0836-02/10/DE
WP 179

Stellungnahme 8/2010 zum anwendbaren Recht

Angenommen am 16. Dezember 2010

Zusammenfassung

In dieser Stellungnahme wird der Anwendungsbereich der Richtlinie 95/46/EG und insbesondere ihres Artikels 4 präzisiert, der bestimmt, welche auf der Grundlage dieser Richtlinie erlassenen einzelstaatlichen Vorschriften auf die Verarbeitung personenbezogener Daten Anwendung finden. Des Weiteren wird auf bestimmte Bereiche eingegangen, in denen Raum für Verbesserungen besteht.
Eine präzisere Bestimmung der Anwendung des EU-Rechts auf die Verarbeitung personenbezogener Daten dient auch dazu, den Anwendungsbereich des EU-Datenschutzrechts sowohl in der EU bzw. im EWR als auch im größeren internationalen Kontext zu klären. Eine klare Vorstellung davon, welches Recht zur Anwendung kommt, wird sowohl den für die Verarbeitung Verantwortlichen als auch den Betroffenen und anderen Beteiligten mehr Rechtssicherheit vermitteln. Eine korrekte Auslegung der Vorschriften zum anwendbaren Recht dürfte überdies gewährleisten, dass der durch die Richtlinie 95/46 gebotene weit reichende Schutz personenbezogener Daten keine Rechtslücken oder Schlupflöcher aufweist.

Die Bezugnahme in Artikel 4 Absatz 1 Buchstabe a auf „eine" Niederlassung bedeutet, dass sich das anwendbare Recht nach dem Mitgliedstaat bestimmt, in dem der für die Verarbeitung Verantwortliche eine Niederlassung besitzt; besitzt der Verantwortliche auch Niederlassungen in anderen Mitgliedstaaten, kann auch das Recht dieser Mitgliedstaaten zur Anwendung berufen werden. Für die Anwendung des nationalen Rechts kommt es darauf an, dass die Verarbeitungen im „Rahmen der Tätigkeiten" der Niederlassung ausgeführt werden. Dies bedeutet, dass die *Niederlassung* des für die Verarbeitung Verantwortlichen mit *Tätigkeiten* befasst ist, die sich auf die Verarbeitung personenbezogener Daten beziehen, wobei der Umfang dieser Verarbeitungstätigkeit, die Art der Tätigkeiten und die Notwendigkeit, einen wirksamen Datenschutz zu gewährleisten, zu berücksichtigen sind.

In Bezug auf die Bestimmung in Artikel 4 Absatz 1 Buchstabe c über die zum Zwecke der Datenverarbeitung verwendeten „Mittel", die die Anwendung der Richtlinie auf Verantwortliche außerhalb der EU bzw. des EWR zur Folge haben kann, wird in der Stellungnahme präzisiert, dass diese Bestimmung in den Fällen Anwendung finden sollte, in denen es keine Niederlassung in der EU bzw. im EWR gibt, *die die Anwendung von Artikel 4 Absatz 1 Buchstabe a auslösen würde*, oder in denen die Verarbeitung *nicht im Rahmen der Tätigkeiten einer solchen Niederlassung erfolgt.* Eine weite Auslegung des Begriffs „equipment", die auch durch die Wortwahl in anderen Sprachfassungen („Mittel" in der deutschsprachigen Fassung) gerechtfertigt ist, kann in manchen Fällen dazu führen, dass europäisches Datenschutzrecht auch dann zur Anwendung gelangt, wenn die betreffende Verarbeitung keinen konkreten Bezug zur EU bzw. zum EWR aufweist.

Die Stellungnahme gibt darüber hinaus Auslegungshinweise und Beispiele zu den anderen Bestimmungen des Artikels 4, zu den Sicherheitsanforderungen nach Maßgabe des gemäß Artikel 17 Absatz 3 anwendbaren Rechts sowie zu der Möglichkeit der Datenschutzbehörden, bei einem Verarbeitungsvorgang in ihrem Hoheitsgebiet ihre Untersuchungs- und Eingriffsbefugnisse auch dann auszuüben, wenn das Recht eines anderen Mitgliedstaats anwendbar ist (Artikel 28 Absatz 6).

In der Stellungnahme wird auch angeregt, im Rahmen einer Überarbeitung des allgemeinen Datenschutzrahmens die Richtlinie klarer zu fassen und für eine größere Kohärenz innerhalb des Artikels 4 zu sorgen.

Eine Vereinfachung der Regeln zur Bestimmung des anwendbaren Rechts würde vor diesem Hintergrund auf eine Rückkehr zum Herkunftslandprinzip hinauslaufen: Danach würden alle Niederlassungen eines für die Verarbeitung Verantwortlichen in der EU unabhängig davon, wo diese Niederlassungen jeweils angesiedelt sind, dasselbe Recht anwenden, und zwar das der Hauptniederlassung. Dies wäre jedoch nur dann akzeptabel, wenn das einzelstaatliche Recht, d.h. auch die Sicherheitspflichten, umfassend harmonisiert würde.

Wenn der für die Verarbeitung Verantwortliche außerhalb der EU niedergelassen ist, könnten

zusätzliche Kriterien herangezogen werden, um eine ausreichende Verbindung zum EU-Gebiet sicherzustellen und um gleichzeitig zu vermeiden, dass in Drittländern ansässige Verantwortliche Daten im EU-Gebiet rechtswidrig verarbeiten. Hierfür in Frage kommende Kriterien wären das Anvisieren einzelner Personen (wenn sich die Verarbeitung personenbezogener Daten auf Einzelpersonen in der EU bezieht und die Anwendung des EU-Datenschutzrechts zur Folge hat) oder hilfsweise der begrenzte Rückgriff auf das „equipment"-Kriterium (Verarbeitung personenbezogener Daten durch automatisierte oder nicht automatisierte, im Hoheitsgebiet des betreffenden Mitgliedstaats belegene Mittel) zwecks Erfassung von Grenzfällen (Daten von Drittstaatsangehörigen, Verantwortliche ohne Bezug zur EU), wenn es in der EU eine entsprechende Infrastruktur für die Datenverarbeitung gibt.

Die Gruppe für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten –

eingesetzt gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 (ABl. L 281 vom 23.11.1995, S. 31),

gestützt auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe a und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung,

hat folgende Stellungnahme angenommen:

I. Einleitung

Die Bestimmung des auf die Verarbeitung personenbezogener Daten anwendbaren Rechts nach der Richtlinie 95/46/EG („Datenschutzrichtlinie“) ist aus mehreren Gründen sehr wichtig. Die Vorschriften über das anwendbare Recht bestimmen maßgeblich den Geltungsbereich des EU-Datenschutzrechts, d.h. sie bestimmen, inwieweit das EU-Datenschutzrecht für die Verarbeitung personenbezogener Daten gilt, die ganz oder teilweise außerhalb der EU bzw. des EWR stattfindet, aber dennoch einen hinreichend relevanten Bezug zum EU- beziehungsweise EWR-Gebiet aufweist. Sie bestimmen gleichzeitig aber auch den Geltungsbereich in der EU bzw. im EWR, um Kollisionen und Überschneidungen zwischen den einzelstaatlichen Vorschriften der EU- bzw. EWR-Mitgliedstaaten zur Umsetzung der Richtlinie zu vermeiden[1].

Eine korrekte Auslegung der Vorschriften zum anwendbaren Recht dürfte überdies gewährleisten, dass der durch die Richtlinie 95/46 gebotene weit reichende Schutz personenbezogener Daten keine Rechtslücken oder Schlupflöcher aufweist.

Mit dem anwendbaren Recht befassen sich mehrere Bestimmungen der Richtlinie, insbesondere Artikel 4, Artikel 17 und Artikel 28. In diesen Bestimmungen ist geregelt, welches einzelstaatliche Datenschutzrecht nach Maßgabe der Richtlinie Anwendung findet und welche Behörde für dessen Anwendung zuständig ist. Dabei ist zu bedenken, dass materiellrechtliche Vorschriften und Zuständigkeitsvorschriften nicht losgelöst voneinander zu betrachten sind. Auf diesen Aspekt wird weiter unten im Einzelnen eingegangen.

Sowohl die Umsetzung als auch die Auslegung der Richtlinienbestimmungen zum anwendbaren Recht ist, so heißt es, in der EU bei Weitem noch nicht einheitlich. Die Kommission wies bereits in ihrem ersten Bericht über die Durchführung der Datenschutzrichtlinie darauf hin, dass die Umsetzung des Artikels 4 „in mehreren Fällen fehlerhaft [ist], wodurch genau die Art von Konflikten auftreten könnten, die durch diesen Artikel verhindert werden sollen“[2]. Dem technischen Anhang zu diesem Bericht zufolge, der eine ausführliche Analyse einzelstaatlicher Umsetzungsvorschriften enthält, lässt sich die mangelhafte Umsetzung zum Teil auf die komplexe Regelung des Artikels selbst zurückführen.

Zu einem ähnlichen Ergebnis kommt eine von der Europäischen Kommission in Auftrag gegebene Studie[3], in der auf die Ambiguität und unterschiedliche Umsetzung der Richtlinienvorschriften zum anzuwendenden Recht hingewiesen wird. Dieser Studie zufolge sind bessere, klarere und eindeutige Regelungen zum anzuwendenden Recht dringend erforderlich.

---

1 Die Richtlinie 95/46/EG gilt nach dem EWR-Abkommen auch für die EFTA-Staaten Norwegen, Island und Liechtenstein; vgl. Beschluss des Gemeinsamen EWR-Ausschusses Nr. 83/1999 vom 25. Juni 1999 zur Änderung des Protokolls 37 und des Anhangs XI (Telekommunikationsdienste) zum EWR-Abkommen (ABl. L 296 vom 23.11.2000, S. 41.)

2 Erster Bericht über die Durchführung der Datenschutzrichtlinie (95/46/EG), Mai 2003, S. 17, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:DE:HTML.

3 „Vergleichende Studie über verschiedene Ansätze zur Bewältigung neuer Herausforderungen für den Schutz der Privatsphäre, insbesondere aufgrund technologischer Entwicklungen“, Januar 2010; abrufbar unter http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm.

In ihrem neuen „Gesamtkonzept für den Datenschutz in der Europäischen Union“[4] hat die Kommission unlängst folgende Zusage gemacht: *„Die Kommission wird prüfen, wie die geltenden Vorschriften über das anwendbare Recht sowie die Kriterien zu dessen Bestimmung geändert und präzisiert werden können, um für mehr Rechtssicherheit zu sorgen, die Zuständigkeit der Mitgliedstaaten für die Anwendung der Datenschutzvorschriften zu klären und letztlich den von der Verarbeitung Betroffenen in der EU unabhängig vom geografischen Standort des für die Verarbeitung Verantwortlichen stets ein gleiches Schutzniveau zu garantieren.“*

Die mit dem anwendbaren Recht verbundenen Fragen werden nicht zuletzt auch aufgrund der Globalisierung und der Entwicklung neuer Technologien zunehmend komplexer: Unternehmen, die rund um die Uhr Dienste und Unterstützungsleistungen anbieten, sind immer häufiger in mehreren Mitgliedstaaten und Rechtsordnungen tätig. Mit dem Internet ist es sehr viel einfacher geworden, Dienstleistungen von einem anderen Ort aus zu erbringen und personenbezogene Daten in einer virtuellen Umgebung zu sammeln und auszutauschen. Durch *Cloud Computing* wird es schwerer, den Ort zu bestimmen, an dem sich personenbezogene Daten und die zu einem bestimmten Zeitpunkt eingesetzten elektronischen Mittel befinden.

Es ist daher entscheidend, dass die Richtlinienbestimmungen zum anwendbaren Recht für alle, die mit der Umsetzung der Richtlinie und der Anwendung der nationalen Datenschutzvorschriften sowohl im öffentlichen als auch im privaten Sektor zu tun haben, inhaltlich hinreichend klar sind.

Die Datenschutzgruppe hat deshalb beschlossen, zur Klärung einiger Kernbestimmungen der Richtlinie beizutragen und sich mit dem anwendbaren Recht zu befassen, so wie sie es bereits mit den Begriffen „personenbezogene Daten“, „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ getan hat[5]. Sie nimmt dabei auch auf andere Stellungnahmen Bezug, in denen die Problematik des anwendbaren Rechts im Zusammenhang mit den dort behandelten spezifischen Fragestellungen zur Sprache kam[6].

Ziel der Datenschutzgruppe ist es letztlich, für Rechtssicherheit bei der Anwendung des EU-Datenschutzrechts zu sorgen. Dies impliziert nicht nur, dass den Betroffenen bekannt sein muss, welches Recht für den Schutz ihrer personenbezogenen Daten gilt, sondern dass auch die Geschäftswelt sowie private und öffentliche Einrichtungen wissen müssen, welchen Datenschutzbestimmungen ihre Datenverarbeitung unterliegt.

Es ist wichtig, dass der Begriff des anwendbaren Rechts geklärt wird, unabhängig davon, ob es zu einer Änderung der geltenden Richtlinienbestimmungen kommen wird oder nicht. Die derzeitigen Bestimmungen bleiben gültig, bis und soweit sie geändert werden. Wenn somit die Bestimmungen zum anwendbaren Recht inhaltlich präzisiert werden, trägt dies dazu bei, dass die Richtlinie bis zu ihrer etwaigen Änderung besser befolgt

---

4 KOM(2010) 609 endgültig vom 4.11.2010.

5 Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ (WP 136) und Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ (WP 169), abrufbar unter http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

6 Zu nennen sind insbesondere das Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU (WP 56), Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP 128) und Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148).

wird. Bei der Vorbereitung dieser Stellungnahme konnte die Datenschutzgruppe auf ihre Erfahrungen mit der Anwendung der derzeitigen Regelung zurückgreifen, die es ihr ermöglichen, den Gesetzgeber bei einer etwaigen Überarbeitung der Richtlinie zu unterstützen.

Die Vorschriften über die Bestimmung des anwendbaren Rechts in Datenschutzfragen sollen die Anwendung der Richtlinie innerhalb ihres in Artikel 3 definierten sachlichen Geltungsbereichs regeln. Dabei entstehen häufig Einflüsse auf andere Rechtsbereiche, allerdings nicht über den Anwendungsbereich der Richtlinie hinaus[7].

II. Allgemeine Bemerkungen und politische Aspekte

II.1. Vorgeschichte: vom Übereinkommen Nr. 108 zur Richtlinie 95/46/EG

Bereits im Jahr 1981 wiesen die Verfasser des unter der Schirmherrschaft des Europarats ausgearbeiteten Übereinkommens Nr. 108 auf das Risiko einer Normenkollision bzw. Rechtslücke hin, die sich aus der Anwendung verschiedener einzelstaatlicher Rechtssysteme ergeben könnte. Seinerzeit wurden jedoch keine Bestimmungen aufgenommen, um dieses Problem anzugehen: Der Umstand, dass das Übereinkommen einen „gemeinsamen Sockel" an materiellrechtlichen Bestimmungen vorsieht, wurde als wesentliche Garantie dafür angesehen, dass die Grundsätze, die letztlich angewandt werden, dieselben sind und so Unterschiede im Schutzumfang vermieden werden, auch wenn weiterhin divergierende Regelungen bestehen.

Bei der Ausarbeitung der Datenschutzrichtlinie trug die Europäische Kommission der Notwendigkeit Rechnung, Anknüpfungskriterien zur Bestimmung des anwendbaren Rechts festzulegen. In ihrem ursprünglichen Vorschlag[8] bestimmte die Kommission als Hauptanknüpfung den Ort, an dem sich die Dateien befinden, und als zweite Anknüpfung die Niederlassung des für die Verarbeitung Verantwortlichen, wenn sich die Dateien in einem Drittland befinden.

Im Laufe der Beratungen im Europäischen Parlament und im Rat der EU wurde der Standort der Datei zugunsten des Orts der Niederlassung des für die Verarbeitung Verantwortlichen aufgegeben. Für den Fall, dass der für die Verarbeitung Verantwortliche nicht in der EU niedergelassen ist, wurde als zweites Anknüpfungskriterium der Ort festgelegt, an dem die Mittel für die Datenverarbeitung belegen sind.

