5035/01/DE/endg.
WP 56

Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU

Angenommen am 30. Mai 2002

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und 30 Absatz1 Buchstabe a und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung und insbesondere Artikel 12 und 14 -

hat folgendes Arbeitsdokument angenommen:

1. Hintergrund

Dieses Papier beschäftigt sich mit der Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts, wenn Websites, die außerhalb der Europäischen Union angesiedelt sind, personenbezogene Daten verarbeiten und insbesondere erheben[2]. Speziell in diesen Fällen soll es für die für die Verarbeitung Verantwortlichen und deren Berater ein sinnvolles Werkzeug und Bezugsdokument darstellen. Da es sich hierbei um ein äußerst kompliziertes Gebiet handelt und das Internet ein sehr dynamisches Umfeld darstellt, enthält das Papier keine endgültigen Lösungen zu allen etwaigen, dieses Thema betreffenden Fragen.

In ihrem Arbeitspapier „Privatsphäre im Internet“[3] hat die Artikel 29-Datenschutzgruppe deutlich gemacht, wie wichtig es ist, die konkrete Anwendung der Bestimmung der Datenschutzrichtlinie über das anwendbare Recht (Artikel 4 Absatz 1 Buchstabe c)[4] zu spezifizieren, vor allem mit Blick auf die Online-Verarbeitung personenbezogener Daten, wenn der für diese Verarbeitung Verantwortliche nicht in der Gemeinschaft niedergelassen ist. Die Kontrollstellen in den Mitgliedstaaten erhalten regelmäßig Anfragen von Unternehmen und Privatpersonen zu diesem Thema.

Ob nationales Recht in Fällen anwendbar ist, in denen Verbindungen zu mehreren Ländern bestehen, muss nicht nur für den Datenschutz, das Internet oder die Europäische Union festgelegt werden. Es ist eine generelle Frage des Völkerrechts, wenn Online- und Offline-Fälle wenigstens ein Element beinhalten, das mehr als ein Land betrifft. Es muss entschieden werden, welches nationale Recht anwendbar ist, bevor eine Lösung in der Sache gefunden werden kann.

---

[1] ABl. L 281 vom 23.11.1995, S. 31, verfügbar unter http://www.europa.eu.int/comm/internal_market/de/datatprot/index.htm

[2] Die Datenschutzrichtlinie 95/46/EG gilt auch im Europäischen Wirtschaftsraum (EWR). Wenn in diesem Papier von der Europäischen Union die Rede ist, sollte darunter also auch der EWR verstanden werden.

[3] “Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz“, WP 37, 21. November 2000.

[4] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31; siehe: http://europa.eu.int/eur-lex/de/lif/dat/1995/de_395L0046.html

Bei solchen Entscheidungen müssen mehrere Faktoren berücksichtigt werden; in erster Linie das Bestreben eines Staates, die Rechte und die Interessen seiner Bürger, seiner Einwohner, seiner Wirtschaft und anderer im nationalen Recht verankerten Rechtspersönlichkeiten zu schützen. In vielen Ländern erhebt das Strafrecht (also das Gegenteil der Normen, die Rechte und Freiheiten einräumen) am extensivsten Anspruch auf internationale Anwendbarkeit. Bekannte Fälle wie Yahoo![5] oder CompuServe[6] zeigen, wie die Gerichte nationales Strafrecht anwenden, um den Zugriff auf pornographische oder rassistische Inhalte ausländischer Internetserver zu verhindern. Der Bundesgerichtshof hat kürzlich eine Person verurteilt, die die „Auschwitz-Lüge" auf einer australischen Website veröffentlichte, obwohl nicht bewiesen war, dass auf diese Site tatsächlich von Deutschland aus zugegriffen wurde[7]. Nach Auffassung des Gerichts war es in diesem speziellen Fall hinreichend, dass der Inhalt des Internets „geeignet war", die öffentliche Ordnung in Deutschland zu beeinträchtigen; es war unerheblich, ob dies auch wirklich geschah.

Mit solchen international wirksamen Schutzvorschriften wollen der Gesetzgeber bzw. die Rechtsprechung die Bürger in begründeten Fällen schützen, und zwar trotz der Durchsetzungsschwierigkeiten aufgrund der grenzüberschreitenden Situation, und sie wollen diese Regeln in der Praxis anwenden, um sicherzustellen, dass das angestrebte Ziel erreicht wird.

Was das EU-Recht anbetrifft, gibt es mehrere Beispiele für dieses Streben nach Kohärenz.

Auf dem Gebiet des Wettbewerbsrechts kann die Europäische Kommission Beschlüsse fassen und Entscheidungen fällen, die sich auch auf Unternehmen außerhalb der EU auswirken, sofern diese innerhalb der EU geschäftlich tätig sind. Ein gutes Beispiel dafür liefert die kürzlich getroffene Entscheidung[8] der Kommission, den geplanten Zusammenschluss zwischen zwei US-amerikanischen Unternehmen, General Electric und Honeywell[9], zu untersagen. Laut Artikel 1 dieser im Juli 2001 getroffenen Entscheidung würde ein Zusammenschluss beider Unternehmen zu einer beherrschenden Stellung führen, die mit dem Gemeinsamen Markt nicht vereinbar ist. Die Kommission stellte fest, dass beide Unternehmen gemeinschaftsweit einen Umsatz von mehr als 250 Mio. Euro erzielen, und betrachtete den angemeldeten Zusammenschluss folglich als ein Vorhaben von gemeinschaftlicher Tragweite.

Die extraterritoriale Dimension des Gemeinschaftsrechts wird auch im Bereich des Verbraucherrechts erkennbar. Artikel 12 der Fernabsatzrichtlinie[10] besagt, dass ein

[5] TGI Paris, *Ordonnance du référé* vom 20. November 2000, http://legal.edhec.com/DTIC/Decisions/Dec_responsabilite_0.htm

[6] AG München, Urteil vom 28.05.1998 – 8340 Ds 465 Js 173158/95

[7] BGH, Urteil vom 12.12.2000, Az: 1 StR 184/00.

[8] Entscheidung vom 3.7.01 in der Sache COMP/M.2220 gemäß Artikel 8 Absatz 3 der Verordnung (EWG) Nr. 4064/89 über die Kontrolle von Unternehmenszusammenschlüssen.

[9] Dem angemeldeten Zusammenschluss lag eine Vereinbarung zugrunde, wonach Honeywell zu einer hundertprozentigen Tochter von General Electric werden sollte.

[10] Richtlinie 97/7/EG.

Verbraucher den durch diese Richtlinie gewährten Schutz nicht verliert, wenn das Recht eines Drittlands als das auf den Vertrag anzuwendende Recht gewählt wurde und dieses weniger Schutz gewährt als ihm nach dem EU-Recht zusteht. Dies gilt, wenn der Vertrag einen ‚engen Zusammenhang' mit dem Gebiet eines oder mehrerer Mitgliedstaaten aufweist[11]. Der Begriff ‚enger Zusammenhang' geht auf Artikel 7 des Übereinkommens von Rom aus dem Jahr 1980 zurück. Gemäß diesem Artikel sind bei Anwendung des Rechts eines bestimmten Staates den ‚zwingenden Bestimmungen' des Rechts eines anderen Staates, mit dem der Sachverhalt eine ‚enge Verbindung' aufweist, Wirkung zu verleihen.

