Zweites Kapitel: Der Anwendungsbereich der mitgliedstaatlichen Datenschutzgesetze

Der Anwendungsbereich der Schutzprinzipien der Richtlinie wird von den Artikeln 3 und 4 festgelegt. Ein zentrales Element beider Vorschriften ist die in Artikel 2b) der Richtlinie legaldefinierte Verarbeitung personenbezogener Daten. Sie bezeichnet jeden „Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“ wie zum Beispiel das Erheben, Speichern, Nutzen, das Weitergeben durch Übermittlung oder das Löschen der Daten. Dabei unterscheidet sie nicht zwischen Verarbeitungen von öffentlichen und nicht öffentlichen Stellen.

Personenbezogene Daten im Sinne der Richtlinie sind gemäß Artikel 2a) „alle Informationen über eine bestimmte oder bestimmbare natürliche Person“. Es kommt weder auf den Wohnsitz noch auf die Staatsbürgerschaft der Person an.[26] Neben Textdaten erfasst die Richtlinie auch die Verarbeitung von Bild- und Tondaten.[27]

[26] Vgl. Erwägungsgrund (2) der Richtlinie.
[27] Erwägungsgründe (14) bis (17) der Richtlinie.

A. Sachlicher Anwendungsbereich

Den sachlichen Anwendungsbereich[28] der Richtlinie bestimmt Artikel 3, der sich in zwei Absätze untergliedert: der erste Absatz schafft einen Regeltatbestand, während der zweite Absatz einige Ausnahmen dazu vorsieht.

I. Regeltatbestand

Gemäß Artikel 3 Absatz 1 ist der sachliche Anwendungsbereich der Richtlinie eröffnet, sofern personenbezogene Daten entweder ganz oder teilweise automatisiert verarbeitet werden. Dasselbe gilt für eine nicht-automatisierte Verarbeitung, sofern die personenbezogenen Daten in einer Datei gespeichert sind oder gespeichert werden sollen. Während also die automatisierte Datenverarbeitung personenbezogener Daten immer in den Anwendungsbereich der Richtlinie fällt, ist die manuelle Verarbeitung nur erfasst, sofern die Daten in einer „strukturierte(n) Sammlung (...) nach bestimmten Kriterien zugänglich sind“[29] beziehungsweise eine solche Sammlung vorgesehen ist.

1. Die automatisierte Verarbeitung

Aus dem Umkehrschluss zu den Anwendungsvoraussetzungen der Richtlinie auf die manuelle Verarbeitung ergibt sich, dass die automatisierte Datenverarbeitung keiner dateiförmigen Struktur bedarf.

Das gilt ebenfalls für den automatisierten Verarbeitungsabschnitt bei einer teilweise automatisierten Verarbeitung. Fraglich ist indessen, wann nur ein Teil der Verarbeitung automatisiert ist und wie weit sein Vorliegen die Anwendbarkeit der Richtlinie auf einen gesamten Verarbeitungskomplex auszudehnen vermag.

Ein Blick auf die Definition der Verarbeitung in Artikel 2b) der Richtlinie legt nahe, dass es sich bei einer teilweise automatisierten Verarbeitung um eine partiell automatisiert durchgeführte Verarbeitungsvariante handeln muss, wie etwa das teilweise automatisierte Erheben, Speichern oder Nutzen der Daten. Die Richtlinie würde sodann zum Beispiel für die gesamte Speicherung gelten, nicht aber für die diese begleitenden manuellen Verarbeitungsschritte.

---

[28] Dammann/Simitis, EG-Datenschutzrichtlinie *(- Simitis*), Einleitung, Rn. 19; *ders*., NJW 1997, S. 281, S. 283.
[29] Artikel 2c) der Richtlinie 95/46/EG.

Andererseits erläutert die Begründung zu Artikel 3 des geänderten Vorschlags zur Richtlinie[30], dass die zusätzliche Erwähnung der *teilweise* automatisierten Verarbeitung in Artikel 3 Absatz 1 darauf hinweisen solle, „dass eine Verarbeitung eine Einheit darstell(e), auch wenn nur ein Teil (beispielsweise der Index) informatisiert (sei)“[31].

Im Gegensatz zu der Betrachtung der einzelnen Verarbeitungsschritte müsste danach zur Feststellung einer teilweise automatisierten Verarbeitung das gesamte Verfahren im Rahmen einer bestimmten Aufgabe oder Zweckbestimmung beurteilt werden. Würde dabei nur ein einzelner Verarbeitungsabschnitt, also zum Beispiel die Organisation der personenbezogenen Daten, in automatisierter Form erfolgen, gölte das Gesamtverfahren als teilweise automatisiert. Infolgedessen wären die Bestimmungen der Richtlinie auf alle Verarbeitungsvorgänge im Rahmen der betreffenden Maßnahme anzuwenden, ungeachtet ihrer eigenen Automatisierung oder Nichtautomatisierung, ihrer dateiförmigen Struktur oder völligen Systemlosigkeit.

In der Praxis werden zum Beispiel Gerichtsakten mit so genannten Barcodes versehen, die bei jedem neuen Vorgang mit Scannerstiften in ein automatisiertes System eingelesen werden, um etwa das Auffinden einzelner Dokumente, Rückschlüsse auf den Inhalt oder eine statistische Auswertung zu erleichtern.[32]

Zöge man das Gesamtverfahren als Maßstab für die partielle Automatisierung der Verarbeitung heran, würde die Registrierung vorhandener manueller Aktenbestände mit Hilfe eines EDV-gestützten Systems zur Anwendung der Richtlinie auf den gesamten Umgang mit den Akten führen.[33] Die Akten wären sonach als physische Ergänzung informatisierter Datensammlungen von den Schutzprinzipien erfasst.[34]

---

[30] *Begründung des geänderten Vorschlags*, abgedruckt in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 3, S. 118 f.

[31] *Begründung des geänderten Vorschlags*, abgedruckt in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 3, S. 119.

[32] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 3, Rn. 13 ff., der aber eine so geführte Aktensammlung unter den Tatbestand der „Datei“ gemäß Artikel 2c) der Richtlinie subsumiert und demnach hier offenbar von einer nicht-automatisierten Verarbeitung ausgeht.

[33] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 3, Rn. 4.

[34] Dieses Ergebnis widerspricht nicht dem letzten Satz des Erwägungsgrundes (27) der Richtlinie, der Akten und Aktensammlungen vom Anwendungsbereich der Richtlinie ausnimmt, sofern sie nicht nach bestimmten Kriterien strukturiert sind. Die Struktur ergibt sich vorliegend mindestens aus dem elektronischen Datenbestand.

Eine andere Auslegung des Terminus der „teilweise automatisierte(n) Verarbeitung“ kann vom Richtliniengeber kaum gewollt sein. Die Reduktion des Anwendungsbereichs auf die jeweiligen Einzelschritte würde jedenfalls eine Regelungslücke aufwerfen, sofern keine dateiförmige Speicherung der Daten vorgesehen ist und die Richtlinie nicht schon deswegen auf die manuelle Verarbeitung anzuwenden wäre.

Die Einzelbetrachtung ließe zu, dass die Richtlinie zwar während eines automatisierten oder teilweise automatisierten Verarbeitungsabschnittes zur Anwendung käme, die Daten hingegen in einem weiteren nicht-automatisierten Schritt nicht mehr oder noch nicht geschützt wären. Das aber widerspräche dem Schutzzweck der Richtlinie, also dem umfassenden Schutz der Privatsphäre. Ist dieser einmal entstanden, kann er für den Datenumgang im Rahmen ein und derselben Aufgabe nicht plötzlich wieder entfallen. Umgekehrt muss bereits eine manuelle Erhebung datenschutzrechtlichen Sanktionen unterliegen können, sofern die personenbezogenen Daten automatisiert gespeichert werden sollen.[35] Der Grund hierfür ist die erhöhte Gefahr eines gegen das Persönlichkeitsrecht verstoßenden Gebrauchs der Daten. Die Automatisierung eines Einzelschrittes vermag die Einsatzmöglichkeiten der personenbezogenen Informationen erheblich zu erweitern und zu flexibilisieren, sodass auch während der nicht-automatisierten Verarbeitungsabschnitte eine stärkere Grundrechtsgefährdung zu besorgen ist.

Nicht zu vergessen ist auch die Umgehungsproblematik: Der für die Verarbeitung Verantwortliche müsste lediglich Wege ersinnen, um entscheidende Verarbeitungsschritte von dem Schutz der Richtlinie auszunehmen, ohne bei der weiteren Verarbeitung auf die Vorteile der automatisierten Informationstechnologie zu verzichten. Zwar wirkt ein solcher Sachverhalt aus heutiger Sicht konstruiert, ist aber in der Zukunft mithilfe innovativer Verarbeitungstechniken auch ohne eine unrechtmäßige Intention des Verarbeiters durchaus vorstellbar. Die Informationssysteme unterlagen im Laufe der letzten Jahre dynamischen Veränderungen.[36] Regelmäßig wurden neue Mechanismen geschaffen, deren Umgehungspotenzial der Gesetzgeber erst nachträglich mit entsprechenden Maßnahmen einzudämmen vermochte.[37] Ein Ende dieses raschen technologischen Fortschritts ist derzeit nicht absehbar.

---

[35] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 3, Rn. 4.
[36] Z. B. *Schaar*, CR 1996, S. 170, S. 172, mit Bezug auf das Internet.
[37] Vgl. *Hobert*, S. 205 ff., der die datenschutzrechtliche Entwicklung der letzten Jahre als Reaktion des Gesetzgebers auf den technischen Fortschritt darstellt; siehe auch *Büllesbach* in: Datenverkehr ohne Datenschutz?, S. 1, S. 16; *Burkert* in: Governance of Global Networks, S. 43, S. 63.

Die Richtlinienbestimmungen sind daher auf den gesamten Verarbeitungsprozess im Rahmen einer bestimmten Aufgabe anzuwenden, sofern ein einzelner Abschnitt automatisiert erfolgt.[38] Die Situation ist letztlich vergleichbar mit der Regelung für manuelle Verarbeitungen von Daten, die in einer Datei gespeichert werden sollen.

2. Die nicht-automatisierte Verarbeitung

Ist der Verarbeitungsprozess nicht, also weder vollständig noch teilweise automatisiert, unterliegt er den Bestimmungen der Richtlinie nur, sofern die personenbezogenen Daten in einer Datei gespeichert sind beziehungsweise gespeichert werden sollen.

Sinn und Zweck der Ausnahme für die nicht in Dateien gespeicherten Daten ist es, den für die Verarbeitung Verantwortlichen im Interesse seiner Informationsfreiheit vor dem Durchführungsaufwand der Richtlinie zu bewahren.[39] Das ist insofern sachgerecht, als dass eine kaum oder nicht organisierte Bearbeitungsform das Persönlichkeitsrecht des Betroffenen nur gering gefährdet. Erst ein systematisches Vorgehen bietet die Möglichkeit eines beliebig ausbaubaren Persönlichkeitsprofils und birgt damit die Gefahr des „gläsernen Menschen“.

Zwar werden dem Betroffenen dadurch auch Rechte abgeschnitten. Allerdings würde zum Beispiel die Geltendmachung eines Auskunftsanspruchs die Grundrechtsgefährdung erst hervorrufen. Der Anspruch könnte nur mithilfe einer systematischen Datenspeicherung erfüllt werden, die wiederum erst den gezielten Zugriff zu anderen Zwecken auf die Daten ermöglichte. Es wäre paradox, die Anwendbarkeit der Richtlinie auf Sachverhalte zu verlangen, die erst aufgrund einer Beachtung der Schutzprinzipien eine Gefahr für die Privatsphäre des Betroffenen darstellen würden.

Derweil ist die Richtlinie bereits anwendbar, sobald Daten erhoben werden, die erst in der Zukunft in einer Datei gespeichert werden sollen. Bei der Prüfung dieser Intention kommt es weniger auf den tatsächlichen Entschluss des für die Verarbeitung Verantwortlichen an, als objektiv auf den bereits erfolgten oder beabsichtigten Gesamtverarbeitungsvorgang. Lässt dieser nach der Art der Daten und dem Verarbei-

[38] *Kopp*, DuD 1995, S. 204, S. 207.
[39] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 3, Rn. 5.

tungszweck nach allgemeiner Erfahrung oder der regelmäßigen Praxis eine Speicherung in einer Datei erwarten, kommen die Schutzbestimmungen der Richtlinie zur Anwendung,[40] und zwar auch auf solche Verarbeitungsvorgänge, die selbst der Existenz einer Datei nicht bedürften.[41]

II. Ausnahmen

Artikel 3 Absatz 2 der Richtlinie befasst sich mit den Ausnahmen zum Anwendungsbereich.

Gemäß Artikel 3 Absatz 2, 1. Spiegelstrich, findet die Richtlinie keine Anwendung auf eine Datenverarbeitung, „die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen". Als Beispiele für diese dynamische Verweisung[42] nennt die Vorschrift die Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, also die Bestimmungen über die Gemeinsame Außen- und Sicherheitspolitik (Titel V) sowie die Bestimmungen über die polizeiliche und justitielle Zusammenarbeit in Strafsachen (Titel VI). Explizit wird zusätzlich darauf hingewiesen, dass die Richtlinie „auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (...) und die Tätigkeiten des Staates im strafrechtlichen Bereich" anzuwenden sei. Im Gegensatz zu der erstgenannten Fallgruppe entfaltet diese Aufzählung konstitutive Wirkung.[43] Sie soll sich also nicht in Kongruenz zum Anwendungsbereich des Gemeinschaftsrechts entwickeln.

Die in Klammern eingefügte Erwähnung des wirtschaftlichen Wohls meint im Übrigen nicht die Wirtschaftspolitik oder die Belange staatlicher Wirtschaftsunternehmen.[44] Wirtschaftliche Gesichtspunkte führen,

---

[40] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 3, Rn. 5.
[41] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 3, Rn. 9.
[42] Der Anwendungsbereich hat hier bereits eine Änderung erfahren: Zur Zeit des Inkrafttretens der Richtlinie 95/46/EG befasste sich der Titel VI des EUV noch mit den Bestimmungen über die Zusammenarbeit in den Bereichen Justiz und Inneres. Titel V war inhaltlich anders gestaltet. Seit dem Amsterdamer Vertrag vom 2.10.1997 haben sich die Politiken und Formen der Zusammenarbeit als Grundlage der Union jedoch zugunsten der genannten Bereiche verschoben.
[43] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 3, Rn. 6.
[44] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 3, Rn. 6.

wie die Vorschrift selbst klarstellt,[45] nur dann zu einer Ausnahme, „wenn die Verarbeitung die Sicherheit des Staates berührt".

Ferner findet die Richtlinie gemäß Artikel 3 Absatz 2, 2. Spiegelstrich, keine Anwendung auf eine Verarbeitung, „die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird." Die Notwendigkeit dieser Ausnahme ergibt sich aus der herzustellenden Konkordanz zwischen zwei konkurrierenden Grundrechtspositionen, namentlich zwischen dem Recht auf informationelle Selbstbestimmung und dem Recht auf eine private Nutzung der Daten als Ausdruck des allgemeinen Persönlichkeitsrechts. Letzterer wird hier der Vorrang eingeräumt,[46] da der persönliche und familiäre Gebrauch[47] personenbezogener Daten nicht die Grundrechte Dritter verletzt.[48] Der private Umgang mit den Daten ist jedoch präzise von gewerblichen und beruflichen Funktionen der Verarbeitung abzugrenzen.[49]

Ursprünglich sollten noch weitere Ausnahmen vom sachlichen Anwendungsbereich der Richtlinie hinzukommen. Nachdem jedoch für eine unübersehbare Vielfalt von Fallgestaltungen eine Sondersituation angenommen worden war, kürzte die Kommission den Ausnahmenkatalog auf die eingangs vorgestellte Fassung mit der Begründung, dass anderenfalls die Rechte der Bürger nicht mehr garantiert seien.[50] Im Sinne

---

[45] Die Klarstellung wurde erst aufgrund der Empfehlung des Parlaments für die zweite Lesung vom 24. Mai 1995 in den Richtlinienentwurf aufgenommen.

[46] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 3, Rn. 7; zu dem entsprechenden Abwägungsergebnis im BDSG kommen *Bergmann/Möhrle/Herb*, § 1 BDSG, Rn. 18.

[47] Z. B. das Führen eines privaten Adressbuchs oder elektronischer Notizbücher zu ausschließlich persönlichen Zwecken, siehe *Kopp*, RDV 1993, S. 1, S. 4 f.; *Bergmann/Möhrle/Herb*, § 1 BDSG, Rn. 20 ff., mit weiteren Beispielen.

[48] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 3, Rn. 23.

[49] *Dammann/Simitis*, EG-Datenschutzrichtlinie (- *Dammann*), Art. 3, Rn. 8.

[50] *Begründung des geänderten Vorschlags*, abgedruckt in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 3, S. 119.

dieser historischen Entwicklung sind die Ausnahmen des Artikels 3 Absatz 2 der Richtlinie eng auszulegen.[51]

[51] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 3, Rn. 29.

B. Räumlicher Anwendungsbereich

Der Artikel 4 Absatz 1 der Richtlinie befasst sich mit dem räumlichen Anwendungsbereich,[52] indem er die Anwendbarkeit der in Umsetzung der Richtlinie 95/46/EG erlassenen nationalen Vorschriften nach territorialen Kriterien zuordnet und koordiniert.

In seiner Funktion als Kollisionsvermeidungsnorm[53] verhindert Artikel 4 der Richtlinie, dass ein und dieselbe Verarbeitung von den Datenschutzgesetzen mehrerer Mitgliedstaaten gleichzeitig geregelt wird. Im Hinblick auf eine einheitliche Anwendung der mitgliedstaatlichen Datenschutzgesetze werden folglich andere Anknüpfungspunkte aus dem Internationalen Privatrecht der Mitgliedstaaten verdrängt.[54]

Zugleich soll der Artikel 4 Absatz 1 der Richtlinie sicherstellen, dass keine örtliche Schutzlücke bei der Verarbeitung personenbezogener Daten entsteht.[55]

Uneinigkeit besteht jedoch bei der Frage, auf welche Weise die Bestimmung diesen Anforderungen gerecht wird. Insoweit stellte die Europäische Kommission in ihrem ersten Bericht über die Durchführung der Richtlinie 95/46/EG im Mai 2003 fest, dass der Artikel 4 die am häufigsten kritisierte Vorschrift der Richtlinie sei.[56]

---

[52] *Korff*, RDV 1994, S. 209, S. 214; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 24; *ders*., NJW 1997, S. 281, S. 284; *Tinnefeld/Ehmann*, Datenschutzrecht, S. 67; *Wuermeling*, Handelshemmnis Datenschutz, S. 73; anders *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 4, Rn. 1, die ohne Begründung von Artikel 4 Absatz 1 den sachlichen Geltungsbereich bestimmt sehen.

[53] Artikel 4 der Richtlinie trifft keine dem Internationalen Privatrecht nachgebildete Kollisionsregel im eigentlichen Sinne, da er bereits im Voraus klärt, wie die mitgliedstaatlichen Datenschutzgesetze ihren Anwendungsbereich definieren sollen. Auf diese Weise kann eine echte Kollision, bei der ein Sachverhalt gleichzeitig von mehreren Gesetzen geregelt wird, gar nicht erst entstehen; so auch Grabitz/Hilf III (- *Brühann*), A 30, Art. 4, Rn. 10; Simitis u. a. (- *Dammann*), BDSG, § 1, Rn. 196.

[54] *Dammann*, RDV 2002, S. 70, S. 73; zum Ausschluss der freien Rechtswahl gemäß Art. 27 i. V. m. Art. 34 EGBGB bezogen auf das Internet: Hoeren/Müglich/Nielen (- *Andexer/Lehmann*), S. 199 f.; Kaminski u. a. (- *Blömer/Moos*), 2. Kap. D, Rn. 5; *Hobert*, S. 83; *Hoeren*, S. 237.

[55] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 4, Rn. 3; *Korff*, RDV 1994, S. 209, S. 213 f.

[56] *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 18; bereits zuvor *Kuner*, DuD 2002, S. 553.

I. Anwendungsgrundsatz

In der Diskussion über die grundsätzliche Regelung des räumlichen Anwendungsbereichs stehen zwei maßgebende Prinzipien. Nach dem so genannten Sitzprinzip ist das Recht des Ortes anzuwenden, an dem der für die Verarbeitung Verantwortliche ansässig ist.[57] Alternativ könnte das Territorialitätsprinzip[58] gelten, bei dem das Recht des Verarbeitungsortes entscheidet.[59] Der Wortlaut des Artikels 4 der Richtlinie wird unterschiedlich zugunsten des einen oder zugunsten des anderen Prinzips interpretiert. Von der Auslegung hängt vor allem ab, ob die Schutzprinzipien der Richtlinie 95/46/EG auf eine ausschließlich in einem Drittland stattfindende Verarbeitung eines in der Europäischen Union ansässigen Verantwortlichen anzuwenden sind oder ob das möglicherweise lückenhafte Datenschutzrecht des Drittlandes entsprechend dem Territorialitätsprinzip Vorrang genießt.[60]

---

[57] Von der Anwendbarkeit des Sitzprinzips gehen u. a. aus: Hoeren/Müglich/Nielen (- *Andexer/Lehmann*), S. 200; Spindler/Wiebe (- *Bizer/Trosch*), Kap. I, Rn. 58; Kaminski u. a. (- *Blömer/Moos*), 2. Kap. D, Rn. 4; Grabitz/Hilf III (- *Brühann*), Vorbem. A 30, Rn. 43; *ders.*, RDV 1996, S. 12, S. 15; Bräutigam/Leupold (- *Büllesbach*), A.III.1., Rn. 102; *Dolderer* u. a., RDV 2001, S. 223, S. 229; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 4, Rn. 4; *Geis*, NJW 1997, S. 288, S. 290; *Gola/Klug*, S. 43; *Hobert*, S. 84; *Löw*, S. 83; *Moos* in: Kröger/Gimmy, S. 3, S. 15; *Schaar*, Datenschutz im Internet, Rn. 233; *Weber*, DuD 1995, S. 698, S. 700; *dies.*, CR 1995, S. 297, S. 299; *Wohlgemuth*, BB 1996, S. 690, S. 692; *Wülfing/Dieckert*, S. 125; *Wuermeling*, Handelshemmnis Datenschutz, S. 74; *Bachmeier*, RDV 1995, S. 49, S. 50, der wegen der umfangreichen Ausnahmen von einem Mischmodell zwischen Sitz- und Territorialitätsprinzip ausgeht, dessen Ausgangspunkt jedoch das Sitzprinzip sei.