---

7 Die Richtlinie enthält zwar Vorschriften zu Haftung (Artikel 23) und Sanktionen (Artikel 24), aber, wie Erwägungsgrund 21 der Richtlinie zu entnehmen ist, die allgemeinen Grundsätze des Zivil- und Strafrechts bleiben prinzipiell unberührt. Sie kommen nur ins Spiel, soweit dies notwendig ist, um eine Verletzung von Datenschutzgrundsätzen zu ahnden. Die Richtlinie wurde in den Mitgliedstaaten so umgesetzt, dass in manchen Fällen strafrechtliche Sanktionen möglich sind. Ein weiteres Beispiel sind die Verarbeitungsvoraussetzungen in Artikel 2 Buchstabe h, Artikel 7 Buchstabe a und Artikel 8 Absatz 2 Buchstabe a (Notwendigkeit der Einwilligung) und Artikel 7 Buchstabe b (Erfüllung von Vertragspflichten). Trotz dieser Bestimmungen greift die Richtlinie darüber hinaus weder in das Vertragsrecht (z.B. Voraussetzungen für den Vertragsabschluss, anwendbares Recht) noch in andere Aspekte des Zivilrechts ein.

8 KOM(1990) 314/2 vom 18.7.1990, Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung pesonenbezogener Daten.

Der Rat ergänzte diese Kriterien und führte den Begriff der Niederlassung weiter aus. Dem geänderten Vorschlag der Kommission[9] zufolge sollte die Verarbeitung „im Rahmen der Tätigkeiten einer Niederlassung" des für die Verarbeitung Verantwortlichen erfolgen. Dabei wurde die Möglichkeit berücksichtigt, dass der für die Verarbeitung Verantwortliche mehrere Niederlassungen in verschiedenen Mitgliedstaaten besitzen könnte. Eine wichtige Änderung betraf den Umstand, dass als Hauptanknüpfung zur Bestimmung des anwendbaren Rechts nicht der Ort herangezogen wurde, an dem der für die Verarbeitung Verantwortliche seine Hauptniederlassung hat, sondern der Ort, an dem sich *eine* Niederlassung des Verantwortlichen befindet. Die Folgen dieser Änderungen in Gestalt einer distributiven statt einheitlichen Anwendung einzelstaatlichen Rechts bei mehreren Niederlassungen werden nachstehend erläutert.

II.2. Begrifflichkeiten

II.2.a) Kontext und strategische Bedeutung

Eine präzisere Bestimmung der Anwendung des EU-Rechts auf die Verarbeitung personenbezogener Daten dient, wie bereits erwähnt, auch dazu, den Anwendungsbereich des EU-Datenschutzrechts sowohl in der EU bzw. im EWR als auch im größeren internationalen Kontext zu klären. Eine klare Vorstellung davon, welches Recht zur Anwendung kommt, verhilft sowohl den für die Verarbeitung Verantwortlichen als auch den Betroffenen und anderen Beteiligten zu mehr Rechtssicherheit.

Die Bestimmung des anwendbaren Rechts hängt eng damit zusammen, wer der für die Verarbeitung Verantwortliche ist[10] und wo sich seine Niederlassung(en) befindet bzw. befinden: Mit dieser Verknüpfung wird in erster Linie die Verantwortung des für die Verarbeitung Verantwortlichen und seines Vertreters (falls der für die Verarbeitung Verantwortliche in einem Drittland niedergelassen ist) bestätigt.

Wie im Folgenden ausgeführt wird, bedeutet dies nicht, dass es stets nur ein anwendbares Recht gibt, insbesondere dann nicht, wenn der für die Verarbeitung Verantwortliche mehrere Niederlassungen besitzt: Es kommt auch auf den Ort dieser Niederlassungen und die Art ihrer Tätigkeiten an. Eine eindeutige Anknüpfung an den für die Verarbeitung Verantwortlichen kann jedoch Garant für eine wirksame Rechtsanwendung und –durchsetzung sein, vor allem wenn es um Sachverhalte geht, bei denen es schwierig oder mitunter gar unmöglich ist, den Standort einer Datei ausfindig zu machen (z.B. beim *Cloud Computing*).

Mit klaren Leitlinien zum anwendbaren Recht dürfte es auch möglich sein, auf neue Entwicklungen technologischer Art (Internet, netzgestützte Dateien bzw. *Cloud Computing*) und kommerzieller Art (multinationale Unternehmen) zu reagieren.

---

9 KOM(1992) 422 endgültig vom 15.10.1992.

10 Vgl. Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" (WP 169).

II.2.b) <u>Anwendungsbereich des EU-Rechts und des nationalen Rechts innerhalb der EU und des EWR</u>

Hauptanknüpfungskriterien zur Bestimmung des anwendbaren Rechts sind der Ort der Niederlassung des für die Verarbeitung Verantwortlichen und, wenn Letzterer außerhalb des EWR niedergelassen ist, der Ort, an dem die für die Verarbeitung verwendeten Ausrüstungsgegenstände bzw. Mittel[11] belegen sind. Dies bedeutet, dass weder die Staatsangehörigkeit noch der gewöhnliche Aufenthalt der betroffenen Personen, noch der Ort, an dem sich die personenbezogenen Daten befinden, für die Bestimmung des anwendbaren Rechts ausschlaggebend sind[12].

All das legt einen weiten Anwendungsbereich nahe, der Rechtswirkungen besitzt, die über den EWR hinausgehen: Die Richtlinie und die einzelstaatlichen Umsetzungsvorschriften gelten sowohl für die Verarbeitung personenbezogener Daten außerhalb des EWR (wenn die Verarbeitung im Rahmen von Tätigkeiten einer Niederlassung des für die Verarbeitung Verantwortlichen im EWR erfolgt) als auch für außerhalb des EWR niedergelassene Verantwortliche (wenn sich die für die Verarbeitung verwendeten Mittel im EWR befinden). Infolgedessen kann sich die Anwendung der Richtlinie auf Dienstleistungen mit einer internationalen Dimension erstrecken (z.B. Suchmaschinen, soziale Netze im Internet und *Cloud Computing*. Diese Beispiele werden nachfolgend erläutert.

Werden personenbezogene Daten von einem für die Verarbeitung Verantwortlichen X verarbeitet, dessen einzige Niederlassung sich in Mitgliedstaat A befindet, findet auf die Verarbeitung, unabhängig davon, wo sie stattfindet, das Recht des Mitgliedstaats A Anwendung.

Hat X auch eine Niederlassung Y in Mitgliedstaat B, unterliegt die von Y ausgeführte Datenverarbeitung dem Recht des Mitgliedstaats B, sofern die Verarbeitung im Rahmen der Tätigkeiten der Niederlassung Y erfolgt. Erfolgt die von Y ausgeführte Verarbeitung im Rahmen der Tätigkeiten der Niederlassung X in Mitgliedstaaten A, ist auf die Verarbeitung das Recht des Mitgliedstaats A anzuwenden.

Werden personenbezogene Daten von einem Auftragsverarbeiter verarbeitet, der nicht in einem Mitgliedstaat niedergelassen ist, unterliegt die Verarbeitung dem Recht des Mitgliedstaats, in dem sich die vom Auftragsverarbeiter für die Verarbeitung verwendeten Mittel befinden. Auf Beispiele für diese verschiedenen Fallgestaltungen wird in dieser Stellungnahme an anderer Stelle eingegangen.

---

11 Wie unter III.2.b erläutert, wurde der englische Begriff „equipment“ in anderen EU-Sprachen im Sinne von „Mittel“ wiedergegeben, was für eine weite Auslegung dieses Begriffs spricht und erklärt, warum in der englischen Fassung dieser Stellungnahme neben „equipment“ eben auch „means“ verwendet wird.

12 In diesem Sinne auch Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt. Für das auf Sicherheitsmaßnahmen anwendbare Recht ist als Anknüpfungspunkt auch der Ort relevant, an dem der Auftragsverarbeiter niedergelassen ist (Artikel 17). Es handelt sich hierbei jedoch nicht um eine eigenständige Anknüpfung, sondern dieses Kriterium muss in Verbindung mit der Hauptanknüpfung, d.h. der Niederlassung des für die Verarbeitung Verantwortlichen, angewandt werden.

Mit dem weiten Anwendungsbereich soll in erster Linie gewährleistet werden, dass Betroffenen nicht der Schutz vorenthalten wird, der ihnen nach der Richtlinie zusteht; gleichzeitig soll damit auch eine Gesetzesumgehung verhindert werden.

Die Richtlinie enthält Kriterien, nach denen sich bestimmt,

i) ob EU-Recht – gegebenenfalls zusammen mit dem Recht eines Drittstaats – auf eine bestimmte Verarbeitung personenbezogener Daten Anwendung findet, und
ii) welches mitgliedstaatliche Recht auf die Verarbeitung Anwendung findet, wenn EU-Recht für die Verarbeitung EU-Recht maßgebend ist.

Es sei auch darauf hingewiesen, dass bestimmte Verarbeitungsvorgänge innerhalb der EU außerhalb des Anwendungsbereichs der Richtlinie liegen. Sie können allerdings die Anwendung anderer EU-Rechtsinstrumente bewirken, beispielsweise des Rahmenbeschlusses 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden[13], oder der Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft[14] oder anderer Regelungen über bestimmte EU-Einrichtungen oder Informationssystemen (Europol, Eurojust, SIS, ZIS usw.)[15].

II.2.c) Vermeidung von Rechtslücken und Überschneidungen

Durch eindeutige Kriterien für die Bestimmung des anwendbaren Rechts soll eine Umgehung des einzelstaatlichen Rechts der Mitgliedstaaten und eine Überschneidung mitgliedstaatlicher Regelungen vermieden werden. Ob eine oder mehrere Rechtsordnungen zur Anwendung berufen werden, hängt davon ab, ob der für die Verarbeitung Verantwortliche mehrere Niederlassungen besitzt und welche Tätigkeiten dort ausgeführt werden:

- Hat der für die Verarbeitung Verantwortliche nur eine Niederlassung, findet im gesamten EU- bzw. EWR-Gebiet nur ein Recht Anwendung, das sich nach dem Ort dieser Niederlassung bestimmt[16].

- Gibt es mehrere Niederlassungen, bestimmt sich das anzuwendende einzelstaatliche Recht nach der Tätigkeit, die die einzelne Niederlassung ausübt.

Mit diesen Kriterien soll verhindert werden, dass mehrere einzelstaatliche Rechtsordnungen auf dieselbe Verarbeitungstätigkeit Anwendung finden.

---

13 Rahmenbeschluss 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60).

14 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

15 Europol: Beschluss 2009/371/JI des Rates (ABl. L 121 vom 15.5.2009, S. 37); Eurojust: Beschluss 2002/187/JI des Rates (ABl. L 63 vom 6.3.2002, S. 1), geändert durch den Beschluss 2009/426/JI des Rates (ABl. L 138 vom 4.6.2009, S. 14).

16 Hiervon ausgenommen sind Sicherheitsmaßnahmen: Für sie ist nach Artikel 17 Absatz 3 der Richtlinie das Recht am Sitz des Auftragsverarbeiters maßgebend.

II.2.d) Anwendbares Recht und gerichtliche Zuständigkeit im Richtlinienkontext

Im Bereich des Datenschutzes ist es besonders wichtig, zwischen dem Begriff des *anwendbaren Rechts* (d.h. des auf einen bestimmten Sachverhalt anzuwendenden Rechts) und dem Begriff der *gerichtlichen Zuständigkeit* (nach der sich die Befugnis eines einzelstaatlichen Gerichts richtet, über einen Fall zu urteilen oder ein Urteil oder einen Beschluss zu vollstrecken) zu unterscheiden. Bei bestimmten Datenverarbeitungen müssen das anwendbare Recht und die gerichtliche Zuständigkeit nicht unbedingt deckungsgleich sein.

Die Außenwirkung des EU-Rechts ist Ausdruck der Fähigkeit der EU, Vorschriften zum Schutz grundlegender Interessen innerhalb ihrer Gerichtsbarkeit zu erlassen. Die Richtlinie bestimmt auch, inwieweit das einzelstaatliche Recht der Mitgliedstaaten zur Anwendung gelangt, greift aber nicht in die Zuständigkeit der nationalen Gerichte für die Verhandlung einschlägiger Rechtsstreitigkeiten ein. Dafür enthält sie Hinweise auf den räumlichen Zuständigkeitsbereich der Kontrollstellen, die das nach Maßgabe der Richtlinie bestimmte Recht anwenden und durchsetzen können.

Obwohl die beiden Begriffe (anwendbares Recht und Zuständigkeit der Kontrollstellen) in den meisten Fällen auf ein und dieselbe Rechtsordnung verweisen (was zur Folge hat, dass das Recht des Mitgliedstaats A von den Behörden des Mitgliedstaats A angewandt wird), ist in der Richtlinie ausdrücklich die Möglichkeit einer anderen Regelung vorgesehen. Artikel 28 Absatz 6 impliziert, dass die nationalen Datenschutzbehörden in der Lage sein sollten, ihre Befugnisse auch dann auszuüben, wenn das Datenschutzrecht eines anderen Mitgliedstaats auf die in ihrem Zuständigkeitsbereich erfolgende Verarbeitung personenbezogener Daten Anwendung findet. Die Datenschutzgruppe wird den praktischen Folgen dieser Zuständigkeitsregelung in einer anderen Stellungnahme nachgehen.

Die vorstehend beschriebenen Fälle mit grenzüberschreitender Wirkung machen es erforderlich, dass die zuständigen Datenschutzbehörden unter Berücksichtigung ihrer jeweiligen Durchführungsbefugnisse zusammenarbeiten. Ebenso machen sie deutlich, dass die einschlägigen Richtlinienbestimmungen ordnungsgemäß in innerstaatliches Recht umgesetzt werden müssen, da dies für eine effiziente grenzüberschreitende Zusammenarbeit und Rechtsanwendung ausschlaggebend sein kann.

III. Analyse der einschlägigen Richtlinienbestimmungen

Die Kernbestimmungen zum anwendbaren Recht finden sich in Artikel 4, der bestimmt, welche auf der Grundlage dieser Richtlinie erlassenen einzelstaatlichen Datenschutzregelungen auf die Verarbeitung personenbezogener Daten Anwendung finden.

III.1. Für die Verarbeitung Verantwortlicher mit einer Niederlassung in einem oder mehreren Mitgliedstaaten (Artikel 4 Absatz 1 Buchstabe a)

Artikel 4 Absatz 1 regelt zuerst den Fall, dass der für die Verarbeitung Verantwortliche eine oder mehrere Niederlassungen im Hoheitsgebiet der EU besitzt. Dort heißt es, dass jeder Mitgliedstaat sein eigenes Datenschutzrecht auf die Verarbeitung personenbezogener Daten anwendet, *„die im Rahmen der Tätigkeiten einer*

Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält."

Der Begriff „für die Verarbeitung Verantwortlicher" ist in Artikel 2 Buchstabe d der Richtlinie definiert. Auf diese Definition wird hier nicht weiter eingegangen, da sie bereits in der Stellungnahme der Datenschutzgruppe zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter"[17] behandelt wurde.

Es sei ferner darauf hingewiesen, dass eine Niederlassung keine Rechtspersönlichkeit haben muss und dass somit die Begriffe „Niederlassung" und „Kontrolle" in keinem eindeutigen Verhältnis zueinander stehen. Der für die Verarbeitung Verantwortliche kann mehrere Niederlassungen besitzen, und gemeinsam für die Verarbeitung Verantwortliche können ihre Tätigkeiten auf eine Niederlassung konzentrieren oder auf mehrere Niederlassungen verteilen. Für eine Niederlassung im Sinne der Richtlinie ist die effektive und tatsächliche Ausübung einer Tätigkeit entscheidend, in deren Rahmen personenbezogene Daten verarbeitet werden.

a) „Niederlassung […], die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt"

Der Begriff der Niederlassung ist in der Richtlinie nicht definiert. In Erwägungsgrund 19 der Richtlinie heißt es jedoch: *„Eine Niederlassung im Hoheitsgebiet eines Mitgliedstaats setzt die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus. Die Rechtsform einer solchen Niederlassung, die eine Agentur oder eine Zweigstelle sein kann, ist in dieser Hinsicht nicht maßgeblich.*"

Zur Niederlassungsfreiheit nach Artikel 49 AEUV (ex-Artikel 43 EGV) hat der Gerichtshof der Europäischen Union (EuGH) festgestellt, dass eine feste Niederlassung *„ein ständiges Zusammenwirken von persönlichen und Sachmitteln voraussetzt, die für die Erbringung der betreffenden Dienstleistungen erforderlich sind"*[18].