Darüber hinaus verfolgt die Rechtsprechung einen ähnlichen Ansatz im Zusammenhang mit der Handelsvertreterrichtlinie[12]. Nach einem Urteil des Gerichtshofs der Europäischen Gemeinschaften[13] kann ein Unternehmer mit Sitz in einem Drittland, dessen Handelsvertreter seine Tätigkeit innerhalb der Gemeinschaft ausübt, die Bestimmungen der Richtlinie nicht schlicht durch eine Rechtswahlklausel umgehen, die das Recht eines Drittlandes als das auf das Verhältnis anwendbare Recht erklärt. Der Gerichtshof stellte fest, dass das Gemeinschaftsrecht anwendbar sein muss, wenn der Sachverhalt einen starken Gemeinschaftsbezug aufweist.

Ein weiteres praktisches Beispiel liefert die Luftfahrtindustrie. Der Rat hat eine Verordnung verabschiedet über einen ‚Verhaltenskodex im Zusammenhang mit computergesteuerten Buchungssystemen'[14]. Diese Verordnung (die vorschreibt, wie computergesteuerte Buchungssysteme zu verwenden sind) gilt für ‚alle computergesteuerten Systeme zur Buchung von Luftverkehrsprodukten …, sofern diese Systeme im Gebiet der Gemeinschaft angeboten oder benutzt werden, und zwar ungeachtet des Status oder der Staatsangehörigkeit des Systemverkäufers … oder des Standorts der entsprechenden zentralen Datenverarbeitungsanlage'. Wenn also aus der EU auf ein System zugegriffen werden kann, ist automatisch EU-Recht anwendbar, selbst wenn die zentrale Datenverarbeitungsanlage ihren Standort außerhalb der EU hat (und Daten über Endgeräte in der EU oder auf andere Weise in dieses System eingegeben werden).

Aus der Prüfung der Anwendbarkeit des EU-Rechts in diesen Fällen, die eine extraterritoriale Dimension aufweisen, kann folglich geschlossen werden, dass ähnliche Kriterien generell gelten. Unabhängig davon, ob das Verhältnis eine gemeinschaftliche Dimension oder einen starken Gemeinschaftsbezug aufweist, halten der Gerichtshof der Europäischen Gemeinschaften, das Europäische Parlament, der Rat der Europäischen Union und die Europäische Kommission es in bestimmten Situationen für angebracht, Instanzen, die nicht in der EU niedergelassen sind, dem EU-Recht zu unterstellen.

---

[11] Artikel 6 Absatz 2 der Richtlinie 93/13/EWG über missbräuchliche Klauseln in Verbraucherverträgen und Artikel 7 Absatz 2 der Richtlinie 99/44/EG zu bestimmten Aspekten des Verbrauchsgüterkaufs und der Garantien für Verbrauchsgüter sind Artikel 12 Absatz 2 sehr ähnlich. Sie stellen beide auf die Anwendung des EU-Rechts ab, und beide verwenden den Begriff ‚enger Zusammenhang'.

[12] Richtlinie 86/653/EWG.

[13] Ingmar GB Ltd. and Eaton Leonard Technologies, Rechtssache C-381/98.

[14] Verhaltenskodex im Zusammenhang mit computergesteuerten Buchungssystemen (CRS) (gemäß Verordnung des Rates Nr. 2299/89, geändert durch Verordnung Nr. 3089/93, geändert durch Verordnung Nr. 323/99).

In anderen Ländern, z. B. in den Vereinigten Staaten von Amerika, legen die Gerichte und die Rechtsvorschriften ähnliche Maßstäbe an, um ausländische Websites den innerstaatlichen Vorschriften zu unterwerfen: Das US-amerikanische Gesetz Children's Online Privacy Protection Act 1998 (COPPA) ist auch auf ausländische Websites anwendbar, die von Kindern im Hoheitsgebiet der Vereinigten Staaten personenbezogene Informationen sammeln[15]. Nach diesem Bundesgesetz muss der Betreiber einer Website, die sich an Kinder unter 13 Jahre richtet (oder die sich zwar an die Allgemeinheit richtet, von der der Betreiber aber weiß, dass sie Informationen von Kindern sammelt), die COPPA-Vorschriften beachten. Das Gesetz schreibt vor, welche Informationen ein Betreiber in seiner Bekanntmachung der Datenschutzpolitik angeben muss, wann und wie er die nachweisliche Zustimmung eines Elternteils einholen und wie er die Privatsphäre und die Sicherheit von Kindern online schützen muss. Interessant in diesem Zusammenhang ist, dass dieses Gesetz nicht speziell für US-amerikanische Unternehmen gilt, sondern für Unternehmen ‚im Internet', weshalb es für das Gesetz unerheblich ist, wo sich die Website tatsächlich befindet; entscheidend ist, dass sie in den Vereinigten Staaten geschäftlich aktiv ist. Ist dies der Fall, unterliegt die Website dem einschlägigen US-amerikanischen Recht.

Eine grobe Analyse des internationalen Rechts ergibt, dass die Staaten den Anwendungsbereich des nationalen Rechts anhand verschiedener alternativer Kriterien eher extensiv auslegen, um im Interesse eines möglichst weitgehenden Schutzes von Verbrauchern und Wirtschaft möglichst viele Fälle abzudecken. Dies hat zwangsläufig zur Folge, dass auf einen Fall mit grenzüberschreitendem Aspekt verschiedene nationale Gesetze anwendbar sind. Internationale Rechtsinstrumente versuchen daher, die ausschlaggebenden Kriterien in objektiver und nicht diskriminierender Weise festzulegen. Allerdings scheiterte der jüngste Versuch, im Rahmen der „Haager Konferenz" einen Entwurf eines Übereinkommens über das auf Vertragsverhältnisse anwendbare Recht voranzubringen, weil die Staaten sich nicht auf das ausschlaggebende Kriterium verständigen konnten. Dies verdeutlicht das Kernproblem in der Frage des anwendbaren Rechts: Die unterschiedlichen Interessen der beteiligten Länder müssen angemessen gegeneinander abgewogen werden.

Vor diesem Hintergrund muss darauf hingewiesen werden, dass die EU-Datenschutzrichtlinie das anwendbare Recht ausdrücklich regelt und ein Kriterium vorgibt. Unabhängig davon, ob diese Vorschrift einfach zu verstehen und zu handhaben ist, ist es für den Einzelnen und für die Wirtschaft doch von Vorteil, dass die Datenschutzrichtlinie sich mit dieser zentralen Frage befasst.

