WM WERTPAPIER MITTEILUNGEN Zeitschrift für Wirtschafts- und Bankrecht

1

6. Januar 1994
48. Jahrgang
Seiten 1–44

Datenschutz in Europa

– Der zweite Entwurf einer EG-Datenschutzrichtlinie und dessen Auswirkungen auf die deutsche Privatwirtschaft –

Von Dr. iur. Lic. theol. Thomas Hoeren, Münster

I. Vorüberlegungen

Informationsmanagement und Jurisprudenz stehen seit je her auf Kriegsfuß zueinander – und das aus zwei Gründen:

1. Neue Technik versus altes Recht

Der EDV-Markt hat sich im Laufe von zwanzig Jahren zu einer immer expansiveren Größe entwickelt und alle Lebensbereiche grundlegend verändert. Die Jurisprudenz fühlt sich von dieser ungeheuren Dynamik überfordert; die durch den Siegeszug des Computers eingeläutete, technologische Revolution macht die Antiquiertheit des juristischen Denkens manifest. Der Jurist arbeitet mit einem methodischen Instrumentarium, das im 19. Jahrhundert grundgelegt wurde. Er fühlt nun, daß diese Hilfsmittel untauglich werden und im DV-Zeitalter ihren Sinn verlieren.

Einen unmittelbaren Ausdruck hat dieses panische Gefühl im Datenschutzrecht gefunden[1]. Deutschland verfügt derzeit über die schärfsten Datenschutzgesetze der Welt. Bereichsspezifische Regelungen existieren für viele Bereiche (Sozialdatenschutz; Meldewesen; Post- und Fernmeldebereich). Die Verarbeitung personenbezogener Daten bei Landesbehörden werden über eigene Landesdatenschutzgesetze und entsprechende Landesdatenschutzbeauftragte überwacht.

Bundesbehörden und die Privatwirtschaft finden im Bundesdatenschutzgesetz restriktive Regelungen zum Schutz personenbezogener Daten. Bereits das erste Bundesdatenschutzgesetz aus dem Jahre 1977[2] enthielt ein Verbot der Verarbeitung jedes personenbezogenen Datums in oder aus einer Datei, das nur für einige, enumerativ aufgezählte Fälle aufgehoben wurde. Dieses Verbot ist auch im neuen BDSG enthalten, das am 1. Juni 1991 in Kraft getreten ist[3].

2. Internationale Vernetzung versus nationale Justiz

Informationsmanagement ist von seiner Struktur her keine national begrenzte Größe. Für den Austausch von Daten, für die Entwicklung von Netzstrukturen spielen nationale Grenzen technisch kaum eine Rolle. So erfreulich dieser Aspekt für „Informationsmanager" ist, so unerfreulich ist er für Juristen: Recht ist prinzipiell national, geschaffen von nationalen Gesetzgebern, durchgesetzt von nationalen Gerichten und Behörden.

Die Schwierigkeiten, die die internationale Verflechtung von DV-Netzen mit sich bringt, wird in besonderer Weise offenbar bei grenzüberschreitendem Datentransfer („Transborder data flow"; im folgenden „TBDF" abgekürzt). Dieses Phänomen stellt eines der zentralsten Probleme des Datenschutzrechtes dar[4]: Im Zeitalter umfassender Vernetzung ist es technisch mühelos möglich, daß ein deutsches Unternehmen Daten, die in einem italienischen Rechenzentrum gespeichert sind, ohne zeitliche Verzögerung abzurufen und zu nutzen. Diese Möglichkeit kann von Unternehmen geschickt ausgenutzt werden, um nationale Datenschutzgesetze zu umgehen: Paßt einem Unternehmen das nationale Datenschutzgesetz und die damit verbundene staatliche Kontrolle nicht, wickelt es alle EDV-Dienstleistungen über das Ausland ab: Alle wichtigen personenbezogenen Daten (insbesondere von Arbeitnehmern) werden in einem ausländischen Rechenzentrum gespeichert und von dort aus bei Bedarf abgerufen; dadurch sind sie grundsätzlich nicht dem unerwünschten nationalen Recht unterworfen.