Der deutliche Hinweis in den Erwägungsgründen der Richtlinie auf die *„effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung"* nimmt eindeutig auf die vom EuGH zum Zeitpunkt des Erlasses der Richtlinie angeführte *„feste Niederlassung"* Bezug. Ob sich diese und nachfolgende Auslegungen des EuGH zur Niederlassungsfreiheit gemäß Artikel 49 ff. AEUV uneingeschränkt auf Sachverhalte anwenden lassen, die unter Artikel 4 der Datenschutzrichtlinie fallen, ist zwar nicht ganz

---

17 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" (WP 169).

18 EuGH, Urteil vom 4. Juli 1985, *Bergholz*, (Rs. 168/84, Slg. 1985, 2251, Rdnr. 14 ff.) und Urteil vom 7. May 1998, *Lease Plan Luxembourg / Belgische Staat* (Rs. C-390/96, Slg. 1998, I-2553). Im letzteren Fall ging es darum, ob ein Server, der sich in einem anderen Land befindet als der Dienstleistungserbringer, als feste Niederlassung anzusehen ist. Von der Beantwortung dieser Frage hing es ab, in welchem Land die Mehrwertsteuer zu entrichten war. Das Gericht lehnte es ab, Computereinrichtungen als virtuelle Niederlassung anzusehen - und kehrte damit zu einem „klassischeren" Niederlassungsbegriff zurück als dem in einem früheren Urteil vom 17. Juli 1997, *ARO Lease / Inspecteur der Belastingdienst Grote Ondernemingen te Amsterdam* (Rs. C-190/95, Slg. 1997, I-4383).

geklärt, aber die Auslegung des Gerichtshofs in den betreffenden Fällen kann bei der Analyse des Wortlauts der Richtlinie nützliche Anhaltspunkte liefern.

Diese Auslegung wird in den folgenden Beispielen herangezogen:

- Wenn beispielsweise die „effektive und tatsächliche Ausübung der Tätigkeit" in einer Staatsanwaltschaft als „feste Einrichtung" erfolgt, würde diese Staatsanwaltschaft als Niederlassung gelten.

- Ein Server oder Computer dürfte kaum als Niederlassung in Frage kommen, da es sich lediglich um eine technische Einrichtung oder ein Instrument für die Verarbeitung von Informationen handelt[19].

- Ein nur mit einer Person besetztes Büro würde von der Definition erfasst, solange es sich nicht bloß um die Vertretung eines für die Verarbeitung Verantwortlichen handelt, der an einem anderen Ort niedergelassen ist, und das Büro aktiv in Tätigkeiten einbezogen ist, in deren Rahmen personenbezogene Daten verarbeitet werden.

- Die Form des „Büros" ist nicht entscheidend: Auch ein einfacher Bevollmächtigter kann als feste Niederlassung gelten, wenn seine Präsenz in dem betreffenden Mitgliedstaat hinreichend stabil ist.

Beispiel 1: Publikation für Reisende

Ein in Mitgliedstaat A niedergelassenes Unternehmen erhebt Daten über die Leistungen von Tankstellen in Mitgliedstaat B, um eine Publikation für Reisende zu erstellen. Die Daten werden von einem Angestellten erhoben, der durch B reist und dabei Fotos und Kommentare an seinen Auftraggeber in A übermittelt. In diesem Fall werden die Daten in B erhoben (ohne dass es in B eine „Niederlassung" gibt) und im Rahmen der Tätigkeiten der Niederlassung in A verarbeitet: Anwendbar ist das Recht von Mitgliedstaat A.

Artikel 4 Absatz 1 Buchstabe a, in dem auf *eine* Niederlassung des *für die Verarbeitung Verantwortlichen* im Hoheitsgebiet des *Mitgliedstaats* Bezug genommen wird, wirft (abgesehen von dem Begriff „Niederlassung") mehrere Fragen auf, die einer Klärung bedürfen.

So bedeutet zum einen die Bezugnahme auf „eine" Niederlassung, dass sich das anwendbare Recht nach dem Mitgliedstaat bestimmt, in dem der für die Verarbeitung Verantwortliche eine Niederlassung besitzt; besitzt der Verantwortliche auch Niederlassungen in anderen Mitgliedstaaten, kann auch das Recht dieser Mitgliedstaaten zur Anwendung berufen werden.

Auch wenn sich die Hauptniederlassung dieser Person in einem Drittstaat befindet, kann allein aufgrund der Existenz einer Niederlassung in einem Mitgliedstaat das Recht dieses Mitgliedstaats zur Anwendung berufen werden, wenn die übrigen Voraussetzungen von Artikel 4 Absatz 1 Buchstabe a gegeben sind (siehe die nachstehenden Ausführungen zu Buchstabe b). Dies wird auch durch den zweiten Teil der Bestimmung bestätigt, der

[19] Ob eine andere Einstufung - z.B. als „Mittel" - in Frage kommt, wird an anderer Stelle in dieser Stellungnahme erörtert.

ausdrücklich vorsieht, dass der für die Verarbeitung Verantwortliche bei Niederlassungen in mehreren Mitgliedstaaten dafür sorgen muss, dass jede Niederlassung dem jeweils anwendbaren einzelstaatlichen Recht nachkommt.

b) Verarbeitungen personenbezogener Daten, die „im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden“

Die Richtlinie knüpft die Anwendbarkeit des mitgliedstaatlichen Datenschutzrechts an die Verarbeitung personenbezogener Daten. Auf den Begriff „Verarbeitung“ ist die Datenschutzgruppe bereits in anderen Stellungnahmen kurz eingegangen, in denen ausgeführt wurde, dass verschiedene Verarbeitungsvorgänge oder Vorgangsreihen gleichzeitig oder in verschiedenen Phasen bzw. Stadien durchgeführt werden können[20]. Im Zusammenhang mit der Bestimmung des anwendbaren Rechts kann dies durchaus bedeuten, dass je nach Verarbeitungsphase unterschiedliche nationale Rechtsordnungen zur Anwendung berufen werden.

Da somit die Gefahr einer Vervielfältigung des anwendbaren Rechts besteht, sollte überlegt werden, inwieweit es möglich ist, die verschiedenen Verarbeitungstätigkeiten auf einer übergeordneten Ebene miteinander zu verknüpfen, um so nur ein einziges nationales Recht zur Anwendung zu berufen. Um bestimmen zu können, ob eine oder mehrere Rechtsordnungen in den verschiedenen Verarbeitungsphasen zur Anwendung gelangen, gilt es sich ein Gesamtbild von den Verarbeitungsvorgängen zu machen: Eine Reihe von Verarbeitungsvorgängen, die in mehreren Mitgliedstaaten stattfinden, aber einem einzigen Zweck dienen, können durchaus in die Anwendung nur eines nationalen Datenschutzrechts münden.

In diesem Fall ist nicht der Standort der Daten, sondern der „Rahmen der Tätigkeiten“ der für die Bestimmung des anwendbaren Rechts ausschlaggebende Faktor.

Der Begriff „Rahmen der Tätigkeiten“ bedeutet, dass das nicht Recht des Mitgliedstaats zur Anwendung gelangt, in dem der *für die Verarbeitung Verantwortliche* niedergelassen ist, sondern das Recht des Mitgliedstaats, in dem eine *Niederlassung* des für die Verarbeitung Verantwortlichen an Tätigkeiten beteiligt ist, die mit der Datenverarbeitung im Zusammenhang stehen.

Anhand verschiedener Fallbeispiele lässt sich besser nachvollziehen, was mit dem Begriff „Rahmen der Tätigkeiten“ gemeint ist und wie dieser Begriff die Bestimmung des auf die einzelnen Verarbeitungsvorgänge in verschiedenen Ländern anzuwendenden Rechts beeinflusst.

a. Ein für die Verarbeitung Verantwortlicher besitzt eine Niederlassung in Österreich und verarbeitet dort personenbezogene Daten im Rahmen der Tätigkeiten dieser Niederlassung. In diesem Fall gilt eindeutig österreichisches Recht, d.h. das Recht des Landes, in dem sich die Niederlassung befindet.

b. Der für die Verarbeitung Verantwortliche besitzt eine Niederlassung in Österreich und verarbeitet im Rahmen der Tätigkeiten dieser Niederlassung personenbezogene Daten, die er über seine Website erhoben hat. Die Website ist für Nutzer in verschiedenen Ländern zugänglich. Auch in diesem Fall gilt österreichisches

[20] Vgl. u.a. Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ (WP 169).

Datenschutzrecht, d.h. das Recht des Landes, in dem sich die Niederlassung befindet. Der Ort, an dem sich die Nutzer und die Daten befinden, ist unerheblich.

c. Der für die Verarbeitung Verantwortliche ist in Österreich niedergelassen und beauftragt einen Auftragsverarbeiter in Deutschland mit der Verarbeitung der Daten. Die Datenverarbeitung in Deutschland erfolgt im Rahmen der Tätigkeiten des für die Verarbeitung Verantwortlichen in Österreich. Mit anderen Worten: Die Datenverarbeitung wird für die geschäftlichen Zwecke der österreichischen Niederlassung und nach deren Anweisungen ausgeführt. Die vom Auftragsverarbeiter in Deutschland erledigte Datenverarbeitung unterliegt österreichischem Recht. Darüber hinaus unterliegt der Auftragsverarbeiter in Bezug auf die Sicherheitsmaßnahmen, die er im Zusammenhang mit der Datenverarbeitung treffen muss, den Anforderungen des deutschen Rechts[21]. Wird die Datenverarbeitung in dieser Weise ausgeführt, ist eine zwischen den deutschen und österreichischen Datenschutzbehörden abgesprochene Kontrolle erforderlich.

d. Der für die Verarbeitung Verantwortliche mit Sitz in Österreich eröffnet eine Vertretung in Italien, die die italienischen Inhalte der Website betreut und Anfragen der italienischen Nutzer bearbeitet. Die von der italienischen Vertretung ausgeführte Datenverarbeitung erfolgt im Rahmen der Tätigkeiten der italienischen Niederlassung, so dass italienisches Recht anzuwenden ist.

Eine Aussage zum anwendbaren Recht ist nur möglich, wenn klar ist, was genau unter dem Begriff „im Rahmen der Tätigkeiten“ der Niederlassung zu verstehen ist. Die nachstehenden Überlegungen sollten in diese Analyse einbezogen werden:

Es kommt entscheidend darauf an, in welchem Maß die Niederlassung(en) an den Tätigkeiten, in deren Rahmen personenbezogenen Daten verarbeitet werden, beteiligt ist bzw. sind. Um feststellen zu können, ob die Niederlassung als Anknüpfungspunkt für die Anwendung des nationalen Datenschutzrechts geeignet ist, gilt es also zu prüfen, welche Tätigkeiten von welcher Niederlassung ausgeführt werden (Wer macht was?). Verarbeitet eine Niederlassung personenbezogene Daten im Rahmen ihrer eigenen Tätigkeiten, ist das Recht des Mitgliedstaats maßgebend, in dem sich die Niederlassung befindet. Verarbeitet die Niederlassung personenbezogene Daten im Rahmen der Tätigkeiten einer anderen Niederlassung, ist das Recht des Mitgliedstaats maßgebend, in dem sich die andere Niederlassung befindet.

Die Frage, welcher Art die Tätigkeiten der Niederlassungen sind, ist eigentlich zweitrangig, hilft aber bei der Ermittlung des auf die jeweilige Niederlassung anwendbaren Rechts: Ob eine Tätigkeit eine Datenverarbeitung mit sich bringt und welche Verarbeitung im Rahmen welcher Tätigkeit erfolgt, hängt weitgehend von der Art der Tätigkeit ab. Ebenso wirkt sich die Tatsache, dass unterschiedliche Niederlassungen

[21] Nach Artikel 17 Absatz 3 der Richtlinie 95/46/EG ist der Auftragsverarbeiter im Hinblick auf die Sicherheitsmaßnahmen an die Pflichten gebunden, die sich aus dem Recht des Mitgliedstaats ergeben, in dem der Auftragsverarbeiter niedergelassen ist. Im Falle einer Kollision zwischen den materiellrechtlichen Sicherheitspflichten des Rechts des Auftragsverarbeiters und jenen des Rechts des für die Verarbeitung Verantwortlichen geht das Recht des Auftragsverarbeiters (*lex loci*) vor. Zwar liegt die Haftung letzten Endes bei dem für die Verarbeitung Verantwortlichen, doch muss der Auftragsverarbeiter nachweisen, dass er alle im Vertrag mit dem für die Verarbeitung Verantwortlichen vorgesehenen notwendigen Schritte unternommen hat und den Sicherheitspflichten nachgekommen ist, die im Recht des Mitgliedstaats, in dem der Auftragsverarbeiter niedergelassen ist, vorgeschrieben sind (siehe im Einzelnen III.5).

völlig verschiedenen Tätigkeiten nachgehen können, in deren Rahmen personenbezogene Daten verarbeitet werden, auf das anwendbare Recht aus. Diese Überlegungen werden in Beispiel 4 veranschaulicht.

Auch sollte das Gesamtziel der Richtlinie berücksichtigt werden: die Sicherstellung eines wirksamen Schutzes der Personen auf einfache, machbare und vorhersagbare Weise.

Beispiel 2: Übermittlung personenbezogener Daten in Verbindung mit dem Verkauf von Schuldforderungen

Ein italienisches Stromversorgungsunternehmen übermittelt zwecks Verkauf von Schuldforderungen Informationen über seine Schuldner an eine französische Anlagebank. Die Schulden sind aus nicht bezahlten Stromrechnungen entstanden. Die betreffenden Informationen einschließlich der personenbezogenen Kundendaten werden an die Zweigstelle (d.h. die Niederlassung) der französischen Anlagebank in Italien übermittelt.

Die französische Anlagebank ist in diesem Fall der Verantwortliche für die mit der Datenübermittlung verbundenen Verarbeitungsvorgänge, und ihre italienische Niederlassung nimmt die Schuldenverwaltung und -eintreibung in ihrem Namen vor. Die betreffenden Daten werden von dem für die Verarbeitung Verantwortlichen sowohl in Frankreich als auch in seiner italienischen Niederlassung verarbeitet. Der französische für die Verarbeitung Verantwortliche setzt über seine italienische Niederlassung alle italienischen Kunden über die oben genannten Vorgänge in Kenntnis.

Die italienische Zweigstelle ist eine Niederlassung im Sinne der Richtlinie, und ihre Tätigkeit (Verarbeitung personenbezogener Daten zwecks Unterrichtung der Kunden über die getroffene Vereinbarung) muss daher im Einklang mit den italienischen Datenschutzvorschriften stehen. Auch müssen etwaige Sicherheitsmaßnahmen der italienischen Niederlassung die Bedingungen der italienischen Datenschutzvorschriften erfüllen, während der französische für die Verarbeitung Verantwortliche die französischen Sicherheitsbestimmungen für die in seiner Niederlassung in Frankreich verarbeiteten Daten einzuhalten hat. Die betroffenen Personen (d.h. die Schuldner) können sich an die italienische Niederlassung wenden, um von ihren Datenschutzrechten (bezüglich Zugang, Richtigstellung oder Löschung) nach italienischem Recht Gebrauch zu machen.

Für die Analyse dieser Kriterien bietet sich ein funktioneller Ansatz an: Ausschlaggebende Faktoren sollten nicht so sehr die von den Beteiligten mit Blick auf das anwendbare Recht durchgeführten theoretischen Bewertungen, sondern vielmehr ihr praktisches Vorgehen und ihre Interaktion sein: Welche Rolle haben die einzelnen Niederlassungen konkret, und welche Tätigkeit erfolgt in welcher Niederlassung?

Ferner ist darauf zu achten, in welchem Umfang die einzelne Niederlassung an den Tätigkeiten, in deren Rahmen personenbezogene Daten verarbeitet werden, beteiligt ist. Zu wissen, was unter der Formulierung „im Rahmen von“ zu verstehen ist, ist daher auch in komplexen Fällen nützlich, wenn es um die Zuordnung unterschiedlicher Tätigkeiten verschiedener EU-Niederlassungen eines Unternehmens geht.