2. Artikel 4 der Richtlinie 95/46/EG über anwendbares Recht

Artikel 4 der Richtlinie hat folgenden Wortlaut: Anwendbares einzelstaatliches Recht

1. Jeder Mitgliedstaat wendet die Vorschriften, die er zur Umsetzung dieser Richtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten an,

[15] 15 U.S.C. § 6502 (1)(A)(I), zitiert nach Joel R. Reidenberg, siehe Fußnote 5.

a) die im Rahmen der Tätigkeit 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;

b) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht in seinem Hoheitsgebiet, aber an einem anderen Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet;

c) 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.

2. In dem in Absatz 1 Buchstabe c genannten Fall hat der für die Verarbeitung Verantwortliche einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter zu benennen, unbeschadet der Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst.

Dieser Artikel behandelt die Fälle, in denen es um die Frage geht, welches Recht auf die Verarbeitung personenbezogener Daten anwendbar ist, wenn mindestens ein Aspekt der Datenverarbeitung mehr als einen Mitgliedstaat betrifft. Beispiele: Ein Direktmarketingunternehmen stellt Versandlisten von Verbrauchern in mehreren Mitgliedstaaten zusammen und nutzt sie in einem ganz bestimmten Mitgliedstaat, damit es Werbematerial an diese Verbraucher versenden kann, oder eine US-amerikanische Website kopiert ein Cookie auf den PC einer betroffenen Person in der EU, damit die Website den PC identifizieren und diese Information mit anderen zusammenführen kann.

Die Richtlinie unterscheidet ganz allgemein zwischen Situationen, in denen die grenzüberschreitenden Aspekte lediglich die EU-Mitgliedstaaten bzw. Gebiete außerhalb der geographischen Grenzen der Union betreffen, in denen jedoch aufgrund des internationalen Privatrechts das Recht eines Mitgliedstaats gilt (der so genannte „diplomatische Fall“)[16], und Situationen, in denen die Verarbeitung Aspekte umfasst, die über die Grenzen der Europäischen Union hinausgehen[17].

Gemeinschaftsintern verfolgt die Richtlinie zwei Ziele: Sie will Lücken (in denen kein Datenschutzgesetz greift) schließen und die vielfache/doppelte Anwendung einzelstaatlicher Gesetze vermeiden. Da in der Richtlinie die Frage des anwendbaren

[16] Dieser Fall wird hier nicht behandelt. Es sei ferner darauf hingewiesen, dass die Richtlinie und mithin Artikel 4 für die Verarbeitung personenbezogener Daten, die unter Gemeinschaftsrecht fallen, sowohl durch private als auch durch öffentliche Organisationen gilt. Das vorliegende Arbeitspapier behandelt jedoch nicht die Anwendung von Artikel 4 auf Fälle des öffentlichen Bereichs.

[17] Diese Unterscheidung gilt im wesentlichen für den für die Verarbeitung Verantwortlichen. Es sollte in jedem Fall klar gestellt werden, dass die Anwendbarkeit der Richtlinie nicht dadurch beeinflusst wird, dass ein Verantwortlicher in der EU einen außerhalb der EU tätigen Verarbeiter hat. Auch in diesem Fall gilt die Richtlinie für die Gesamtheit der Verarbeitungsverfahren.

Rechts geregelt und ein Kriterium zur Bestimmung des für die Lösung eines Einzelfalls geltenden Rechts festgelegt wird, sorgt die Richtlinie selbst für eine „Konfliktregelung", so dass nicht auf andere Kriterien des internationalen Privatrechts zurückgegriffen werden muss.

Um dieses Problem zu lösen, bedient man sich in der Richtlinie des Kriteriums oder Bezugsfaktors „*Ort der Niederlassung des für die Verarbeitung Verantwortlichen*", mit anderen Worten des im Binnenmarkt üblichen Herkunftslandprinzips. Konkret bedeutet dies:

Wird die Verarbeitung im Rahmen von Tätigkeiten einer Niederlassung durchgeführt, die der Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt, sind die Datenschutzvorschriften dieses Mitgliedstaats auf die Verarbeitung anzuwenden.

Hat derselbe für die Verarbeitung Verantwortliche in mehreren Mitgliedstaaten eine Niederlassung, muss jede Niederlassung bei einer Verarbeitung im Rahmen ihrer Tätigkeiten, die Verpflichtungen erfüllen, die sich aus dem Recht des jeweiligen Mitgliedstaats ergeben. Dies ist keine Ausnahme vom Herkunftslandprinzip. Es ist lediglich seine strenge Anwendung. Hat der für die Verarbeitung Verantwortliche nicht nur eine, sondern mehrere Niederlassungen, reicht es nicht, wenn alle seine Tätigkeiten im gesamten Binnenmarkt nur dem Gesetz eines Landes genügen. Er sieht sich vielmehr der Situation gegenüber, dass für die einzelnen Niederlassungen, die Gesetze der jeweiligen Mitgliedstaaten gelten. Die Gruppe wird sich gegebenenfalls zu einem späteren Zeitpunkt mit dieser Frage beschäftigen.

Die Anwendung des Herkunftslandprinzips im Binnenmarkt ist gerechtfertigt, denn dort bieten nationale Datenschutzgesetze gleichwertigen Schutz, weil die Datenschutzrechte von Privatpersonen und die Pflichten der Wirtschaft und anderer für die Verarbeitung personenbezogener Daten Verantwortlicher harmonisiert wurden. Auf diese Weise hat das Herkunftslandprinzip, das in gewisser Hinsicht den Anwendungsbereich der nationalen Datenschutzgesetze in den Mitgliedstaaten einschränkt, keine negativen Auswirkungen auf die Rechte und Interessen der Bürger und der Wirtschaft. Selbst wenn die Gesetze eines Mitgliedstaats nicht auf jede Verarbeitung anwendbar sind, die einen Bürger dieses Staates betrifft oder im Hoheitsgebiet dieses Staates stattfindet, so hat doch die Tatsache, dass allein das Gesetz eines anderen Mitgliedstaates anwendbar ist, sehr geringe Auswirkungen, da beide Gesetze durch die Richtlinie harmonisiert und somit gleichwertig sind. Darüber hinaus schafft die Zusammenarbeit zwischen den nationalen Datenschutzbehörden unabhängig von dem jeweils anwendbaren Recht Vertrauen und gewährleistet eine wirksame Durchsetzung. [18]

Anders ist die Situation, wenn ein Verarbeiter aus einem Drittland beteiligt ist. Die Gesetze der Drittländer sind nicht harmonisiert, die Richtlinie gilt in diesen Ländern nicht und der Schutz des Einzelnen bei der Verarbeitung personenbezogener Daten ist daher möglicherweise überhaupt nicht oder nur eingeschränkt gewährleistet. Das Herkunftslandprinzip, das verknüpft ist mit der Niederlassung eines für die Verarbeitung Verantwortlichen, kann nicht mehr zur Feststellung dienen, welches Recht anwendbar ist. Es muss auf einen anderen Bezugsfaktor zurückgegriffen werden. Das Europäische

[18] Siehe Artikel 28 Absatz 6 Satz 1 der Richtlinie 95/46/EG („Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gemäß Absatz 3 übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist") sowie den letzten Satz desselben Absatzes bezüglich der Pflicht der Kontrollstellen zur gegenseitigen Zusammenarbeit.

