsichtsbehörden aufgeweicht wurde, ohne durch alternative Mechanismen ersetzt zu werden. Ferner werden die Einschränkungen des Auskunftsrechts des Betroffenen kritisiert und eine Konkretisierung und Vervollständigung des Haftungssystems gefordert.