[58] Der Begriff des Territorialitätsprinzips findet seinen datenschutzrechtlichen Ursprung in der öffentlich-rechtlichen Datenverarbeitung. Nach diesem Grundsatz wendet jede öffentliche Stelle bei einer Datenverarbeitung das nationale Recht ihres Staates an. Das soll auch für die Aufsichtsbehörden entsprechend ihrer örtlichen Zuständigkeit bei der Kontrolle der privaten Verarbeiter gelten. Eine wirksame Kontrolle könne eine Behörde aber nur im Hinblick auf die Verarbeitungen im eigenen Land durchführen, sodass für die privaten Stellen automatisch das Recht des Verarbeitungsortes gelte (siehe dazu *Bergmann*, S. 233; *Korff*, RDV 1994, S. 209, S. 211; *Rigaux*, R.C.D.I.P. 1980, S. 443, S. 467 ff.).

[59] So etwa: *Boehme/Neßler*, S. 289; *Hoeren/Queck*, S. 274; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 25; *ders.*, NJW 1997, S. 281, S. 284; nicht ganz eindeutig *Tinnefeld/Ehmann*, Datenschutzrecht, S. 67, die zwar vom Territorialitätsprinzip sprechen, sich aber auf den Sitz der verantwortlichen Stelle beziehen; ebenso *Moritz* in: Datenverkehr ohne Datenschutz?, S. 95, S. 103, der jedoch von einem eingeschränkten Territorialitätsprinzip spricht; vgl. auch *Däubler*, Rn. 348, der den Anwendungsbereich durch ein modifiziertes Territorialitätsprinzip geregelt sieht; siehe auch das italienische Datenschutzgesetz (Legge n. 675 del 31 dicembre 1996), das seinem Wortlaut nach in Art. 2 das Territorialitätsprinzip normiert.

[60] So ist zum Beispiel nach dem Wortlaut des § 4 Absatz 1 des dänischen Datenschutzgesetzes (Act No. 429 vom 31. Mai 2000) dessen Anwendungsbereich auf die Europäische Union beschränkt.

Die Fallgruppen in Artikel 4 Absatz 1a) bis c) der Richtlinie regeln, welches nationale Recht im Einzelfall Anwendung finden soll.

Nach Buchstabe a) fallen solche Verarbeitungen in den Anwendungsbereich eines mitgliedstaatlichen Datenschutzgesetzes, „die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt." Unterhalte der Verantwortliche Niederlassungen in mehreren Mitgliedstaaten, so solle er dafür sorgen, dass jede dieser Niederlassungen das für ihre Tätigkeiten jeweils geltende einzelstaatliche Recht einhalte.

Die Vorschrift dezentralisiert die Anwendbarkeit der mitgliedstaatlichen Datenschutzgesetze auf die Verarbeitungen eines einzelnen Verantwortlichen, um Sachverhalte mit der für die jeweiligen Anwender und Betroffenen national näheren Rechtsordnung zu regeln. Dieses Niederlassungsprinzip weist eine Nähe zum Territorialitätsprinzip auf,[61] da im Zweifel der Mitgliedstaat, in dessen Hoheitsgebiet sich die Niederlassung befindet, der Ort der Verarbeitung sein wird.[62]

Andererseits sagt die Vorschrift entsprechend ihrem Wortlaut auch aus, dass die gesamte Datenverarbeitung im Rahmen der Tätigkeit der jeweiligen Niederlassung dem Recht des Niederlassungsortes unterliegt. Damit sind auch Vorgänge gemeint, die sich außerhalb des Hoheitsgebietes des jeweiligen Mitgliedstaates abspielen, in dem sich die Niederlassung befindet.[63] Aus dieser Perspektive gleicht die Vorschrift eher einem abgeschwächten[64] oder dezentralisierten Sitzprinzip.

Das Niederlassungsprinzip kann folglich sowohl auf das Sitz- als auch auf das Territorialitätsprinzip zurückgeführt werden. Der Rückschluss auf eine grundsätzliche Geltung eines der beiden Prinzipien ist nicht ohne weiteres möglich.

---

[61] *Bergmann/Möhrle/Herb*, § 1 BDSG, Rn. 38; *Dolderer* u. a., RDV 2001, S. 223, S. 229; *Hamburger DuD-Kommentierung zum BDSG,* DuD 2002, S. 5, S. 6; *Tinnefeld/Ehmann*, Datenschutzrecht, S. 67; *Wohlgemuth*, BB 1996, S. 690, Fn. 34; *Bachmeier*, RDV 1995, S. 49, S. 50, der von einem abgeschwächten Territorialitätsprinzip spricht; Kaminski u. a. (- *Blömer/Moos*), 2. Kap. D, Rn. 4, die das Niederlassungsprinzip mit dem Territorialitätsprinzip gleichsetzen.

[62] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 4, Rn. 2 und 3; wohl auch *Gounalakis/Mand*, CR 1997, S. 431, S. 435; vgl. aber Simitis u. a. (- *Dammann*), BDSG, § 1, Rn. 198, der inzwischen von einem abgeschwächten oder modifizierten Sitzprinzip spricht.

[63] *Dammann*, RDV 2002, S. 70, S. 71; *Lütkemeier*, DuD 1995, S. 597, S. 599.

[64] *Draf*, S. 51; *Koch*, S. 328; *Wuermeling*, Handelshemmnis Datenschutz, S. 75.

Artikel 4 Absatz 1b) der Richtlinie bestimmt, dass darüber hinaus Verarbeitungen dem Anwendungsbereich der Richtlinie unterfallen, deren Verantwortlicher zwar nicht im Hoheitsgebiet eines Mitgliedstaates, „aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet". Die Vorschrift stellt klar, dass Verarbeitungen personenbezogener Daten durch eine europäische Botschaft, eine diplomatische oder konsularische Vertretung[65] sowie durch eine sonstige den Regeln der Exterritorialität unterliegenden Stelle[66] den nationalen Schutzvorschriften zur Umsetzung der Richtlinie 95/46/EG genügen müssen. Es wird also so getan, als befänden sich diese Stellen auf dem Hoheitsgebiet des jeweiligen Mitgliedstaates. Auch hier werden der Ort der Verarbeitung und der Sitz der verantwortlichen Stelle regelmäßig räumlich zusammenfallen, sodass die Ausführungen zu Buchstabe a) entsprechend übertragen werden können.

Der Tatbestand des Artikels 4 Absatz 1c) bezieht schließlich solche Verantwortliche in den Anwendungsbereich der Richtlinie ein, die „nicht im Gebiet der Gemeinschaft niedergelassen" sind, aber „zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreif(en), die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind". Diese Regelung entspricht im Grundsatz[67] dem Territorialitätsprinzip.[68] Auf den Sitz des Verantwortlichen kommt es nur insoweit an, als dass er nicht in der Europäischen Union bestehen darf.

Während also die Buchstaben a) und b) sowohl zugunsten des einen als auch des anderen Prinzips ausgelegt werden können, enthält Buchstabe c) eine am Territorialitätsprinzip orientierte Regelung. Die einfache Bilanz der Regeln ergibt folglich ein Überwiegen des Territorialitätsprinzips und legt dessen grundsätzliche Geltung nahe. Andererseits kann es sich dabei aber auch um die Bilanz der Ausnahmeregeln zum Sitzprinzip handeln. Denn bei grundsätzlicher Geltung des Territorialitätsprinzips könnte man den Artikel 4 Absatz 1c) der Richtlinie als redundant empfinden. Indessen nimmt zum Beispiel das neue deutsche Bundesdatenschutzgesetz diese Wirkung des in Umsetzung des Artikels 4 Absatz

[65] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 4, Rn. 5.
[66] *Weber*, CR 1995, S. 297, S. 299.
[67] Siehe dazu ausführlich Gliederungspunkt B.II.2. dieses Kapitels.
[68] *Begründung der Bundesregierung zum Entwurf des Bundesdatenschutzgesetzes*, BT-Drs. 14/4329 vom 13.10.2000, S. 31 f.; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 4, Rn. 6; *Wuermeling*, Handelshemmnis Datenschutz, S. 78.

1c) der Richtlinie erlassenen § 1 Absatz 5 Satz 2 BDSG bei allgemeiner Geltung des Territorialitätsprinzips bewusst in Kauf.[69]

Ob das Bundesdatenschutzgesetz damit der Richtlinie folgt, ist anhand des Wortlautes des Artikels 4 nicht festzustellen.

Ein Indiz kann sich derweil aus der historischen Auslegung der Richtlinie 95/46/EG ergeben. In dem ersten Richtlinienvorschlag[70] richtete sich der örtliche Anwendungsbereich noch nach dem Standort der Datei.[71] Hintergrund dieser Anknüpfung war die inhaltliche Orientierung dieses ersten Richtlinienentwurfs.[72] Anders als die schließlich verabschiedete Version der Richtlinie basierte er nicht auf dem Begriff der „*Verarbeitung* personenbezogener Daten", sondern wählte als zentrales Element die „*Datei*".[73] Bei der Festlegung des Anwendungsbereichs wurde also mit der Wahl des Standortes der *Datei* an den zentralen Gegenstand der damaligen Richtlinienfassung angeknüpft. Da in der endgültigen Richtlinie die „*Verarbeitung* personenbezogener Daten" in den Mittelpunkt der Schutzprinzipien gerückt ist, müsste in logischer Fortsetzung des ursprünglichen Richtlinienaufbaus heute der Ort der *Verarbeitung* den Anwendungsbereich der Richtlinie beziehungsweise der sie umsetzenden nationalen Gesetze bestimmen. Diese Entwicklung stützt die Annahme einer grundsätzlichen Geltung des Territorialitätsprinzips.

---

[69] *Begründung der Bundesregierung zum Entwurf des Bundesdatenschutzgesetzes*, BT-Drs. 14/4329 vom 13.10.2000, S. 32; siehe aber auch *Dammann*, RDV 2002, S. 70, S. 73, der darauf hinweist, dass § 1 Absatz 5 Satz 2 BDSG das internationale Privatrecht des EGBGB verdränge und daher sehr wohl eine eigenständige rechtliche Bedeutung habe.

[70] *Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (90/C 277/03)*, KOM (90) 314 endg. – SYN 287, von der Kommission vorgelegt am 27. Juli 1990, ABl. EG Nr. C 277 vom 5.11.1990, S. 3.

[71] Artikel 4 (1. Vorschlag):
(1) Jeder Mitgliedstaat wendet die Bestimmungen dieser Richtlinie an auf: a) alle in seinem Hoheitsgebiet befindlichen Dateien; b) den Verantwortlichen der Datei, der in seinem Hoheitsgebiet ansässig ist und der von diesem aus eine in einem Drittland angesiedelte/befindliche Datei benutzt, dessen Rechtsvorschriften kein angemessenes Schutzniveau garantieren, sofern diese Benutzung nicht nur vereinzelt erfolgt.
(2) Jeder Mitgliedstaat wendet die Bestimmungen der Artikel 5, 6, 8, 9, 10, 17, 18 und 21 auf den Benutzer an, der von einem im Hoheitsgebiet eines Mitgliedstaats befindlichen Datenendgerät aus eine außerhalb der Gemeinschaft befindliche Datei abfragt, sofern es sich dabei nicht um eine vereinzelte Abfrage handelt.
(3) Wird eine Datei vorübergehend von einem Mitgliedstaat in einen anderen Mitgliedstaat verbracht, so wird dies von diesem Mitgliedstaat weder behindert noch wird irgendeine zusätzliche Förmlichkeit verlangt, die über die Regelungen in dem Mitgliedstaat hinausgeht, in dem die Datei sich ständig befindet.

[72] *Korff*, RDV 1994, S. 209, S. 211 und S. 214.

[73] *Begründung des Rates zum gemeinsamen Standpunkt*, ABl. EG Nr. C 93 vom 13.4.1995, S. 19, S. 20; vgl. auch Artikel 3 des ersten Vorschlags.

Gegen eine solche Theorie spricht jedoch der zweite Vorschlag[74] zur Richtlinie. Gemäß Artikel 4[75] Absatz 1a) der geänderten Fassung war das anzuwendende Recht an den Ort gebunden, an dem der für die Verarbeitung Verantwortliche ansässig ist. Dieser Grundsatz sollte für Datenverarbeiter mit Sitz in einem Mitgliedstaat ausnahmslos und unabhängig von dem tatsächlichen Verarbeitungsort gelten.[76] Begründet wurde die Verwerfung des Territorialitätsgrundsatzes zugunsten des Sitzprinzips in erster Linie mit Erwägungen über die Praktikabilität. Da eine Datei oft auf Datenbanken in verschiedenen Mitgliedstaaten verteilt ist, dürfte es in vielen Fällen praktisch unmöglich sein, ihren Standort eindeutig zu bestimmen.[77] Insbesondere die digitale Kommunikation im Wege des Internets erschwert eine nachträgliche Feststellung der Speicher- und Verarbeitungsvorgänge bei der Übertragung von Dateien wegen deren Aufspaltung in Datenpakete, die oftmals auf einem willkürlichen und jeweils unterschiedlichem Weg zum Empfänger gelangen.[78] Das letzte Beispiel verdeutlicht, dass diese Argumentation aufgrund derselben Schwierigkeiten unterschiedslos auf die Feststellung des Verarbeitungsortes übertragen werden kann. Das Territorialitätsprinzip birgt mithin wegen der oft unübersichtlichen Sach- und Rechtslage, die bei Verarbeitungen in verschiedenen Mitgliedstaaten entstehen kann, eine große Gefahr fehlerhafter Anwendungen der Schutzprinzipien.

---

[74] *Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (92/C 311/04)*, KOM (92) 422 endg. – SYN 287, gemäß Artikel 149 Absatz 3 des EWG-Vertrages von der Kommission vorgelegt am 16. Oktober 1992, ABl. EG Nr. C 311 vom 27. 11.1992, S. 30.

[75] Artikel 4 (2. Vorschlag):
(1) Jeder Mitgliedstaat wendet die zur Durchführung dieser Richtlinie erlassenen Bestimmungen auf alle Verarbeitungen personenbezogener Daten an: a) deren Verantwortlicher in seinem Hoheitsgebiet ansässig ist oder unter seine Staatsgewalt fällt; b) deren Verantwortlicher nicht im Hoheitsgebiet der Gemeinschaft ansässig ist, wenn dieser Verantwortliche für die Verarbeitung personenbezogener Daten automatisierte oder nichtautomatisierte Mittel im Hoheitsgebiet dieses Mitgliedstaats verwendet.
(2) In dem in Absatz 1 Buchstabe b) genannten Fall hat der Verantwortliche der Verarbeitung einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter zu benennen, der in die Rechte und Pflichten des Verantwortlichen eintritt.

[76] A. A. *Dressel*, S. 251, der ohne Begründung nur Verarbeitungen innerhalb des Hoheitsgebietes eines Mitgliedstaates erfasst sah.

[77] *Begründung des geänderten Vorschlags*, abgedruckt in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 4, S. 126; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 4, Rn. 8.

[78] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 4, Rn. 9 und 10; *Schaar*, Datenschutz im Internet, Rn. 74.

Allerdings konnte auch das reine Sitzprinzip im gemeinsamen Standpunkt[79] und in der diesem inhaltlich[80] entsprechenden[81] Endfassung der Richtlinie nicht bestehen.

Es erschien befremdend und unpraktikabel, Datenverarbeitungen einer zum Beispiel in Deutschland angesiedelten Filiale eines in Finnland ansässigen Verantwortlichen nach finnischem Datenschutzrecht zu beurteilen. Das reine Sitzprinzip hätte dem finnischen Verantwortlichen zwar den Vorteil eingebracht, in allen Filialen dasselbe Datenschutzrecht anwenden zu können. Eventuell wäre das den Betroffenen insoweit zugute gekommen, als dass die unternehmenseinheitliche Spezialisierung auf ein bestimmtes Datenschutzrecht die Einrichtung eines effektiveren und sachgerechteren Schutzmechanismus bewirkt hätte.[82] Andererseits aber beurteilt sich die Rechtslage auch in anderen Tätigkeitsbereichen einer ausländischen Filiale, etwa im Gewerbe-, Arbeits- oder Baurecht, nach der Rechtsordnung des Ortes der Niederlassung.[83]

Zudem hätten sich die Aufsichtsbehörden und die Betroffenen trotz inländischer Sachverhalte umfassende internationale Rechtskenntnisse aneignen müssen, um Verfügungen zu erlassen beziehungsweise Ansprüche gegen eine im Inland stattfindende Datenverarbeitung geltend zu machen. Im Beispiel wäre also der deutsche Arbeitnehmer der deutschen Filiale gezwungen gewesen, seine Rechte nach dem finnischen Datenschutzgesetz zu verfolgen. Abgesehen von der abschreckenden Wirkung dieses Erfordernisses stellten die zu erwartenden Verständnisprobleme unter dem Gesichtspunkt der Rechtssicherheit eine bedenkliche Hürde dar.[84]

Ferner hätte das reine Sitzprinzip Probleme aufgeworfen, solange noch kein einheitliches Schutzniveau innerhalb der Europäischen Union wegen der noch nicht in allen Mitgliedstaaten erfolgten Umsetzung der Richtlinie vorgelegen hat. In einem Mitgliedstaat wären auf diese Wei-

---

[79] *Gemeinsamer Standpunkt (EG) Nr. 1/95 vom Rat festgelegt am 20. Februar 1995 im Hinblick auf den Erlass der Richtlinie 95/.../EG des Europäischen Parlaments und des Rates vom ... zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/C 93/01)*, ABl. EG Nr. C 93 vom 13.4.1995, S. 1.

[80] Ohne Änderung in der Sache wurde aus dem „Verantwortlichen der Verarbeitung" der „für die Verarbeitung Verantwortliche".

[81] Bezogen auf Artikel 4 der Richtlinie 95/46/EG.

[82] So müssten etwa bei konzerninternen Codes of Conduct nicht die verschiedenen mitgliedstaatlichen Datenschutzgesetze berücksichtigt werden. Mehr dazu unter Gliederungspunkt E.II. des dritten Kapitels.

[83] *Bachmeier*, RDV 1995, S. 49, S. 50.

[84] *Weber*, CR 1995, S. 297, S. 299.

se plötzlich Datenschutzgesetze verschiedenen Schutzstandards zur Anwendung gekommen. Insbesondere auf verfassungsrechtliche Schwierigkeiten wäre dabei die Anwendbarkeit von Datenschutzvorschriften mit geringerem Schutzniveau in jenen Mitgliedstaaten gestoßen, deren strengere Datenschutzgesetze sich aus konstitutionellen Anforderungen[85] ableiten.[86] Der Anregung der Richtlinie zur Fortführung eines höheren und einheitlichen Datenschutzniveaus[87] in dem jeweiligen Unionsland hätte ebenfalls kaum gefolgt werden können.[88]

Das reine Sitzprinzip vermochte also letztlich ebenfalls nicht zu überzeugen.

Der historischen Auslegung kann demnach allenfalls der Hinweis entnommen werden, dass die endgültige Fassung des Artikels 4 der Richtlinie direkt auf den am Sitzprinzip orientierten Entwurf der Vorschrift folgte, ohne sich explizit von dessen grundsätzlicher Aussage zum Anwendungsbereich zu distanzieren.

Auch die systematische Auslegung hilft vorliegend nicht weiter, da weder der Aufbau der Richtlinie noch der des Artikels 4 einen Hinweis auf die Geltung eines der beiden möglichen Prinzipien geben.

Der Umkehrschluss von dem Aufbau des ersten Entwurfs auf den der endgültigen Richtlinie lässt indessen eine Entscheidung zugunsten des Sitzprinzips vermuten. Um zu verhindern, dass die in der Europäischen Union ansässigen Verantwortlichen ihre Datenverarbeitungen ausgliedern und in Drittländern mit niedrigerem Schutzniveau ansiedeln, hatte Artikel 4 Absatz 1b)[89] des ersten Vorschlags diesen Fall in den Anwendungsbereich der Richtlinie einbezogen. Das Fehlen einer äquivalenten Bestimmung in der endgültigen Richtlinie würde bei grundsätzlicher Geltung des Territorialitätsprinzips eine gravierende Schutzlücke erzeugen. Die Umgehung der Richtlinie wäre regelrecht vorprogrammiert.

An Attraktivität gewönne beispielsweise die Auftragsverarbeitung von aus der Europäischen Union exportierten Daten in Drittländern. Zwar

[85] Ein Recht auf Datenschutz bzw. auf informationelle Selbstbestimmung ausdrücklich in ihren Verfassungstext aufgenommen haben nur Finnland (§ 8 der Verfassung), die Niederlande (Art. 10 Absatz 2, 3), Spanien (Art. 18 Absatz 4) und Portugal (Art. 35).
[86] *Korff*, RDV 1994, S. 209, S. 213 ff.
[87] Erwägungsgrund (10) der Richtlinie.
[88] *Weber*, CR 1995, S. 297, S. 299.
[89] Siehe Fn. 71.

ist für die Auftragsverarbeitung keine Ausnahme zu der Regel vorgesehen, dass jede Übermittlung personenbezogener Daten in ein Drittland ein angemessenes Schutzniveau gemäß Artikel 25 oder das Vorliegen einer der Ausnahmen des Artikels 26 der Richtlinie voraussetzt.[90] Indessen macht es für den in der Europäischen Union ansässigen Auftraggeber einen enormen Unterschied, ob er bei grundsätzlicher Geltung des Territorialitätsprinzips lediglich das Schutzniveau in dem Drittland hinsichtlich seiner Angemessenheit überprüft oder ob er die Durchführung des Auftrags dem Sitzprinzip entsprechend zusätzlich an den Normen des jeweiligen mitgliedstaatlichen Datenschutzgesetzes ausrichten muss. Ließe der europäische Verantwortliche zudem die personenbezogenen Daten in der Europäischen Union grenzüberschreitend durch den Auftragsverarbeiter erheben, würden unter Umständen nicht einmal die Vorschriften über den Drittländertransfer eingreifen.