Parlament und der Rat entschieden sich für die klassischen Bezugsfaktoren des Völkerrechts, also den physischen Zusammenhang zwischen der Handlung und einem Rechtssystem. Der EU-Gesetzgeber wählte somit das Land, in dem sich der Standort der Mittel befindet, auf die zurückgegriffen wird[19]. Die Richtlinie ist daher auch dann anwendbar, wenn der für die Verarbeitung Verantwortliche zwar nicht auf dem Gebiet der Gemeinschaft niedergelassen ist, er aber personenbezogene Daten zu bestimmten Zwecken verarbeiten will und dazu auf automatisierte oder nicht automatisierte Mittel zurückgreift, die sich im Hoheitsgebiet eines Mitgliedstaats befinden.

Mit dieser Bestimmung in Artikel 4 Absatz 1 Buchstabe c der Richtlinie 95/46/EG soll sichergestellt werden, dass der Einzelne bei Verarbeitungen außerhalb seines Landes auch dann geschützt ist, wenn der für die Verarbeitung Verantwortliche nicht im Gebiet der Gemeinschaft niedergelassen ist. Dies könnte beispielsweise einfach deshalb der Fall sein, weil der Verantwortliche eigentlich nichts mit der Gemeinschaft zu tun hat. Es wäre aber auch denkbar, dass für die Verarbeitung Verantwortliche sich außerhalb der EU niederlassen, um die Anwendung des EU-Rechts zu umgehen.

Es sei noch darauf hingewiesen, dass die betroffene Person nicht unbedingt EU-Bürger oder in der EU physisch anwesend bzw. ansässig sein muss. Die Richtlinie unterscheidet nicht nach Staatsangehörigkeit oder Ort der Anwesenheit, denn sie harmonisiert die in den Rechtsvorschriften der Mitgliedstaaten verankerten Grundrechte, die allen Menschen unabhängig von ihrer Staatsangehörigkeit zustehen. Dies bedeutet, dass es in den nachfolgend beschriebenen Fällen völlig irrelevant ist, ob die betroffene Person beispielsweise Amerikaner oder Chinese ist. Sie fällt genauso unter das EU-Datenschutzrecht wie jeder EU-Bürger. Ausschlaggebend ist allein der Ort, an dem sich die Mittel zu Verarbeitung befinden.

Der Entschluss, die Datenverarbeitung mit in der EU befindlichen Mitteln unter das EU-Datenschutzrecht zu stellen, spiegelt somit das eigentliche Bestreben des Gemeinschaftsgesetzgebers wider, Personen im Hoheitsgebiet der Europäischen Union zu schützen. Auf internationaler Ebene ist anerkannt, dass Staaten einen derartigen Schutz gewähren dürfen. Artikel XIV des GATS erlaubt Ausnahmen von den Freihandelsvorschriften zum Schutz der Persönlichkeit bei der Verarbeitung und Weitergabe personenbezogener Daten, zum Schutz der Vertraulichkeit und zum Zwecke der Durchsetzung dieser Rechtsvorschriften.

In den folgenden Abschnitten werden die Bedingungen erläutert, die bei der Bestimmung des anwendbaren Rechts ausschlaggebend sind:

2.1 Niederlassung

Der Begriff der Niederlassung in Artikel 4 Absatz 1 Buchstabe c der Richtlinie ist von Bedeutung, da der für die Verarbeitung Verantwortliche nicht im Hoheitsgebiet der Gemeinschaft niedergelassen ist. Der Ort, an dem der für die Verarbeitung Verantwortliche niedergelassen ist, setzt die tatsächliche Ausübung der Tätigkeit unter dauerhaften Bedingungen voraus und muss in Übereinstimmung mit der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften bestimmt werden. Dem Gerichtshof

[19] Dies gilt nicht, wenn die Mittel lediglich zum Zweck der Durchfuhr durch das Gebiet der Gemeinschaft verwendet werden.

zufolge umfasst der Begriff der Niederlassung die tatsächliche Ausübung einer wirtschaftlichen Tätigkeit mittels einer festen Einrichtung auf unbestimmte Zeit[20]. Diese Forderung gilt auch dann als erfüllt, wenn ein Unternehmen nur für einen bestimmten Zeitraum gegründet wird.

Ein Unternehmen, das Dienstleistungen über das Internet anbietet, gilt dort als niedergelassen, wo es seine wirtschaftliche Tätigkeit ausübt, und nicht dort, wo sich die technischen Einrichtungen für diese Website befinden oder wo auf die Website zugegriffen werden kann[21]. Beispiel: Ein Direktmarketingunternehmen ist in London registriert und entwickelt dort seine EU-weiten Kampagnen. Die Tatsache, dass es Webserver in Berlin und Paris benutzt, ändert nichts daran, dass es in London niedergelassen ist.

2.2 Der für die Verarbeitung Verantwortliche

Der *für die Verarbeitung Verantwortliche* ist ein allgemeiner Begriff der Richtlinie und bezeichnet nach Artikel 2 Buchstabe d der Richtlinie 95/46/EG die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Hinsichtlich der Niederlassung ist die Definition neutral. Sie ist umfassend, da die gesamte Verarbeitung einem oder mehreren Verantwortlichen zuortbar sein muss. Im Zusammenhang mit Artikel 4 Absatz 1 Buchstabe c der Richtlinie bedeutet dies, dass es irgendwo einen für die Verarbeitung Verantwortlichen im Sinne der Richtlinie geben muss. Es erscheint auch notwendig, dass die Verarbeitung im Laufe einer Tätigkeit erfolgt, die unter das Gemeinschaftsrecht und somit unter die Richtlinie fällt. Die Verarbeitung durch eine natürliche Person im Laufe einer rein persönlichen oder privaten Tätigkeit fällt nicht unter die Richtlinie.

Damit Artikel 4 Absatz 1 Buchstabe c der Richtlinie wirksam wird, muss der für die Verarbeitung Verantwortliche „zum Zwecke der Verarbeitung personenbezogener Daten auf … Mittel *zurückgreifen*“ (und nicht nur für die Durchfuhr verwenden), die ihren Standort im Hoheitsgebiet eines Mitgliedstaats haben[22]. Dies setzt wohl voraus, dass der für die Verarbeitung Verantwortliche eine Tätigkeit ausübt und eine bestimmte Absicht verfolgt. Seine Entscheidung über die Zwecke und die Mittel der Verarbeitung beinhaltet somit diesen Aspekt.