Das alte BDSG kannte diese Möglichkeit noch nicht und ging hierauf nicht ein[5]; erstaunlicherweise enthält auch das neue BDSG kaum Regelungen für TBDF (vgl.

---

[1] Vgl. auch *Simitis*, TDR 1989, 23 ff.

[2] „Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 27.1.1977 – Bundesdatenschutzgesetz" (BGBl. I, S. 201). Dieses Gesetz trat am 1.1.1978 in Kraft. Vgl. hierzu den Überblick von *Simitis*, NJW 1977, 729 ff.

[3] „Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes" (BGBl. I, S. 2954). Vgl. hierzu auch *Büllesbach*, NJW 1991, 2593 ff.; *Dammann*, NVwZ 1991, 640; *Gola/Wronka*, RDV 1991, 165 ff.; *Dörr*, DB 1991, 427 ff.; *Ungnade/Gorynia*, WM 1991, 121 ff.; *Walz*, CR 1991, 364 ff.

[4] Siehe zum folgenden auch *Hamelink*, Transnational Data flow in the Information Age, 1984; *Wellington Brown*, Economic and Trade-Related Aspects of Transborder Data Flow, 1986; *Lawford/de Gapre/Gräfstein*, University of Toronto Law Journal 20 (1970), 337 ff.; *Novotny*, Comparative Law Journal 3 (1981), 111 ff.

[5] Vgl. zu dieser Problematik auch *Simitis*, Festschrift für Murad Ferid, 1978, S. 354 ff.

§ 3 Abs. 9 Satz 2; § 17). Auch die bisher vorhandenen internationalen Regelungswerke werden der besonderen Problematik des TBDF nicht gerecht[6]:

- Die Empfehlung der OECD vom 23. September 1980 hinsichtlich der Leitlinien über den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr von personenbezogenen Daten ist unverbindlich und inhaltlich zu abstrakt[7].
- Die Konvention des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten ist zwar in deutsches Recht transformiert worden[8] und damit bindend. Allerdings enthält sie nur allgemeine Rahmengrundsätze, die in unterschiedlichster Weise umgesetzt werden können. Darüber hinaus wurde sie nur von sieben EG-Mitgliedstaaten ratifiziert.

In jüngster Zeit droht TBDF zu einer großen Gefahr für die Entwicklung eines einheitlichen europäischen Binnenmarktes zu werden: Derzeit besitzen nur acht EG-Mitgliedstaaten Rechtsvorschriften zum Datenschutz (Deutschland, Dänemark, Frankreich, Irland, Portugal, Luxemburg, Niederlande und Großbritannien); alle anderen Staaten kennen keine speziellen Datenschutzgesetze. Insofern ist innerhalb Europas ein starkes Nord-Süd-Gefälle entstanden: Im Süden Europas (und zusätzlich Belgien) ist jegliche Verarbeitung von personenbezogenen Daten (noch) fast ohne jede rechtliche Beschränkung möglich, während im Norden Europas detaillierte Kontrollmechanismen geschaffen wurden. Damit entsteht aber die Gefahr, daß sich besondere „Datenoasen" herausbilden: Unternehmen könnten gefahrlos ihre Daten in Italien oder Spanien[9] verarbeiten lassen, um dem rigiden Datenschutz deutscher oder englischer Provenienz zu entgehen.

II. Aktivitäten der EG

Deshalb mußte die EG auf diesem Gebiet tätig werden[10]. Bereits 1976 hat das Europäische Parlament mehrere Entschließungen angenommen[11], in denen die EG-Kommission zur Ausarbeitung einer EG-Datenschutzrichtlinie angefordert wurde. Die EG-Kommission ließ sich jedoch mit dieser Bitte Zeit: Erst am 18. Juli 1990 verabschiedete sie ein Maßnahmenbündel zu Fragen des Datenschutzes[12]. Dieses Bündel umfaßte u. a.:

- den Vorschlag für eine Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten
- den Vorschlag für eine Richtlinie zum Schutz personenbezogener Daten im Telekommunikationsbereich.