Beispiel 3: Erhebung von Kundendaten durch Geschäfte

Eine Kleiderwarenkette mit Hauptsitz in Spanien unterhält Ladenlokale in der gesamten EU. In jedem dieser Geschäfte werden Kundendaten gesammelt und anschließend zum Hauptsitz in Spanien übermittelt, an dem bestimmte Datenverarbeitungsvorgänge erfolgen (Analyse von Kundenprofilen, Kundendienst, Zielgruppenwerbung).

Tätigkeiten wie das direkte Anschreiben der über ganz Europa verteilten Kunden zu Marketingzwecken werden ausschließlich durch den Hauptsitz in Spanien gesteuert. Sie erfolgen somit im Rahmen der Tätigkeiten der spanischen Niederlassung und unterliegen folglich den auf derartige Verarbeitungstätigkeiten anwendbaren spanischen Rechtsvorschriften.

Die einzelnen Geschäfte sind gleichwohl für jene Aspekte der Verarbeitung der personenbezogenen Daten ihrer Kunden verantwortlich, die im Rahmen ihrer eigenen Tätigkeiten erfolgen (beispielsweise die Erhebung personenbezogener Daten ihrer Kunden). Insofern diese Verarbeitung im Rahmen der Tätigkeiten der einzelnen Geschäfte erfolgt, unterliegt sie dem Rechts des Landes, in dem das einzelne Geschäft niedergelassen ist.

Eine unmittelbare praktische Folge hiervon ist, dass jedes Geschäft die erforderlichen Maßnahmen ergreifen muss, um seine einzelnen Kunden über die Bedingungen der Erhebung und Verarbeitung ihrer Daten nach Maßgabe des nationalen Rechts zu informieren.

Kunden, die sich beschweren wollen, können sich direkt an die Datenschutzbehörde ihres Landes wenden. Falls sich die Beschwerde auf die direkten, im Rahmen der Tätigkeiten des spanischen Hauptsitzes erfolgten Vermarktungsmaßnahmen bezieht, muss die örtliche Datenschutzbehörde die Beschwerde an die spanische Datenschutzbehörde weiterleiten.

Denkbar ist somit, dass eine Niederlassung mehreren unterschiedlichen Tätigkeiten nachgeht, und dass auf die im Rahmen dieser unterschiedlichen Tätigkeiten erfolgende Datenverarbeitung Rechtsvorschriften mehrerer Länder anwendbar sind. Um ein vorhersagbares, praktikables Vorgehen in Situationen zu ermöglichen, in denen auf die verschiedenen Tätigkeiten ein und derselben Niederlassung Rechtsvorschriften mehrerer Länder anwendbar sind, sollte ein funktioneller Ansatz verfolgt werden, der insbesondere dem weiteren rechtlichen Kontext Rechnung trägt.

Beispiel 4: zentrale Personaldatenbank

Immer häufiger kommt es in der Praxis vor, dass ein und dieselbe Datenbank Rechtsvorschriften mehrerer Länder unterliegt. Oftmals ist dies auf dem Gebiet der Personalverwaltung der Fall, wenn Tochterunternehmen bzw. Niederlassungen in unterschiedlichen Ländern Personaldaten in einer einzigen zentralen Datenbank erfassen. Gewöhnlich erfolgt diese Maßnahme aus ökonomischen Gründen. Auf die den einzelnen Niederlassungen nach geltendem örtlichem Recht obliegenden Verantwortlichkeiten sollte sie allerdings keine Auswirkungen haben. Dies gilt nicht nur aus datenschutzrechtlicher Perspektive, sondern auch mit Blick auf die Vorschriften des Arbeitsrechts und der öffentlichen Ordnung.

Wenn beispielsweise Daten der Beschäftigten einer irischen Tochterfirma (also einer Niederlassung) zu einer zentralen Datenbank im VK übermittelt werden, in der auch Daten der Beschäftigten der Tochterfirma bzw. Niederlassung im VK gespeichert werden, sind die Datenschutzvorschriften zweier Länder (nämlich Irlands und des VK) anwendbar.

Dass die Rechtsvorschriften zweier verschiedener Länder zur Anwendung gelangen, ist keineswegs als simple Folge der Tatsache zu sehen, dass die betreffenden Daten aus zwei verschiedenen Ländern stammen. Ursache ist vielmehr der Umstand, dass die Verarbeitung der irischen Personaldaten durch die Niederlassung im VK im Rahmen der Tätigkeiten erfolgt, denen die irische Niederlassung in ihrer Eigenschaft als Arbeitgeber nachkommt.

Dieses Beispiel zeigt, dass für die Frage, welches nationales Recht anwendbar ist, keineswegs der Ort, an den die Daten übermittelt werden bzw. an dem sich die Daten befinden, ausschlaggebend ist. Die entscheidenden Faktoren sind vielmehr die Art und der Ort der normalen Tätigkeiten, die den „Rahmen" für die Datenverarbeitung bilden. Personal- oder Kundendaten unterliegen somit normalerweise dem Datenschutzrecht desjenigen Landes, in dem die Tätigkeit, in deren Rahmen die Daten verarbeitet werden, erfolgt. Hier bestätigt sich zudem, dass sich der Geltungsbereich des nationalen Rechts keineswegs mit der territorialen Zuständigkeit der nationalen Gerichte deckt, denn eben dieses nationale Recht kann ja auch außerhalb der territorialen Gerichtshoheit gelten.

Zusammenfassend lässt sich also sagen, dass die für die Bestimmung des anwendbaren Rechts verwendeten Kriterien in mehrfacher Hinsicht von maßgeblicher Bedeutung sind:

- Sie helfen bei der Klärung der Frage, ob die Datenschutzvorschriften der EU überhaupt auf die betreffende Datenverarbeitung anwendbar sind;

- In den Fällen, in denen die Datenschutzvorschriften der EU anwendbar sind, lässt sich bezüglich der einzelnen Mitgliedstaaten anhand der Kriterien bestimmen,
  a) wessen Datenschutzvorschriften anwendbar sind, bzw.
  b) wessen Datenschutzvorschriften auf welche Datenverarbeitungstätigkeit anwendbar sind (falls es mehrere Niederlassungen in verschiedenen Mitgliedstaaten gibt);

- Die Kriterien sind in allen Fällen hilfreich, in denen es eine außereuropäische Dimension der Verarbeitungstätigkeiten gibt (siehe das nachfolgende Beispiel, bei dem der für die Verarbeitung Verantwortliche außerhalb des EWR niedergelassen ist).

Beispiel 5: Internetdienstanbieter

Ein Internetdienstanbieter (der für die Verarbeitung Verantwortliche) hat seinen Sitz außerhalb der EU, beispielsweise in Japan. Er unterhält Geschäftsstellen in den meisten Mitgliedstaaten der EU sowie ein Büro in Irland, das mit Tätigkeiten befasst ist, die mit der Verarbeitung personenbezogener Daten verbunden sind (u.a. die IT-Unterstützung). Der für die Verarbeitung Verantwortliche errichtet in Ungarn ein Datenzentrum, dessen Angestellte und Server Daten der Nutzer der von ihm erbrachten Dienstleistungen verarbeiten und speichern.

Der für die Verarbeitung Verantwortliche in Japan besitzt weitere Niederlassungen in verschiedenen Mitgliedstaaten der EU, die mit unterschiedlichen Tätigkeiten befasst sind:

- Das Datenzentrum in Ungarn ist ausschließlich für die technische Instandhaltung zuständig;

- Die Geschäftsstellen des Internetdienstanbieters führen allgemeine Werbekampagnen durch;

- Das Büro in Irland ist (abgesehen von den Datenübermittlungen vom Sitz der japanischen Hauptgeschäftsstelle) die einzige Niederlassung in der EU, die Tätigkeiten nachgeht, in deren Rahmen personenbezogene Daten verarbeitet werden.

Die Tätigkeiten des Büros in Irland lösen die Anwendung des EU-Datenschutzrechts aus: Da im Rahmen seiner Tätigkeiten personenbezogene Daten verarbeitet werden, unterliegt diese Datenverarbeitung den Datenschutzvorschriften der EU.

Maßgeblich für die im Rahmen der Tätigkeiten des Büros in Irland erfolgende Datenverarbeitung sind allein die irischen Datenschutzvorschriften. Ob die Verarbeitung konkret in Portugal, Italien oder einem anderen Mitgliedstaat erfolgt, ist dabei unerheblich.

In diesem hypothetischen Beispiel wären also für die in dem Datenzentrum in Ungarn erfolgende Verarbeitung der personenbezogenen Daten der Nutzer des Internetdienstanbieters die irischen Datenschutzvorschriften maßgeblich. Unbeschadet davon wären jedoch die ungarischen Datenschutzvorschriften auf jede von dem ungarischen Datenzentrum im Rahmen seiner eigenen Tätigkeiten vorgenommene Verarbeitung personenbezogener Daten anwendbar (also beispielsweise auf die Verarbeitung personenbezogener Daten von Angestellten des Datenzentrums).

Für die Geschäftsstellen in den anderen Mitgliedstaaten gilt, dass sie nicht den Datenschutzvorschriften der EU unterliegen, solange ihre Tätigkeit auf allgemeine, nicht nutzerspezifische Werbekampagnen begrenzt ist, bei denen ja keine personenbezogenen Daten verarbeitet werden. Falls die Geschäftsstellen jedoch beschließen, im Rahmen ihrer Tätigkeiten personenbezogene Daten von Einzelpersonen in dem Land, in dem sie niedergelassen sind, zu bearbeiten (beispielsweise um für ihre eigenen geschäftlichen Zwecke gezielte Werbesendungen an bestehende und an möglich künftige Nutzer zu verschicken), müssen sie sich an die örtlichen Datenschutzvorschriften halten.

Auch wenn sich kein Zusammenhang zwischen der Datenverarbeitung und der Niederlassung in Irland herstellen lässt (weil die IT-Unterstützung sehr begrenzt ist und keine personenbezogenen Daten verarbeitet werden), können andere Bestimmungen der Datenschutzrichtlinie die Anwendung von Datenschutzgrundsätzen auslösen - beispielsweise, wenn der für die Verarbeitung Verantwortliche „Mittel“ in der EU verwendet. Dieser Fall wird in Kapitel III.3 näher behandelt.

III.2. Für die Verarbeitung Verantwortlicher mit einer Niederlassung an einem Ort, an dem das einzelstaatliche Recht des betreffenden Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet (Artikel 4 Absatz 1 Buchstabe b)

Artikel 4 Absatz 1 Buchstabe b regelt den weniger häufigen Fall, dass die Datenschutzvorschriften eines Mitgliedstaats auf einen für die Verarbeitung Verantwortlichen anwendbar sind, der nicht in seinem Hoheitsgebiet, sondern an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet.

III.2.a) Der für die Verarbeitung Verantwortliche ist nicht im Hoheitsgebiet des Mitgliedstaates niedergelassen, …

Diese erste Bedingung sollte aus Gründen der Konsistenz von Artikel 4 Absatz 1 dahingehend ausgelegt werden, dass der für die Verarbeitung Verantwortliche keine Niederlassung im Hoheitsgebiet des Mitgliedstaates besitzt, die die Anwendbarkeit von Artikel 4 Absatz 1 Buchstabe a nach sich zieht (siehe auch III.3.a). Mit anderen Worten: Wenn keine relevante Niederlassung in der EU existiert, lässt sich nach Artikel 4 Absatz 1 Buchstabe a kein anwendbares nationales Datenschutzrecht ermitteln.

III.2.b) … aber an einem Ort, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet.

In bestimmten Situationen können gleichwohl externe, auf dem internationalen öffentlichen Recht fußende Kriterien bestimmen, dass die Anwendung eines nationalen Datenschutzrechts über die Landesgrenzen des betreffenden Mitgliedstaates hinaus ausgeweitet wird. Möglich ist dies beispielsweise, wenn das internationale öffentliche Recht oder internationale Abkommen das in einer Botschaft oder in einem Konsulat anwendbare Recht oder das auf ein Schiff oder ein Flugzeug anwendbare Recht bestimmen. Falls der für die Verarbeitung Verantwortliche an einem dieser Orte niedergelassen ist, wird das anwendbare nationale Datenschutzrecht durch das internationale Recht bestimmt.

Gleichwohl sei darauf hingewiesen, dass das nationale Datenschutzrecht möglicherweise nicht für Auslandsmissionen oder internationale Organisationen im Hoheitsgebiet der EU gilt, die einen durch ein allgemeines Abkommen oder ein sogenanntes *Headquarter Agreement* geregelten Sonderstatus nach internationalem Recht besitzen: Eine derartige Ausnahme würde die Anwendung von Artikel 4 Absatz 1 Buchstabe a auf die betreffende Mission bzw. internationale Organisation verhindern.

Beispiel 6: ausländische Botschaften

Eine Botschaft eines EU-Mitgliedstaats in Kanada unterliegt dem Datenschutzrecht des betreffenden Mitgliedstaats, nicht dem kanadischen Datenschutzrecht.

Ausländische Botschaften in den Niederlanden unterliegen nicht dem niederländischen Datenschutzrecht, da sie einen Sonderstatus nach internationalem Recht besitzen. Ein im Rahmen der Tätigkeiten einer ausländischen Botschaft begangener Verstoß gegen die Datensicherheit würde daher nicht die Anwendung des niederländischen Datenschutzrechts und entsprechende Durchsetzungsmaßnahmen nach sich ziehen.

Für eine nichtstaatliche Einrichtung mit Büros in verschiedenen EU-Mitgliedstaaten würde im Prinzip keine solche Ausnahme gelten, es sei denn, diese wäre in einem internationalen Abkommen mit dem Gastland ausdrücklich vorgesehen.

III.3. Der für die Verarbeitung Verantwortliche ist nicht im Gebiet der Gemeinschaft niedergelassen, greift aber zum Zwecke der Verarbeitung personenbezogener Daten auf im Hoheitsgebiet eines Mitgliedstaats belegene Mittel zurück (Artikel 4 Absatz 1 Buchstabe c)

Artikel 4 Absatz 1 Buchstabe c stellt darauf ab, dass das in der EU-Richtlinie verankerte Recht auf den Schutz personenbezogener Daten auch dann sichergestellt ist, wenn der für die Verarbeitung Verantwortliche nicht im Hoheitsgebiet der EU bzw. des EWR niedergelassen ist, aber – wie im Erwägungsgrund 20[22] erwähnt – zwischen der Verarbeitung personenbezogener Daten und diesem Hoheitsgebiet eine klare Verbindung besteht.

Konkret sieht Artikel 4 Absatz 1 Buchstabe c vor, dass jeder Mitgliedstaat die Vorschriften, die er zur Umsetzung der Datenschutzrichtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten anwendet, *„die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden. "*

Besonders relevant ist diese Bestimmung im Lichte der Entwicklung neuer Technologien wie dem Internet, durch die es zunehmend einfacher wird, personenbezogene Daten aus der Ferne zu erheben und zu verarbeiten, ohne dass der für die Verarbeitung Verantwortliche überhaupt im Hoheitsgebiet der EU bzw. des EWR körperlich anwesend sein muss[23].

> a) Der für die Verarbeitung Verantwortliche ist nicht im Gebiet der Gemeinschaft niedergelassen, …

Diese Bestimmung greift, wenn der für die Verarbeitung Verantwortliche im Hoheitsgebiet der EU bzw. des EWR keine Präsenz hat, die als Niederlassung im Sinne von Artikel 4 Absatz 1 Buchstabe a der Richtlinie (siehe oben) angesehen werden kann.