2.3 Mittel (“equipment”)

[20] Rechtssache C-221/89 Factortame, 1991, Slg I-3905, Randnr. 20

[21] Richtlinie 2000/31/EG, Erwägungsgrund 19

[22] Es sei darauf hingewiesen, dass das Wort “equipment” der englischen Fassung von Artikel 4 Absatz 1 Buchstabe c in anderen Sprachfassungen mit Begriffen wiedergegeben wurde, die eher dem englischen Wort “means” (Mittel) entsprechen. Die Terminologie der anderen Fassungen von Artikel 4 Absatz 1 Buchstabe c stimmt mit dem Wortlaut von Artikel 2 Buchstabe d überein, in dem der für die Verarbeitung Verantwortliche definiert ist: die Person, die über die Zwecke und “Mittel” der Verarbeitung entscheidet. Aber auch der englische Text der Richtlinienentwürfe (beispielsweise der geänderte Vorschlag von 1992) enthielt den Begriff “means”. Im Laufe der Verhandlungen wurde dieser jedoch relativ spät durch “equipment” ersetzt, wie aus dem gemeinsamen Standpunkt von März 1995 ersichtlich ist.

Die Richtlinie enthält keine Definition dieses Begriffs. Laut “Collins” (Wörterbuch der englischen Sprache) umfasst “equipment” eine Gruppe von Werkzeugen und Vorrichtungen, die zu einem bestimmten Zweck zusammengestellt wurden.
Beispiele für “equipment” sind PCs, Rechner und Server, die für fast alle Verarbeitungsarten eingesetzt werden können.

Die Richtlinie stellt klar, dass *Mittel* („equipment“) als solche automatisiert oder nicht automatisiert sein können, solange sie nicht ausschließlich für die Durchfuhr von Informationen durch das Gebiet der Gemeinschaft benutzt werden.

Ein typisches Beispiel für Mittel, die einzig zur Durchfuhr eingesetzt werden, sind die Telekommunikationsnetze (Backbones, Kabel usw.), die Teil des Internet sind und über die die Internetkommunikation vom Ausgangspunkt zum Zielpunkt geführt wird.

2.4 Verwendung der Mittel

Die Bestimmung des Umstands, wann der für die Verarbeitung Verantwortliche gemäß Artikel 4 Absatz 1 Buchstabe c der Richtlinie „zum Zwecke der Verarbeitung personenbezogener Daten auf Mittel zurückgreift“ ist von entscheidender Bedeutung für die Anwendung des Datenschutzrechts in der EU.

Die Gruppe empfiehlt, bei Anwendung dieser Bestimmung der Datenschutzrichtlinie auf konkrete Fälle äußerst vorsichtig vorzugehen. Es soll sichergestellt werden, dass die betroffenen Personen den Schutz nationaler Datenschutzgesetze genießen und dass die Datenverarbeitung von den nationalen Datenschutzbehörden überwacht wird, wo dies nötig ist, wo es sinnvoll ist und wo unter Berücksichtigung der grenzüberschreitenden Situation ein angemessenes Maß an Durchsetzbarkeit gewährleistet ist.

Eingedenk dessen ist die Gruppe der Ansicht, dass nicht jedes Zusammenwirken zwischen einem Internetbenutzer in der EU und einer Website außerhalb der EU unbedingt zur Anwendung des EU-Datenschutzrechts führt. Ihrer Auffassung nach sollten die Mittel dem für die Verarbeitung Verantwortlichen für die Verarbeitung personenbezogener Daten zur Verfügung stehen.

Dagegen ist es nicht erforderlich, dass der Verantwortliche eine umfassende Kontrolle über die Mittel ausübt. Der Umfang, in dem die Mittel dem Verantwortlichen zur Verfügung stehen, kann variieren. Der entscheidende Grad der Verfügbarkeit wird dann erreicht, wenn der Verantwortliche bestimmt, in welcher Weise die Mittel eingesetzt werden, und er damit die Ausschlag gebenden Entscheidungen hinsichtlich des Dateninhalts und der Art ihrer Verarbeitung trifft. Mit anderen Worten: Der Verantwortliche bestimmt, welche Daten in welcher Weise und zu welchem Zweck gesammelt, gespeichert, übermittelt und verändert werden.

Die Datenschutzgruppe ist der Ansicht, dass der Begriff „zurückgreifen“ zwei Tatbestandsmerkmale voraussetzt: eine Tätigkeit des für die Verarbeitung Verantwortlichen und seine Absicht, personenbezogene Daten zu verarbeiten. Dies impliziert, dass nicht jedes „Zurückgreifen“ auf „Mittel“ innerhalb der Europäischen Union die Anwendung der Richtlinie zur Folge hat.

Die Frage der Verfügungsgewalt des für die Verarbeitung Verantwortlichen sollte jedoch weder in seinem Fall noch im Falle der betroffenen Person mit der Frage verwechselt

werden, wer Besitzer oder Eigentümer der Mittel ist. De facto misst die Richtlinie der Frage keinerlei Bedeutung bei, in wessen Eigentum die Mittel stehen.

Die Interpretation der Datenschutzgruppe deckt sich mit der Begründung, die der EU-Gesetzgeber für Artikel 4 Absatz 1 Buchstabe c der Richtlinie gegeben hat. In Erwägungsgrund 20 heißt es: *„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."* Dies ist die notwendige Voraussetzung, um das weiter reichende Ziel der Richtlinie zu erreichen, nämlich *„zu vermeiden, dass einer Person der gemäß dieser Richtlinie gewährleistete Schutz vorenthalten wird"*.

3. Praktische Beispiele

In diesem Abschnitt soll versucht werden, die Leitlinien des Artikels 4 in konkrete Lösungen für typische Fälle umzusetzen. Ein Aspekt ist allen nachstehend erörterten Fällen gemein: Der Internetnutzer weiß nicht unbedingt in jedem Fall, ob die Website, die er besuchen wird und der er (wissentlich oder unwissentlich) Daten zur Verfügung stellt, in der EU oder außerhalb angesiedelt ist. Die sog. Domain-Names ohne geografische Kennung können ohne Zusatzinformationen physisch nicht zugeordnet werden, und selbst bei denen, die geografische Kennungen enthalten, gibt es keine Garantie, dass die Website tatsächlich auf einem Hostserver im angegebenen Land installiert ist.

Fall A: Cookies

Der für die Verarbeitung Verantwortliche beschließt, personenbezogene Daten mit Hilfe einer Textdatei (Cookie) zu erheben, die auf der Festplatte des Nutzer-PCs installiert wird, wobei gleichzeitig eine Kopie von der Website oder einem Dritten aufbewahrt werden kann[23]. Bei der weiteren Kommunikation greift die Website auf die in dem *Cookie* (und dem Nutzer-PC) gespeicherten Informationen zu, um den PC gegenüber dem für die Verarbeitung Verantwortlichen zu identifizieren. Der für die Verarbeitung Verantwortliche kann dadurch alle Informationen, die er in früheren Sitzungen gesammelt hat, immer wieder mit neuen Informationen verknüpfen und auf diese Weise recht detaillierte Benutzerprofile erstellen.