Dieser Entwurf wurde zunächst an den Wirtschafts- und Sozialausschuß weitergeleitet, der am 24. April 1991 eine umfassende Stellungnahme hierzu abgab[13]. Am 11. März 1992 nahm das Europäische Parlament (nach entsprechenden Beschlüssen des Ausschusses für Recht und Bürgerrechte) zu dem Entwurf Stellung: Es befürwortete zwar grundsätzlich den Entwurf, verlangte aber in zahlreichen Punkten z. T. weitgehende Änderungen[14].

Die EG-Kommission erarbeitete daraufhin einen geänderten Vorschlag, der am 15. Oktober 1992 veröffentlicht wurde[15]; wann dieser Vorschlag endgültig verabschiedet wird, ist derzeit offen. Auf jeden Fall wird die Richtlinie zu erheblichen Änderungen des BDSG führen.

Von seiten der Spitzenorganisationen der deutschen Wirtschaft ist die gesamte Konzeption der Richtlinie zu Recht kritisiert worden:

„Wir sind der Meinung, daß sich eine EG-Regelung darauf beschränken sollte, Staaten ohne Datenschutzgesetz (Spanien, Portugal, Griechenland, Belgien) zum Erlaß brauchbarer Regelungen zu veranlassen, für nationale Sachverhalte ein mittleres Niveau vorgeben und sich im übrigen auf den Abbau von Hindernissen für grenzüberschreitenden Datenfluss konzentrieren sollte."[16]

Insbesondere war es nicht notwendig, den Datenschutz im öffentlichen Bereich zu regeln; der Datenfluß in diesem Bereich tangiert die Verwirklichung des Binnenmarktes nicht. Die Frage, woher die Kommission eine Kompetenz zur Regelung dieses Bereichs hernimmt, ist zumindest diskussionswürdig (s. u.).

III. Einzelheiten der geplanten EG-Richtlinie

Im folgenden sollen einige Schwerpunkte der Richtlinie dargestellt werden, die gerade aus der Sicht des privatwirtschaftlichen Informationsmanagements von großer Bedeutung sind[17].

1. Gleichstellung von privatem und öffentlichem Bereich

Die EG-Kommission hat es sich zum Ziel gesetzt, sowohl den öffentlichen wie den privaten Bereich datenschutzrechtlich in einer Richtlinie zu regeln.

---

[6] Vgl. hierzu allgemein *Mengel*, Internationale Organisationen und transnationaler Datenschutz, 1984; *Bing*, Comparative Law Yearbook 2 (1979), 149 ff.; *Hondius*, Netherlands International Law Review 30 (1983), 103 ff.; *Kirby*, Law and Computer Technology 1979, 53 ff.; *Patrick*, Jurimetrics Journal 21 (1989), 405 ff.

[7] Siehe hier *Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr, 1990, S. 520 ff.; *Bing*, Michigan Yearbook of International Legal Studies 5 (1984), 271 ff.; *Sepel*, TDR 1981, 2 ff.

[8] BGBl. 1985 II, S. 539. Vgl. zur Konvention *Henke*, Die Datenschutzkonvention des Europarats, 1986, sowie *Auernhammer*, DuD 1985, 7 ff.; *Burkert*, CR 1988, 751 ff.; *Clarana*, Revista de Instituciones Europeas 8 (1981), 1 ff.; *Simitis*, CR 1991, 161 ff.

[9] In Spanien ist allerdings zum 31. Januar 1993 ein Datenschutzgesetz in Kraft getreten; vgl. die Hinweise in Clifford Chance Computer and Communications Bulletin, März 1993, S. 3.

[10] Vgl. hierzu allgemein *Evans*, American Journal of Comparative Law 29 (1981), 571 ff.; *Papapavlou*, RDVB 1990, 113 ff.; *Riegel*, ZRP 1990, 132 ff.; *ders.*, CR 1991, 279 ff.

[11] EG-ABl. Nr. C 1000 vom 3.5.1976, S. 27, ebenso EG ABl. Nr. C 140 v. 5.6.1979, S. 34; EG-ABl. Nr. C 87 vom 5.4.1982, S. 39.