Es ist wichtig, zu klären, wie die Formulierung „ist nicht niedergelassen" auszulegen ist. Es liegt auf der Hand, dass Artikel 4 Absatz 1 Buchstabe c nur anwendbar ist, wenn Artikel 4 Absatz 1 Buchstabe a nicht anwendbar ist, sprich: wenn der für die Verarbeitung Verantwortliche in der EU bzw. im EWR keine Niederlassung hat, *die für*

---

22 *„Die Niederlassung des für die Verarbeitung Verantwortlichen in einem Drittland darf dem Schutz der Personen gemäß dieser Richtlinie nicht entgegenstehen. In diesem Fall sind die Verarbeitungen dem Recht des Mitgliedstaats zu unterwerfen, in dem sich die für die betreffenden Verarbeitungen verwendeten Mittel befinden, und Vorkehrungen zu treffen, um sicherzustellen, dass die in dieser Richtlinie vorgesehenen Rechte und Pflichten tatsächlich eingehalten werden."*

23 Siehe hierzu das von der Datenschutzgruppe vorgelegte Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU (WP 56).

die fraglichen Tätigkeiten relevant ist. Die Tatsache, dass ein für die Verarbeitung Verantwortlicher, der außerhalb der EU bzw. des EWR niedergelassen ist, im Mitgliedstaat A, in dem er keine Niederlassung hat, Mittel verwendet, kann folglich nicht die Anwendbarkeit des Rechts dieses Mitgliedstaats auslösen, falls der für die Verarbeitung Verantwortliche bereits eine Niederlassung im Mitgliedstaat B hat und die personenbezogenen Daten im Rahmen der Tätigkeiten dieser Niederlassung verarbeitet. Sowohl die Verarbeitung im Mitgliedstaat A (in dem Mittel verwendet werden) als auch die Verarbeitung im Mitgliedstaat B (in dem sich die Niederlassung befindet) unterliegen in diesem Fall dem Recht von Mitgliedstaat B. Dies hat die Datenschutzgruppe in ihrer Stellungnahme zu Datenschutzfragen im Zusammenhang mit Suchmaschinen[24] klargestellt.

Andererseits ist Artikel 4 Absatz 1 Buchstabe c anwendbar, wenn der für die Verarbeitung Verantwortliche eine „nicht relevante" Niederlassung in der EU hat. Gemeint ist, dass der für die Verarbeitung Verantwortliche zwar Niederlassungen in der EU hat, deren Tätigkeiten aber *in keinem Zusammenhang mit der Verarbeitung personenbezogener Daten stehen*. Die Existenz derartiger Niederlassungen kann daher nicht die Anwendung von Artikel 4 Absatz 1 Buchstabe a auslösen.

Da es ja keine Rechtslücken oder Inkonsistenzen bei der Anwendung der Richtlinie geben soll, bedeutet dies, dass die Anwendung des „equipment"-Kriteriums durch die Existenz einer nicht relevanten Niederlassung nicht zwangsläufig verhindert werden muss: Verhindert wird sie nur, wenn die betreffende Niederlassung im Rahmen derselben Tätigkeiten personenbezogene Daten verarbeitet.

Daraus folgt wiederum, dass ein Unternehmen mit unterschiedlichen Tätigkeiten die Anwendung sowohl von Artikel 4 Absatz 1 Buchstabe a als auch von Artikel 4 Absatz 1 Buchstabe c auslösen kann, wenn es Mittel verwendet und Niederlassungen in unterschiedlichen Kontexten hat. Anders ausgedrückt: Ein für die Verarbeitung Verantwortlicher, der außerhalb der EU bzw. des EWR niedergelassen ist und Mittel in der EU verwendet, muss die Bestimmungen von Artikel 4 Absatz 1 Buchstabe c auch dann einhalten, wenn er eine Niederlassung in der EU hat, die *im Rahmen anderer Tätigkeiten* personenbezogene Daten verarbeitet. Die Existenz dieser Niederlassung löst die Anwendung von Artikel 4 Absatz 1 Buchstabe a auf diese spezifischen Tätigkeiten aus.

Bei der Überarbeitung des Datenschutzrahmens wird sich vielleicht Gelegenheit bieten, den Geltungsbereich von Artikel 4 Absatz 1 Buchstabe c im Geiste der Richtlinie und insbesondere von Erwägungsgrund 20 näher zu klären und zu präzisieren, was mit der Formulierung „der für die Verarbeitung Verantwortliche ist nicht im Hoheitsgebiet der Gemeinschaft niedergelassen" gemeint ist. In der Präambel der Richtlinie wird klar gesagt, dass die Richtlinie auf den Schutz der Personen abstellt und Lücken in der Anwendung ihrer Grundsätze vermieden werden sollen. Daher ist die Datenschutzgruppe der Auffassung, dass Artikel 4 Absatz 1 Buchstabe c auch für jene Fälle gelten sollte, in denen keine Niederlassung in der EU bzw. im EWR existiert, *die die Anwendung von Artikel 4 Absatz 1 Buchstabe a auslöst* oder in denen die Verarbeitung *nicht im Rahmen der Tätigkeiten* einer solchen Niederlassung erfolgt.

[24] Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148).

b) … und greift zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurück, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind …

Der entscheidende Faktor, der die Anwendbarkeit dieses Artikels und somit des Datenschutzrechts eines Mitgliedstaats bestimmt, ist die Verwendung von im Hoheitsgebiet des Mitgliedstaats belegenen Mitteln.

Die Datenschutzgruppe hat bereits klargestellt, dass der Begriff „Verwendung" zwei Aspekte beinhaltet: eine Tätigkeit des für die Verarbeitung Verantwortlichen und dessen klare Absicht, personenbezogene Daten zu verarbeiten[25]. Somit führt zwar nicht jede Verwendung von Mitteln in der EU bzw. im EWR zur Anwendung der Richtlinie, aber damit die Verarbeitung in den Anwendungsbereich der Richtlinie fällt, ist es auch nicht erforderlich, dass der für die Verarbeitung Verantwortliche die für die Verarbeitung verwendeten Mittel besitzt oder volle Kontrolle über sie hat.

Ferner ist darauf hinzuweisen, dass ein Unterschied zwischen dem in Artikel 4 Absatz 1 Buchstabe c des englischen Originals der Richtlinie verwendeten Begriff „equipment" und den in den anderen Sprachfassungen der Richtlinie verwendeten Begriffen besteht, die mehr dem in der deutschen Sprachfassung verwendeten Begriff „Mittel" entsprechen. Die in den anderen Sprachfassungen verwendete Terminologie entspricht also mehr dem in Artikel 2 Buchstabe d des englischen Originals verwendeten Begriff „means".

Angesichts dessen versteht die Datenschutzgruppe den Begriff „equipment" als „means"[26]. Sie nimmt ferner zur Kenntnis, dass es sich laut der Richtlinie dabei um „automatisierte oder nicht automatisierte" Mittel handelt.

Dies wiederum führt dazu, dass dieses Kriterium weit ausgelegt wird, nämlich dahingehend, dass auch Mittler und/oder technische Mittel (wie sie beispielsweise bei Erhebungen bzw. Umfragen oder bei Informationsanfragen eingesetzt werden) eingeschlossen sind. Das Kriterium gilt somit auch für mittels Fragebögen durchgeführte Datenerhebungen (beispielsweise im Rahmen pharmazeutischer Studien).

Gleichwohl stellt sich die Frage, ob ausgelagerte Tätigkeiten (insbesondere von Auftragsverarbeitern), die im Hoheitsgebiet der EU bzw. des EWR im Namen eines für die Verarbeitung Verantwortlichen durchgeführt werden, als „Mittel" betrachtet werden können. Nach der oben genannten weiten Auslegung ist dies zu bejahen, sofern die Verarbeitung nicht im Rahmen der Tätigkeiten einer Niederlassung des für die Verarbeitung Verantwortlichen im EWR erfolgt (was die Anwendung von Artikel 4 Absatz 1 Buchstabe a auslösen würde). Hierbei sollte allerdings berücksichtigt werden, welche unerwünschten Folgen eine solche Auslegung bisweilen mit sich bringen kann (siehe III.4): Für die Verarbeitung Verantwortliche, die in verschiedenen Ländern der Welt niedergelassen sind und ihre Daten in einem Mitgliedstaat der EU verarbeiten lassen, in dem die betreffende Datenbank und der Auftragsverarbeiter belegen sind, unterliegen dem Datenschutzrecht dieses Mitgliedstaats.

---

25 WP56, op. cit.

26 In diesem Zusammenhang sei daran erinnert, dass in den vorhergehenden englischsprachigen Fassungen der Richtlinie, beispielsweise in dem geänderten Vorschlag KOM (92) 422 endg. aus dem Jahr 1992, ebenfalls der Begriff „means" verwendet wurde. Dieser wurde, wie aus dem gemeinsamen Standpunkt vom März 1995 ersichtlich ist, in den anschließenden Verhandlungen - also erst in einem späten Stadium - durch „equipment" ersetzt.

Folglich bedarf es jeweils einer einzelfallspezifischen Bewertung, bei der analysiert wird, wie das betreffende Mittel konkret dazu verwendet wird, personenbezogene Daten einzuholen und zu verarbeiten. Die Datenschutzgruppe hat auf der Grundlage dieser Überlegungen anerkannt, dass eine mittels Zugriff auf die Computer von Nutzern erfolgende Erhebung personenbezogener Daten (beispielsweise durch Cookies oder Javascript-Banner) die Anwendung von Artikel 4 Absatz 1 Buchstabe c der Richtlinie (und somit des EU-Datenschutzrechts) auf in Drittstaaten niedergelassene Internetdienstanbieter auslösen kann[27].

Diese Auslegung der Bestimmung über die „Verwendung von Mitteln" bringt einen weiten Anwendungsbereich mit sich. Sie kann, wie bereits erwähnt, allerdings auch die nicht zufriedenstellende Folge haben, dass das Datenschutzrecht der EU auch in Fällen anwendbar ist, in denen nur eine begrenzte Verbindung zur EU besteht (beispielsweise wenn ein für die Verarbeitung Verantwortlicher, der außerhalb der EU niedergelassen ist, ausschließlich mit in der EU belassenen Mitteln Daten von Nicht-EU-Bürgern verarbeitet). Hier bedarf es ganz offensichtlich größerer Klarheit und weiterer Bedingungen für die Anwendung dieses Kriteriums, um den künftigen Datenschutzrahmen noch zuverlässiger zu machen. Auf diesen Punkt wird in den Schlussfolgerungen dieser Stellungnahme näher eingegangen.

Ebenso ist, um ein weiteres Beispiel zu nennen, nicht klar, inwieweit Telekommunikationsendgeräte oder Teile solcher Geräte als „Mittel" anzusehen sind. Die Tatsache, dass ein derartiges Gerät dafür ausgelegt ist oder überwiegend dazu verwendet wird, personenbezogene Daten zu sammeln oder weiter zu verarbeiten, kann diesbezüglich als Indikator betrachtet werden. Jedenfalls wird die Anwendung der Richtlinie auch dann ausgelöst, wenn ein für die Verarbeitung Verantwortlicher wissentlich durch Verwendung derartiger Mittel in der EU personenbezogene Daten zusammenträgt, sei es auch nur beiläufig.

Beispiel 7: Geolocation-Dienste

Ein in Neuseeland niedergelassenes Unternehmen setzt weltweit (d.h. auch in Mitgliedstaaten der EU) Pkw dazu ein, Informationen über Funkzugangspunkte (WAP), die auch Daten über private Endgeräte von Einzelpersonen einschließen, zu sammeln, um seinen Kunden einen Geolocation-Dienst anzubieten. Diese Tätigkeit bringt in vielen Fällen eine Verarbeitung personenbezogener Daten mit sich.

Die Anwendung der Datenschutzrichtlinie wird in diesem Fall auf zweifache Weise ausgelöst:

- zum einen durch die Tatsache, dass die Pkw, mit denen die Informationen beim Durchfahren der Straßen eingeholt werden, als Mittel im Sinne von Artikel 4 Absatz 1 Buchstabe c betrachten werden können;
- zum anderen durch den Umstand, dass der für die Verarbeitung Verantwortliche bei der Erbringung des Geolocation-Dienstes gegenüber einzelnen Personen auf die betreffenden mobilen Geräte dieser Personen zurückgreift (und zwar durch speziell für diesen Zweck in den Geräten installierte Software), d.h. sie als Mittel für die Übermittlung von konkreten Informationen über den Standort der Geräte und ihrer Nutzer verwendet.

[27] WP56, op. cit., S. 10 f.

Sowohl die zur Erbringung dieser Dienstleistung dienende Erhebung der Informationen als auch die Erbringung des Geolocation-Dienstes an sich muss im Einklang mit den Bestimmungen der Richtlinie stehen.

Beispiel 8: *Cloud computing*

Ein besonders komplexes Beispiel für die Anwendung der Datenschutzrichtlinie ist das *Cloud computing*, denn dabei werden personenbezogene Daten an unterschiedlichen Orten in der ganzen Welt auf Servern verarbeitet und gespeichert. Wo genau sich die Daten jeweils befinden, ist nicht immer bekannt, auch kann der Ort mit der Zeit wechseln. Für die Ermittlung des anwendbaren Rechts ist dies allerdings nicht entscheidend. Für die Auslösung der Anwendung des EU-Rechts nach Maßgabe von Artikel 4 Absatz 1 Buchstabe c der Richtlinie reicht es schon aus, wenn der für die Verarbeitung Verantwortliche im Rahmen der Tätigkeiten einer in der EU belegenen Niederlassung personenbezogene Daten verarbeitet oder wenn die für die Verarbeitung verwendeten Mittel im Hoheitsgebiet der EU belegen sind.

In derartigen Fällen gilt es zunächst den für die Verarbeitung Verantwortlichen zu ermitteln und festzustellen, welche Tätigkeiten auf welcher Ebene erfolgen. Dabei lassen sich zwei Perspektiven unterscheiden:

Der Nutzer des *Cloud computing* kann ein für die Verarbeitung Verantwortlicher sein, beispielsweise ein Unternehmen, das auf einen Online-Termindienst zurückgreift, um Zusammenkünfte mit seinen Kunden zu organisieren. Falls das Unternehmen diesen Dienst im Rahmen der Tätigkeiten seiner in der EU belegenen Niederlassung nutzt, ist auf diese über den Online-Termindienst erfolgende Datenverarbeitung EU-Recht nach Maßgabe von Artikel 4 Absatz 1 Buchstabe a anwendbar. Das Unternehmen sollte daher sicherstellen, dass der Dienst ausreichende Datenschutzvorkehrungen einschließt, insbesondere zum Schutz der in der „Rechnerwolke" gespeicherten Daten. Außerdem ist es verpflichtet, seine Kunden über den Zweck und die Bedingungen der Verwendung ihrer Daten zu unterrichten.

Unter bestimmten Umständen kann auch ein Anbieter von *Cloud computing* ein für die Verarbeitung Verantwortlicher sein, beispielsweise wenn dieser Dienst einen Online-Terminplan einschließt, in dem Privatpersonen private Termine eintragen können, und zusätzliche Dienstleistungen wie die Termin- und Kontaktsynchronisierung angeboten werden. Falls ein solcher Anbieter von *Cloud Computing* in der EU belegene Mittel verwendet, unterliegt er dem EU-Datenschutzrecht nach Maßgabe von Artikel 4 Absatz 1 Buchstabe c der Richtlinie. Wie weiter unten aufgezeigt wird, wird die Anwendung der Richtlinie nicht ausgelöst, wenn die betreffenden Mittel nur zum Zweck der Durchfuhr verwendet werden, aber sie wird sehr wohl ausgelöst, wenn spezifischere Mittel verwendet werden (beispielsweise wenn im Rahmen des Dienstes auf Computerberechnungen, Java-Skripts oder Cookies zurückgegriffen wird, um personenbezogene Daten von Nutzern zu speichern oder abzufragen). Der Dienstanbieter hat in diesem Fall die Nutzer darüber zu informieren, wie ihre Daten verarbeitet, gespeichert und möglicherweise von Dritten eingesehen werden und muss ausreichende Sicherheitsmaßnahmen zum Schutz der Informationen ergreifen.

Beispiel 9: Ein für die Verarbeitung Verantwortlicher veröffentlicht nach Ländern geordnete Pädophilenlisten

Ein für die Verarbeitung Verantwortlicher, der in einem Mitgliedstaat der EU bzw. des EWR niederlassen ist, veröffentlich nach Ländern geordnete Listen von Personen, die wegen Straftaten mit Minderjährigen verurteilt wurden bzw. derartiger Straftaten verdächtigt werden. Das anwendbare Recht, nach dem die Rechtmäßigkeit dieser Datenverarbeitung bewertet werden sollte, ist, was das Recht der in den Listen genannten Personen auf Schutz personenbezogener Daten anbelangt, das Datenschutzrecht des Mitgliedstaats, in dem der für die Verarbeitung Verantwortliche niedergelassen ist.

Für die Bestimmung des anwendbaren Datenschutzrechts ist nicht relevant, ob der für die Verarbeitung Verantwortliche Mittel in anderen Mitgliedstaaten verwendet (beispielsweise Internetserver mit unterschiedlichen Top-Level-Domains wie .fr, .it, oder .pl), oder ob er sich durch eine speziell zu diesem Zweck erfolgende Datenverarbeitung unmittelbar an Bürger anderer EU-Länder wendet (indem er beispielsweise landesspezifische Namenslisten in der Sprache dieser Länder veröffentlicht).