[23] *Cookies* sind Daten, die von einem Webserver erzeugt werden und in Form von Textdateien auf der Festplatte des Internutzers installiert werden können; eine Kopie kann bei der Website verbleiben. Sie sind normaler Bestandteil des HTTP-Verkehrs und können als solche ungehindert im IP-Verkehr übertragen werden. Ein *Cookie* kann eine eindeutige Identifikationsnummer enthalten (GUID, Global Unique Identifier), die einen besseren Personenbezug ermöglicht als dynamische IP-Adressen. Auf diese Weise hat die Website die Möglichkeit, bestimmte Nutzungsmuster und Nutzerpräferenzen zu verfolgen.

Cookies enthalten eine Reihe von URL-Adressen, für die sie gelten. Trifft der Browser wieder auf eine dieser URL-Adressen, schickt er die entsprechenden *Cookies* an den Webserver.
Es gibt unterschiedliche Arten von *Cookies*. Es gibt dauerhafte, aber auch temporäre, sogenannte "session cookies".

Cookies sind normaler Bestandteil des HTTP-Verkehrs und können als solche ungehindert im IP-Verkehr übertragen werden. Sie enthalten Informationen über den Betroffenen, die von der Website gelesen werden können, die sie gesetzt hat. Ein Cookie kann alle Informationen aufnehmen, die die Website wünscht: besuchte Seiten, angeklickte Werbung, Nutzerkennung usw.[24]

Das Set-Cookie wird in den HTTP-Antwortheader[25] gesetzt, sprich: in unsichtbare Hyperlinks. Soll das Cookie eine bestimmte Lebensdauer haben[26], wird es für diesen Zeitraum auf der Festplatte des Internetnutzers gespeichert und zu der Website zurückgeschickt, die das Cookie gesetzt hat (oder zu anderen Websites der gleichen Subdomain). Die Rücksendung erfolgt ohne Zutun des Nutzers in Form eines Cookie-Felds beim oben beschriebenen „Chattering" auf HTTP-Ebene.

Wie bereits gesagt, kann der PC eines Nutzers als ein Mittel im Sinne von Artikel 4 Absatz 1 Buchstabe c der Richtlinie 95/46/EG angesehen werden. Er befindet sich im Gebiet eines Mitgliedstaats. Der für die Verarbeitung Verantwortliche hat beschlossen, dieses Mittel zum Zwecke der Verarbeitung personenbezogener Daten zu nutzen. Wie bereits in den vorstehenden Absätzen erläutert, laufen jetzt einige technische Operationen ab, die nicht unter der Kontrolle der betroffenen Person stehen. Der für die Verarbeitung Verantwortliche verfügt damit über die Mittel des Nutzers und diese Mittel werden nicht nur zum Zwecke der Durchfuhr durch das Gebiet der Gemeinschaft verwendet.

Die Datenschutzgruppe ist daher der Ansicht, dass für die Beantwortung der Frage, unter welchen Bedingungen die personenbezogenen Daten des PC-Nutzers durch Setzen von Cookies auf dessen Festplatte erhoben werden dürfen, das Recht des Mitgliedstaates heranzuziehen ist, in dem sich der PC des Nutzers befindet.

Wie bereits in einer früheren Empfehlung der Datenschutzgruppe kurz dargelegt[27], sollte der Nutzer informiert werden, wenn die Internetsoftware ein Cookie empfangen, speichern oder versenden soll. In der Nachricht an den Nutzer sollte klar verständlich angegeben werden, welche Information zu welchem Zweck in dem Cookie gespeichert werden und wie lange das Cookie gültig sein soll. Anschließend sollte dem Nutzer die Möglichkeit geboten werden, die Zusendung oder Speicherung eines Cookie insgesamt zu akzeptieren oder zurückzuweisen; ferner sollte er bestimmen dürfen, welche Informationen beibehalten oder aus dem Cookie entfernt werden sollten, z. B. je nachdem, wie lange das Cookie gültig sein soll oder wer die sendende oder empfangende Website ist[28].

---

[24] Vgl. HAGEL III, J und SINGER, M., Net Worth: the emerging role of the informediary in the race for customer information, Harvard Business School Press, 1999, S. 275.

[25] Technisch ist es auch möglich, Cookies per JavaScript oder Meta-Tags im HTML-Code zu implementieren.

[26] Cookies ohne Verfalldatum werden als "session cookies" bezeichnet und verschwinden, wenn der Browser oder der Socket geschlossen werden.

[27] Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware - WP 17

[28] Weitere Informationen über das Wesen von Cookies und wie sie am besten zu behandeln sind, finden sich in dem Arbeitspapier WP 37 5063/00 ‚Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz'.
Auf Seite 16 findet sich eine allgemeine Beschreibung: „Cookies sind Datensequenzen, die in Textdateien abgelegt und auf der Festplatte des Internet-Nutzers gespeichert werden können, während eine Kopie

Fall B: Javascripts, Banner und andere ähnliche Anwendungen

Bei Javascripts handelt es sich um Software, die eine Website an den Computer des Nutzers versendet und die es Fremdservern ermöglicht, auf dem Nutzer-PC Anwendungen durchzuführen. Je nach Inhalt der Software können Javascripts eingesetzt werden, um Informationen einer Webseite auf dem Bildschirm darzustellen, aber auch um Viren in den Computer einzuschleusen (so genannte böswillige Java-Anwendungen) und/oder um personenbezogene Daten, die im Computer gespeichert sind, auszulesen und zu verarbeiten. Wenn der für die Verarbeitung Verantwortliche diese Instrumente verwendet, um personenbezogene Daten einzusammeln und zu verarbeiten, nutzt er Mittel im Sinne der Richtlinie und muss folglich die EU-Rechtsvorschriften beachten.

Ein Werbeunternehmen weist den Browser des Betroffenen (grob gesagt dessen Computer) aufgrund einer Vereinbarung mit Eigentümern bestimmter Sites (z. B. Sites von Suchmaschinen) an, sich nicht nur mit der von ihm gewünschten Suchmaschine zu verbinden, sondern auch mit dem Server des Werbeunternehmens. Auf diese Weise kann das Werbeunternehmen nicht nur Banner[29] auf den Bildschirm des Betroffenen senden, sondern mit Hilfe des Browsers des Nutzers auch Adress– und Inhaltsdaten sammeln, die der Betroffene an die Suchmaschine sendet. Die Bannerwerbung wird über einen unsichtbaren Hyperlink zum Werbeunternehmen auf der gewünschten Website installiert[30]. Der für die Verarbeitung Verantwortliche kontrolliert daher von seiner Niederlassung aus den Browser des Betroffenen, damit dieser die Verbindung zu einem Dritten herstellt und Informationen an diesen Dritten überträgt.

Um darüber hinaus dem Kunden die Möglichkeit zu bieten, seine Bannerwerbung möglichst gezielt einzusetzen, erstellen die Werbeunternehmen mit Hilfe von Cookies, die über einen unsichtbaren Hyperlink gesetzt werden, Profile. Bei entsprechender Konfiguration des Browsers erfährt der Nutzer, dass ein Cookie gesetzt werden soll und kann dem zustimmen oder auch nicht. Das Kundenprofil ist mit der Identifikationsnummer des Cookies des Werbeunternehmens verknüpft, so dass es jedes Mal erweitert werden kann, wenn der Kunde eine Website besucht, die mit dem Werbeunternehmen einen Vertrag hat. Auf diese Weise werden jedes Mal, wenn der Internetnutzer die Website mit dem Banner besucht, über seinen Computer und ohne sein Zutun zusätzliche personenbezogene Daten erhoben.