Demgemäß geht die Europäische Kommission davon aus, dass auch für Auftragsverarbeitungen von aus der Europäischen Union exportierten Daten in Drittländern das Recht desjenigen Mitgliedstaates gilt, in dem der verantwortliche Auftraggeber ansässig ist. Aus Erwägungsgrund (14) in Verbindung mit Artikel 3 f) der „Entscheidung der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG“[91] ergibt sich, dass das anzuwendende Recht von dem Ort der Auftragsverarbeitung der Daten unabhängig ist und sich allein nach dem Sitz der verantwortlichen Stelle richtet. Das Fehlen einer Spezialvorschrift[92] zum räumlichen Anwendungsbereich der Richtlinie für die Auftragsverarbeitung spricht daher für eine grundsätzliche Geltung des Sitzprinzips.

Ferner tragen die Erwägungsgründe zur Interpretation der Richtlinie bei. Erwägungsgrund (18) hebt in Satz 1 hervor, dass „auf jede in der Gemeinschaft erfolgte Verarbeitung personenbezogener Daten die Rechtsvorschriften eines Mitgliedstaats angewandt werden“ müssen.

---

[90] *Innenministerium Baden-Württemberg*, Hinweise Nr. 39, RDV 2001, S. 158, S. 159; *Dolderer* u. a., RDV 2001, S. 223, S. 229 f.

[91] ABl. EG Nr. L 6 vom 10.1.2002, S. 52, S. 54 bzw. S. 55.

[92] Artikel 17 Absatz 3, 2. Spiegelstrich, in Verbindung mit Artikel 17 Absatz 1 der Richtlinie bestimmen zwar, dass die Vorschriften über die technischen und organisatorischen Maßnahmen zur Datensicherheit desjenigen Mitgliedstaates zur Anwendung kommen sollen, in dem der Auftragsverarbeiter seinen Sitz hat. Diese Ausnahmeregelung untermauert jedoch die generelle Geltung des Sitzprinzips. Sie soll sicherstellen, dass der Auftragnehmer seine Datenverarbeitungsanlagen bei wechselnden Auftraggebern nicht ständig einem anderen mitgliedstaatlichen Datenschutzgesetz anpassen muss, was bei genereller Geltung des Sitzprinzips bei Auftragsverarbeitungen in anderen Mitgliedstaaten sonst der Fall wäre.

Damit rückt die Verarbeitung als Anknüpfungspunkt zunächst in den Vordergrund. Andererseits betont Satz 2, dass es „angebracht (sei), auf die Verarbeitung(en), die von einer Person, die dem in dem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen unterstellt ist, vorgenommen werden, die Rechtsvorschriften dieses Staates anzuwenden." Hier wird eindeutig zugunsten des Sitzprinzips entschieden. Es liegt nahe, darin einen Grundsatz zu erblicken, der in allen Zweifelsfällen gelten soll, also immer dann, wenn keiner der in Artikel 4 aufgezählten Tatbestände vorliegt.

Teilweise wird jedoch die Formulierung „es ist angebracht" auch so ausgelegt, dass Satz 2 nur einen Ausnahmefall betreffe. *Simitis*, der von einer generellen Geltung des Territorialitätsprinzips ausgeht,[93] glaubt aus der Formulierung des Satzes 2 lediglich ein in „etwas umständliche(r) Sprache und mit einem unverkennbar resignativen Unterton" akzeptiertes Zugeständnis an das Sitzprinzip herauszulesen, das nur bei wechselnden, eher zufälligen Verarbeitungsorten, etwa bei Verarbeitungen von Geschäftsreisenden, gelten solle.[94] Mag man der Ausdrucksweise des Richtliniengebers tatsächlich eine gewisse Halbherzigkeit zuerkennen, so ist dieser Argumentation jedoch entgegenzuhalten, dass beispielsweise die französische[95] und die englische[96] Richtlinienfassung einen solchen Unterton gänzlich vermeiden. Die französische Version nimmt zwar die Formulierung „es ist angebracht" („il est opportun") auf, stellt aber sodann mit dem Einschub „à cet égard" („mit Rücksicht darauf" oder „in dieser Hinsicht") einen Bezug zu Satz 1 her. Dadurch wird deutlich, dass der umfassende Schutz bei allen Verarbeitungen innerhalb der Europäischen Union mithilfe der Formel des Satzes 2 erreicht werden soll. Die englische Fassung stellt dieselbe Verbindung mit den Worten „in this connection" („in diesem Zusammenhang") her und legt noch klarer fest, dass das Recht desjenigen Mitgliedstaates angewandt werden sollte, in dem der für die Verarbeitung

[93] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 26; *ders.*, NJW 1997, S. 281, S. 284.
[94] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 25.
[95] „(18) considérant qu'il est nécessaire, afin d'éviter qu'une personne soit exclue de la protection qui lui est garantie en vertu de la présente directive, que tout traitement de données à caractère personnel effectué dans la Communauté respecte la législation de l'un des États membres; *que, a cet égard, il est opportun* de soumettre les traitements de données effectués par toute personne opérant sous l'autorité du responsable du traitement établi dans un État membre à l'application de la législation de cet État".
[96] „(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, *in this connection, processing* carried out under the responsibility of a controller who is established in a Member State *should be governed* by the law of that State".

Verantwortliche niedergelassen ist („should be governed....“). Insbesondere aber die italienische Fassung[97] widerlegt mit der Überleitung „a questo proposito, è opportuno“ („zu diesem Zweck ist es angebracht“) zum zweiten Teil des Erwägungsgrundes (18) den Charakter einer Notlösung.

Zudem ist nicht ersichtlich, warum Simitis die Geltung des Sitzprinzips nur auf Fälle mit ständig wechselnden und eher zufälligen Verarbeitungsorten wie bei Geschäftsreisenden beschränkt und damit offensichtlich die bereits angedeutete Schutzlücke bei der Auftragsverarbeitung in Drittländern zulassen will. Zwar ist dies die logische Konsequenz seiner Einordnung der Richtlinie als eindeutig binnengerichtete, sich auf Verarbeitungen innerhalb der Europäischen Union beziehende Regelung[98]. Der Richtliniengeber selbst hat eine solche Klassifikation jedoch nicht vorgenommen. Wenngleich er in Erwägungsgrund (18) nur den Schutz bei Verarbeitungen in der Europäischen Union anspricht, hat er sowohl im ersten Vorschlag als auch mittels des reinen Sitzprinzips im zweiten Vorschlag Verarbeitungen der in der Europäischen Union ansässigen Verantwortlichen in Drittländern in den Anwendungsbereich der Richtlinie ausdrücklich einbezogen. Es ist nicht ersichtlich, dass dieses Konzept unter Billigung der oben bereits angesprochenen Schutzlücke in der abschließenden Richtlinienfassung aufgegeben wurde. Die Richtlinie strebt überdies nicht an, Konflikte mit drittländischen Datenschutzgesetzen zu vermeiden.[99] Die gleichzeitige Anwendbarkeit des in dem betreffenden Drittland geltenden Datenschutzrechts steht dem Sitzprinzip daher ebenfalls nicht entgegen. Mithin müssen die Schutzprinzipien der Richtlinie auch für ständige Verarbeitungen in einem Drittland gelten, sofern der für die Verarbeitung Verantwortliche seinen Sitz in der Europäischen Union hat.[100]

Gemäß diesen Erwägungen spricht also insbesondere das Telos der Richtlinie für eine allgemeine Geltung des Sitzprinzips. Zwar würde das Territorialitätsprinzip an den zentralen Gegenstand der Richtlinie,

---

[97] „(18) considerando che, onde evitare che una persona venga privata della tutela cui ha diritto in forza della presente direttiva, è necessario che qualsiasi trattamento di dati personali effettuato nella Comunità rispetti la legislazione di uno degli Stati membri; *che, a questo proposito, è opportuno* assoggettare i trattamenti effettuati da una persona che opera sotto l'autorità del responsabile del trattamento stabilito in uno Stato membro alla legge di tale Stato".

[98] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 24; *ders.*, NJW 1997, S. 281, S. 284.

[99] *Korff*, RDV 1994, S. 209, dort Fn. 24.

[100] Davon gehen offenbar auch aus: Hoeren/Müglich/Nielen (- *Andexer/Lehmann*), S. 201; Grabitz/Hilf III (- *Brühann*), Vorbem. A 30, Rn. 43; *Hoeren*, S. 238; *Kaspersen* in: *e*Directives, S. 119, S. 123; a. A. wohl *Däubler*, CR 1999, S. 49, S. 51 (ohne Begründung).

nämlich die Verarbeitung anknüpfen. Der Notwendigkeit eines lückenlosen Datenschutzes kommt jedoch ein deutlich größeres Gewicht zu. Eine Kombination aus Territorialitäts- und Niederlassungsprinzip erscheint außerdem wenig sachlogisch. Denn obgleich dabei generell der Ort der Verarbeitung entscheidend wäre, käme es bei der Existenz einer Niederlassung auf das Recht des Sitzes dieser Niederlassung an.

Die Gesamtbetrachtung der die Richtlinie 95/46/EG begleitenden Umstände lässt daher keinen Zweifel an der grundsätzlichen Geltung des Sitzprinzips. Die Anwendbarkeit der Schutzprinzipien der Richtlinie hängt sonach generell von dem Sitz der verantwortlichen Stelle in der Europäischen Union ab. Der Ort der Verarbeitung sowie der Aufenthaltsort, der Wohnsitz oder die Staatsbürgerschaft[101] der betroffenen Person sind demgegenüber unbeachtlich.[102]

Die Auffangfunktion des Sitzprinzips ist in der Praxis jedoch von untergeordneter Bedeutung, da die meisten Sachverhalte bereits unter das Niederlassungsprinzip beziehungsweise den Tatbestand des Artikels 4 Absatz 1c) der Richtlinie subsumiert werden können. Die gegen den zweiten Vorschlag zur Richtlinie vorgetragenen Schwächen einer generellen Geltung des Sitzprinzips sind daher nur in wenigen Einzelfällen hinzunehmen.

II. Die Tatbestände des Artikels 4 Absatz 1 der Richtlinie im Einzelnen

Zu klären bleibt, welche Sachverhalte im Einzelnen von den Tatbeständen des Artikels 4 Absatz 1 der Richtlinie erfasst sind. Da die Auslegung des Artikels 4 Absatz 1b) der Richtlinie seinem Wortlaut entspricht, beschränkt sich die nachfolgende Analyse auf die Tatbestände der Buchstaben a) und c).

1. Artikel 4 Absatz 1a) der Richtlinie

Wie oben bereits erläutert, bestimmt Artikel 4 Absatz 1a) der Richtlinie, dass für Verarbeitungen eines Verantwortlichen, die im Rahmen der Tätigkeit einer in der Europäischen Union angesiedelten Niederlassung stattfinden, das Recht des Ortes dieser Niederlassung anzuwenden ist. Das gilt sowohl für Niederlassungen der in der Europäischen Union

[101] *Brühann*, RDV 1996, S. 12, S. 14. Im Grunde ergibt sich das zwangsläufig aus Erwägungsgrund (2) der Richtlinie.
[102] *Wuermeling*, Handelshemmnis Datenschutz, S. 76.

ansässigen Verantwortlichen als auch für Niederlassungen von verantwortlichen Stellen, die ihren Sitz in einem Drittland haben.

Vereinzelt wird sogar angenommen, dass Artikel 4 Absatz 1a) der Richtlinie mit dieser Regelung unmittelbar das Sitzprinzip enthalte.[103] Natürlich bestimmt die Vorschrift auch, dass auf Datenverarbeitungen im Rahmen der Tätigkeiten der Hauptniederlassung[104] des Verantwortlichen das Recht des Ortes dieser Hauptniederlassung anzuwenden ist.[105] Denn der Begriff der Niederlassung ist nicht etwa auf Zweigniederlassungen reduziert.[106]

Dennoch ist die Annahme einer ausdrücklichen Regelung des Sitzprinzips mit Zweifeln behaftet, da zum Beispiel eine natürliche Person ebenso an ihrem Wohnsitz[107] oder ein Verein an seinem Vereinssitz Daten verarbeiten kann. Auch diese Sachverhalte müssten dementsprechend von dem Tatbestand des Buchstabens a) erfasst sein. Letztlich kommt es also darauf an, wie der Begriff der Niederlassung im Sinne der Richtlinie definiert ist.

Gemäß Erwägungsgrund (19) der Richtlinie ist für das Vorliegen einer Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung entscheidend. Das erinnert an die Auslegung des Begriffs der Niederlassung im Rahmen der Niederlassungsfreiheit gemäß Artikel 43 EGV[108] (alt: Artikel 52 EGV). Im Gegensatz dazu fordert der Erwägungsgrund (19) allerdings nicht die Ausübung einer Erwerbstätigkeit und somit nicht unmittelbar das Vorliegen eines wirtschaftlichen Sachverhalts.

---

[103] *Gounalakis/Mand*, CR 1997, S. 431, S. 434; *Weber*, DuD 1995, S. 698, S. 700.

[104] Dabei kommt es nicht auf den Hauptsitz eines Unternehmens an, sondern jene Niederlassung, die als Verantwortlicher über die Zwecke und die Mittel der Verarbeitung entscheidet. Eine Tochtergesellschaft kann demnach im Rahmen ihrer eigenen Entscheidungsbefugnisse selbst Verantwortlicher der Verarbeitung sein.

[105] *Kopp*, DuD 1995, S. 204, S. 206; *Wuermeling*, Handelshemmnis Datenschutz, S. 74; a. A. *Dolderer* u. a., RDV 2001, S. 223, S. 230, die nur Zweigniederlassungen von dem Begriff der Niederlassung erfasst sehen und dies ohne weitere Erläuterungen dem Gesamtzusammenhang der Richtlinie und Erwägungsgrund (19) entnehmen wollen.

[106] Gounalakis (- *Pfeiffer*), § 12, Rn. 186; *Tinnefeld/Ehmann*, Datenschutzrecht, S. 67; *Wuermeling*, Handelshemmnis Datenschutz, S. 74.

[107] Grabitz/Hilf III (- *Brühann*), A 30, Art. 4, Rn. 10; *Wuermeling*, Handelshemmnis Datenschutz, S. 81 f.

[108] Grabitz/Hilf I (- *Randelzhofer/Forsthoff*), Art. 43 EGV, Rn. 13: „(...) die Niederlassung (ist) eine feste Einrichtung, die bei Eingliederung in die nationale Volkswirtschaft der tatsächlichen Ausübung einer selbstständigen Erwerbstätigkeit zu dienen bestimmt ist (...)."

Dennoch wird zur Abgrenzung des Begriffs der Niederlassung in der Richtlinie von Teilen der Literatur der Rückgriff auf die zu Artikel 43 EGV entwickelte Definition empfohlen.[109] Neben einer Homogenität mit der Auslegung des Gemeinschaftsvertrages spricht hierfür, dass Erwägungsgrund (19) als Beispiele Agenturen und Zweigstellen nennt, sich also derselben Termini bedient wie die Ausdehnung der Niederlassungsfreiheit in Artikel 43 Absatz 1 Satz 2 EGV auf die so genannten sekundären[110] Niederlassungen. Eine wirtschaftliche Ausrichtung des Begriffs im Rahmen der Richtlinie liegt daher nahe.

Ebenfalls erläutern die englische und die französische Version der Richtlinie den Begriff der Niederlassung mit einem Vokabular aus dem Wirtschaftsgebrauch. So kann ein „établissement“ in der französischen Fassung des Erwägungsgrundes (19) etwa in Form einer „succursale“ (Zweigniederlassung) oder einer „filiale“ (Tochtergesellschaft) vorliegen. In englischer Sprache wird der Begriff „establishment“ an derselben Stelle mit den Beispielen „branch“ (Filiale) und „subsidiary“ (Tochtergesellschaft) illustriert. Im Übrigen sind auch diese Begriffe dem Artikel 43 Absatz 1 Satz 2 EGV in der jeweiligen Sprache entlehnt.

Es deutet also vieles darauf hin, dass eine Niederlassung wirtschaftliche Zwecke verfolgen muss,[111] sodass etwa der Wohnsitz des Verantwortlichen nicht von Artikel 4 Absatz 1a) der Richtlinie erfasst wäre.

Zweifel an dieser Eingrenzung kommen allerdings bei einem Vergleich der Richtlinie mit der englischen[112] und der französischen[113] Version des Artikels 4 Absatz 1a) aus dem zweiten Vorschlag zur Richtlinie auf. Denn dort ist das deutsche Wort „ansässig“ bereits mit „established“ beziehungsweise „établi“ übersetzt. Man könnte infolgedessen unterstellen, dass entweder der zweite Vorschlag zur Richtlinie nicht vom reinen Sitzprinzip ausging oder eine Beschränkung des Tatbestandsmerkmals Niederlassung in der Richtlinie auf wirtschaftliche Zwecke nicht vorgesehen ist. Jedoch umfassen die Ausdrücke „established“ und

[109] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 4, Rn. 3; *Wuermeling*, Handelshemmnis Datenschutz, S. 76 (dort insb. Fn. 357 und Fn. 358).
[110] Grabitz/Hilf I (- *Randelzhofer/Forsthoff*), Art. 43 EGV, Rn. 46.
[111] *Dutch DPA*, International aspects of the WBP.
[112] *2. Vorschlag:* Article 4 (1) Each Member State shall apply the national provisions adopted under this Directive to all processing of personal data: a) of which the controller is established in its territory or is within its jurisdiction;(....).
[113] *2. Vorschlag*: Article 4.1. Chaque État membre applique les dispositions nationales prises par la mise en œuvre de la présente directive à tous les traitements de données à caractère personnel: a) dont le responsable est établi sur son territoire ou relève de sa compétence; (...).

„établi“ in ihrer herkömmlichen Übersetzung sämtliche Formen des Sichansiedelns. Eine mit der Konkretisierung der Niederlassung in Erwägungsgrund (19) der Richtlinie vergleichbare Definition ist in dem zweiten Vorschlag zur Richtlinie indessen nicht enthalten.[114] Ein Rückschluss auf die endgültige Richtlinienfassung ist daher nicht möglich.

Von einer Definition, die den Begriff der Niederlassung an wirtschaftliche Zusammenhänge bindet, sind aber längst nicht alle Anwendungsfälle der Richtlinie erfasst. Vielmehr reguliert die Richtlinie ausweislich ihres sachlichen Anwendungsbereichs auch darüber hinausgehende Datenverarbeitungen.

Das bestätigen auch das deutsche Bundesdatenschutzgesetz sowie der britische Data Protection Act 1998. Die Begründung der Bundesregierung zum Gesetzesentwurf[115] des neuen Bundesdatenschutzgesetzes verweist zwar auf die Legaldefinition der Niederlassung in Artikel 42 Absatz 2 Gewerbeordnung, der die Ausübung eines Gewerbes voraussetzt.[116] Allerdings differenziert das Bundesdatenschutzgesetz zwischen einer Niederlassung und dem Sitz der verantwortlichen Stelle, sodass deren Tätigkeit nicht zwingend gewerblicher Natur sein muss. Dagegen wählt der Data Protection Act 1998 zur Klarstellung des territorialen Anwendungsbereichs den Weg einer eigenen Definition des Begriffs „established“. In Section 5.3 listet er unter dem Buchstaben (a) den Wohnsitz einer natürlichen Person auf. Private Vereine oder wissenschaftliche Einrichtungen dürften unter die Buchstaben (b)[117] und (c)[118] subsumiert werden können.

Demgegenüber vertritt Generalanwalt *Tizzano* in seinen Schlussanträgen zur Rechtssache *Bodil Lindqvist gegen Åklagarkammaren Könköping*, dem ersten Verfahren vor dem Europäischen Gerichtshof bezogen auf die Richtlinie 95/46/EG, eine Reduzierung des Anwendungsbereichs der Richtlinie auf Datenverarbeitungen im Rahmen wirt-

[114] Vgl. Erwägungsgründe (11) und (12) des 2. Vorschlags zur Richtlinie.
[115] *Begründung der Bundesregierung zum Entwurf des Bundesdatenschutzgesetzes,* BT-Drs. 14/4329 vom 13.10.2000, S. 31.
[116] *Franzen*, DB 2001, S. 1867, S. 1868, weist allerdings mit Blick auf eine richtlinienkonforme Auslegung zutreffend darauf hin, dass der Begriff der Niederlassung im BDSG gemeinschaftsrechtlich zu interpretieren sei; so im Ergebnis auch *Bergmann/Möhrle/Herb*, § 1 BDSG, Rn. 42 f.
[117] „a body incorporated under the law of, or of any part of, the United Kingdom“.
[118] „a partnership or other unincorporated association formed under the law of any part of the United Kingdom“.

schaftlicher Tätigkeiten.[119] In dem betreffenden Verfahren ging es um die Frage des sachlichen Anwendungsbereichs des schwedischen Datenschutzgesetzes, welcher gemäß den Materialien zu diesem Gesetz jenem der Richtlinie entsprechen solle.[120]

Diese Einschränkung des sachlichen Anwendungsbereichs der Richtlinie 95/46/EG entnimmt Generalanwalt *Tizzano* dem Artikel 3 Absatz 2 der Richtlinie, nach dem die Schutzprinzipien nicht auf Verarbeitungen außerhalb des Anwendungsbereichs des Gemeinschaftsrechts anzuwenden sind. Das Gemeinschaftsrecht könne vor allem deswegen nur Verarbeitungen personenbezogener Daten im Rahmen einer wirtschaftlichen Tätigkeit regeln, da sich die Richtlinie 95/46/EG auf Artikel 100a EGV (neu: Artikel 95 EGV) stütze.

Diese Ermächtigungsgrundlage lässt entsprechend ihrem Wortlaut nur solche Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zu, welche die Errichtung und das Funktionieren des Binnenmarktes zum Gegenstand haben. Gemäß Artikel 14 Absatz 2 EGV muss es sich also um Maßnahmen handeln, die den freien Verkehr von Waren, Personen, Dienstleistungen und Kapital innerhalb des Gemeinschaftsgebietes fördern. Dazu würden gemäß Generalanwalt *Tizzano* zwar Vorschriften zum Zweck der Förderung des freien Verkehrs personenbezogener Daten zählen, nicht jedoch solche, die sich allein aus sozialen Erfordernissen ergäben oder dem Schutz der Grundrechte und insbesondere der Privatsphäre dienten. Bei einer Analyse der Beweggründe des Richtliniengebers zur Herstellung eines einheitlichen Datenschutzniveaus in den Mitgliedstaaten könne vor diesem Hintergrund nur der Absicht Gewicht zukommen, die Hemmnisse für den Verkehr personenbezogener Daten zu beseitigen, die sich aus unterschiedlichen nationalen Schutzstandards ergäben. Anderenfalls stünde sogar die Gültigkeit der Richtlinie wegen einer möglichen Unvereinbarkeit mit Artikel 5 EGV infrage.