Bezüglich der Bearbeitung von Beschwerden, die von in anderen Mitgliedstaaten ansässigen Personen eingereicht werden, kann die Kontrollstelle des Niederlassungsmitgliedstaats in jedem Fall von anderen Kontrollstellen um Zusammenarbeit ersucht werden.

Selbstverständlich können in anderen Rechtsbereichen andere Anknüpfungskriterien und somit anwendbare Rechtsvorschriften angewendet werden, beispielsweise um eine straf- oder zivilrechtliche Klage wegen Verleumdung einzureichen.

c) „…es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden …“

Die Anwendung des nationalen Rechts eines Mitgliedstaats der EU ist ausgeschlossen, wenn die von dem für die Verarbeitung Verantwortlichen verwendeten Mittel in dem betreffenden Mitgliedstaat belegen sind und lediglich zur Sicherstellung der Durchfuhr durch das Hoheitsgebiet der Europäischen Union benutzt werden. Dies ist beispielsweise der Fall bei (kabelgebundenen) Kommunikationsnetzen oder bei Postdiensten, die lediglich die Durchfuhr von Mitteilungen durch EU-Gebiet auf ihrem Weg zu Drittländern sicherstellen.

Da es sich hierbei um eine Ausnahme vom „equipment“-Kriterium handelt, sollte diese Bestimmung eng ausgelegt werden. Zudem sei darauf hingewiesen, dass diese Ausnahme in der Praxis immer seltener angewendet wird, da immer mehr Telekommunikationsdienstleister derartige Durchfuhrdienste nur noch im Paket mit Zusatzdienstleistungen wie Spamfiltern oder sonstigen Formen der Datenverarbeitung zum Zeitpunkt der Übermittlung anbieten. Die schlichte Punkt-zu-Punkt-Übermittlung per Kabel wird immer seltener. Dies sollte bei den Überlegungen zur Neufassung des Datenschutzrahmens berücksichtigt werden.

d) „… hat der für die Verarbeitung Verantwortliche einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter zu benennen …“ (Artikel 4 Absatz 2)

Die Richtlinie legt dem für die Verarbeitung Verantwortlichen die Pflicht auf, einen „Vertreter“ zu benennen, der im Hoheitsgebiet des Mitgliedstaats ansässig ist, dessen Recht kraft der von dem für die Verarbeitung Verantwortlichen in diesem Mitgliedstaat zur Verarbeitung personenbezogener Daten verwendeten Mittel anwendbar ist. Dies gilt „unbeschadet der Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst“.

Wie die Erfahrungen der Mitgliedstaaten gezeigt haben, ergeben sich im letztgenannten Fall bestimmte praktische Fragen bezüglich der Durchsetzung dieser Bestimmung gegenüber dem Vertreter – beispielsweise dann, wenn der einzige Vertreter des für die Verarbeitung Verantwortlichen in der EU eine Anwaltskanzlei ist. In den mitgliedstaatlichen Umsetzungsvorschriften ist nicht einheitlich geregelt, ob der Vertreter von dem für die Verarbeitung Verantwortlichen zivil- oder strafrechtlich belangt und bestraft werden kann. Entscheidend ist jeweils, welcher Art die Beziehung zwischen dem Vertreter und dem für die Verarbeitung Verantwortlichen ist. In einigen Mitgliedstaaten tritt der Vertreter auch in Bezug auf die Durchsetzung und etwaige Sanktionen an die Stelle des für die Verarbeitung Verantwortlichen, in anderen Mitgliedstaaten verfügt er nur über eine einfache Ermächtigung. In einigen Mitgliedstaaten[28] sieht das nationale Recht ausdrücklich Geldbußen bzw. –strafen gegen die Vertreter vor, in anderen Mitgliedstaaten[29] ist diese Möglichkeit jedoch nicht vorgesehen.

Hier bedarf es einer EU-weiten Harmonisierung, damit die Rolle des Vertreters wirksamer wird. Insbesondere müssten die betroffenen Personen ihre Rechte gegenüber dem Vertreter – unbeschadet der Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst – geltend machen können.

III.4. Überlegungen über die praktischen Folgen der Anwendung von Artikel 4 Absatz 1 Buchstabe c

Ein entscheidender Aspekt der Anwendung von Artikel 4 Absatz 1 Buchstabe c sind die praktischen Folgen für den für die Verarbeitung Verantwortlichen. Selbst wenn letzterer außerhalb der EU bzw. des EWR ansässig ist, hat er die Grundsätze der Richtlinie anzuwenden, falls er im Hoheitsgebiet der EU belegene Mittel zur Verarbeitung personenbezogener Daten verwendet. Hier stellt sich die Frage, ob diese Grundsätze nur auf den in der EU erfolgenden Teil der Datenverarbeitung anwendbar sind, oder aber auf den für die Verarbeitung Verantwortlichen als solchen, d.h. auf sämtliche Phasen der Bearbeitung (also auch auf die in Drittländern erfolgenden Phasen). Besondere Bedeutung kommt dieser Frage in Netzumgebungen wie dem *Cloud Computing* oder bei multinationalen Unternehmen zu.

---

[28] Siehe das belgische Datenschutzgesetz vom 8. Dezember 1992 (belgisches Amtsblatt vom 18. März 1993), das niederländische Gesetz vom 6. Juli 2000 über den Schutz personenbezogener Daten (Staatsblad 302 vom 20. Juli 2000) sowie das griechische Datenschutzgesetz (Artikel 3 Absatz 3 Buchstabe b in Verbindung mit Artikel 21 Absatz 1 des Gesetzes Nr. 2472/1997).

[29] Im französischen Datenschutzgesetz Nr. 78/17 vom 6. Januar 1978 beispielsweise sind keine derartigen Geldbußen bzw. -strafen gegen die Vertreter vorgesehen.

Interessant sind beispielsweise die Folgen für in mehreren Ländern der Welt niedergelassene für die Verarbeitung Verantwortliche, die Daten in Frankreich verarbeiten lassen, wo sowohl die betreffende Datenbank als auch die Verarbeitungsmittel belegen sind: Wenn die verschiedenen für die Verarbeitung Verantwortlichen Infrastrukturen in Frankreich verwenden, ist Artikel 4 Absatz 1 Buchstabe c anwendbar, so dass alle für die Verarbeitung Verantwortlichen die einschlägigen französischen Rechtsvorschriften einhalten müssen. Dies könnte allerdings unerwünschte Folgen in Bezug auf die wirtschaftlichen Auswirkungen und die Durchsetzbarkeit haben.

Es gibt also bestimmte praktische Erwägungen, die für eine weniger strikte Anwendung des „equiment"-Kriteriums sprechen, doch dem steht die Tatsache entgegen, dass die Grundsätze des Datenschutzes auf den Schutz eines Grundrechtes abstellen. Eine Begrenzung der Rechte der Personen auf bestimmte Teile der Verarbeitung ihrer Daten wäre daher nicht akzeptabel. Ebenso wenig wäre es annehmbar, den Umfang des Schutzes aller in der EU ansässigen Personen zu vermindern, denn das Grundrecht auf den Schutz personenbezogener Daten gilt ja unabhängig von der Staatszugehörigkeit und vom Wohnort. Das in Artikel 4 Absatz 1 Buchstabe c verankerte Kriterium hat also zur Folge, dass die Grundsätze der Richtlinie auf den für die Verarbeitung Verantwortlichen als solchen anwendbar sind, d.h. auf sämtliche Phasen der Bearbeitung - und somit selbst auf die in Drittländern erfolgenden Phasen.

Die Anwendung der Richtlinie auf für die Verarbeitung Verantwortliche während der gesamten Bearbeitungsphase sollte unterstützt werden, so lange ein konkreter Bezug zur EU besteht (also kein loser Zusammenhang wie beispielsweise bei einer unbeabsichtigten Verwendung von Mitteln in einem Mitgliedstaat).

Im Sinne größerer Rechtssicherheit wäre es nützlich, wenn es als sinnvolle Ergänzung zum „equipment"-Kriterium einen genaueren Anknüpfungspunkt für das „Anvisieren" der betreffenden Personen gäbe (auf diesen Punkt wird in den Schlussfolgerungen näher eingegangen). Ein solches Kriterium wäre keineswegs ein Novum, wird es doch bereits im Recht der EU[30] bzw. der Vereinigten Staaten auf dem Gebiet des Schutzes der Privatsphäre von Kindern im Internet[31] verwendet. Gleiches gilt für bestimmte mitgliedstaatliche Gesetze zur Umsetzung der Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr[32], welche vorsehen, dass Dienstanbieter, die nicht im EWR niedergelassen sind, in den Anwendungsbereich dieser mitgliedstaatlichen

---

30 Vergleiche Artikel 15 Absatz 1 Buchstabe c der Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (ABl. L 12 vom 16.1.2001, S. 1) sowie (in Bezug auf die Auslegung dieser Bestimmung) die Schlussanträge von Generalanwalt Trstenjak in der Rechtssache C-144/09 (*Hotel Alpenhof*) vom 18. Mai 2010.

31 Die Anwendung des US-Gesetzes zum Schutz der Privatsphäre von Kindern im Internet (Children's Online Privacy Protection Act, COPPA) kann entweder dadurch ausgelöst werden, dass die Person, die derartige Daten auf einer Website veröffentlicht, im Hoheitsgebiet der Vereinigten Staaten ansässig ist, oder aber dadurch, dass sich die betreffende Website speziell an Kinder richtet. Außerhalb der Vereinigten Staaten belegene Webseiten und Internetdienste haben die Bestimmungen des COPPA einzuhalten, wenn sie sich an in den Vereinigten Staaten ansässige Kinder richten oder wissentlich personenbezogene Daten dieser Kinder sammeln oder offenlegen. Siehe insbesondere 16 CFR 312.2 (verfügbar unter http://www.ftc.gov/os/1999/10/64fr59888.pdf), S. 59912.

32 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. L 178 vom 17.7.2000, S. 1.

Rechtsvorschriften fallen, wenn sie speziell auf ihr Hoheitsgebiet zugeschnittene Dienste anbieten.

Folglich könnte im Rahmen künftiger Diskussionen über die Neufassung des Datenschutzrahmens auch über die Anwendung eines ähnlichen Kriteriums im Datenschutzrecht der EU nachgedacht werden.

Ferner wirkt sich die Anwendung von Artikel 4 Absatz 1 Buchstabe c auch auf das Zusammenspiel zwischen dieser Bestimmung und den Artikeln 25 und 26 der Richtlinie aus. Wenn ein für die Verarbeitung Verantwortlicher, der außerhalb der EU bzw. des EWR niedergelassen ist, Mittel im Hoheitsgebiet der EU bzw. des EWR verwendet (und daher alle einschlägigen Bestimmungen der Richtlinie einzuhalten hat), kann dies nämlich die Anwendung der Artikel 25 und 26 nach sich ziehen. Allerdings kann es sich in der Praxis als schwierig erweisen, die möglichen Folgen eines solchen Falls zu bestimmen.

Wenn beispielsweise der außerhalb des EWR niedergelassene für die Verarbeitung Verantwortliche X durch Verwendung von im Hoheitsgebiet der EU belegenen Mitteln personenbezogene Daten (z.B. mittels Cookies oder über einen Auftragsverarbeiter) sammelt, hat er sich in allen Verarbeitungsphasen an die Richtlinie zu halten. Hier besteht eine gewisse Parallele zu dem Fall, dass ein für die Verarbeitung Verantwortlicher, der im EWR niedergelassen ist, personenbezogene Daten an einen außerhalb des EWR niedergelassenen Auftragsverarbeiter übermittelt: In beiden Fällen unterliegt sowohl der für die Verarbeitung Verantwortliche als auch der außerhalb des EWR niedergelassene Auftragsverarbeiter der Richtlinie. Wie diese Grundsätze in der Praxis nach Maßgabe der Angemessenheitsanforderung von Artikel 25 und 26 der Richtlinie in unter Artikel 4 Absatz 1 Buchstabe c fallenden Fällen, in denen der für die Verarbeitung Verantwortlicher außerhalb des EWR niedergelassen ist, umgesetzt werden sollen, ist nicht ganz klar. Die Datenschutzgruppe ist der Auffassung, dass es weiterer Überlegungen über die bestehenden Instrumente zur Regelung der Bedingungen für die etwaige Übermittlung von Daten bedarf, um diese Fälle besser zu erfassen.

III.5. Anzuwendende Sicherheitsvorschriften (Artikel 17 Absatz 3)

Artikel 17 Absatz 3 besagt, dass der Vertrag oder Rechtsakt, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist, insbesondere vorzusehen hat, dass die Sicherheitsvorschriften, die im Recht des Mitgliedstaats, in dem der Auftragsverarbeiter seinen Sitz hat, niedergelegt sind, einzuhalten sind.

Dieser Grundsatz stellt darauf ab, einheitliche landesweite Anforderungen bezüglich der Sicherheitsmaßnahmen in den einzelnen Mitgliedstaaten zu schaffen und somit ihre Durchsetzung zu vereinfachen. Allerdings unterscheiden sich, was die EU anbelangt, diese Sicherheitsanforderungen von Mitgliedstaat zu Mitgliedstaat noch immer erheblich: Während es in einigen Mitgliedstaaten sehr ausführliche Bestimmungen gibt, haben andere Mitgliedstaaten lediglich die allgemeinen Formulierungen der Richtlinie übernommen. Dort wo die nationalen Gesetze allgemein gehalten sind und die Formulierungen aus der Richtlinie übernommen wurden, hat dies keine praktischen Auswirkungen. So ist es für einen Auftragsverarbeiter nicht schwierig, sich an ausführlichere Bestimmungen zu halten, die der für die Verarbeitung Verantwortliche ihm nach Maßgabe seines nationalen Rechts auferlegt, und ebenso wenig fällt es einem

für die Verarbeitung Verantwortlichen schwer, ausführlichere Anforderungen nach Maßgabe des Rechts des Auftragsverarbeiters zu erfüllen. Nur in Fällen, in denen die einschlägigen Vorschriften unterschiedlich sind oder gar im Widerspruch zueinander stehen, entscheidet Artikel 17 Absatz 3 zu Gunsten des Rechts des Auftragsverarbeiters[33]. Gleichwohl erscheint es ratsam, die Frage einer weiteren Harmonisierung in der Diskussion über die Neufassung des Datenschutzrahmens anzusprechen.

III.6. Befugnisse und Zusammenarbeit von Kontrollstellen (Artikel 28 Absatz 6)

Wie bereits in Abschnitt II.2.d erwähnt, stellt Artikel 28 Absatz 6 darauf ab, etwaige Lücken zu schließen, die auf dem Gebiet des Datenschutzes im Binnenmarkt zwischen dem anwendbaren Recht und der gerichtlichen Zuständigkeit entstehen könnten.

Die nationalen Datenschutzbehörden sind demnach befugt, die Umsetzung der Datenschutzvorschriften auf dem Gebiet des Mitgliedstaats, in dem sie belegen sind, zu beaufsichtigen. Selbst wenn das Recht eines anderen Mitgliedstaats in ihrem Hoheitsgebiet anwendbar wäre, wären die Durchsetzungsbefugnisse der Datenschutzbehörde nicht begrenzt: Die über das anwendbare Recht entscheidenden Kriterien der Richtlinie sehen die Möglichkeit vor, dass eine Datenschutzbehörde einen in ihrem Hoheitsgebiet erfolgenden Verarbeitungsvorgang auch dann überprüfen darf (und eventuell nachfolgend einschreiten kann), wenn es sich bei dem anwendbaren Recht um das Recht eines anderen Mitgliedstaats handelt.

III.6.a) Vom anwendbaren einzelstaatlichen Recht unabhängige Zuständigkeit der Kontrollstelle

Durch die diesbezügliche Bestimmung wird den nationalen Kontrollstellen die Befugnis übertragen, unabhängig davon, ob es sich bei dem anwendbaren Recht um ihr eigenes nationales Datenschutzrecht oder aber um das Datenschutzrecht eines anderen Mitgliedstaats handelt, jederzeit innerhalb der Grenzen ihrer territorialen Zuständigkeit tätig zu werden.