Die Richtlinie wäre auch auf Informationen anwendbar, die mittels sog. „Spyware“ (Spionageprogramme) erhoben werden. Dabei handelt es sich um kleine Computerprogramme, die u. a. beim Herunterladen umfangreicherer Software (z. B. einer Software zum Abspielen von Musik) heimlich auf dem Computer des Betroffenen installiert werden, um personenbezogene Informationen des Betroffenen zurückzusenden (z. B. die Musiktitel, die dieser gerne hört). Diese Softwareprogramme werden allgemein als E.T.-Anwendungen bezeichnet, da sie, sobald sie auf dem Computer des Nutzers

---

davon auf der Website verbleiben kann.“ Auf Seite 79 werden ‚Cookie-Killer‘ behandelt und die Ansätze, mit denen das Problem der Cookies gelöst werden soll, zum einen den Ansatz der Wirtschaft (Cookie-Abwehrverfahren der Softwarehersteller), zum anderen den Ansatz, den Vorkämpfer für den Schutz der Privatsphäre verfolgen, nämlich Löschprogramme wie *Cookie Washer*, *Cookie Cutter* und *Cookie Master*.

[29] Banner sind kleine Kästchen, die den Inhalt der Website überlagern oder dort integriert sind.

[30] Mehr Informationen finden Sie in Kapitel 8, Cybermarketing, von WP 37, Privatsphäre im Internet.

installiert sind und wissen, was sie wissen wollten, das tun, was auch Steven Spielbergs Außerirdischer tat: zu Hause anrufen[31].
Diese neue Kontrollsoftware bedient sich häufig JavaScripts und ähnlicher Techniken und nutzt eindeutig die Mittel des Betroffenen (Computer, Browser, Festplatte usw.), um Daten zu erheben und an einen anderen Ort zurückzusenden. Da diese Technologien per definitionem ohne Wissen des Nutzers verwendet werden (der Name Spyware spricht für sich), stellen sie eine Form der unsichtbaren und unrechtmäßigen Verarbeitung dar.

*****

Die Artikel 29 Datenschutzgruppe ist sich der Tatsache bewusst, dass es neben den beiden in den vorgenannten Abschnitten beschriebenen Beispielen weitere konkrete internetbezogene Fälle gibt, die Auslegungsprobleme aufwerfen können, zum Teil auf Grund der technischen Komplexität einiger der benutzten Systeme.

Die Datenschutzgruppe wird sich weiterhin mit diesen Fällen befassen und weitere konkrete Fälle möglicherweise im Lichte der nationalen Erfahrungen und der technischen Entwicklungen, die eine wichtige Rolle spielen könnten, zu einem späteren Zeitpunkt behandeln.

Die Gruppe weist darauf hin, dass sie auch in den Fällen, in denen die Anwendung der Richtlinie umstritten ist, beabsichtigt, die Gespräche mit Unternehmen und Organisationen in Drittländern, die personenbezogene Daten in der Europäischen Union erheben, fortzuführen, um angemessene Datenschutzstandards für die Betroffenen zu schaffen.

4. Was bedeutet dies in der Praxis?

a) Anwendung der Grundsätze über die Erhebung personenbezogener Daten

In all diesen Fällen bedeutet die Anwendung des EU-Datenschutzrechts unter anderem folgendes:

- Damit die Erhebung den Grundsätzen von Treu und Glauben entspricht und rechtmäßig erfolgt, muss der für die Verarbeitung Verantwortliche den Verarbeitungszweck eindeutig festlegen.

- Der Verantwortliche muss ferner sicherstellen, dass die Daten dem Erhebungszweck entsprechen, dafür erheblich sind und nicht darüber hinausgehen.

- Die Erhebung muss rechtmäßig sein (zweifelsfreie Einwilligung, Erfüllung eines Vertrags, Erfüllung einer gesetzlichen Verpflichtung, Wahrung der legitimen Interessen des Verantwortlichen usw.), ferner ist die betroffene Person berechtigt, auf ihre Daten zuzugreifen, sie zu berichtigen oder sie zu löschen.

- Die betroffene Person muss zumindest über die Identität des Verantwortlichen und - sofern vorhanden - seines Vertreters, den Zweck der Verarbeitung, die Empfänger sowie über ihre Rechte informiert werden[32].

[31] S. auch Titelgeschichte des Time Magazine von Adam COHEN am 31. Juli 2000: *How to protect your privacy: who's watching you? They're called E.T: programs. They spy on you and report back by "phoning home". Millions of people are unwittingly downloading them.*

- Ein anderer wichtiger Aspekt ist die Sicherheit der Verarbeitung; diese könnte es erforderlich machen, dass der Verantwortliche unmittelbar mit Beginn der Erhebung spezifische technische und organisatorische Maßnahmen ergreift, um die Daten gegen zufällige oder unrechtmäßige Zerstörung oder zufälligen Verlust, Veränderung, unrechtmäßige Weitergabe oder unrechtmäßigen Zugriff zu schützen, vor allem wenn die Daten über ein Netz übermittelt werden. Diese Maßnahmen gewährleisten ein Sicherheitsniveau, das den beschriebenen Risiken und der Art der Daten entspricht.

- Die Erhebung sensibler Daten wird in besonderen Vorschriften geregelt, die vor allem auf die Sicherheitserfordernisse abzielen[33].

Weitere Einzelheiten über die Anwendung der Datenschutzrichtlinie auf die Verarbeitung von Daten durch Websites finden sich in der Empfehlung der Datenschutzgruppe 2/2001 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union[34].

b) Verfahrenstechnische Aspekte

Gemäß Artikel 4 Absatz 2 der Richtlinie 95/46/EG hat der für die Verarbeitung Verantwortliche einen Vertreter zu benennen, der im Hoheitsgebiet des Mitgliedstaats ansässig ist, in dem sich die Mittel befinden.

Die Information über die Identität des für die Verarbeitung Verantwortlichen und über die Identität des Vertreters könnte ohne Weiteres in die Bekanntmachung der Datenschutzpolitik auf der Website aufgenommen werden oder in die allgemeinen Angaben zur Identifizierung des für die Verarbeitung Verantwortlichen auf der Website, damit der Verantwortliche der Website leicht identifiziert und kontaktiert werden kann.

Es könnte ferner empfohlen werden, weitestgehend von der Möglichkeit Gebrauch zu machen, dass ein einziger Vertreter im Namen mehrerer Verantwortlicher handelt, oder andere pragmatische Lösungen zu finden.