---

[119] Schlussanträge des Generalanwalts *Antonio Tizzano* vom 19.09.2002, Rechtssache C-101/01, Rn. 35 ff. (noch nicht in der Rechtsprechungssammlung des EuGH veröffentlicht; abrufbar unter: http://curia.eu.int/jurisp/cgi-bin/form.pl?lang=de&Submit=Suchen&docrequire=judgements&numaff=C-101%2F01&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100); *ders.*, Schlussanträge vom 14.11.2002 in den verbundenen Rechtssachen C-465/00, C-138/01 und C-139/01, Sammlung der Rechtsprechung 2003, I-04989, Rn. 51 ff. (abrufbar unter: http://curia.eu.int/jurisp/cgi-bin/gettext.pl?lang=de&num=79969479C19000465&doc=T&ouvert=T&seance=ARRET).

[120] Schlussanträge des Generalanwalts *Tizzano*, Rechtssache C-101/01, Rn. 16 (vgl. vorherige Fn.).

Dem hält die Europäische Kommission entgegen, dass sich das Gemeinschaftsrecht nicht darauf beschränke, Tätigkeiten wirtschaftlicher Natur zu regeln. So schreibe etwa Artikel 6 EUV die Wahrung der Grundrechte als allgemeine Grundsätze der Gemeinschaftsrechtsordnung vor. Da die Richtlinie entsprechend ihren Erwägungsgründen auch einen Beitrag zum sozialen Fortschritt und zum Wohlergehen des Einzelnen zu leisten beabsichtige, könnten auch nicht wirtschaftliche Tätigkeiten, die im Rahmen der Integration und des Funktionierens des Binnenmarktes ausgeübt würden, von ihr geregelt werden.[121]

Augenscheinlich wird in diesem Zusammenhang allein um die Frage gestritten, ob der Gemeinschaftsgesetzgeber zu dem Erlass einer Datenschutzrichtlinie ausschließlich im Hinblick auf den Schutz der Privatsphäre oder aufgrund sozialer Erfordernisse befugt ist. Darauf kommt es hier jedoch gar nicht an. Vielmehr muss im Hinblick auf Artikel 100a EGV geklärt werden, ob die Regulierung von Datenverarbeitungen im Rahmen von Tätigkeiten ohne wirtschaftlichen Bezug auf rein mitgliedstaatlicher Ebene das Funktionieren des Binnenmarktes negativ zu beeinflussen vermag. Bei einer Reduktion des Anwendungsbereichs der Richtlinie auf wirtschaftliche Zusammenhänge bliebe es nämlich den Mitgliedstaaten unbenommen, ihre nationalen Datenschutzgesetze dennoch auf alle Datenverarbeitungen in ihrem jeweiligen Einflussbereich anzuwenden. Um Daten, die im Rahmen einer nicht in den Anwendungsbereich des Gemeinschaftsrechts fallenden Tätigkeit zu schützen, könnte die Übermittlung solcher personenbezogener Informationen in andere Mitgliedstaaten von dem dortigen Schutzniveau für diese Daten abhängig gemacht werden. So stellt etwa das deutsche Bundesdatenschutzgesetz in § 4b Absatz 2 an Übermittlungen, die nicht im Rahmen von Tätigkeiten erfolgen, die ganz oder teilweise in den Anwendungsbereich des Gemeinschaftsrechts fallen, dieselben Voraussetzungen wie an einen Drittländertransfer.[122]

Erkennt man die Förderung des freien Verkehrs personenbezogener Daten nur deswegen als grundlegendes Ziel des Binnenmarktes an, weil damit unweigerlich der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital verbunden ist, mögen derartige Hemmnisse außerhalb wirtschaftlicher Sachverhalte für sich betrachtet den Binnenmarkt zwar nicht behindern. Sobald es jedoch zwischen den Parteien einer

[121] Schlussanträge des Generalanwalts *Tizzano*, Rechtssache C-101/01, Rn. 32 (vgl. vorherige Fn.).
[122] Vgl. dazu *Gerhold/Heil*, DuD 2001, S. 377, S. 378, die offenbar von einer Eingrenzung des Anwendungsbereichs der Richtlinie 95/46/EG auf wirtschaftliche Sachverhalte ausgehen.

Übermittlung zu Unstimmigkeiten und Unsicherheiten über die Beurteilung der wirtschaftlichen Bedeutung der jeweiligen Verarbeitung kommt, sind Übermittlungshürden im Zusammenhang mit Tätigkeiten wirtschaftlichen Charakters und somit auch Funktionsbeeinträchtigungen auf dem Binnenmarkt geradezu vorprogrammiert. Dieses Hindernis einer komplizierten Abgrenzung wäre im Grunde nur durch den Einbezug auch nicht wirtschaftlicher Tätigkeiten in den Anwendungsbereich der Richtlinie vermeidbar, da sodann stets eine einheitliche Anwendung der Schutzprinzipien in allen Mitgliedstaaten gewährleistet wäre.[123] Entgegen dem ersten Eindruck würden die Abgrenzungsschwierigkeiten dadurch auch nicht auf die Ebene der Definition von persönlichen und familiären Tätigkeiten verlagert werden, da dieser Bereich im Hinblick auf die in allen Mitgliedstaaten einheitlich ausfallende Grundrechtsabwägung von keinem der nationalen Datenschutzgesetze reglementiert wird.[124]

Die Richtlinie 95/46/EG ist mithin im Interesse der Integration und des Funktionierens des Binnenmarktes auch auf Datenverarbeitungen anzuwenden, die nicht im Rahmen einer wirtschaftlich ausgerichteten Tätigkeit erfolgen.[125] Die Intention des Richtliniengebers zum Einbezug derartiger Sachverhalte ergibt sich nicht zuletzt daraus, dass er anderenfalls nicht ausdrücklich persönliche und familiäre Tätigkeiten vom Anwendungsbereich der Richtlinie ausgeschlossen hätte. Denn dieser

---

[123] Mit Abgrenzungsschwierigkeiten begründet auch der *EuGH* sein Urteil, dass die Anwendbarkeit der Richtlinie auf eine Verarbeitung personenbezogener Daten nicht davon abhängen könne, dass ein hinreichender Zusammenhang mit der Ausübung der durch den EG-Vertrag garantierten Grundfreiheiten bestehe. In dem konkreten Fall stritten die Parteien, ob durch die streitgegenständliche Datenverarbeitung in die Arbeitnehmerfreizügigkeit eingegriffen worden war und somit überhaupt die Richtlinie zur Anwendung gelange (Urteil des Europäischen Gerichtshofes vom 20. Mai 2003 in den verbundenen Rechtssachen C-465/00, C-138/01 und C-139/01, Sammlung der Rechtsprechung 2003, I-04989, Rn. 42 ff.; abgedruckt in EuGRZ 2003, S. 232; abrufbar unter: http://curia.eu.int/jurisp/cgi-bin/gettext.pl?lang=de&num=79969479C19000465&doc=T&ouvert=T&seance=ARRET). Dagegen beruft sich auch in diesem Verfahren Generalanwalt *Tizzano* auf seine bereits dargestellte Argumentation.

[124] Allein das österreichische Bundesgesetz über den Schutz personenbezogener Daten (DSG 2000) reglementiert die Verarbeitung zu persönlichen und privaten Zwecken. Eine Übermittlung dieser Daten darf nach § 45 Absatz 2 DSG 2000 jedoch nur mit Zustimmung des Betroffenen erfolgen, sodass auch die Zulässigkeit eines Transfers innerhalb des Binnenmarktes niemals von einem angemessenen Schutzniveau im Empfängerland abhängt.

[125] Dem folgend der *EuGH*, Urteil des Europäischen Gerichtshofes vom 6. November 2003 in der Rechtssache C-101/01, Rn. 37 ff. (noch nicht in der Rechtsprechungssammlung des EuGH veröffentlicht, abrufbar unter: http://curia.eu.int/jurisp/cgi-bin/form.pl?lang=de&Submit=Suchen&docrequire=judgements&numaff=C-101%2F01&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100).

eng[126] auszulegende Ausnahmetatbestand fiele ohnehin nie in den Anwendungsbereich des Gemeinschaftsrechts. Auch Artikel 8 Absatz 2d) unterstellt die Anwendbarkeit der Richtlinie auf Verarbeitungen von politisch, philosophisch, religiös oder gewerkschaftlich ausgerichteten Stiftungen, Vereinigungen oder sonstige Organisationen, die keinen Erwerbszweck verfolgen.[127]

Die Schutzprinzipien gelten folglich zum Beispiel auch für private Vereine unabhängig von deren Zweck. Ob der Wohnsitz eine Niederlassung ist, hängt von der Art der dort ausgeübten Tätigkeit ab. Handelt es sich um eine Erwerbstätigkeit, liegt eine Niederlassung im Sinne der Richtlinie vor,[128] sodass Artikel 4 Absatz 1a) der Richtlinie einschlägig wäre. Verarbeitet der Verantwortliche indessen Daten in einem anderen Zusammenhang, beurteilt sich der Sachverhalt nach dem übergeordneten Sitzprinzip; es sei denn, die Verarbeitung dient ausschließlich persönlichen oder familiären Zwecken.

Die Regelung des Sitzprinzips findet sich demnach nicht unmittelbar in Artikel 4 Absatz 1a) der Richtlinie, da nicht jede für eine Verarbeitung personenbezogener Daten im Sinne des Artikels 3 der Richtlinie verantwortliche Stelle an ihrem Sitz eine Niederlassung unterhält.

Weder einen Sitz noch eine Niederlassung im Sinne des Artikels 4 Absatz 1a) der Richtlinie betreiben indessen neben den bereits erwähnten Geschäftsreisenden ohne eigene Geschäftsräume in dem bereisten Mitgliedstaat zum Beispiel auch Messestände oder Briefkastenfirmen.[129] Dasselbe gilt für technische Stützpunkte, da eine Niederlassung beziehungsweise ein Sitz eine menschliche Aktivität voraussetzen.[130] In diesen Fällen kommt daher entsprechend dem Sitzprinzip das Recht desjenigen Mitgliedstaates zur Anwendung, in dem der für die Verarbeitung Verantwortliche ansässig ist. Unterhält letzterer keine Niederlassung in der Europäischen Union, ist unter Umständen der Tatbestand des Artikels 4 Absatz 1c) der Richtlinie erfüllt.

---

[126] Vgl. dazu Gliederungspunkt A.II. dieses Kapitels.

[127] Dementsprechend sieht z. B. *Singleton*, 11 CL&P, S. 140, S. 141, Datenverarbeitungen von Tierschutzverbänden oder reinen Wohltätigkeitsorganisationen von der Richtlinie erfasst.

[128] Grabitz/Hilf I (- *Randelzhofer/Forsthoff*), Art. 43 EGV, Rn. 50.

[129] *Dammann*, RDV 2002, S. 70, S. 71.

[130] *Dammann*, RDV 2002, S. 70, S. 71; a. A. *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 4, Rn. 15, die bereits einen Server für eine Niederlassung halten, dabei aber übersehen, dass eine Niederlassung nicht nur den Eintritt eines Handlungserfolgs auf dem Hoheitsgebiet eines Mitgliedstaates voraussetzt, sondern gemäß Erwägungsgrund (19) der Richtlinie auch die Ausübung der entsprechenden Tätigkeit; auch a. A. ohne maßgebliche Begründung *Löw*, S. 83 f., die dasselbe zusätzlich für Einwahlknoten annimmt.

2. Artikel 4 Absatz 1c) der Richtlinie

Einer intensiveren Betrachtung bedarf auch der Artikel 4 Absatz 1c) der Richtlinie. Danach ist ein mitgliedstaatliches Datenschutzgesetz auf solche Verarbeitungen anzuwenden, deren Verantwortlicher zwar nicht in der Europäischen Union niedergelassen ist, jedoch auf ein in dem jeweiligen Mitgliedstaat belegenes automatisiertes oder nicht automatisiertes Mittel zum Zwecke der Verarbeitung zurückgreift. Die Vorschrift zielt darauf ab, dass sich eine verarbeitende Stelle nicht der Hürden des Datenschutzes entledigen kann, indem sie auf eine Niederlassung in der Europäischen Union verzichtet und sich stattdessen der Hilfe eines unbemannten Stützpunktes in einem Mitgliedstaat bedient.[131]

a. Das Zurückgreifen auf automatisierte und nicht automatisierte Mittel

Ein klassischer Sachverhalt des Zurückgreifens auf ein automatisiertes Mittel ist das Abfragen von Kundendaten von einem in der Europäischen Union belegenen EDV-System, das vollautomatisch Warenbestellungen entgegennimmt und ohne Niederlassung des Verantwortlichen in einem der Mitgliedstaaten von einem Drittland aus verwaltet wird.[132]

(1) Automatisierte und nicht automatisierte Mittel

Neben EDV-Systemen werden als Mittel im Sinne des Artikels 4 Absatz 1c) der Richtlinie zum Beispiel Fragebögen oder Terminals[133] verstanden, aber auch Personalcomputer, Server,[134] Modems, Einwahlknoten von Internetprovidern[135] und unter Umständen sogar eine Software, wenn das Angebot in der Europäischen Union gehostet wird.[136]

---

[131] *Dammann*, RDV 2002, S. 70, S. 74; *Hobert*, S. 93.

[132] *Duhr/Naujok/Schaar*, MMR 7/2001, S. XVI, S. XVII; *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 7.

[133] *Begründung des geänderten Vorschlags*, abgedruckt in: Dammann/*Simitis*, EG-Datenschutzrichtlinie, Art. 4, S. 125 f.

[134] *Gola/Klug*, S. 45; *Moos* in: Kröger/Gimmy, S. 411, S. 416; *WP 56*, S. 10; *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 4, Rn. 15, halten den Server dagegen bereits für eine Niederlassung; so auch *Löw*, S. 83 f., die dasselbe für Einwahlknoten annimmt; zu allen a. A. *Moritz* in: Datenverkehr ohne Datenschutz?, S. 95, S. 103 f., da Mittel im Sinne der Vorschrift nur Mittel der Datenverarbeitung seien und nicht Mittel der Telekommunikation wie etwa ein Server. Diese Eingrenzung nimmt die Richtlinie jedoch nicht vor, zumal auch mithilfe eines Servers Daten aktiv verarbeitet werden.

[135] *Duhr/Naujok/Schaar*, MMR 7/2001, S. XVI, S. XVII; *Moritz/Winkler*, NJW-CoR 1997, S. 43, S. 48; Gounalakis *(- Pfeiffer)*, § 12, Rn. 187; *Wendel*, S. 57; a. A. *Moritz* in: Datenverkehr ohne Datenschutz?, S. 95, S. 103 f. (Begründung wie vorherige Fn.); so auch *WP 56*, S. 10, da

Voraussetzung ist, dass das Mittel physisch in einem der Mitgliedstaaten belegen ist. Die Legitimation für die Anwendung des europäischen Rechts ergibt sich also erst aus der technischen Präsenz des Verantwortlichen in der Europäischen Union.[137] Auf das oben bereits angesprochene EDV-System zur Entgegennahme von Warenbestellungen wären die Schutzprinzipien der Richtlinie dementsprechend nicht anwendbar, wenn es in einem Drittland situiert und nur über das Telekommunikationsnetz für Kunden aus der Europäischen Union zugänglich wäre.[138]

Auf die Kostentragung und das zivilrechtliche Eigentum des Mittels kommt es nicht an.[139] So wird etwa über das Internet[140] auf den Computer eines Nutzers in der Europäischen Union von einem Drittstaat aus zurückgegriffen, wenn auf dem PC installierte Programme oder Programmkomponenten (zum Beispiel Java-Applets, Active-X-Controls) auf Veranlassung einer außereuropäischen Stelle heimlich Nutzungsinformationen übertragen.[141]

Ebenfalls liegt ein Fall des Artikels 4 Absatz 1c) der Richtlinie bei dem Setzen von Cookies vor, mit deren Hilfe das Nutzungsverhalten des In-

---

es sich bei Mitteln des Telekommunikationsnetzwerks wie Backbones oder Kabeln nur um Mittel der Durchfuhr handele. Vgl. auch *Dieselhorst*, ZUM 1998, S. 293, S. 297, der unentschlossen ist, ob der Begriff Mittel auch Einwahlknotenpunkte oder Telekommunikationsleitungen meint, da diese nicht aktiv auf die Datenverarbeitung einwirkten. Aber auch das fordert die Richtlinie nicht. Entscheidend ist nur gemäß Artikel 4c Absatz 1c) der Richtlinie, dass das Mittel nicht ausschließlich der Durchfuhr dient.

[136] *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 7; *Schaar*, Datenschutz im Internet, Rn. 239; *Scholz*, S. 179 f.; *Verbiest/Wéry*, Rn. 889.

[137] *Dammann*, RDV 2002, S. 70, S. 74.

[138] *Duhr/Naujok/Schaar*, MMR 7/2001, S. XVI, S. XVII; *Schaar*, Datenschutz im Internet, Rn. 238.

[139] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 4, Rn. 6; *WP 56*, S. 10 f.

[140] Im Bereich der elektronischen Kommunikation gilt zwar seit dem 31.7.2002 die Richtlinie 2002/58/EG (ABl. EG Nr. L 201 vom 31.07.2002, S. 37), die bis zum 31.10.2003 in den Mitgliedstaaten umgesetzt werden sollte (seit diesem Tag ist die Richtlinie 97/66/EG zum Datenschutz im Telekommunikationsbereich (ABl. EG Nr. L 024 vom 30.01.1998, S. 1) aufgehoben). Mangels Spezialvorschrift zum räumlichen Anwendungsbereich dieser Richtlinie ist jedoch auf Art. 4 der Rahmenrichtlinie 95/46/EG zurückzugreifen.

[141] *Duhr/Naujok/Schaar*, MMR 7/2001, S. XVI, S. XVII; *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 7; Roßnagel/Banzhaf/Grimm (- *Roßnagel*), S. 144 f.; *Schaar*, Datenschutz im Internet, Rn. 241; *WP 56*, S. 13 f.

ternet-Users registriert wird[142] und somit sein Nutzungsprofil erstellt werden kann.[143]

(2) Das Zurückgreifen

Des Weiteren steht die Bedeutung der Formulierung des Zurückgreifens infrage.

Anhaltspunkte für den Aussagegehalt dieses Tatbestandsmerkmals liefert die Legaldefinition der „Verarbeitung personenbezogener Daten" aus Artikel 2b) der Richtlinie. Danach umfasst die Datenverarbeitung jeden Vorgang und jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Der Begriff der Verarbeitung ist derart weit definiert, dass ein Rückgriff auf ein Mittel zum Zwecke der Verarbeitung personenbezogener Daten, der nicht bereits selbst unter diesen Tatbestand subsumiert werden kann, kaum vorstellbar scheint. Demnach wäre jedes Zurückgreifen auf automatisierte oder nicht automatisierte Mittel zum Zwecke der Verarbeitung im Grunde selbst immer schon eine Form der Verarbeitung.

Bedenken gegen eine solche Annahme wirft jedoch die Frage auf, warum der Richtliniengeber gerade diese Formulierung anstelle des Begriffs der Verarbeitung gewählt hat, wenn er doch eine Verarbeitung meint. Unter diesem Aspekt könnte man dazu geneigt sein, dem Zurückgreifen auf Mittel eine eigenständige Bedeutung beizumessen, die sich inhaltlich von jener der Verarbeitung unterscheidet.

Der Aussagegehalt der beiden Termini ist tatsächlich nicht deckungsgleich. Denn nicht jede Form der Verarbeitung in den Mitgliedstaaten erfordert ein Zurückgreifen auf automatisierte oder nicht automatisierte Mittel.[144] So könnte ein Geschäftsreisender personenbezogene Daten, die er ohne Hilfe von automatisierten oder nicht automatisierten Mitteln erhoben hat, seinem in einem Drittland ansässigen Arbeit- oder Auftraggeber fernmündlich oder erst nach seiner Rückkehr mitteilen.[145]

---

[142] Hoeren/Müglich/Nielen (- *Andexer/Lehmann*), S. 193 f.; *Arndt*, Festschrift f. Rudolf, S. 393 f.; *Boehme-Neßler*, S. 285; *Determann*, S. 92; *Hoeren*, S. 261 f.; Bettinger/Leistner (- *Klein*), Teil 2 E, Rn. 62.

[143] *Dammann*, RDV 2002, S. 70, S. 75; *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 7; *Pinet*, Data Protection Conference, Brüssel 2002, S. 4; *Terwangne/Louveaux*, MMR 1998, S. 451, S. 455; *Verbiest/Wéry*, Rn. 889; *WP 56*, S. 11 f.

[144] A. A. *Wuermeling*, Handelshemmnis Datenschutz, S. 78, der offenbar davon ausgeht, dass die Definition der Verarbeitung in Artikel 2b) der Richtlinie bereits das Vorhandensein der Mittel und deren Nutzung in den Mitgliedstaaten voraussetzt.

[145] *Dammann*, RDV 2002, S. 70, S. 73.

Die Wortwahl des Artikels 4 Absatz 1c) der Richtlinie schränkt daher das reine Territorialitätsprinzip dahingehend ein, dass nicht jede Verarbeitung personenbezogener Daten innerhalb der Europäischen Union durch einen in einem Drittland ansässigen Verantwortlichen in den Anwendungsbereich der Richtlinie einbezogen ist.[146] Im Interesse einer einfacher zu realisierenden Durchsetzung ihrer Bestimmungen knüpft die Richtlinie, wie oben bereits erwähnt, an die technische Präsenz des Verantwortlichen in den Mitgliedstaaten als Legitimation für die Anwendung des europäischen Rechts an.

Gewiss widerspricht das dem ersten Satz des Erwägungsgrundes (18), nach dem jede Verarbeitung in den Mitgliedstaaten von einem mitgliedstaatlichen Datenschutzgesetz geregelt werden soll. Mit dem Spezialfall der Verarbeitungen drittländischer Stellen befasst sich allerdings Erwägungsgrund (20). Dieser reduziert die Aussage des Erwägungsgrundes (18), indem er lediglich die Handhabe für Verarbeitungen erläutert, die eines Rückgriffs auf ein in den Mitgliedstaaten belegenes Mittel bedürfen. Die Erwägungsgründe bestätigen daher das bisherige Ergebnis.