III.6.b) Befugnisausübung der Kontrollstelle im Hoheitsgebiet ihres Mitgliedstaats

Falls es sich bei dem anwendbaren Datenschutzrecht um das eines anderen Mitgliedstaats handelt, kann die Kontrollstelle in ihrem Hoheitsgebiet die ihr durch das nationale Recht übertragenen Befugnisse in vollem Umfang ausüben. Dies schließt Untersuchungsbefugnisse, Einwirkungsbefugnisse, das Klagerecht bzw. eine Anzeigebefugnis und die Befugnis zur Verhängung von Sanktionen ein.

In Fällen, in denen mehrere Datenschutzbehörden einschließlich der örtlichen Datenschutzbehörde und der Datenschutzbehörden, deren Recht anwendbar ist, beteiligt sind, ist es von wesentlicher Bedeutung, dass eine Zusammenarbeit organisiert wird und dass die Rolle jeder einzelnen Datenschutzbehörde klar ist. Daher sollten insbesondere folgende Fragen geklärt werden:

- verfahrenstechnische Fragen wie die Ermittlung der federführenden Behörde und ihrer Zusammenarbeit mit den anderen Datenschutzbehörden;

---

[33] Dadurch soll vermieden werden, dass der Rückgriff auf einen Auftragsverarbeiter in einem anderen Land, in dem weniger strenge Vorschriften gelten, als Verstoß gegen die Pflichten des für die Verarbeitung Verantwortlichen betrachtet werden kann.

- die Frage des Umfangs der von den einzelnen Datenschutzbehörden auszuübenden Befugnisse: In wie weit wird die örtliche Datenschutzbehörde von ihren Befugnissen zur Anwendung der materiellrechtlichen Grundsätze und der Sanktionen Gebrauch machen? Sollte sie die Ausübung ihrer Befugnisse auf die Überprüfung von Fakten begrenzen oder aber Sicherungsmaßnahmen oder gar endgültige Maßnahmen ergreifen dürfen? Sollte sie die Bestimmungen des anwendbaren Rechts selbst auslegen dürfen, oder sollte dies das Vorrecht der Datenschutzbehörde des Mitgliedstaats sein, dessen Recht anwendbar ist? In diesem Zusammenhang sei darauf hingewiesen, dass die Möglichkeit, gegen alle Beteiligten Sanktionen zu verhängen, nicht in allen mitgliedstaatlichen Rechtsordnungen vorgesehen ist[34].

Eine weit gehende Harmonisierung der den Kontrollstellen nach Artikel 28 der Richtlinie übertragenen Aufsichtsbefugnisse ist eine wesentliche Voraussetzung für die wirksame, diskriminierungsfreie und länderübergreifende Einhaltung von Datenschutzbestimmungen. Dieses Thema bedarf weiterer Analysen, und die Datenschutzgruppe wird in einer separaten Stellungnahme entsprechende Leitlinien vorgeben.

Beispiel 10: grenzübergreifende Verarbeitung personenbezogener Daten in der EU

Die Verarbeitungstätigkeiten erfolgen im Vereinigten Königreich, allerdings im Rahmen der Tätigkeiten einer Niederlassung des für die Verarbeitung Verantwortlichen, der in Deutschland ansässig ist. Dies hat folgende Konsequenzen:

- Auf die im Vereinigten Königreich erfolgende Verarbeitung ist das deutsche Recht anwendbar;

- Die Datenschutzbehörde des Vereinigten Königreichs muss befugt sein, die im Vereinigten Königreich belegenen Örtlichkeiten einer Kontrolle zu unterziehen, und sie muss Feststellungen treffen, welche sodann an die deutsche Datenschutzbehörde zu übermitteln sind;

- Die deutsche Datenschutzbehörde sollte befugt sein, auf der Grundlage der ihr von der Datenschutzbehörde des Vereinigten Königreichs übermittelten Feststelllungen Sanktionen gegen den in Deutschland niedergelassenen für die Verarbeitung Verantwortlichen zu verhängen.

Falls es sich bei der Niederlassung im Vereinigten Königreich um einen Auftragsverarbeiter handelt, unterliegen die Sicherheitsaspekte der Verarbeitung außerdem dem Datenschutzrecht des Vereinigten Königreichs, was die Frage aufwirft, wie dessen Anforderungen ordnungsgemäß durchgesetzt werden könnten.

III.6.c) Zur Erfüllung der Kontrollaufgaben notwendige gegenseitige Zusammenarbeit

Alle Kontrollstellen sind zur Zusammenarbeit verpflichtet („sorgen für die…Zusammenarbeit"), wobei diese Pflicht auf das zur Erfüllung ihrer Kontrollaufgaben notwendige Maß begrenzt ist. Kooperationsersuchen sollten folglich

[34] Im griechischen Recht beispielsweise sind Sanktionen nur für die für die Verarbeitung Verantwortlichen und ihre Vertreter vorgesehen, nicht jedoch für Auftragsverarbeiter.

im Zusammenhang mit der Ausübung ihrer Befugnisse stehen und sich üblicherweise auf Fälle mit grenzüberschreitender Bedeutung beziehen.

In dieser Bestimmung wird insbesondere auf den Austausch „sachdienlicher Informationen“ Bezug genommen, also beispielsweise von Angaben über die einschlägigen Bestimmungen und Rechtsakte, die auf einen gegebenen Fall anwendbar sind. Gleichwohl ist es auch wahrscheinlich, dass die Zusammenarbeit auf unterschiedlichen Ebenen erfolgt (Bearbeitung grenzübergreifender Beschwerden, Beweiserhebung für andere Datenschutzbehörden oder Verhängung von Sanktionen).

Noch komplexer wird dieses Thema, wenn ein internationaler Kontext besteht und weltweit operierende für die Verarbeitung Verantwortliche betroffen sind, was Verbesserungen bei der Vollzugszusammenarbeit erforderlich macht. Initiativen wie das *Global Privacy Enforcement Network* (GPEN), in dem Datenschutzbehörden verschiedener Erdteile mitwirken, sind ein notwendiger und begrüßenswerter Schritt in diese Richtung.

Fall 11: ein soziales Netz mit Sitz in einem Drittland und einer Niederlassung in der EU

Ein soziales Netz hat seinen Sitz in einem Drittland und eine Niederlassung in einem Mitgliedstaat der EU. Seine Politik für die Verarbeitung personenbezogener Daten von EU-Bürgern wird von der Niederlassung festgelegt und umgesetzt. Das soziale Netz richtet sich aktiv an alle in den Mitgliedstaaten ansässigen Personen. Ein Großteil seiner Kunden und auch seiner Einnahmen stammen aus diesem Personenkreis. Das soziale Netz arbeitet mit Cookies, die es auf den Rechnern der in der EU ansässigen Benutzer setzt.

Gemäß Artikel 4 Absatz 1 Buchstabe a ist in diesem Fall das Datenschutzrecht des Mitgliedstaats, in dem das Unternehmen seinen EU-Sitz hat, das anwendbare Recht. Ob das soziale Netz Mittel verwendet, die im Hoheitsgebiet eines anderen Mitgliedstaats belegen sind, ist hierbei irrelevant, da die gesamte Verarbeitung im Rahmen der Tätigkeiten der einzigen Niederlassung erfolgt und eine kumulative Anwendung von Artikel 4 Absatz 1 Buchstabe a und Artikel 4 Absatz 1 Buchstabe c laut der Richtlinie ausgeschlossen ist.

Gleichwohl ist die Kontrollstelle des Mitgliedstaats, in dem das soziale Netz seinen EU-Sitz hat, nach Artikel 28 Absatz 6 verpflichtet, mit anderen Kontrollstellen zusammenzuarbeiten, um beispielsweise Anträge oder Beschwerden von Bürgern anderer EU-Länder zu bearbeiten.

Fall 12: Plattform für EU-weite elektronische Gesundheitsdienste

Auf europäischer Ebene wird eine Plattform eingerichtet, durch die die grenzübergreifende Verarbeitung von Patientendaten vereinfacht werden soll. Die Plattform ermöglicht unter anderem den Austausch von Patienten-Kurzakten, Arzneimittelakten und Verschreibungen, um Gesundheitsdienste bei Auslandsreisen zu erleichtern.

Ungeachtet der Tatsache, dass der Informationsaustausch durch diese Plattform erleichtert wird, besteht weiterhin in jedem Mitgliedstaat mindestens eine Niederlassung, die im Rahmen ihrer Tätigkeiten Patientendaten verarbeitet. Wenn also beispielsweise ein bulgarischer Staatsbürger auf einer Reise in Portugal eine dringende Behandlung benötigt, wird seine Patientenakte von den portugiesischen ärztlichen Diensten über die Plattform und nach Maßgabe des portugiesischen Datenschutzrechts verarbeitet. Falls der Patient nach seiner Rückkehr nach Bulgarien Schadensersatzansprüche gegen die Verarbeitung seiner Daten durch den portugiesischen für die Verarbeitung Verantwortlichen erheben möchte, muss er diese bei der bulgarischen Datenschutzbehörde geltend machen. Die bulgarische Datenschutzbehörde arbeitet sodann mit der portugiesischen Datenschutzbehörde zusammen, um den Sachverhalt zu klären und um zu prüfen, ob ein Verstoß gegen das portugiesische Recht vorliegt.

Wenn die Europäische Kommission durch Organisation des Datenflusses und durch Sicherstellung der Systemsicherheit in die Arbeitsweise der Plattform eingreift, kann auch dies als eine Verarbeitung personenbezogener Daten gesehen werden, die die Anwendung der Verordnung (EG) Nr. 45/2001 auslöst. Im vorliegenden Beispiel würde die bulgarische Datenschutzbehörde bei einer Beschwerde eines bulgarischen Staatsbürgers über eine vermeintlichen Verstoß gegen die Sicherheit seiner medizinischen Daten mit dem Europäischen Datenschutzbeauftragten zusammenarbeiten, um die Bedingungen und die Konsequenzen eines solchen Verstoßes in Erfahrung zu bringen.

IV. Schlussfolgerungen

Ziel dieser Stellungnahme ist die Klärung des Anwendungsbereichs der Richtlinie 95/46/EG und insbesondere von Artikel 4. Zudem soll auf bestimmte Bereiche hingewiesen werden, in denen weitere Verbesserungen möglich sind. Nachfolgend werden die wichtigsten Schlussfolgerungen zu diesen beiden Aspekten vorgestellt.

IV.1. Klärung der bestehenden Bestimmungen

Die Bestimmung der Anwendung des EU-Rechts auf die Verarbeitung personenbezogener Daten dient der Klärung des Anwendungsbereichs des Datenschutzrechts der EU sowohl in der EU bzw. im EWR als auch im weiteren internationalen Kontext. Ein klares Verständnis des anwendbaren Rechts trägt sowohl zur Rechtssicherheit für die für die Verarbeitung Verantwortlichen als auch zu einem klaren Rahmen für die Betroffenen und sonstigen Beteiligten bei. Zudem dürfte eine korrekte Auslegung des anwendbaren Rechts sicherstellen, dass das hohe Maß an Schutz,

das durch die Richtlinie 95/46 für personenbezogene Daten geboten wird, keine Rechtslücken oder Schlupflöcher aufweist.

Die zentrale Bestimmung über das anwendbare Recht ist Artikel 4, welcher bestimmt, welche nach Maßgabe der Richtlinien angenommenen nationalen Datenschutzvorschriften auf die Verarbeitung personenbezogener Daten anwendbar sein können.

Gemäß Artikel 4 Absatz 1 Buchstabe a hat jeder Mitgliedstaat seine nationalen Datenschutzvorschriften auf alle Verarbeitungen personenbezogener Daten anzuwenden, die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Ausschlag gebend für die Ermittlung einer für die Zwecke von Artikel 4 Absatz 1 Buchstabe a relevanten Niederlassung ist die Frage, ob die betreffende Organisation effektiv und tatsächlich derartige Tätigkeiten ausübt. Die Formulierung „einer Niederlassung" besagt, dass die Anwendbarkeit des Rechts eines Mitgliedstaats durch den Ort ausgelöst wird, an dem sich eine Niederlassung des für die Verarbeitung Verantwortlichen in diesem Mitgliedstaat befindet, und dass die Anwendbarkeit des Rechts anderer Mitgliedstaaten durch die Orte ausgelöst werden könnte, an denen sich etwaige andere Niederlassungen des für die Verarbeitung Verantwortlichen in diesen Mitgliedstaaten befinden.

Der „Rahmen der Tätigkeiten" – und nicht der Ort, an dem sich die Daten befinden – ist ein bestimmender Faktor bei der Ermittlung des Anwendungsbereichs des anwendbaren Rechts. Der Begriff „Rahmen der Tätigkeiten" impliziert nämlich, dass nicht das Recht des Mitgliedstaats, in dem der *für die Verarbeitung Verantwortliche* niedergelassen ist, das anwendbare Recht ist, sondern das Recht des Mitgliedstaats, in dem eine *Niederlassung* des für die Verarbeitung Verantwortlichen *Tätigkeiten* vornimmt, die die Verarbeitung personenbezogener Daten mit sich bringen. Vor diesem Hintergrund ist es von entscheidender Bedeutung, in welchem Maße die Niederlassung(en) Tätigkeiten durchführt bzw. durchführen, in deren Rahmen personenbezogene Daten verarbeitet werden. Zu berücksichtigen ist zudem, welcher Art die Tätigkeiten der Niederlassungen sind, und auch der Notwendigkeit der Sicherstellung eines wirksamen Schutzes der Rechte des Einzelnen ist Rechnung zu tragen. Bei der Analyse dieser Kriterien sollte ein funktioneller Ansatz verfolgt werden: Ausschlaggebende Faktoren sollten nicht so sehr die von den Beteiligten mit Blick auf das anwendbare Recht durchgeführten theoretischen Bewertungen, sondern vielmehr ihr praktisches Vorgehen und ihre Interaktion sein.

Artikel 4 Absatz 1 Buchstabe b regelt den weniger häufigen Fall, dass das Datenschutzrecht eines Mitgliedstaats auch auf Fälle anwendbar ist, in denen der für die Verarbeitung Verantwortliche „nicht in seinem Hoheitsgebiet, aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet". In bestimmten Situationen können nämlich externe, auf dem internationalen öffentlichen Recht fußende Kriterien bestimmen, dass die Anwendung eines nationalen Datenschutzrechts über die Landesgrenzen des betreffenden Mitgliedstaates hinaus ausgeweitet wird (beispielsweise auf Botschaften oder Schiffe).

Artikel 4 Absatz 1 Buchstabe c stellt darauf ab, dass das in der EU-Richtlinie verankerte Recht auf den Schutz personenbezogener Daten auch dann sichergestellt ist, wenn der für die Verarbeitung Verantwortliche nicht im Hoheitsgebiet der EU bzw. des EWR

niedergelassen ist, aber zwischen der Verarbeitung personenbezogener Daten und diesem Hoheitsgebiet eine klare Verbindung besteht. Um die Konsistenz innerhalb von Artikel 4 sicherzustellen und Lücken in der Anwendung der Datenschutzvorschriften zu vermeiden, sollte die Anwendung von Artikel 4 Absatz 1 Buchstabe c nach dem Dafürhalten der Datenschutzgruppe nicht durch die Existenz einer im Hoheitsgebiet der EU bzw. des EWR belegenen Niederlassung des für die Verarbeitung Verantwortlichen verhindert werden, wenn es sich dabei nicht um eine für die Zwecke von Artikel 4 Absatz 1 Buchstabe a relevante Niederlassung handelt. Stattdessen sollte die sich auf die Verwendung von Mitteln beziehende Bestimmung von Artikel 4 Absatz 1 Buchstabe c auch für den Fall gelten, dass es im Hoheitsgebiet der EU bzw. des EWR keine Niederlassung gibt, *die die Anwendung von Artikel 4 Absatz 1 Buchstabe a auslöst* oder dass die Verarbeitung *nicht im Rahmen einer solchen Niederlassung erfolgt.*

Entscheidend für die Anwendbarkeit von Artikel 4 Absatz 1 Buchstabe c und somit des Datenschutzrechts eines Mitgliedstaats ist die Verwendung von im Hoheitsgebiet dieses Mitgliedstaats belegenen Mitteln. Der Begriff „Verwendung" impliziert zwei Dinge: zum einen eine wie auch immer geartete Tätigkeit des für die Verarbeitung Verantwortlichen und zum anderen dessen klare Absicht, personenbezogene Daten zu verarbeiten. Somit zieht einerseits nicht jede beliebige Verwendung von Mitteln in der EU bzw. im EWR die Anwendung der Richtlinie nach sich, aber andererseits ist es, damit die Verarbeitung in den Anwendungsbereich der Richtlinie fällt, auch nicht erforderlich, dass sich diese Mittel im Besitz oder gänzlich unter der Kontrolle des für die Verarbeitung Verantwortlichen befinden.