Was die Meldung des beabsichtigten Verarbeitungsverfahrens (vor allem die Erhebung) an die nationalen Kontrollstellen anbetrifft, bietet die Richtlinie mehrere Möglichkeiten an. Artikel 18 Absatz 1 erster Satz sieht eine Meldung des für die Verarbeitung Verantwortlichen oder seines Vertreters bei der Kontrollstelle vor, bevor die Verarbeitung oder eine Mehrzahl von Verarbeitungen durchgeführt werden. Artikel 19 Absatz 1 Buchstabe a legt fest, dass die Meldung mindestens den Namen und die Anschrift des für die Verarbeitung Verantwortlichen und seines Vertreters enthalten muss.

---

[32] Nach Artikel 10 der Richtlinie sollte der Betroffene bei Cookies die Möglichkeit haben, das Setzen eines Cookies zu akzeptieren oder abzulehnen und zu bestimmen, welche Daten vom Cookie verarbeitet werden und welche nicht.

[33] Einige Mitgliedstaaten verlangen möglicherweise eine Überprüfung vor Beginn der Verarbeitung sensibler Daten.

[34] Vgl. Empfehlung 2/2001 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union, WP43. Es sollte erörtert werden, ob alle in WP 43 genannten Elemente auch auf die Online-Erhebung von Daten in der EU anzuwenden sind, die von außerhalb der EU ansässigen Verantwortlichen durchgeführt wird.

Nach Artikel 18 Absatz 2 zweiter Gedankenstrich können die Mitgliedstaaten in zwei Fällen eine Vereinfachung oder eine Ausnahme von der Meldepflicht vorsehen: bei Kategorien von Verarbeitungsverfahren, die die Rechte und Freiheiten der Betroffenen voraussichtlich nicht beeinträchtigen, oder wenn der für die Verarbeitung Verantwortliche einen Datenschutzbeauftragten bestellt, der in unabhängiger Weise die interne Anwendung der Datenschutzvorschriften sicherstellt[35].
Die Datenschutzgruppe ist sich darüber im klaren, dass die Anwendung dieser Vorschriften möglicherweise zu praktischen Problemen führt, und wird sich wahrscheinlich zu einem späteren Zeitpunkt mit diesen Fragen beschäftigen.

c) Durchsetzung

Die Durchsetzung von Vorschriften ist auf internationaler Ebene selbstverständlich nicht so einfach wie innerhalb eines bestimmten Landes. Dies muss dem Bürger klar sein (klar gemacht werden). Es gibt jedoch einige Möglichkeiten, die im Hinblick auf ein vernünftiges Durchsetzungsniveau weiter ausgebaut werden können.

Damit die Vorschriften auf einem möglichst hohen Niveau eingehalten werden, müssten zunächst einmal sowohl die europäischen als auch die internationalen Organisationen mit den Anforderungen der Richtlinie in bezug auf die Datensammlung in der Europäischen Union vertraut gemacht werden. Eine möglichst weite Verbreitung dieser Empfehlung kann nur der erste Schritt sein. Nötig wären auch technische Lösungen, die eine vordefinierte Struktur für die Sammlung personenbezogener Daten bereitstellen und die beschriebenen Anforderungen in die zur Sammlung personenbezogener Daten verwendeten Softwareinstrumente integrieren. Die Datenschutzgruppe hat bereits auf die Möglichkeit verwiesen, Produktgenehmigungsverfahren zu entwerfen, in deren Rahmen auch die Einhaltung der gesetzlichen Anforderungen zum Schutz personenbezogener Daten geprüft werden könnte. Ein europäisches System von Labeln/Vertrauenssiegeln, das auch Websites außerhalb der EU offen steht, könnte der Grundstein einer solcher Maßnahme sein.

In einem konkreten Fall könnte ein Betroffener in der EU, der Probleme mit einer Website außerhalb der EU hat, sich darüber hinaus an die zuständige nationale Kontrollstelle wenden. Diese legt fest, ob die Richtlinie oder das nationale Datenschutzrecht anwendbar ist. Ist dies der Fall, kann die Kontrollstelle die ausländische Website kontaktieren, um den Fall zu lösen. Kommt der Fall vor ein Gericht in dem Mitgliedstaat, in dem der Betroffene ansässig ist, entscheidet das Gericht, ob es in diesem Fall zuständig ist (was nach internationalem Verfahrensrecht der Fall sein könnte, da die am stärksten betroffene Partei, nämlich der Betroffene, im gleichen Hoheitsgebiet ansässig ist wie das Gericht). Ist das Gericht zuständig, wendet es Artikel 4 der Richtlinie 95/46/EG bzw. die entsprechende nationale Umsetzungsvorschrift an und kommt gegebenenfalls zu dem Schluss, dass die ausländische Website die personenbezogenen Daten des Betroffenen unrechtmäßig und nicht nach Treu und Glauben verarbeitet hat. Viele Drittländer ermöglichen bereits die Anerkennung und Durchsetzung des Urteils; aber auch dort, wo dies nicht der Fall ist, gibt es Beispiele dafür, dass die ausländische Website dem Urteil folgt und die Datenverarbeitung im Hinblick auf eine gute Unternehmenspraxis anpasst, um ihren guten Ruf nicht zu verlieren.

[35] Bezüglich der besonderen Rechtsvorschriften, mit denen dieser Artikel der Richtlinie umgesetzt wurde, siehe http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm

In Drittländern, in denen es Datenschutzvorschriften und Kontrollstellen gibt, ist die Durchsetzung natürlich weniger problematisch.

5. Fazit

- Die Artikel 29 Datenschutzgruppe ist der Ansicht, dass die Auslegung der nationalen Rechtsvorschriften, so wie sie in diesem Arbeitspapier erfolgte, außerordentlich vorteilhaft wäre im Hinblick auf die Schaffung von Rechtssicherheit für Websites, die außerhalb der Europäischen Union niedergelassen sind. Die Gruppe ist davon überzeugt, dass ein hohes Schutzniveau für die betroffenen Personen nur erreicht werden kann, wenn Websites, die zwar außerhalb der Europäischen Union niedergelassen sind, aber wie in diesem Arbeitspapier dargelegt auf Mittel in der EU zurückgreifen, die Garantien für die Verarbeitung personenbezogener Daten insbesondere bezüglich der Datensammlung bieten, sowie die Rechte schützen, die den betroffenen Personen auf europäischer Ebene eingeräumt werden und ohnehin für alle Websites gelten, die in der Europäischen Union ansässig sind.
- Die Artikel 29 Datenschutzgruppe ist der Auffassung, dass die praxisorientierte Entwicklung eines Programms zur Förderung europäischer Datenschutzvorschriften den für die Verarbeitung Verantwortlichen in Drittländern helfen könnte, die Vorschriften besser zu verstehen, anzuwenden und einzuhalten. Ein europäisches System von Labels/Vertrauenssiegeln, das auch Websites außerhalb der EU offen steht, könnte die Grundlage für diese Maßnahme sein.

- Die Datenschutzgruppe nach Artikel 29 ersucht die Kommission, dieses Arbeitspapier bei ihrer künftigen Arbeit zu berücksichtigen.

Brüssel, den 30. Mai 2002
Für die Gruppe
Der Vorsitzende
Stefano RODOTA