Die Feststellung, dass nicht jede von einem Drittland aus gesteuerte Verarbeitung den Tatbestand des Artikels 4 Absatz 1c) der Richtlinie erfüllt, erschüttert jedoch nicht die Auffassung, dass umgekehrt jeder Rückgriff auf technische Hilfsmittel aus den Mitgliedstaaten zum Zwecke der Verarbeitung eine Verarbeitung im Sinne des Artikels 2b) der Richtlinie ist.

Allerdings ist eine Sachverhaltsvariante denkbar, die diese These widerlegen könnte. So ist fraglich, ob der Bezug eines datenverarbeitenden Gerätes aus einem Mitgliedstaat, um damit in einem Drittland erhobene Daten in diesem Drittland zu verarbeiten, unter den Verarbeitungsbegriff fällt.

Dieser Erwerb stünde zwar in einem mittelbaren Zusammenhang mit personenbezogenen Daten, sodass es sich rein tatbestandlich um eine

[146] Dagegen erklären sich § 3 Absatz 1 des österreichischen Bundesgesetzes über den Schutz personenbezogener Daten (DSG 2000), § 1 Absatz 5 Satz 2 des deutschen BDSG sowie § 4 Absatz 3 Nr. 2 des dänischen Datenschutzgesetzes (Act No. 429 vom 31. Mai 2000) bereits auf die Verwendung bzw. Verarbeitung und Erhebung von personenbezogenen Daten im eigenen Hoheitsgebiet für anwendbar, ohne dass es auf das Zurückgreifen auf dort belegene Mittel ankäme. Diese Vorschriften sind richtlinienkonform restriktiv auszulegen; so für das deutsche und das dänische Gesetz: *Dammann*, RDV 2002, S. 70, S. 73 und S. 74.

Verarbeitung im Sinne der Richtlinie handeln könnte. Zweifel daran weckt jedoch die in diesem Stadium des Verarbeitungszusammenhangs noch fehlende Datenschutzrelevanz. Aufschluss über die Reichweite des Verarbeitungsbegriffs geben in diesem Kontext die gezielteren Formulierungen der englischen und der französischen Richtlinienversion. Die erstgenannte bezeichnet „any operation or set of operations which is *performed upon* personal data“[147] als Verarbeitung personenbezogener Daten, während letztere an derselben Stelle von „toute opération ou ensemble d'opérations (...) *appliquées à* des données à caractère personnel“[148] spricht. Nach dem Wortlaut dieser Definitionen sind eindeutig nur solche Vorgänge gemeint, die einen unmittelbaren Bezug zu personenbezogenen Daten aufweisen. In einem derart engen Zusammenhang steht der Erwerb eines datenverarbeitenden Gerätes nicht. Das bedeutet zwar einerseits, dass es ein Zurückgreifen auf automatisierte oder nicht automatisierte Mittel gibt, das nicht von dem Verarbeitungsbegriff der Richtlinie erfasst ist. Andererseits ist ein solches Zurückgreifen aber noch nicht datenschutzrelevant, sodass es nicht den Schutzbereich der Richtlinie berührt und auch nicht von dieser geregelt werden soll.

Zu demselben Ergebnis führt die Argumentation, dass es zur Eröffnung des sachlichen Anwendungsbereichs der Richtlinie einer Verarbeitung innerhalb der Europäischen Union bedürfe.[149] Dem ist jedoch entgegenzuhalten, dass Artikel 3 der Richtlinie seinem Wortlaut gemäß keinen Verarbeitungsvorgang innerhalb eines Mitgliedstaates voraussetzt. Das wäre auch überraschend, da es sich hierbei nicht um eine Frage des sachlichen, sondern des räumlichen Anwendungsbereichs handelt, der wiederum ausschließlich von Artikel 4 der Richtlinie bestimmt wird. Artikel 4 Absatz 1c) der Richtlinie stellt aber gerade klar, dass eine Verarbeitung in einem Drittland vom Anwendungsbereich der mitgliedstaatlichen Datenschutzgesetze erfasst ist, sofern zum Zweck dieser Verarbeitung auf Mittel aus der Europäischen Union zurückgegriffen wird. Zudem geht auch das Sitzprinzip davon aus, dass bestimmte Verarbeitungen in Drittländern von der Richtlinie geregelt werden.[150] Die Begründung über den sachlichen Anwendungsbereich ist daher nicht nachzuvollziehen.

---

[147] (...) jeder Vorgang oder Vorgangsreihe, *die mit* personenbezogenen Daten *durchgeführt werden* (...).

[148] (...) jeder Vorgang oder Vorgangsreihe *bezogen/ angewandt auf* personenbezogene Daten (...).

[149] So offenbar vertreten von *Wuermeling*, Handelshemmnis Datenschutz, S. 78.

[150] So auch *Wuermeling* in seiner Matrix der Kollisionsregeln, Handelshemmnis Datenschutz, S. 82.

Wie oben bereits erläutert, erfüllt dennoch jeder datenschutzrelevante Rückgriff auf ein automatisiertes oder nicht automatisiertes Mittel zum Zwecke der Verarbeitung den Tatbestand der „Verarbeitung personenbezogener Daten“. Folglich sind die zum Verarbeitungsbegriff entwickelten Grundsätze anzuwenden.

(3) Der für die Verarbeitung Verantwortliche

Da es sich bei dem Zurückgreifen auf ein automatisiertes oder nicht automatisiertes Mittel zum Zwecke der Verarbeitung um eine „Verarbeitung personenbezogener Daten“ im Sinne des Artikels 2b) der Richtlinie handelt, ist alsdann der für den Rückgriff Verantwortliche festzustellen.[151] Entsprechend dem Wortlaut des Artikels 4 Absatz 1c) der Richtlinie muss dieser in einem Drittland ansässig sein und darf keine Niederlassung in einem Mitgliedstaat unterhalten. Teilweise wird zudem angenommen, dass die verantwortliche Stelle in dem Drittland eine Niederlassung pflegen müsse, ein Wohnsitz aber nicht ausreiche.[152] Dafür liefert die Richtlinie jedoch keinerlei Anhaltspunkte.

Eine Stelle ist gemäß Artikel 2d) der Richtlinie für eine Verarbeitung verantwortlich, sofern sie über deren Zwecke und deren Mittel entscheidet. Eine solche Entscheidung ist objektiv nur möglich, wenn die Stelle im Sinne einer tatsächlichen Gelegenheit und aufgrund eines eigenen Entschlusses zu dem Rückgriff imstande ist. Regelmäßig entfällt diese Voraussetzung, sobald das Mittel hinsichtlich der betreffenden Verarbeitung in irgendeiner Weise fremdgesteuert wird.[153] Der Verantwortliche muss das Mittel im Hinblick auf den Rückgriff also gewissermaßen beherrschen.[154]

Das Erfordernis der Mittelbeherrschung wird teilweise infrage gestellt.[155] Die Richtlinie liefere keine Anhaltspunkte dafür, dass eine über die normale Bindung des Verantwortlichen an die Verarbeitung hinausgehende Intensität der Beziehung bestehen müsse. Diese Ansicht

[151] *Wuermeling*, Handelshemmnis Datenschutz, S. 78.
[152] So *Wuermeling*, Handelshemmnis Datenschutz, S. 79.
[153] Vgl. *Schaar*, RDV 2002, S. 4, S. 5, der ein steuerndes Zugreifen auf das Mittel verlangt; *ders*., Datenschutz im Internet, Rn. 239 ff.; siehe auch *Dammann*, RDV 2002, S. 70, S. 75, der von einem bestimmenden Einfluss auf Inhalt und Zweck des Datenumgangs spricht.
[154] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 4, Rn. 6; vgl. auch *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 7, die von einer partiellen Kontrolle spricht.
[155] *Wuermeling*, Handelshemmnis Datenschutz, S. 78.

verkennt jedoch, dass die Beherrschung des Mittels hinsichtlich der betreffenden Verarbeitung notwendig ist, um überhaupt von einer Entscheidung über die Zwecke und die Mittel der Verarbeitung sprechen zu können. Die Unabhängigkeit der verarbeitenden Stelle hinsichtlich des Rückgriffs von dem Einfluss eines Dritten auf das Mittel ist also unabdingbar, um eine Verantwortlichkeit für die Verarbeitung zu begründen.

Darüber hinaus setzt die Entscheidung nach Artikel 2d) der Richtlinie subjektiv voraus, dass sich die Stelle des Verarbeitens personenbezogener Daten gewahr ist, und impliziert die Absicht, die bestimmte Verarbeitung vornehmen zu wollen.[156] Letztlich muss die Verarbeitung der Stelle also nach Treu und Glauben und im Rahmen der allgemeinen Lebenserfahrung subjektiv zurechenbar sein.

Eine allein an das Vorhandensein der personenbezogenen Daten im eigenen Herrschaftsbereich knüpfende Zustandsverantwortung begründet die Richtlinie indessen nicht, da ihr Anwendungsbereich durch die Verarbeitung personenbezogener Daten, also durch eine Handlung,[157] und nicht etwa durch das Innehaben einer bestimmten Position, wie zum Beispiel im ersten Entwurf die Verantwortlichkeit für eine Datei,[158] eröffnet wird[159].

Als problematisch erweist sich die Feststellung der Verantwortlichkeit oftmals bei dem Zurückgreifen auf ein automatisiertes Mittel zum Zweck der Datenerhebung bei dem Betroffenen, da es hierzu im Gegensatz zu den anderen Verarbeitungsformen einer Abgrenzung der Einflussmöglichkeiten auf das Mittel zwischen dem Datenempfänger und dem Betroffenen bedarf.

Geklärt ist diesbezüglich die Anwendbarkeit der Richtlinie auf Sachverhalte, bei denen der Verarbeiter aus dem Drittland Programme auf dem Computer des Betroffenen installiert, die heimlich Nutzungsinformationen übertragen.[160] Da die Datenübermittlung auf Veranlassung des Datenempfängers erfolgt und sich regelmäßig ohne Kenntnis des Betroffenen vollzieht, kommt überhaupt nur die drittländische Stelle als Verantwortlicher der Verarbeitung in Betracht.

---

[156] *WP 56*, S. 9 und S. 10.
[157] *Gounalakis/Mand*, CR 1997, S. 431, S. 434.
[158] Vgl. z. B. Artikel 4 Absatz 1b) des ersten Vorschlags zur Richtlinie.
[159] *Runge*, RDV 1998, S. 109 und S. 110.
[160] Siehe dazu Gliederungspunkt B.II.2.a.(1). dieses Kapitels.

Größere Schwierigkeiten bereitet indes die Frage der Anwendbarkeit der mitgliedstaatlichen Datenschutzgesetze auf Websites, die sich auf Servern in Drittländern befinden, aber in der Europäischen Union aufgerufen werden können.

Einerseits greift auch hier der Betroffene wie in dem Beispiel des in einem Drittland befindlichen EDV-Systems[161] selbstständig über das Telekommunikationsnetz beziehungsweise über die virtuelle Verbindung des Internets auf die Website zu. Aus dieser Perspektive ist schon das Vorliegen eines in den Mitgliedstaaten belegenen Mittels ausgeschlossen. Andererseits werden bei dem Aufsuchen der Website von dem Computer des Nutzers automatisch die IP-Adresse,[162] Daten über den verwendeten Rechner[163], oftmals die E-Mail-Adresse des Nutzers[164] sowie die URL der aufgerufenen und der zuvor aufgerufenen Seite übertragen,[165] sodass ein Zurückgreifen des Datenempfängers aus dem Drittland auf den Personalcomputer des Nutzers vorliegen könnte.[166]

Entscheidend für die Anwendbarkeit der Richtlinienbestimmungen auf diesen Sachverhalt ist gemäß Artikel 4 Absatz 1c), dass der Website-Anbieter trotz der automatischen Datenübertragung für das Auslösen des Transfers zum Zweck der Datenerhebung verantwortlich ist.[167]

Ein Rückgriff auf den Computer des Nutzers ist objektiv möglich, sobald der Nutzer die entsprechende Website aufruft. Zwar ist der Datenempfänger insoweit auf das Verhalten des Internet-Nutzers angewiesen. Jedoch ist auch in allen übrigen Fällen des Zugriffs auf den Computer des Betroffenen eine aus der Sicht des Datenempfängers willkürliche Verbindung zum Internet notwendig. Es kann nicht darauf ankommen, wie viele Bedingungen erfüllt sein müssen, damit der Zugriff durch-

[161] Siehe dazu Gliederungspunkt B.II.2.a.(1). dieses Kapitels.
[162] Ausführlich zu der Frage des Personenbezugs von IP-Adressen: *Schaar*, Datenschutz im Internet, Rn. 168 ff.; siehe auch *Boehme-Neßler*, S. 292 f.; *Börner* u. a., S. 97; Hamann/Weidert (- *Hamann*), S. 42; Bettinger/Leistner (- *Klein*), Teil 2 E, Rn. 13; *Strömer*, S. 354 f.; *TEIA*, Datenschutz im Internet, S. 607; *Terwangne/Louveaux*, MMR 1998, S. 451, S. 452; *Wülfing/Dieckert*, S. 105.
[163] Z. B. Betriebssystem, Bildschirmgröße oder Typ und Version des Browsers.
[164] *Köhler/Arndt*, S. 278.
[165] *Arndt*, Festschrift f. Rudolf, S. 393, S. 394; *Bleisteiner*, S. 38; *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 7.
[166] Differenzierend bei der Feststellung des Personenbezugs dieser Daten: *Verbiest/Wéry*, Rn. 808 ff.
[167] Anders *Pinet*, Data Protection Conference, Brüssel 2002, S. 2, der es für entscheidend hält, ob die Website ein automatisiertes Mittel im Sinne des Artikels 4 Absatz 1c) der Richtlinie ist.

führbar ist. Entscheidend ist allein, dass das Mittel im Hinblick auf die konkrete Verarbeitung nicht fremdgesteuert wird.

Das Aufrufen der Website liegt danach zwar eindeutig in der Hand des Betroffenen, sodass er die dadurch ausgelöste Datenübertragung gewissermaßen selbst veranlasst. Es erscheint jedoch äußerst fragwürdig, aus diesem objektiven Umstand ohne weiteres die Verantwortlichkeit des Betroffenen[168] für die Instrumentalisierung seines Computers herzuleiten und damit jene des Datenempfängers auszuschließen.[169] Die Übermittlung erfolgt automatisch und ist dem Betroffenen oftmals, jedenfalls hinsichtlich der Art und des Umfangs der übermittelten Daten, nicht einmal bewusst.[170] Der Betroffene geht höchstens davon aus, dass eventuell von irgendeiner Stelle im Netz zur Kenntnis genommen wird, welche Website er gerade aufruft. Im Zweifel ahnt er jedoch nicht, dass weitere Informationen von seinem Computer abgerufen werden. Die Situation scheint insofern vergleichbar mit der heimlichen Übertragung von Daten mithilfe von Java-Applets, Active-X-Controls oder Cookies. Nicht auszuschließen ist daher, dass der Website-Anbieter den Betroffenen bei dem Aufrufen der Website als Werkzeug für seinen Zugriff auf den PC einsetzt.

Die Verantwortlichkeit des Website-Anbieters kann jedenfalls nicht wegen der Tatsache abgelehnt werden, dass der Betroffene den die Datenübertragung auslösenden Schritt objektiv selbst in der Hand hat. Entscheidend für das Vorliegen eines Rückgriffs auf den Computer des Betroffenen ist vielmehr, ob die Verantwortlichkeit des Website-Anbieters positiv begründet werden kann. Nur sofern das nicht möglich ist, obliegt dem Betroffenen die Verantwortung für das Aussenden der Daten durch seinen Computer als allgemeines Risiko der auf seiner eigenen, freien Entscheidung beruhenden Internetbenutzung.

Allerdings hat auch der Website-Anbieter keinen Einfluss auf den konkreten, ihn erreichenden Datenzugang, da er die Daten aufgrund eines Automatismus erhält. Der Umfang der an die empfangende Stelle im Drittland übermittelten Daten ist durch technische Protokolle festgelegt, sodass sich der Empfänger im Grunde nicht gegen den Datenzu-

[168] Der Betroffene wäre natürlich nur im buchstäblichen Sinne selbst verantwortlich und nicht gemäß Artikel 2d) der Richtlinie, da der Richtliniengeber den Betroffenen nicht vor sich selbst schützen will und kann.
[169] So aber *Dammann*, RDV 2002, S. 70, S. 74; *Duhr/Naujok/Schaar*, MMR 7/2001, S. XVI, S. XVII; *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 7; *Schaar*, Datenschutz im Internet, Rn. 242; *Scholz*, S. 180 f.
[170] *Köhler/Arndt*, S. 279.

wachs wehren kann, solange er seine Website für jedermann zugänglich in das Internet stellt.[171] Der Computer des Nutzers könnte demnach auch aus der Sicht des Website-Anbieters fremdgesteuert sein.

Da es sich bei der Datenübertragung um einen technisch automatisierten Vorgang handelt, kommt allerdings auch kein Dritter als Verantwortlicher in Betracht. Nach objektiven Kriterien könnte der Website-Anbieter mithin verantwortlich sein, indem er durch das Einrichten der Website das die Datenübertragungen auslösende Instrument schafft und damit die Möglichkeit zur Kommunikation mit dem Betroffenen über das Internet einschließlich des Aussendens und des Erhalts der personenbezogenen Informationen von dessen Computer eröffnet. Objektiv ist daher ein Rückgriff auf den Computer des Betroffenen mithilfe der Website jedenfalls nicht auszuschließen.

Demgegenüber ist die subjektive Zurechenbarkeit eines Rückgriffs kaum herzuleiten. Allein die Schaffung der Möglichkeit, eine Website zu besuchen, vermag keinen entsprechenden Willen zu begründen, auf Computer aus aller Welt und insbesondere aus den Mitgliedstaaten zum Zweck der Datenerhebung zurückzugreifen.

Gerade kleinere Anbieter oder Unternehmen, denen es oftmals nur um das Hinterlegen einer Visitenkarte im Netz geht, adressieren ihre Website lediglich an Bewohner ihres Heimatlandes oder einer bestimmten Region. Das ergibt sich meistens schon aus der Beschränkung auf die eigene Landessprache. Zwar wird teilweise eine zusätzliche Version in englischer Sprache angeboten, sodass einige Websites auch inhaltlich einem internationalen Publikum zugänglich sind. Die Übersetzung darf aber wohl in den überwiegenden Fällen als Serviceleistung verstanden werden, die nicht von der Absicht motiviert ist, weltweit personenbezogene Daten durch den Rückgriff auf die Computer der Nutzer zu erheben.

Aber selbst wenn eine Website ihrem Inhalt gemäß einen unbestimmten Besucherkreis anspricht und wie die Mehrzahl der aus den USA stammenden Websites in Englisch geschrieben ist, rechtfertigt sich noch nicht die Annahme, dass sich der Anbieter durch einen Rückgriff auf den Computer des Nutzers ausgerechnet die oben genannten Daten überhaupt von irgendeinem Besucher seiner Website beschaffen möchte. Diese fehlende Erhebungsabsicht ist insofern bedeutsam, als dass das

[171] *Schaar*, RDV 2002, S. 4, S. 5.

Vorliegen eines Rückgriffs auf ein Mittel im Sinne des Artikels 4 Absatz 1c) der Richtlinie mit der bezweckten Datenverarbeitung untrennbar verknüpft ist. Beabsichtigt der Anbieter mit der Einrichtung seiner Website keine Datenerhebung, erübrigt sich folglich die Frage nach dem Rückgriff.

Die Absicht zu einer Datenerhebung ist bei der Einrichtung einer Website tatsächlich nicht überzeugend zu begründen. Zwar wird häufig vor dem Erstellen von Nutzungsprofilen und ihrem Verkauf insbesondere im Bereich der Werbewirtschaft gewarnt.[172] Auf der anderen Seite sind jedoch viele Anbieter an den protokollierten Daten gar nicht interessiert, da die Auswertung der in beträchtlichen Mengen anfallenden Informationen oftmals unverhältnismäßig aufwendig[173] und daher unrentabel ist. Diesen Website-Anbietern dient das Internet lediglich als Informations- und Werbeforum, bei dem sie durch das Aufrufen der Website durch den Nutzer beiläufig dessen personenbezogene Daten erhalten. Aus dieser Unbestimmtheit heraus ist ein Erhebungs- beziehungsweise Rückgriffswille jedoch nicht zu konstruieren.

Etwas anderes könnte jedoch gelten, sofern der Website-Anbieter von vornherein eine Speicherung der empfangenen Daten in so genannten Logprotokollen plant. Mithilfe dieser Registrierung können die Aktivitäten der Besucher einer Website hinsichtlich der Häufigkeit des Aufrufens der Website oder der Art der verwendeten Betriebssysteme und Browser ausgewertet werden.[174] Zudem ist ein Abgleich der Protokolle mit anderen Informationen, etwa Anfragen in Suchmaschinen, zur Anfertigung eines Nutzungsprofils möglich.[175]

Sofern derartige technische Vorkehrungen getroffen werden, um die übertragenen Informationen systematisch zu sammeln, kann der Tatbestand der Erhebung nicht von vornherein ausgeschlossen werden.[176] Der Website-Anbieter beabsichtigt aber auch dann keinen Rückgriff auf den Computer des Betroffenen. Zwar mag sein Wille darauf gerichtet sein, möglichst viele Informationen über den Betroffenen zu erhalten. Dabei

---

[172] So z. B. von Hoeren/Müglich/Nielen (- *Andexer/Lehmann*), S. 198; *Boehme-Neßler*, S. 301 ff.; *Moos* in: Kröger/Gimmy, S. 411, S. 414; *Strömer*, S. 347; *Wülfing/Dieckert*, S. 100 f.
[173] *Bleisteiner*, S. 38; *Hobert*, S. 209; *Kunze*, c't 12/96, S. 100.
[174] *Schaar*, DuD 2001, S. 383, S. 384.
[175] Siehe zu den umfangreichen Möglichkeiten zur Erstellung eines Online Profils und zur Beschaffung von Informationen: *Schaar*, Datenschutz im Internet, Rn. 38 ff.
[176] *Strömer*, S. 346 f.; so wohl auch *TEIA*, Datenschutz im Internet, S. 607 f.; vgl. ebenso Kilian/Heussen (- *Weichert*), Nr. 132, Rn. 96 und Rn. 97, der u. a. von einer Erhebung ausgeht, wenn Geräte (z. B. Anrufbeantworter, Videokameras oder PCs) derart eingerichtet wurden, dass sie ohne weiteres Zutun personenbezogene Daten empfangen können.

ist es für ihn jedoch ohne Belang, ob der Betroffene seine Daten bewusst versendet oder der Computer selbsttätig ohne Kenntnis des Betroffenen dessen Daten verschickt. In jedem Fall intendiert der Anbieter der Website keine Einflussnahme auf die Art und den Umfang der Informationen in dem Maße, dass er auf den Computer des Betroffenen steuernd einwirken möchte. Das ergibt sich insbesondere daraus, dass der Website-Anbieter keine Maßnahmen trifft, um bestimmte Daten von bestimmten Computern abzurufen, sondern es dem Zufall überlässt, ob und in welchem Umfang es zu einer Übertragung kommt. Ohne eine bestimmte Übermittlung zu initiieren, sammelt er nur die Datenspuren, die von den Besuchern seiner Website hinterlassen werden[177] und dadurch automatisch in seinen Verfügungsbereich gelangen.