Die Tatsache, dass der englische Begriff „equipment" in anderen Sprachfassungen als „Mittel" wiedergegeben wird, kann eine weite Auslegung der Kriterien bewirken, was wiederum einen weiten Anwendungsbereich nach sich ziehen kann. Eine derartige Auslegung kann in bestimmten Fällen dazu führen, dass das EU-Datenschutzrecht selbst dann anwendbar ist, wenn die betreffende Verarbeitung keinen tatsächlichen Bezug zur EU bzw. zum EWR aufweist. In jedem Fall löst die durch in der EU oder im EWR belegene Mittel erfolgende Verarbeitung personenbezogener Daten durch einen für die Verarbeitung Verantwortlichen, der außerhalb der EU bzw. des EWR niedergelassen ist, die Anwendung der Richtlinie gemäß Artikel 4 Absatz 1 Buchstabe c aus – und dies bedeutet, dass auch alle anderen einschlägigen Bestimmungen der Richtlinie anwendbar sind.

Die Anwendung des nationalen Rechts eines Mitgliedstaats der EU ist ausgeschlossen, wenn die von dem für die Verarbeitung Verantwortlichen verwendeten Mittel in dem betreffenden Mitgliedstaat belegen sind und lediglich zur Sicherstellung der Durchfuhr durch das Hoheitsgebiet der Europäischen Union benutzt werden. Dies ist beispielsweise der Fall bei (kabelgebundenen) Kommunikationsnetzen oder bei Postdiensten, die lediglich die Durchfuhr von Mitteilungen durch EU-Gebiet auf ihrem Weg zu Drittländern sicherstellen.

Artikel 4 Absatz 2 legt dem für die Verarbeitung Verantwortlichen die Pflicht auf, einen Vertreter zu benennen, der im Hoheitsgebiet des Mitgliedstaats ansässig ist, dessen Recht kraft der von dem für die Verarbeitung Verantwortlichen in diesem Mitgliedstaat zur Verarbeitung personenbezogener Daten verwendeten Mittel anwendbar ist. Die Durchsetzung gegenüber einem Vertreter kann in diesem Fall eine Herausforderung sein.

In Artikel 17 Absatz 3 ist festgelegt, dass der Vertrag oder Rechtsakt, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist, insbesondere vorzusehen hat, dass die Sicherheitsvorschriften, die im Recht des Mitgliedstaats, in dem der Auftragsverarbeiter seinen Sitz hat, niedergelegt sind, einzuhalten sind. Dieser Grundsatz stellt darauf ab, einheitliche landesweite Anforderungen bezüglich der Sicherheitsmaßnahmen in den einzelnen Mitgliedstaaten zu schaffen und somit ihre Durchsetzung zu vereinfachen.

Um etwaigen Lücken vorzubeugen, die auf dem Gebiet des Datenschutzes im Binnenmarkt zwischen dem anwendbaren Recht und der gerichtlichen Zuständigkeit entstehen könnten, sieht Artikel 28 Absatz 6 vor, dass die nationalen Datenschutzbehörden in der Lage sein sollten, ihre Kontroll- und Eingriffsbefugnisse auch dann auszuüben, wenn das Datenschutzrecht eines anderen Mitgliedstaats auf die in ihrem Zuständigkeitsbereich erfolgende Verarbeitung personenbezogener Daten Anwendung findet.

IV.2. Verbesserung der geltenden Bestimmungen

Die obigen Hinweise und Beispiele sollen dazu beitragen, dass bei der Bestimmung des auf eine Verarbeitung personenbezogener Daten anwendbaren Datenschutzrechts größere Rechtssicherheit herrscht und die Rechte der Personen besser geschützt sind. Bei ihrer Ausarbeitung sind einige Mängel deutlich geworden, auf die nachfolgend näher eingegangen wird.

Es wäre sinnvoll, wenn im Rahmen der Neufassung des allgemeinen Datenschutzrahmens die in der Richtlinie verwendeten Formulierungen geklärt und die Konsistenz zwischen den einzelnen Teilen von Artikel 4 verbessert würden. Konkret besteht nach dem Dafürhalten der Datenschutzgruppe Klärungsbedarf in folgenden Punkten:

a. Es ist erforderlich, die Inkonsistenzen zu beseitigen, die in der Formulierung von Artikel 4 Absatz 1 Buchstabe a und von 4 Absatz 1 Buchstabe c in Bezug auf den Begriff „Niederlassung“ und die Formulierung, dass der für die Verarbeitung Verantwortliche „nicht im Gebiet der Gemeinschaft niedergelassen“ ist, bestehen. Um die Konsistenz mit Artikel 4 Absatz 1 Buchstabe a herzustellen, in dem ja das Kriterium der „Niederlassung“ verwendet wird, sollte Artikel 4 Absatz 1 Buchstabe c auf alle Fälle anwendbar sein, in denen es in der EU keine *Niederlassung* gibt, *die die Anwendung von Artikel 4 Absatz 1 Buchstabe a auslöst* oder in denen die Verarbeitung *nicht im Rahmen der Tätigkeiten* einer solchen Niederlassung erfolgt.

b. Auch wäre eine Klärung der Formulierung „im Rahmen der Tätigkeiten“ nützlich. Die Datenschutzgruppe hat bereits auf die Notwendigkeit hingewiesen, den *Umfang der Verarbeitungstätigkeit* der Niederlassung(en) zu bewerten, also zu prüfen, wer in welcher Niederlassung welcher Tätigkeit nachgeht. Bei der Auslegung dieses Kriteriums werden die vorbereitenden Arbeiten für die Richtlinie ebenso berücksichtigt wie das seinerzeit vorgegebene Ziel, in Bezug auf die Rechtsvorschriften, die auf die verschiedenen Niederlassungen des für die Verarbeitung Verantwortlichen in der EU anwendbar sind, einen distributiven Ansatz zu verfolgen. Die Datenschutzgruppe ist der Auffassung, dass Artikel 4 Absatz 1 Buchstabe a in seiner jetzigen Form zwar machbare, aber bisweilen eben

komplexe Lösungen ermöglicht und dies dafür spräche, sich auf einen zentraleren, harmonisierten Ansatz zu verlegen.

c. Eine solche auf die Vereinfachung der Vorschriften für die Bestimmung des anwendbaren Rechts abstellende Änderung würde in einer Rückverlagerung auf das Ursprungsland-Prinzip bestehen: Alle Niederlassungen eines für die Verarbeitung Verantwortlichen in der EU hätten in diesem Fall unabhängig davon, in welchem Hoheitsgebiet sie belegen sind, ein und dasselbe Gesetz anzuwenden. Das erste anzuwendende Kriterium wäre somit der Ort der Hauptniederlassung des für die Verarbeitung Verantwortlichen. Die Tatsache, dass mehrere verschiedene Niederlassungen in der EU bestehen, würde keine distributive Anwendung der einschlägigen nationalen Rechtsvorschriften der betreffenden Mitgliedstaaten auslösen.

d. Dies wäre allerdings nur akzeptabel, wenn keine erheblichen Unterschiede zwischen den einschlägigen Rechtsvorschriften der Mitgliedstaaten bestehen. Eine wirksame Anwendung des Ursprungsland-Prinzips würde sonst nämlich zu einem „forum shopping" in jenen Mitgliedstaaten führen, deren Recht als günstiger für die für die Verarbeitung Verantwortlichen angesehen wird. Für die von der Datenverarbeitung betroffenen Personen wäre dies natürlich von Nachteil. Rechtssicherheit wäre für die für die Verarbeitung Verantwortlichen und für die betroffenen Personen nur sichergestellt, wenn eine umfassende Harmonisierung der mitgliedstaatlichen Rechtsvorschriften einschließlich der Sicherheitsvorschriften durchgeführt würde. Die Datenschutzgruppe fordert daher eine weit gehende Harmonisierung der Datenschutzgrundsätze – auch als Voraussetzung für eine mögliche Rückverlagerung auf das Ursprungsland-Prinzip.

e. Für Fälle, in denen der für die Verarbeitung Verantwortliche seinen Sitz außerhalb der EU hat, sollten zusätzliche Kriterien gelten, damit sichergestellt ist, dass eine hinreichende Verbindung zum Hoheitsgebiet der EU besteht und vermieden wird, dass das EU-Gebiet für illegale Datenverarbeitungstätigkeiten von in Drittländern niedergelassenen für die Verarbeitung Verantwortlichen missbraucht wird. Zu diesem Zweck könnten die beiden folgenden Kriterien verwendet werden:

   – das Anvisieren von Einzelpersonen („dienstleistungsorientierter Ansatz"): Es würde ein Kriterium für die Anwendung des EU-Datenschutzrechts eingeführt, welches besagt, dass die die Verarbeitung personenbezogener Daten einschließende Tätigkeit Einzelpersonen in der EU betrifft. Hier wäre ein gezieltes Anvisieren erforderlich, das sich auf eine konkrete Verbindung zwischen der Einzelperson und einem spezifischen EU-Land gründet bzw. dieser Rechnung trägt. Denkbar wären beispielsweise folgende Anknüpfungspunkte: die Tatsache, dass ein für die Verarbeitung Verantwortlicher personenbezogene Daten im Rahmen von Dienstleistungen erhebt, die ausdrücklich EU-Bürgern zugänglich bzw. an diese gerichtet sind (Informationsanzeige in EU-Sprachen); das Anbieten von Dienstleistungen oder Erzeugnissen in EU-Ländern, wobei der Zugang von der Verwendung einer EU-Kreditkarte abhängig gemacht wird; das Übersenden von Werbung in der Sprache des Nutzers oder für in der EU verfügbare Erzeugnisse und Dienstleistungen. Der Datenschutzgruppe ist bewusst, dass dieses Kriterium bereits auf dem Gebiet des Verbraucherschutzes verwendet wird: Seine Anwendung im Datenschutzbereich würde größere Rechtssicherheit für die

für die Verarbeitung Verantwortlichen bedeuten, wenn diese ein und dasselbe Kriterium auf Tätigkeiten, die in vielen Fällen sowohl die Anwendung von Verbraucherschutzvorschriften als auch die Anwendung von Datenschutzvorschriften auslösen, anzuwenden hätten;

- das „equipment"-Kriterium: Dieses Kriterium hat nachweislich unerwünschte Folgen (u.a. eine mögliche universelle Anwendung des EU-Rechts). Gleichwohl gilt es zu vermeiden, dass die EU aufgrund einer Rechtslücke als Zufluchtsort für eine unregulierte Datenverarbeitung – beispielsweise mit ethisch unzulässigen Aspekten – missbraucht werden kann. Das „equipment"-Kriterium könnte daher in abgeschwächter, auf die Wahrung der Grundrechte ausgerichteter Form beibehalten werden. Es käme nur noch als dritte Möglichkeit ins Spiel und wäre in jenen Fällen anwendbar, in denen die beiden anderen Möglichkeiten nicht zum Tragen kommen, sprich: Es würde Grenzfälle abdecken, in denen zwar in der EU eine relevante mit der Datenverarbeitung verknüpfte Infrastruktur besteht, es aber um Daten von nicht in der EU ansässigen Personen geht und die für die Verarbeitung Verantwortlichen keine Verbindung zur EU haben. Für diesen letztgenannten Fall könnte auch vorgesehen werden, dass nur bestimmte Datenschutzgrundsätze (z.B. in Bezug auf die Rechtmäßigkeit oder die Sicherheit der Daten) anwendbar sein sollen. Ein solcher Ansatz, der natürlich noch weiterentwickelt und verfeinert werden müsste, würde wahrscheinlich die meisten Probleme, die sich derzeit aus Artikel 4 Absatz 1 Buchstabe c ergeben, lösen helfen.

f. Als letzte Empfehlung spricht sich die Datenschutzgruppe dafür aus, die Pflicht des in einem Drittland niedergelassenen für die Verarbeitung Verantwortlichen, einen Vertreter in der EU zu bestimmen, weiter zu harmonisieren, damit der Vertreter eine effektivere Rolle spielen kann. Insbesondere sollte geklärt werden, inwieweit die betroffenen Personen ihre Rechte gegenüber dem Vertreter geltend machen können.

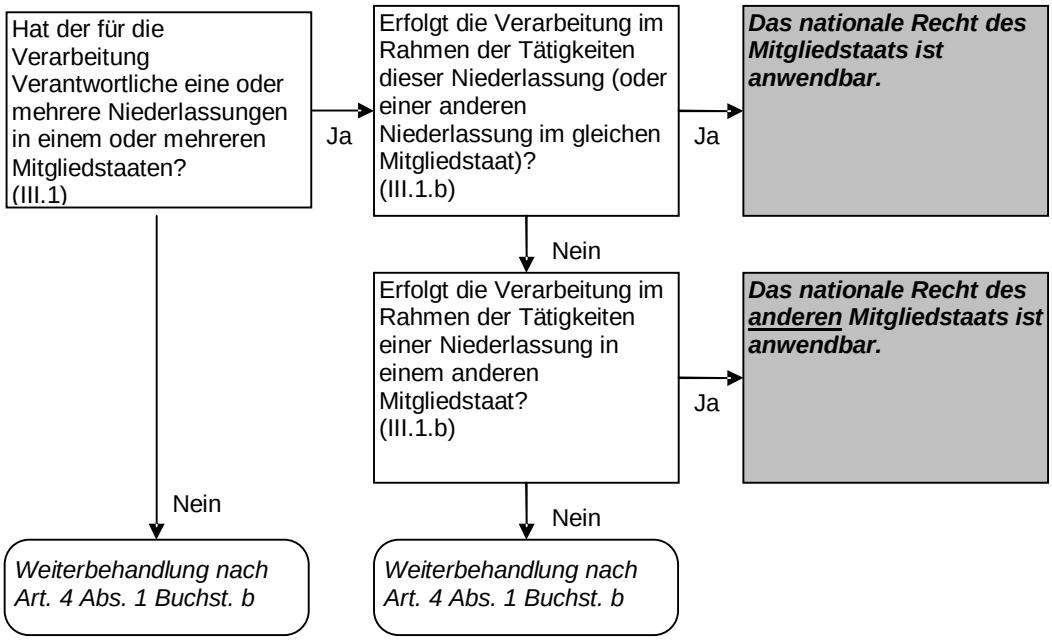
Brüssel, 16. Dezember 2010

Für die Datenschutzgruppe

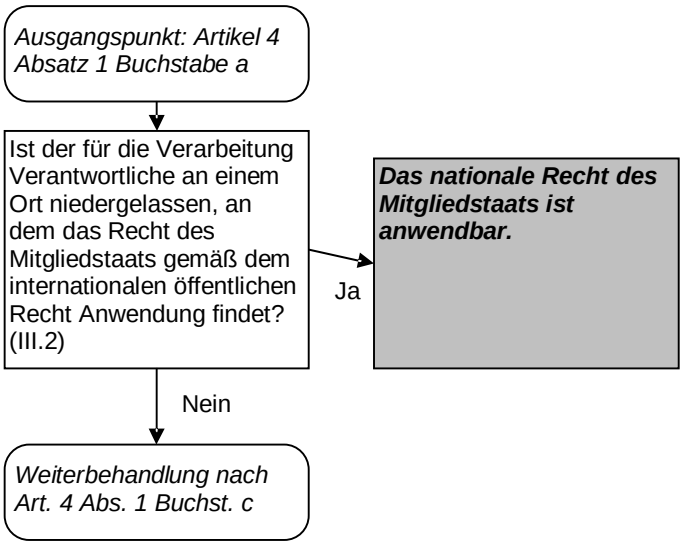
Der Vorsitzende
Jacob KOHNSTAMM

ANHANG

Artikel 4 Absatz 1 Buchstabe a



Artikel 4 Absatz 1 Buchstabe b



Artikel 4 Absatz 1 Buchstabe c