Der Internet-User wird nicht einmal um die Preisgabe seiner personenbezogenen Informationen gebeten. Die Bereitstellung der Website kann jedenfalls nicht als eine solche Aufforderung interpretiert werden, da der Nutzer die Website auch ohne Übertragung seiner personenbezogenen Daten aufsuchen könnte. Nähme er dazu zum Beispiel den Computer einer öffentlichen Bibliothek oder eines Internetcafés in Anspruch, bliebe seine Person für die empfangende Stelle trotz der Datenübertragung unbestimmbar. Auch das Vorschalten eines Proxy-Servers oder eines Firewall-Systems kann die Identifikation des Nutzers verhindern.[178]

Die subjektive Zurechenbarkeit eines Rückgriffs ist nach Treu und Glauben sowie nach allgemeiner Lebenserfahrung daher nicht möglich. Der Nutzer wird folglich nicht als Werkzeug zu der Datenübertragung von der empfangenden Stelle veranlasst, indem er dieser durch das Aufrufen der bereitgestellten Website einen Rückgriff aus seinen Computer zum Zweck der Erhebung der genannten Daten ermöglicht.

Davon abgesehen erscheint es auch rechtspolitisch kaum vertretbar, dem Website-Anbieter für das automatische Aussenden der Daten infolge des Website-Besuchs die Verantwortung aufzuerlegen. Der Betroffene könnte jederzeit durch eigene Initiative die Anwendbarkeit des europäischen Rechts auf Datenverarbeitungen in Drittländern auslösen und würde damit komplexe Massenverarbeitungen, sei es nur in Form einer Aufbewahrung oder einer Löschung, in einem hohen, oft unkalkulierbaren Maße verkomplizieren. So müssten etwa Datenströme nach Herkunftsländern getrennt werden. Das Zurückführen der IP-Adresse

[177] *TEIA*, Datenschutz im Internet, S. 608; *Terwangne/Louveaux*, MMR 1998, S. 451, S. 457.
[178] *Schaar*, Datenschutz im Internet, Rn. 169.

auf einen einzelnen Nutzer bedürfte bei einer dynamischen Vergabe von IP-Nummern sogar der Mitwirkung des Internet Access Providers.[179] Bei der Einwahl in das Internet mit einem mobilen Endgerät käme es für die Frage des anzuwendenden Rechts zudem auf die Zufälligkeit des Eingabeortes an.[180]

Alternativ bliebe nur die Anwendung der von der Richtlinie aufgestellten Schutzprinzipien auf die Gesamtheit der Datenzugänge. Aber auch dann käme es mindestens zu Kollisionen zwischen den mitgliedstaatlichen Datenschutzgesetzen. Den Anbietern würden auf diese Weise Verpflichtungen aufgebürdet, die sie bei der Einrichtung ihrer Website selbst mit viel Weitsicht vernünftigerweise nicht in Betracht ziehen müssen.

Die Datenübermittlung im Rahmen eines Website-Aufrufs stellt somit keinen Rückgriff auf automatisierte oder nicht automatisierte Mittel dar, da die empfangende Stelle nicht als für die Verarbeitung Verantwortlicher auf den Personalcomputer des Nutzers zurückgreift, sondern der Nutzer für die Datenübermittlung aufgrund des freiwillig eingegangenen Risikos einer Gefährdung seines Persönlichkeitsrechts während einer Internet-Nutzung selbst einzustehen hat.[181]

Umstritten ist allerdings, ob Entsprechendes für den Fall gilt, dass die Website-Nutzung eine Registrierung über elektronische Fragebögen erfordert.

Das ist insofern zweifelhaft, als dass die Einstellung eines Fragebogens in das Internet einen Erhebungswillen des Website-Anbieters selbstredend dokumentiert[182] und der Zweck der Erhebung ein zurechenbares Zurückgreifen auf den Computer des Betroffenen indiziert.

---

[179] *Schaar*, DuD 2001, S. 383, S. 384.
[180] Bräutigam/Leupold (- *Grapentin*), B.X.8., Rn. 87.
[181] So im Ergebnis auch *Dammann*, RDV 2002, S. 70, S. 74; *Hamburger DuD-Kommentierung zum BDSG*, DuD 2002, S. 5, S. 7; *Schaar*, Datenschutz im Internet, Rn. 242; ebenso, aber ohne genauere Begründung: Bettinger/Leistner (- *Klein*), Teil 2 E, Rn. 35; *Moos* in: Kröger/Gimmy, S. 411, S. 416; *Verbiest/Wéry*, Rn. 890; vgl. auch *WP 56*, S. 10, nach dem nicht jede Interaktion zwischen Unionsbürgern und einer außereuropäischen Website die Anwendung eines mitgliedstaatlichen Datenschutzgesetzes auslöst; a. A. *Pinet*, Data Protection Conference, Brüssel 2002, S. 2 f., dessen Argumentation sich allerdings ausschließlich an einem möglichst umfassenden Datenschutz für Unionsbürger orientiert.
[182] So wohl auch *Schaar*, Datenschutz im Internet, Rn. 192, der bei einem Bereitstellen von Formularen im Internet automatisch eine Datenerhebung unterstellt.

Teilweise wird dennoch unterstellt, es fehle an einem konkretisierten Erhebungswillen der befragenden Stelle, da der Adressatenkreis des Fragebogens zu unbestimmt sei. Die Entscheidung über die tatsächliche Datenpreisgabe liege ausschließlich bei dem Betroffenen, sodass die Registrierungsmöglichkeit mit der Rechtsfigur der „invitatio ad offerendum" aus der Rechtsgeschäftslehre hinsichtlich der Abgabe einer Willenserklärung vergleichbar sei.[183]

Zweifelhaft ist jedoch, ob der Erhebungstatbestand einen derart konkretisierten Erhebungswillen voraussetzt.[184] Das hätte jedenfalls auch Konsequenzen für rein mitgliedstaatliche Sachverhalte. Von einer Datenbeschaffung über elektronische Fragebögen abgesehen könnte eine Erhebung zum Beispiel bei dem Ausfüllen von in Geschäften ausgelegten Kundenfragebögen verneint werden.[185] Das jeweilige Datenschutzgesetz käme dort dann erst bei der späteren Auswertung zur Anwendung, bei der man schließlich eine Verarbeitung nicht mehr abstreiten könnte.

Für das Vorhandensein eines Erhebungswillens des Website-Anbieters spricht indessen, dass der Nutzer, anders als bei dem bloßen Aufrufen einer Website, um seine Daten ersucht wird. Zwar werden nicht von vornherein bestimmte Personen angesprochen. Der Adressatenkreis ist aber insoweit konkretisiert, als dass sich der Wille des Anbieters auf die Erhebung der Daten aller Interessenten des Website-Angebots richtet,[186] und zwar anhand des vorgegebenen Fragenkatalogs. Möchte der Datenimporteur den Informationszugang aus bestimmten Ländern vermeiden, hat er das Formular für diese Regionen zu sperren. Im Gegensatz zu der Situation bei der automatischen Datenübertragung anlässlich eines Website-Besuchs kann man das hier von ihm erwarten. Da es dem Anbieter des elektronischen Fragebogens eindeutig und aus-

[183] So *Dammann*, RDV 2002, S. 70, S. 74; dem folgend Roßnagel/Banzhaf/Grimm (- *Roßnagel*), S. 145, dort Fn. 124; *Scholz*, S. 181, dort Fn. 349, die jedoch beide nicht auf den Vergleich mit einer „invitatio ad offerendum" eingehen.

[184] Vgl. z. B. *Bergmann/Möhrle/Herb*, § 3, Rn. 69, die die Bestimmbarkeit der Person noch nicht zum Zeitpunkt der Erfassung verlangen; so wohl auch Simitis u. a. (- *Dammann*), BDSG-Dokumentation, § 3, Rn. 114 f.

[185] Siehe dazu jedoch *Nungesser*, HDSG, § 2, Rn. 37, der den Tatbestand der Erhebung nicht erfüllt sieht, sofern der Betroffene die Daten auf vorgedruckten Antragsformularen einer Behörde mitteilt. Eine Erhebung liege nur dann vor, wenn die Behörde den Betroffenen zum Ausfüllen des Formulars auffordere. Die Interessenlage ist jedoch bei dem Auslegen von Kundenfragebögen insoweit anders, als dass die verarbeitende Stelle sich im Gegensatz zu einer Behörde mit dem Auslegen des Fragebogens tatsächlich Daten über ihren Kundenstamm verschaffen möchte.

[186] Vgl. dazu Hamann/Weidert (- *Hamann*), S. 36, der betont, dass viele Geschäftsmodelle im Internet primär darauf gerichtet seien, Kunden durch das Angebot von Gratisdiensten zur Preisgabe ihrer Daten anzuregen.

schließlich um das Sammeln von personenbezogenen Informationen geht, muss er auf den Datenzugang einschließlich seiner datenschutzrechtlichen Konsequenzen eingerichtet sein. Ein aufgedrängter Datenzuwachs ist daher nicht ersichtlich.

Obwohl der Betroffene die Daten freiwillig und bewusst beibringt, ist er außerdem zur Offenlegung der gefragten Informationen gezwungen, wenn er das Website-Angebot wahrnehmen möchte. Würde man in solchen Fällen den Erhebungstatbestand verneinen, wären sämtliche Verarbeiter, die Daten ohne einen gesetzlichen Auftrag abfragen, während der Befragung regelmäßig nicht nach den Vorschriften zum Datenschutz und zur Datensicherheit verpflichtet. Für eine solche Ausnahme liefert die Richtlinie jedoch keinerlei Anhaltspunkte.

Der Datenempfänger erhebt daher mittels des elektronischen Formulars die personenbezogenen Daten der sich registrierenden Nutzer,[187] sodass ein Zurückgreifen auf den Computer des Betroffenen indiziert ist.

Dennoch ist zweifelhaft, ob der Website-Anbieter tatsächlich auf ein in der Europäischen Union belegenes Mittel zurückgreift. Die Verantwortlichkeit für den Rückgriff könnte bereits an den objektiven Kriterien scheitern.

Die Vorgänge des Ladens, Ausfüllens und Abschickens des elektronischen Formulars werden ganz allein von dem Internet-User durchgeführt. Der Website-Anbieter greift nicht nach seinem Belieben auf sämtliche Computer zu, die seine Registrierungsseite aufsuchen. Vielmehr bedient sich der Betroffene selbst seines PCs, um die einzelnen Registrierungsschritte durchzuführen. Im Gegensatz zu der automatischen Übertragung von Daten bei dem Aufrufen einer Website sendet er seine Daten aktiv und bewusst an die erhebende Stelle, sodass er selbst seinen Computer als automatisiertes Mittel instrumentalisiert. Ungeachtet eines möglicherweise parallel zu der Erhebung über das Formular ablaufenden Fremdrückgriffs auf seinen Computer setzt der Betroffene den technischen Prozess gezielt und ohne Fremdsteuerung selbst in Gang. Die technischen Details müssen ihm dabei nicht bekannt sein, da es allein auf die eigenverantwortliche und bewusste Instrumentalisierung der Informationstechnologie zur Versendung seiner Daten ankommt. Ein Rückgriff auf den Computer des Betroffenen liegt folglich nicht deswegen vor, weil das Laden und Abschicken des For-

[187] Davon auch ausgehend Spindler/Wiebe (- *Bizer/Trosch*), Kap. I, Rn. 2, im Hinblick auf die Anmeldung zu Online-Auktionen.

mulars den Arbeitsspeicher des PCs und möglicherweise die Nutzung eines Cookies[188] seitens der erhebenden Stelle erfordert.[189]

Da der Betroffene seinen PC hinsichtlich der betreffenden Verarbeitung selbst steuert, trägt der Datenempfänger nicht die Entscheidung über die Zwecke und die Mittel des Zurückgreifens, sodass seine Verantwortlichkeit nicht begründet zu werden vermag.[190]

Dieses Ergebnis ist insofern erstaunlich, als dass die Begründung zum zweiten Richtlinienvorschlag[191] Fragebögen explizit als Mittel im Sinne des Artikels 4 Absatz 1c) der Richtlinie anführt. Voraussetzung dafür ist jedoch, dass der Fragebogen von der verarbeitenden Stelle und nicht von dem Betroffenen instrumentalisiert wird. Ferner muss der Fragebogen in einem der Mitgliedstaaten lokalisiert sein. Zwar wird auch ein elektronisches Formular auf dem PC des Nutzers geladen. Letztlich handelt es sich aber nur um eine Website, die auf einem Server in einem Drittland belegen ist und die schon deswegen nicht den Tatbestand eines innerhalb der Europäischen Union situierten Mittels erfüllt.

In der untersuchten Fallgestaltung ist daher nicht der elektronische Fragebogen das in einem Mitgliedstaat belegene Mittel, sondern allein der Computer des Nutzers.

Die Befürworter einer weiten Auslegung des Artikels 4 Absatz 1c) der Richtlinie halten es hingegen im Interesse eines umfassenden Datenschutzes der Unionsbürger für unabdingbar, die mitgliedstaatlichen Datenschutzgesetze auf elektronische Fragebögen anzuwenden.[192] Allein

---

[188] Die über den Cookie erhobenen Daten werden indessen gemäß Artikel 4 Absatz 1c) der Richtlinie von dem einschlägigen mitgliedstaatlichen Datenschutzgesetz geschützt.

[189] So aber Spindler/Wiebe (- *Bizer/Trosch*), Kap. I, Rn. 59, die einen Rückgriff unterstellen, weil der Arbeitsspeicher des PCs beansprucht wird und möglicherweise Cookies für die Übertragung des Formulars erforderlich sind.

[190] So auch *Dammann*, RDV 2002, S. 70, S. 74, der jedoch bereits den Tatbestand der Erhebung verneint; aus Erwägungen der Praktikabilität im Ergebnis auch Bräutigam/Leupold (- *Grapentin*), B.X.8., Rn. 87; a. A. Spindler/Wiebe (- *Bizer/Trosch*), Kap. I, Rn. 59 (vgl. vorherige Fn.); Hoeren/Müglich/Nielen (- *Andexer/ Lehmann*), S. 201, die ohne Begründung offenbar bereits das elektronische Formular für ein in den Mitgliedstaaten belegenes Mittel halten; ebenfalls zu den Vertretern dieser Ansicht gezählt wird *Weber*, DuD 1995, S. 698, S. 700, die sich jedoch m. E. nicht eindeutig äußert, indem sie zunächst einen Rückgriff auf ein automatisiertes oder nicht automatisiertes Mittel voraussetzt und sodann beispielhaft das elektronische Abrufen der Daten oder das Ausfüllen von Erhebungsbögen nennt, ohne sich dabei von dem Erfordernis des Rückgriffs auf ein Mittel zu distanzieren.

[191] *Begründung des geänderten Vorschlags*, abgedruckt in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 4, S. 125 f.

[192] So *Pinet*, Data Protection Conference, Brüssel 2002, S. 4 ff., der damit für die französische „Commission Nationale de l'Informatique et des Libertés" (CNIL) spricht.

die Visualisierung einer Website in einem Mitgliedstaat genüge bereits den Voraussetzungen des Artikels 4 Absatz 1c) der Richtlinie, da technische Argumente bei der Lokalisierung des Mittels nicht zur Schutzlosigkeit der Unionsbürger bei der Nutzung des Internets führen dürften.

Das ließe sich zwar nicht juristisch eindeutig begründen, da auch für die an technischen Gesichtspunkten orientierte Auslegung des Artikels 4 Absatz 1c) der Richtlinie gewichtige Gründe sprächen. Aus ökonomischer und sozialer Sicht sei es aber undenkbar, den Unionsbürgern den von der Richtlinie gewährleisteten Datenschutz bei dem Besuch von Websites abzusprechen, nur weil diese sich auf außereuropäischen Servern befänden.[193] Die Gründe hierfür seien zum einen in der teilweise absichtlichen Umgehung der Schutzprinzipien der Richtlinie durch eine gezielte Verlegung von Websites in so genannte Datenoasen zu suchen. Überdies würden die Unionsbürger bei dem Ausfüllen eines Fragebogens darauf vertrauen, dass der europäische Datenschutzstandard bei der Verarbeitung beachtet werde.[194]

Diese Argumentation sei gestützt durch diverse Urteile europäischer Gerichte, in denen das Internet eine zentrale Rolle gespielt habe.[195]

So hätten etwa das Amtsgericht München im CompuServe-Urteil[196] sowie der TGI Paris im Verfahren gegen Yahoo![197] das nationale Strafrecht für anwendbar erklärt, sofern Websites im Hoheitsgebiet des jeweiligen Staates aufgerufen werden konnten. Entscheidend sei für die Gerichte allein die Visualisierung der Seite in dem jeweiligen Land gewesen.

Diese beiden Urteile liefern jedoch keine Erkenntnisse zur Feststellung des Anwendungsradius der mitgliedstaatlichen Datenschutzgesetze. Zum einen ist der Anwendungsbereich des Strafrechts ohnehin vom

---

[193] *Pinet*, Data Protection Conference, Brüssel 2002, S. 5 f.
[194] Um dieser Konsequenz des Artikels 4 Absatz 1c) zu begegnen, hat das griechische ‚Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data' in Art. 3.3b) Verarbeitungen von nicht in Griechenland angesiedelten Verantwortlichen, die sich auf in Griechenland ansässige Personen beziehen, zusätzlich in den Anwendungsbereich des Gesetzes einbezogen. Diese Regelung dürfte jedoch entsprechend dem Harmonisierungsgedanken der Richtlinie sehr restriktiv auszulegen sein.
[195] *Pinet*, Data Protection Conference, Brüssel 2002, S. 3.
[196] *AG München*, Urteil vom 28. Mai 1998, 8340 Ds 465 Js 173158/95, abgedruckt in: MMR 1998, S. 429.
[197] *Tribunal de Grande Instance de Paris*, Beschluss vom 20. November 2000, procédures n° 00/05308 und 00/05309; zusammengefasst in: MMR 2001, S. 309; abrufbar unter: http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm.

Territorialitätsprinzip geprägt.[198] Des Weiteren basierten die Strafbarkeit im CompuServe-Urteil auf der strafbewährten Präsentation pornografischer Inhalte und das Urteil des französischen Gerichts gegen Yahoo! auf dem Verbot der Darstellung von Nazi-Gegenständen. Im Gegensatz zu dem Tatbestand des Artikels 4 Absatz 1c) der Richtlinie, der die Existenz eines unbemannten Stützpunktes in der Europäischen Union verlangt, kam es für die Anwendung der fraglichen Strafvorschriften gerade und auch nur auf die Visualisierung in dem jeweiligen Staatsgebiet und somit allein auf das Aussenden der Websites an. Die Ausdehnung der nationalen Strafvorschriften auf das gesamte Internet begegnet im Übrigen sehr viel Skepsis und soll nur unter besonderen Umständen möglich sein.[199] Die Entscheidungen gegen CompuServe und Yahoo! sind daher nicht als Regelfälle zu werten.

In einem dritten Beispielsfall verurteilte das britische High Court of Justice den Buchmacher William Hill[200] wegen der Verletzung eines europäischen Patents, obgleich das streitgegenständliche Wettsystem auf einem Server auf den Niederländischen Antillen gehostet wurde. Von entscheidender Bedeutung für das Urteil war allerdings, dass die Wettteilnahme die Installation einer Software – von CD-ROM oder per Download aus dem Internet – auf dem Computer des Nutzers erforderte. Damit war ein Teil des patentierten Systems, das sich durch die Gesamtheit der Verbindungskomponenten zwischen dem Computer des Wettenden mit dem Server des Buchmachers und die dadurch ermöglichte Spielteilnahme auszeichnete, in Großbritannien lokalisiert. Darüber hinaus wurde hier nicht um Datenschutz-, sondern um Patentrecht gestritten. Dessen Anwendungsbereich ist aber gerade nicht durch die Bedingung des Rückgriffs auf ein in dem jeweiligen Mitgliedstaat belegenes Mittel begrenzt.

Die Beispiele zeigen zwar eine Tendenz der Gerichte auf, möglichst viele Sachverhalte in den Schutzbereich des europäischen Rechts einzubeziehen. Eine Übertragung dieser Rechtsprechungspraxis auf den Anwendungsbereich der Richtlinie widerspräche jedoch dem Wortlaut des Artikels 4 Absatz 1c).

---

[198] *Börner* u. a., S. 144; *Herzog*, S. 71.

[199] Ausführlich dazu: *Herzog*, S. 71 ff. insb. S. 83 ff. u. S. 86; *Sieber*, NJW 1999, S. 2065 ff; siehe auch *Börner* u. a., S. 144 f. m. w. N.; *Steckler*, S. 67 f.

[200] *High Court of Justice*, 15. März 2002 (Menashe Business Mercantile Ltd., Julian Menashe v. William Hill Organization Ltd., No. HC-01C-04669, U.K. High Ct., Chanc. Div.), Zusammenfassung abrufbar unter: http://www.mealeys.com/tec.html#11.

Gewiss hängt es danach aus der Sicht des Betroffenen regelmäßig vom Zufall ab, ob ein mitgliedstaatliches Datenschutzgesetz anwendbar ist. Zwar kann der Nutzer bei einer Warenbestellung in den USA sicher davon ausgehen, dass er seine Daten in das außereuropäische Ausland verschickt, sodass ihm die bewusste Inkaufnahme eines geringeren Datenschutzniveaus unterstellt werden darf.[201] Die geografische Zuordnung einer „com"-Domain lässt sich indessen nicht einmal erahnen.[202] Das mag dem Anliegen eines möglichst umfassenden Datenschutzes abträglich sein, da gerade im Bereich des Internets die Gefahr einer Verletzung des Persönlichkeitsrechts eines Nutzers besonders groß ist[203]. Andererseits liefe die Umdeutung aller Website-Angebote in eine technische Präsenz in den Mitgliedstaaten dem das Internet prägenden Interaktionscharakter zuwider.[204]

Zudem sind die Daten regelmäßig auch außerhalb des Anwendungsbereichs der Richtlinie nicht völlig ungeschützt. So wurde die Datenschutzproblematik nicht nur in Europa als drohendes Hindernis für eine fehlende Akzeptanz des Internets als Handelsforum erkannt,[205] sondern rief inzwischen weltweit Regulierungsinitiativen[206] hervor.[207]

Exemplarisch sei hier zum einen der von dem National Internet Advisory Committee (NIAC) in Singapur herausgegebene „Model Data Protection Code for the Private Sector"[208] genannt, der Privatunternehmen die Rahmenbedingungen für einen angemessenen Datenschutz im Sinne des Artikels 25 der Richtlinie 95/46/EG erläutert.[209] Zum anderen hat etwa in den USA die aus einem Workshop zum Thema Online Profiling[210] der Federal Trade Commission und dem amerikanischen Handelsministerium hervorgegangene Network Advertising Initiative (NAI) Prinzipien zur Selbstregulierung der amerikanischen Internet-

---

[201] *Ende/Klein*, S. 13.
[202] *Koch*, S. 298; *WP 56*, S. 11.
[203] Zu den Gefahren im Einzelnen: *Arndt*, Festschrift f. Rudolf, S. 393, S. 396; *Deutscher Bundestag*, Sicherheit und Schutz im Netz, S. 227 ff.; *Hobert*, S. 208 f.; *Schaar*, CR 1996, S. 170, S. 172; *Scholz*, S. 93 ff.; *Terwangne/Louveaux*, MMR 1998, S. 451; siehe auch *Determann*, S. 91 f., der auf die mangelhafte Vertraulichkeit des Internets aufgrund der oft unverschlüsselten Datentransporte und Zwischenspeicherungen hinweist.
[204] *Dammann*, RDV 2002, S. 70, S. 74.
[205] *Deutscher Bundestag*, Deutschlands Weg in die Informationsgesellschaft, S. 35.
[206] Zahlreiche Beispiele bei *White & Case*, Survey Of 15 Major Jurisdictions.
[207] *White & Case*, Privacy Law Survey.
[208] Abrufbar unter:
http://www.mda.gov.sg/MDA/documents/Report_on_a_Model_Data_Protection_Code.PDF.
[209] *Lai*, CRi 2003, S. 30; *Schulz*, ITRB 2002, S. 226.
[210] Erstellen von Nutzungsprofilen.

Werbewirtschaft formuliert, deren Vorgaben dem deutschen Datenschutzrecht sehr nahe kommen.[211]

Von einem weltweit zufrieden stellenden Datenschutz im Internet kann zwar auch unter diesen Umständen im Moment noch nicht gesprochen werden. Das ändert aber nichts an der Entscheidung des Richtliniengebers, nur jene Verarbeitungen gemäß Artikel 4 Absatz 1c) in den Anwendungsbereich der Richtlinie einzubeziehen, zu deren Zweck auf ein in den Mitgliedstaaten belegenes Mittel zurückgegriffen wird.[212]

b. Die Durchfuhr durch das Gebiet der Europäischen Gemeinschaft

Nicht anwendbar sind die Bestimmungen der Richtlinie gemäß Artikel 4 Absatz 1c) indessen, wenn die Mittel der Verarbeitung „nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden."

Da die personenbezogenen Daten weder verändert oder gespeichert werden noch in anderer Form auf sie eingewirkt wird, greift die Durchfuhr als spezielle Verarbeitungsmodalität vergleichsweise gering in das allgemeine Persönlichkeitsrecht des Betroffenen ein[213] und erfordert somit nicht die Beachtung der mitgliedstaatlichen Datenschutzgesetze.

Der Tatbestand der Durchfuhr ist nur erfüllt, wenn bereits zu Beginn des Verarbeitungsvorgangs feststeht, dass im Gemeinschaftsgebiet selbst keine Datenverarbeitung stattfinden wird, die nicht unmittelbar dem Vorgang der Durchfuhr dient.[214] Zwingend erforderlich für diese Prognose ist zum Beispiel die Kenntnis, dass der endgültige Datenempfänger nicht in der Gemeinschaft ansässig sein wird.

Eine Durchfuhr liegt etwa vor, wenn die Daten bei einem Transfer durch das Internet lediglich über einen sich in der Europäischen Union befindenden Rechner geroutet werden.[215] Zulässig ist eine Veränderung der durchgeleiteten Daten aufgrund übertragungsbedingter Zwischen-

[211] *Schaar*, DuD 2001, S. 383, S. 387 f.
[212] Trotz der bekannten Schwierigkeiten bei der Anwendung dieser Vorschrift hielt die *Europäische Kommission* in ihrem ersten Bericht über die Durchführung der Datenschutzrichtlinie an dem Erfordernis des Rückgriffs auf ein Mittel fest und bekräftigte dessen Relevanz bei der Feststellung des Anwendungsbereichs der Richtlinie (Bericht vom 15.05.2003, KOM (2003) 265 endgültig, S. 18).
[213] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 4, Rn. 9.
[214] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 4, Rn. 17.
[215] *Schaar*, RDV 2002, S. 4, S. 5; *Scholz*, S. 181.

speicherungen, sofern diese Speicherungen lediglich einer ordnungsgemäßen Durchfuhr dienen und keine grundrechtsrelevante Verarbeitung oder Kenntnisnahme beinhalten.[216]

Die Privilegierung der Durchfuhr kommt jedoch nur dem drittländischen Datenversender zugute. Sofern bei den Providern, die mit der Durchleitung befasst sind, personenbezogene Daten entstehen, gilt das mitgliedstaatliche Datenschutzgesetz ihres jeweiligen Sitzlandes.[217]

Teilweise wird erwogen, die Ausnahmebestimmung auf solche Auftragsverarbeitungen zu erstrecken,[218] für die gemäß Artikel 4 Absatz 1c) der Richtlinie eigentlich die mitgliedstaatlichen Datenschutzgesetze gelten würden. Die Schutzvorschriften der Richtlinie kämen dann nicht zur Anwendung, sofern aus einem Drittland importierte Daten in der Europäischen Union im Auftrag eines außereuropäischen Auftraggebers verarbeitet und anschließend wieder in ein Drittland exportiert würden.

Sofern in dem jeweiligen Land des Auftraggebers ohnehin keine Datenschutzbestimmungen existieren, scheint der Schutz auch während der Verarbeitung in den Mitgliedstaaten entbehrlich. Bedenken kommen jedoch auf, falls für das Datenschutzrecht des betreffenden Drittlandes das Territorialitätsprinzip gilt. Die personenbezogenen Daten blieben sodann in der Europäischen Union ungeschützt, obgleich sowohl das Drittland als auch die Gemeinschaft über ein Datenschutzsystem verfügten.[219] Ein durch diese beiden Sachverhalte nahe gelegter Zwei-Klassen-Datenschutz, der sich nach dem jeweiligen Herkunftsland richten müsste, wäre nicht nur völlig unpraktikabel, sondern widerspräche auch dem Grundgedanken der Richtlinie, alle Verarbeitungen in den Mitgliedstaaten an den europäischen Datenschutzprinzipien zu messen.

Zudem ist der Ausnahmecharakter der Durchfuhr, der sich durch eine nur geringe Berührung der Privatsphäre der betroffenen Personen auszeichnet, bei sämtlichen Verarbeitungsmodalitäten der Auftragsverarbeitung nicht gegeben. Die Ausnahme rechtfertigt sich mithin nur bei einer Auftragsdurchfuhr, für die Auftragsverarbeitung schlechthin gilt sie nicht[220].

---

[216] *Wuermeling*, Handelshemmnis Datenschutz, S. 80; *Dammann*, RDV 2002, S. 70, S. 76.
[217] *Schaar*, Datenschutz im Internet, Rn. 244.
[218] *Wuermeling*, Handelshemmnis Datenschutz, S. 79 f.
[219] *Wuermeling*, Handelshemmnis Datenschutz, S. 80.
[220] *Dammann*, RDV 2002, S. 70, S. 76.

Die Richtliniensystematik untermauert dieses Ergebnis. Da der Begriff des Auftragsverarbeiters in Artikel 2e) der Richtlinie legaldefiniert ist, wäre bei der Anwendbarkeit einer Ausnahmevorschrift auf die Auftragsverarbeitung eine ausdrückliche Bezugnahme zu erwarten gewesen.[221]

Selbst wenn also letztlich identische Daten in das Drittland zurückübermittelt werden, sind die Schutzprinzipien der Richtlinie bei der Auftragsverarbeitung zu beachten. Eine Ausnahme ist nur möglich, sofern der Verarbeitungsprozess in den Mitgliedstaaten lediglich der Durchfuhr dient.

c. Die Bestellung eines Inlandvertreters

Gemäß Artikel 4 Absatz 2 der Richtlinie hat ein nach Artikel 4 Absatz 1c) verpflichteter Verantwortlicher einen Vertreter im Hoheitsgebiet desjenigen Mitgliedsstaates zu benennen, in dem sich das betreffende Mittel befindet. Damit soll erreicht werden, dass die verantwortliche Stelle ihre Verpflichtungen nach dem jeweils einschlägigen mitgliedstaatlichen Datenschutzgesetz tatsächlich einhält.[222]

Als generell unbedenklich gilt die gleichzeitige Zuständigkeit eines einzigen Inlandvertreters für verschiedene Verantwortliche[223] beziehungsweise für mehrere Mitgliedstaaten, es sei denn, die ernannte Stelle wird im Einzelfall ihren Aufgaben nicht gerecht.[224]

Der Vertreter nimmt die Rechte und Pflichten der drittländischen Stelle wahr, ohne den Verantwortlichen jedoch zu ersetzen. Der Betroffene sowie die Kontrollbehörden können sich mit ihren Anliegen dementsprechend sowohl an die verantwortliche Stelle im Drittland als auch an den Inlandvertreter wenden, der gewissermaßen als Mittler zwischen den einzelnen Stellen fungiert.[225] Daneben nennen ihn die Artikel 10, 11 und 18 Absatz 1 der Richtlinie ausdrücklich als Verpflichteten der Information des Betroffenen beziehungsweise der Registrierungspflicht.

---

[221] *Wuermeling*, Handelshemmnis Datenschutz, S. 79 f.
[222] *Schaar*, Datenschutz im Internet, Rn. 243.
[223] *WP 56*, S. 15.
[224] *Dammann*, RDV 2002, S. 70, S. 76.
[225] *Begründung der Bundesregierung zum Entwurf des Bundesdatenschutzgesetzes*, BT-Drs. 14/4329 vom 13.10.2000, S. 32.

Die Durchsetzung der den Verantwortlichen treffenden datenschutzrechtlichen Pflichten ist gegenüber dem Vertreter indessen nicht möglich, da die Pflicht zur Ernennung gemäß Artikel 4 Absatz 2 der Richtlinie „unbeschadet der Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst“ besteht.[226] Während also der zweite Richtlinienentwurf noch anordnete, dass der Vertreter in die Rechte und Pflichten der verarbeitenden Stelle eintritt,[227] vermittelt die endgültige Richtlinie nicht mehr die Befugnis, unmittelbar gegen den Vertreter vorgehen zu können. Mangels Sachbefugnis wäre der Vertreter als Beklagter nicht passivlegitimiert, eine Klage gegen ihn folglich materiell unbegründet.[228] Dementsprechend wäre er auch der falsche Adressat einer verwaltungsrechtlichen Verfügung der Aufsichtsbehörde. Eine Erleichterung zivil- und verwaltungsrechtlicher Maßnahmen schafft die Benennung eines Inlandvertreters nur insoweit, als dass er als Empfangsvertreter die an den Verantwortlichen gerichteten Erklärungen und Verfügungen entgegennimmt und somit eine Zustellung im Ausland erspart.[229]

d. Das Verhältnis zu Artikel 25 und 26 der Richtlinie

Sofern an dem Zurückgreifen auf ein automatisiertes oder nicht automatisiertes Mittel zum Zweck der grenzüberschreitenden Datenerhebung durch eine drittländische Stelle auf europäischer Seite ein Dritter beteiligt ist, stellt sich die Frage nach dessen Verpflichtungen aus den Vorschriften über den Drittländertransfer. Zu klären bleibt daher das Verhältnis des Artikels 4 Absatz 1c) zu den Artikeln 25 und 26 der Richtlinie.

In Betracht kommt zunächst eine parallele Anwendbarkeit der Vorschriften. Die europäische Stelle wäre sodann verpflichtet, den grenzüberschreitenden Rückgriff der drittländischen Stelle gemäß Artikel 25 der Richtlinie von der Angemessenheit des Schutzniveaus in dem jeweiligen Drittland abhängig zu machen, während sich letztere gemäß Artikel 4 Absatz 1c) der Richtlinie darüber hinaus an das einschlägige mitgliedstaatliche Datenschutzgesetz gebunden sähe. Das erscheint auf

---

[226] A. A. *Singleton*, 11 CL&P, S. 140, S. 141 (ohne Begründung).
[227] *Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (92/C 311/04)*, KOM (92) 422 endg. – SYN 287, gemäß Artikel 149 Absatz 3 des EWG-Vertrages von der Kommission vorgelegt am 16. Oktober 1992, ABl. EG Nr. C 311 vom 27. 11.1992, S. 30, S. 41.
[228] *Dammann*, RDV 2002, S. 70, S. 76.
[229] *Wuermeling*, Handelshemmnis Datenschutz, S. 94.

den ersten Blick durchaus sinnvoll, da somit für bestimmte Datenverarbeitungen ein doppelter Schutz bestünde.

Dagegen wird jedoch eingewandt, dass die Vorschriften über den Drittländertransfer sodann quasi überflüssig wären.[230] Der Tatbestand des Artikels 4 Absatz 1c) der Richtlinie sei deshalb nur erfüllt, sofern der für die Verarbeitung Verantwortliche sich absichtlich mittels einer außereuropäischen Niederlassung der Anwendung der mitgliedstaatlichen Datenschutzgesetze entziehen wolle, aber weiterhin in der Europäischen Union seine Hauptaktivitäten ausübe, oder sofern der Betroffene durch ein artifizielles Manöver seines Datenschutzes enthoben werde.[231]

Auf diese Weise wäre zwar tatsächlich eine parallele Anwendbarkeit des Artikels 4 Absatz 1c) und der Artikel 25 und 26 der Richtlinie im Rahmen einer Weitergabe zwischen einer europäischen und einer außereuropäischen Stelle tatbestandlich ausgeschlossen. Für eine derartige Auslegung liefert der Artikel 4 Absatz 1c) der Richtlinie allerdings keinerlei Anhaltspunkte.

Dennoch ist fraglich, ob ein und derselbe Vorgang gleichzeitig den Tatbestand der Übermittlung von Daten durch einen Dritten und jenen des Zurückgreifens auf ein in der Europäischen Union belegenes Mittel zum Zweck der Datenverarbeitung erfüllen kann.

Bei genauer Betrachtung dieser Konstellation kommen Zweifel an dieser Möglichkeit auf. Dem reinen Wortsinn der jeweiligen Verarbeitungsvarianten des Zurückgreifens und der Weitergabe durch Übermittlung entsprechend, drängt sich eine Abgrenzung der beiden Tatbestände förmlich auf: Während die empfangende Stelle bei dem Zurückgreifen die aktive Rolle übernimmt, kommt ihr bei einer Übermittlung durch einen Dritten der passive Part zu. Überschneidungen zwischen dem Anwendungsbereich der Richtlinie auf Verarbeitungen außereuropäischer Stellen und der Verpflichtung des mitgliedstaatlichen Datenexporteurs aus den Vorschriften über den Drittländertransfer wären nach dieser Formel ausgeschlossen.

Allerdings widerspräche die Beschränkung des Tatbestandes der Übermittlung auf eine aktive Weitergabe personenbezogener Daten durch die exportierende Stelle dem Schutzgehalt der Artikel 25 und 26 der

[230] So *Poullet*, Data Protection Conference, Brüssel 2002, S. 6.
[231] *Poullet*, Data Protection Conference, Brüssel 2002, S. 6 f.; *Terwangne/Louveaux*, MMR 1998, S. 451, S. 455 f.

Richtlinie. Sinn und Zweck dieser Vorschriften ist es, die Effektivität der Schutzprinzipien auf dem Binnenmarkt zu sichern. Entsprechend der Begründung des Rates zum gemeinsamen Standpunkt zielen sie auf eine gewisse „Undurchlässigkeit" des Systems ab und sollen zugleich „Nachlässigkeiten" bei der Weitergabe personenbezogener Daten in Drittländer verhindern.[232] Obschon der Datenempfänger de facto selbst auf den Datenbestand zurückgreifen muss, liegt daher bei einem Abruf personenbezogener Daten von einer in der Europäischen Union belegenen Datenbank nach allgemeiner Ansicht auch dann eine Übermittlung eines in den Mitgliedstaaten ansässigen Verantwortlichen vor, wenn dieser dem Datenimporteur lediglich den Zugang zu den gespeicherten Informationen eröffnet.[233]

Die Bewertung dieses Sachverhalts mag insofern überraschen, als dass auch bei einer Entlastung des europäischen Verarbeiters von den Verpflichtungen der Artikel 25 und 26 der Richtlinie materiell die Umgehung dieser Vorschriften ausgeschlossen wäre. So hat sich die drittländische Stelle ab dem Zeitpunkt des Rückgriffs auf ein in den Mitgliedstaaten belegenes Mittel gemäß Artikel 4 Absatz 1c) der Richtlinie ebenfalls nach den mitgliedstaatlichen Datenschutzgesetzen einschließlich der Vorschriften über den Drittländertransfer zu richten.[234] Auch ein außereuropäischer Verarbeiter muss also im Rahmen eines Datenabrufs bereits bei einer sich unmittelbar anschließenden Übermittlung in sein Sitzland, etwa im Rahmen einer grenzüberschreitenden Datenerhebung,[235] die Angemessenheit des dortigen Schutzniveaus beachten.[236] Dabei ist ohne Belang, ob der Übermittler die Daten an sich selbst beziehungsweise an eine eigene Datenbank versendet oder im Wege einer Bekanntgabe an eine andere Stelle weitergibt. Ungeachtet des Adressa-

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

[233] Z. B. *Bergmann/Möhrle/Herb*, § 3, Rn. 89 ff.; *Gola/Schomerus*, BDSG, § 3, Rn. 32; *Schaffland/Wiltfang*, BDSG, 5001, § 3, Rn. 40 f.; *Wuermeling*, Handelshemmnis Datenschutz, S. 89 f.; zu der Ausnahmeregelung des § 10 BDSG für automatisierte Abrufverfahren siehe weiter unten in diesem Gliederungspunkt.

[234] A. A. *Terwangne/Louveaux*, MMR 1998, S. 451, S. 455, da die Artikel 25 und 26 nur für Verantwortliche gelten würden, die in der Europäischen Union angesiedelt seien. Dafür bietet die Richtlinie jedoch keinerlei Anhaltspunkte.

[235] *Tröndle*, CR 1999, S. 717, S. 720; *Wuermeling*, Handelshemmnis Datenschutz, S. 205.

[236] Vgl. *Moritz/Winkler*, NJW-CoR 1997, S. 43, S. 48, die Art. 25 und 26 der Richtlinie bei der Versendung von Daten durch den Betroffenen an einen drittländischen Internetprovider anwenden, sofern der Versand über den in einem Mitgliedstaat belegenen Einwahlknoten des Internetproviders erfolgt; siehe auch *Löw*, S. 84, die allerdings den Einwahlknoten als Niederlassung definiert und sonach über Artikel 4 Absatz 1a) der Richtlinie zu demselben Ergebnis gelangt.

ten der personenbezogenen Daten liegt eine Übermittlung in ein Drittland bei jedem grenzüberschreitenden Sachverhalt vor.[237]

Das ergibt sich bereits aus dem Umkehrschluss zu den weiteren Vorschriften der Richtlinie, die sich mit den Fragen einer Übermittlung beschäftigen. Während diese stets von einer Übermittlung an einen Dritten[238] beziehungsweise an einen Empfänger[239] sprechen, setzen die Artikel 25 und 26 der Richtlinie ihrem Wortlaut nach lediglich eine Übermittlung in ein Drittland voraus.

Für diese Auslegung spricht ebenfalls der erste Bericht der Kommission über die Durchführung der Richtlinie, der nicht nur die Übermittlung an einen Empfänger, sondern daneben den Transfer an einen Bestimmungsort nennt.[240] Zwar geht es gemäß der deutschsprachigen Begründung des Rates zum gemeinsamen Standpunkt bei den Artikeln 25 und 26 um eine *Weitergabe* von Daten in ein Drittland,[241] also scheinbar um die Bekanntgabe der Daten an einen mit dem Übermittler nicht identischen Adressaten. Indessen sprechen jedoch zum Beispiel die englische und die französische Version an derselben Stelle von einem „transfer“ beziehungsweise „transfert“ und nicht etwa von einem „disclosure“ und einer „communication“ der Daten. Da die letzten beiden Begriffe in der deutschen Fassung des Artikels 2b) der Richtlinie als Weitergabe übersetzt wurden, ist davon auszugehen, dass die Begründung zum gemeinsamen Standpunkt die Weitergabe lediglich als Synonym für die Übermittlung verwendet.

Die dem Übermittlungsverbot zugrunde liegende besondere Schutzbedürftigkeit von personenbezogenen Daten bei dem Verlassen des Schutzbereichs der Gemeinschaft[242] lässt jedenfalls keine andere Auslegung zu. Zwar ist der für die Verarbeitung Verantwortliche im Zweifel auch noch nach der Übermittlung in ein Drittland an die mitgliedstaatlichen Datenschutzgesetze gebunden, jedoch zugleich im Hinblick auf

---

[237] Grabitz/Hilf III (- *Brühann*), A 30, Art. 25, Rn. 7; *Wuermeling*, Handelshemmnis Datenschutz, S. 89. Das deutsche BDSG, das in § 4b Absatz 2 von einer Übermittlung an eine Stelle spricht bzw. den Begriff der Übermittlung in § 3 Absatz 4 Nr. 3 grundsätzlich als Bekanntgabe an einen Dritten definiert, ist demnach hinsichtlich des grenzüberschreitenden Datenverkehrs richtlinienkonform auszulegen.

[238] Art. 7e), 7f), 11 Absatz 1 und 12c) der Richtlinie.

[239] Art. 12a), 1. Spiegelstrich, der Richtlinie.

[240] *Europäische Kommission*, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46) vom 15.05.2003, KOM (2003) 265 endgültig, S. 21.

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

[242] *Kopp*, DuD 1995, S. 204, S. 209.

seine außereuropäische Niederlassung oder Datenbank regelmäßig den Gesetzen des jeweiligen Drittlandes unterworfen. Der Schutz der Daten wäre trotz der Geltung eines mitgliedstaatlichen Datenschutzgesetzes daher zum Beispiel gefährdet, wenn den Staatsorganen dieses Drittlandes Eingriffsbefugnisse zustünden, die über die Ausnahmetatbestände des Artikels 13 der Richtlinie weit hinausgingen. Inwiefern sich derartige Befürchtungen als unbegründet erweisen, kann erst bei einer Angemessenheitsprüfung im Rahmen eines konkreten Transfers festgestellt werden.

Die Ursache für die Verpflichtung des in der Europäischen Union ansässigen Übermittlers ist folglich nicht in der Anwendbarkeit der materiellen Bestimmungen der Artikel 25 und 26 der Richtlinie zu suchen, sondern in der wirkungsvolleren Durchsetzung der Vorschriften gegenüber einer verarbeitenden Stelle aus den Mitgliedstaaten. Denn während die Tätigkeiten europäischer Verarbeiter effektiv kontrolliert werden können, griffe eine Aktivität der mitgliedstaatlichen Aufsichtsbehörden in einem Drittland ohne eine dies erlaubende völkerrechtliche Grundlage, etwa ein Verwaltungsabkommen oder die Einwilligung des Drittlandes, in fremde Souveränitätsrechte ein[243].

Eine in der Europäischen Union ansässige Stelle soll sich ferner nicht durch ein geschicktes Umgehungsmanöver ihrer Verantwortung für die Datenweitergabe entziehen können, indem sie die Daten nicht verschickt, sondern sie von dem Datenimporteur gewissermaßen abholen lässt.

Wird aber von einer Übermittlung ausgegangen, wenn nach allgemeinem Sprachgebrauch ein Rückgriff auf ein automatisiertes Mittel gegeben ist, so könnte umgekehrt auch ein Zurückgreifen im Sinne des Artikels 4 Absatz 1c) der Richtlinie vorliegen, wenn die Daten an den Empfänger versandt werden.

Eine Abgrenzung des Artikels 4 Absatz 1c) der Richtlinie von den Vorschriften über den Drittländertransfer anhand der reinen Wortbedeutung der jeweiligen Verarbeitungsvarianten scheidet mithin aus.

Die tatbestandlichen Voraussetzungen des Artikels 4 Absatz 1c) der Richtlinie erschöpfen sich indessen nicht in dem Merkmal des Zurückgreifens auf ein automatisiertes oder nicht automatisiertes Mittel.

[243] *Däubler*, CR 1999, S. 49, S. 54; *Ellger*, S. 89; *Giesen*, DuD 1996, S. 394, S. 396.

Vielmehr muss die drittländische Stelle für die grenzüberschreitende Datenverarbeitung verantwortlich sein.

Eine synchrone Verantwortlichkeit sowohl des Datenexporteurs als auch des Datenimporteurs für die Datenübertragung ist angesichts der Definition des für die Verarbeitung Verantwortlichen ausgeschlossen. Zwar geht Artikel 2d) der Richtlinie davon aus, dass es auch mehrere Verantwortliche für eine Verarbeitung geben kann. Dazu muss aber jede dieser Stellen gleichermaßen in der Lage sein, die Zwecke und die Mittel der Verarbeitung zu beeinflussen. Ansonsten kann von einer eigenen Entscheidung nicht mehr die Rede sein. Eine gemeinsame Entscheidung treffen beispielsweise die Mitglieder einer (nicht rechtsfähigen) Personengemeinschaft im Rahmen ihrer gemeinschaftlichen Verantwortung,[244] nicht aber zwei sich gegenüberstehende Parteien mit primär konträren Interessen.

Eine Übermittlung im Sinne der Artikel 25 und 26 der Richtlinie zeichnet sich in der Regel dadurch aus, dass die empfangende Stelle von der Gunst des Datenübermittlers beziehungsweise dessen rechtlicher Einschätzung des Schutzniveaus in dem jeweiligen Drittland abhängig ist. Der Exporteur kann letztlich jederzeit den Versand der Daten oder den Zugriff auf das automatisierte oder nicht automatisierte Mittel verweigern. Zudem ist der grenzüberschreitende Datengebrauch an die von der exportierenden Stelle festgelegten Zwecke und Rückgriffsmodalitäten gebunden. Von einer Verantwortlichkeit des Datenempfängers für den Vorgang des Rückgriffs kann wegen der sonach fehlenden Beherrschung des Mittels kaum mehr gesprochen werden.

Generell erschließt sich daraus, dass eine in einem Drittland ansässige Stelle nur dann für die grenzüberschreitende Verarbeitung verantwortlich sein kann, wenn ihr auf der anderen Seite der Datenübertragung niemand gegenübersteht, der im Hinblick auf den Übermittlungsvorgang nach den Vorschriften zum Drittländertransfer verpflichtet ist.[245] Denn anderenfalls ist der Datenempfänger an die Vorgaben der in der Europäischen Union niedergelassenen Stelle gebunden und demnach nicht im Sinne der Richtlinie verantwortlich für das Zurückgreifen auf das in den Mitgliedstaaten belegene Mittel.[246]

---

[244] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Dammann*), Art. 2, Rn. 11.

[245] A. A. *Koch*, S. 332; *ders.*, Datenschutz-Handbuch, Rn. 439, der ohne nähere Begründung davon ausgeht, dass jeder außereuropäische Datenempfänger einen Inlandvertreter nach Artikel 4 Absatz 1c) i. V. m. Absatz 2 der Richtlinie bestellen müsse.

[246] Dagegen kann die Verantwortung für die bezweckte Erhebung der übermittelten Daten sehr wohl in den Verantwortungsbereich des Datenempfängers fallen. Bei der Erhebung handelt es

In den mitgliedstaatlichen Datenschutzgesetzen finden sich allerdings Ausnahmen zu dem Grundsatz[247], dass die übermittelnde Stelle stets die Verantwortung für einen Datentransfer trägt.

Der deutsche Gesetzgeber hat zum Beispiel eine abweichende Verantwortungsaufteilung zwischen der speichernden und der abrufenden Stelle in dem Spezialfall des automatisierten Abrufverfahrens nach § 10 BDSG gesetzlich festgelegt.

Gemäß § 10 Absatz 4 Satz 1 BDSG trägt die abrufende Stelle die Verantwortung für die Zulässigkeit der einzelnen Abrufe. Die speichernde Stelle, welche die Daten zum Abruf bereit hält, überprüft die Zulässigkeit der jeweiligen Übermittlungen indessen nur, sofern ein konkreter Anlass dazu besteht (Satz 2). Sie hat allerdings zu gewährleisten, dass die Übermittlung durch Stichproben festgestellt und überprüft werden kann (Satz 3). Jeder der beteiligten Stellen obliegt darüber hinaus die Beurteilung, ob die Einrichtung des Verfahrens in dem betreffenden Fall überhaupt zulässig ist, ob sie also gemäß Satz 1 unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen erscheint. Hinter dieser Verantwortungsaufteilung steckt der Gedanke, dass die abrufende Stelle als tatbestandliche Voraussetzung eines automatisierten Abrufverfahrens die Datenübermittlung im Wege einer Selbstbedienung selbstständig veranlasst und die speichernde Stelle mangels Kenntnis des konkreten Abrufs keinen Einfluss nehmen kann.[248]

Aus derselben Erwägung gilt diese Regelung auch für Abrufverfahren, die einen weltweiten Zugriff auf Daten ermöglichen. Weder der Wortlaut noch die Systematik des Bundesdatenschutzgesetzes lassen einen anderen Schluss zu, da sich § 10 BDSG und der in Umsetzung des Artikels 25 der Richtlinie erlassene § 4b BDSG ohne ersichtliche Rangfolge im Allgemeinen Teil des Gesetzes befinden.

---

sich im Verhältnis zu der Übermittlung um einen eigenständigen Verarbeitungsabschnitt, für den es gemäß dem in der Richtlinie funktional verstandenen Begriff des Verantwortlichen trotz des einheitlichen Verarbeitungskomplexes einen unterschiedlichen Verantwortlichen geben kann.

[247] Simitis u. a. (- *Ehmann*), BDSG, § 10, Rn. 96; *Schaffland/Wiltfang*, BDSG, 5001, § 4b, Rn. 6; *TEIA*, Recht im Internet, S. 600; siehe auch § 4b Absatz 5 BDSG für Übermittlungen in das Ausland.

[248] Simitis u. a. (- *Ehmann*), BDSG, § 10, Rn. 15 und 92 f.; *Gola/Schomerus*, BDSG, § 10, Rn. 5 und 10; Kilian/Heussen (- *Weichert*), Nr. 132, Rn. 123.

Allerdings ist bereits im Rahmen der Angemessenheitsprüfung bei der Einrichtung des Abrufverfahrens das besondere Risiko eines Drittländertransfers zu berücksichtigen.[249] Die beteiligten Stellen müssen also schon vor der Einrichtung des Systems sicherstellen, dass jede potentielle Übermittlung den Voraussetzungen der Artikel 25 und 26 der Richtlinie genügen würde. Die Verantwortung für die Übermittlung der Daten in ein Drittland ist also vorverlagert. Die bereithaltende Stelle muss zwar nicht für die Einhaltung der Vorschriften bei dem konkreten Transfer einstehen, wohl aber dafür, dass dieser überhaupt möglich ist.

Bei Abrufsystemen, die ihren Standort außerhalb der Europäischen Union haben, muss zudem bereits die Übermittlung an die Datenbank den Voraussetzungen der Artikel 25 und 26 der Richtlinie genügen. Wird der Datenbestand dagegen in der Europäischen Union vorgehalten, greift ein außereuropäischer Datenempfänger bei einem Abruf auf ein in einem Mitgliedstaat belegenes Mittel zurück. Da ihm kraft Gesetzes die Verantwortung für den Abruf zukommt, ist sodann das jeweils einschlägige mitgliedstaatliche Datenschutzgesetz gemäß Artikel 4 Absatz 1c) der Richtlinie und im konkreten Fall das Bundesdatenschutzgesetz gemäß § 1 Absatz 5 Satz 2 anzuwenden.

Eine weitere Ausnahme zu dem Grundsatz, dass stets die übermittelnde Stelle die Verantwortung für einen Drittländertransfer trägt, ist in den in Umsetzung der Richtlinie 95/46/EG erlassenen mitgliedstaatlichen Datenschutzgesetzen aktuell nicht ersichtlich.

Dennoch wird erwogen, eine Verantwortungsaufteilung im grenzüberschreitenden Datenverkehr zwischen privaten Stellen auch außerhalb automatisierter Abrufverfahren unter Hinweis auf § 15 Absatz 2 Satz 2 des deutschen Bundesdatenschutzgesetzes zuzulassen.[250] Nach dieser Vorschrift soll der Datenempfänger für die Übermittlung verantwortlich sein, sofern der Transfer auf sein Ersuchen erfolgt. Ausdrücklich gilt diese Regelung allerdings nur für Datenübermittlungen zwischen zwei öffentlichen Stellen, also gemäß § 2 Absatz 1 bis 3 BDSG auch nur bei inländischen Sachverhalten. Die Anwendung auf einen grenzüberschreitenden Datentransfer zwischen zwei nicht öffentlichen Stellen erforderte demzufolge eine doppelte Analogie.

[249] Simitis u. a. (- *Ehmann*), BDSG, § 10, Rn. 58.
[250] So *Dammann*, RDV 2002, S. 70, S. 74.

Zweifelhaft ist bereits das Vorliegen einer Regelungslücke, da § 4b Absatz 5 BDSG die Verantwortung für den Transfer in ein Drittland explizit dem Übermittler aufbürdet. Dem § 15 BDSG liegt zudem der Gedanke zugrunde, dass ein öffentlich-rechtlicher Datenempfänger für die ordnungsgemäße Anwendung der für ihn maßgeblichen Fachgesetze einschließlich der betreffenden Erhebungsnorm im Verhältnis zum fachfremden Übermittler besonders qualifiziert ist. Die übermittelnde Behörde darf entsprechend dem Grundsatz der Gesetzmäßigkeit des öffentlichen Verwaltungshandelns auf die Rechtmäßigkeit des Ersuchens der empfangenden Behörde gemäß der Erhebungsnorm vertrauen. Entsprechende Voraussetzungen sind im Verhältnis zu nicht öffentlichen Stellen grundsätzlich nicht gegeben. Das bestätigt im Übrigen auch § 16 BDSG, der die Datenübermittlung einer öffentlichen an eine nicht öffentliche Stelle regelt und in Absatz 2 ausdrücklich und uneingeschränkt die Verantwortung dem Datenübermittler zuspricht. Die Verantwortungsumkehr des § 15 Absatz 2 Satz 2 BDSG kann folglich nur für den Datentransfer zwischen zwei öffentlichen Stellen gelten.

Aufgrund der Möglichkeit zu einer effektiveren Kontrolle der in der Europäischen Union ansässigen Verantwortlichen ist darüber hinaus zweifelhaft, ob eine Verantwortungsumkehr dem Schutzbedürfnis von Datenübermittlungen in Drittländer Rechnung tragen würde. Während diesem Problem bei einem automatisierten Abrufverfahren mittels der Verantwortung der bereithaltenden Stelle für die Einrichtung des Verfahrens abgeholfen wird, ist bei einer regulären Datenweitergabe keine Phase ersichtlich, in der eine vorgelagerte Prüfung der Voraussetzungen der Artikel 25 und 26 der Richtlinie durch den Versender stattfinden könnte, ohne dem Empfänger die Entscheidung über die Zwecke und die Mittel der Verarbeitung aus der Hand zu nehmen. Auch der Wortlaut des § 4b Absatz 1 BDSG deutet darauf hin, dass eine Verantwortungsverlagerung nicht vorgesehen ist.[251] Die Vorschrift ordnet zwar die Beachtung des § 15 Absatz 1 BDSG bei einer Übermittlung in Drittländer an, den Absatz 2 erwähnt sie jedoch nicht.

Außerhalb der besonderen Umstände des automatisierten Abrufverfahrens ist daher grundsätzlich der in der Europäischen Union ansässige Datenübermittler für den Transfer verantwortlich, sodass bei der Beteiligung eines Dritten auf europäischer Seite ein Zurückgreifen auf ein in der Europäischen Union belegenes Mittel gemäß Artikel 4 Absatz 1c)

[251] Simitis u. a. (- *Simitis*), BDSG, § 4b, Rn. 88 f.

der Richtlinie ausgeschlossen ist.[252] Die Frage der Abgrenzung zu den Artikeln 25 und 26 der Richtlinie hängt also in erster Linie nicht von der Aktivität des jeweils Handelnden ab, sondern von seiner Verantwortlichkeit für die entsprechende Datenverarbeitung. Der äußere Vorgang mag hier allenfalls eine bestimmte Wertung indizieren. Ergibt sich danach wie in dem Fall des automatisierten Abrufverfahrens die Verantwortung des Datenempfängers, so setzt die Anwendbarkeit der Richtlinie gemäß Artikel 4 Absatz 1c) zusätzlich die Inanspruchnahme eines in den Mitgliedstaaten lokalisierten Mittels voraus.

e. Ergebnis

Insgesamt erschließt sich, dass die Anwendbarkeit der Richtlinie gemäß Artikel 4 Absatz 1c) hauptsächlich von der Verantwortlichkeit für das Zurückgreifen auf das in der Europäischen Union lokalisierte Mittel abhängt.

Sobald das Mittel hinsichtlich des Rückgriffs durch den Betroffenen oder einen Dritten fremdgesteuert wird, unter Umständen auch nur durch bewusste Billigung eines Zugriffs, ist der Verarbeiter aus dem Drittland seiner die Verantwortung begründenden Entscheidungsfähigkeit regelmäßig enthoben.

Das ist insofern nicht unbillig, als dass die Daten sodann anderweitigen Schutz erfahren. Unterliegen sie nämlich der Verfügungsgewalt eines Dritten, darf dieser die Daten unter anderem nur unter den Voraussetzungen der Artikel 25 und 26 der Richtlinie übermitteln.

Überträgt der Betroffene indessen selbst seine Daten in ein Drittland, kann er bestimmen, ob und welche Daten er freiwillig sendet. Zwar weiß er bei der Benutzung des Internets nur selten, wohin seine Daten gelangen.[253] Das ist aber auch nicht zwingend erforderlich. Entsprechend dem Sinn und Zweck der grenzübergreifenden Richtlinienbestimmungen kommt es vor allem darauf an, dass ein Unionsbürger nicht überraschend schutzlos gestellt ist.[254] Da das Internet der Allgemeinheit als internationales Netzwerk bekannt ist, muss der Betroffene bei einer aktiven Versendung seiner Daten, bei der ihm also die Offenlegung

[252] Vgl. auch *Poullet*, Data Protection Conference, Brüssel 2002, S. 6, der Artikel 4 Absatz 1c) der Richtlinie nur erfüllt sieht, wenn sich der Datenfluss ohne Mitwirkung eines Dritten oder des Betroffenen vollzieht.
[253] *Deutscher Bundestag*, Sicherheit und Schutz im Netz, S. 225.
[254] *Poullet*, Data Protection Conference, Brüssel 2002, S. 6.

seiner Informationen bewusst ist, auch mit Zielen außerhalb der Europäischen Union rechnen. Er hat daher einzukalkulieren, dass ihm der Schutz der mitgliedstaatlichen Datenschutzgesetze versagt bleibt.

Eine Schwierigkeit bei der Anwendung der mitgliedstaatlichen Datenschutzgesetze vermag der Artikel 4 Absatz 1c) der Richtlinie derweil nicht zu überwinden. Da der Verantwortliche zum Zwecke ein und derselben Verarbeitung darauf angewiesen sein könnte, auf Mittel in verschiedenen Mitgliedstaaten zurückzugreifen, steht in Einzelfällen eine von Artikel 4 der Richtlinie gerade nicht gewollte Kollision der verschiedenen mitgliedstaatlichen Datenschutzgesetze zu befürchten.[255] In der Richtlinie finden sich keine Anknüpfungspunkte für eine Anwendung des Rechtes desjenigen Mitgliedstaates, in dem der Schwerpunkt der Verarbeitung liegt, sodass hier allein eine detaillierte Aufspaltung der einzelnen Verarbeitungsschritte und ihre Zuordnung zu dem betreffenden Mittel und somit zu dem örtlich geltenden Datenschutzgesetz in Betracht kommen.[256]

[255] *Korff*, RDV 1994, S. 209, S. 215; *Lütkemeier*, DuD 1995, S. 597, S. 599.
[256] *Korff*, RDV 1994, S. 209, S. 215 f.

C. Gesamtbetrachtung

Aus den bisherigen Erläuterungen ergibt sich, dass insbesondere die Definition des räumlichen Anwendungsbereichs der mitgliedstaatlichen Datenschutzgesetze sich bereits erheblich auf den Schutz des Betroffenen im grenzüberschreitenden Datenaustausch mit Drittländern auswirkt.

Sowohl das Sitzprinzip als auch der Tatbestand des Artikels 4 Absatz 1c) hemmen zusätzlich zu den Artikeln 25 und 26 der Richtlinie beziehungsweise als Bedingung zu deren Anwendbarkeit eine Flucht der Datenverarbeiter in so genannte Datenoasen.

Während das Sitzprinzip unterbindet, dass ein Verantwortlicher der Verarbeitung seine Datenverarbeitungen etwa im Wege einer Auftragsverarbeitung in solche Drittländer verlagert, in denen die Datenverarbeitung nur den Voraussetzungen eines angemessenen Schutzniveaus unterworfen ist, verhindert der Artikel 4 Absatz 1c) der Richtlinie, dass sich Datenverarbeiter aus außereuropäischen Staaten auf dem europäischen Datenmarkt frei bedienen können.

Andererseits hat die Analyse des Anwendungsbereichs auch gezeigt, dass die personenbezogenen Daten eines Betroffenen aufgrund der tatbestandlichen Voraussetzungen des Artikels 4 Absatz 1c) der Richtlinie, namentlich eines verantwortlichen Rückgriffs auf ein in der Europäischen Union belegenes Mittel, grundsätzlich nicht von den Richtlinienbestimmungen und insbesondere den Vorschriften über den Drittländertransfer geschützt werden, falls der Betroffene die Daten selbst in das Drittland übermittelt. Eine Ausnahme zu diesem Grundsatz kommt nur in Betracht, sofern ein in der Europäischen Union ansässiger Verantwortlicher einen in einem Drittland ansässigen Auftragsverarbeiter damit betraut, personenbezogene Daten vom Drittland aus in einem Mitgliedstaat zu erheben.

Die umfassende Durchsetzung der Schutzprinzipien der Richtlinie innerhalb ihres grenzüberschreitenden Anwendungsradius ist allerdings zweifelhaft, da den mitgliedstaatlichen Kontrollbehörden jenseits der nationalen Grenzen aufgrund des völkerrechtlichen Prinzips der Staatensouveränität die notwendigen Durchsetzungsbefugnisse fehlen. Zwar vermögen die Behörden gegen einen in der Europäischen Union ansässigen Verantwortlichen ohne weiteres vorzugehen. Die Ausübung der Datenschutzaufsicht gegenüber einem außereuropäischen Verantwortli-

chen im Rahmen des Artikels 4 Absatz 1c) der Richtlinie scheint indessen nicht zuletzt wegen der fehlenden rechtsgültigen Vertretungsbefugnis des Inlandvertreters fast unmöglich. Aufgrund des sonach fehlenden Kontroll- und Durchsetzungsmechanismus bleibt daher nur zu hoffen, dass die Richtlinienbestimmungen freiwillig von den betreffenden Datenverarbeitern beachtet werden.