[12] KOM (90) 314 final = EG-ABl. C 277/12 vom 5.1.1990, in deutscher Übersetzung abgedruckt als BR-Drucks. 690/90 vom 4.10.1990. Der Text der Übersetzung findet sich auch in RDV 1990, 196. Vgl. zu diesem Entwurf auch die Darstellung von *Simitis*, in: Simitis/Dammann/Geiger/Mallmann/Walz, BDSG, 4. Aufl. 1992, Rdn. 153 ff.

[13] EG-ABl. C vom 17. Juni 1991.

[14] Sitzungsdokument des Europäischen Parlaments vom 15. Februar 1992, A3-0010/92, Dok. EP 160.503. Der Text findet sich in: *J. Dumortier* (Hrsg.), Recent Developments in Data Privacy Law, Leuven 1992, S. 159 ff.
Zur Kritik am ersten Entwurf des Richtlinientextes vgl. auch *Aldhouse*, International Yearbook of Law, Computers and Technology 6 (1992), 171 ff.; *Jütten*, Die Bank 1991, 345; *Steuer*, WM 1992, 7.

[15] KOM (92) 422 fin. – SYN 287 = EG-ABl. C 311/30 vom 27. November 1992.

[16] Stellungnahme vom 16. November 1992, S. 2. Ähnlich ist auch die Haltung des Bundesbeauftragten für den Datenschutz, der mehrfach erklärt hat, daß die EG-Richtlinie nur einen Mindeststandard enthalte und Änderungen des BDSG daher nach Inkrafttreten der Richtlinie nicht notwendig seien.

[17] Vgl. insgesamt zum Entwurf auch *Ellger*, CR 1993, 2 ff.; *Geis*, CR 1993, 31 ff.; *Körner-Dammann*, RDV 1993, 14 ff.; *Kopp*, RDV 1993, 1 ff.; *Schneider*, CR 1993, 35 ff.; *Skipper*, EuZW 1993, 145 ff.; *Rüpke*, EuZW 1993, 149 ff.

a) Kompetenzen der EG-Kommission

Fraglich ist allerdings, woher die EG-Kommission überhaupt eine Kompetenz zur Regelung des Datenschutzes im öffentlichen Bereich nimmt. Der Entwurf stützt sich lediglich auf Art. 100a und Art. 113 EWG-Vertrag. Beide Kompetenzregelungen stehen in einem Zusammenhang mit der Vollendung des Binnenmarktes (siehe Art. 8a EWG-Vertrag), d. h. eines Raums „ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital ... gewährleistet ist". Die „Europäische Wirtschaftsgemeinschaft" ist – wie der Name bereits besagt – durch den Bezug zu Wirtschaft und Handel gekennzeichnet. Damit unvereinbar ist eine Richtlinie, die den gesamten nationalen Staatssektor umfaßt. Zwar möge der Zugang zu einzelnen Datensammlungen der öffentlichen Hand für die Privatwirtschaft von großer Bedeutung sein; die EG-Kommission beschäftigt sich gerade im „Legal Advisory Board" der Generaldirektion XIII mit diesem Problem[16]. Dieses Einzelproblem rechtfertigt es jedoch nicht, jegliche Datenverarbeitung in Bund, Land oder Kommunen einer europäischen Einheitsregelung zuzuführen[17].

b) Probleme der Gleichstellung

Noch problematischer ist die Art und Weise, wie öffentlicher und privater Sektor in der Richtlinie geregelt werden sollen. In der ursprünglichen Fassung der Richtlinie war die Datenverarbeitung privater und öffentlicher strikt voneinander getrennt geregelt; dies war auch angesichts der unterschiedlichen Rechtsfragen in beiden Gebieten sinnvoll. Im neuen Entwurf werden beide Bereiche ineinander geregelt: Dies erleichtert nicht gerade die Lesbarkeit und Verständlichkeit der Richtlinie; im übrigen werden damit disparate Regelungskomplexe unzulässigerweise miteinander vermengt[18]. So wird zum Beispiel in Art. 13 Nr. 5 dem Betroffenen ein Auskunftsrecht bei Entscheidungen durch automatische Mittel (was auch immer das sein mag) gewährt, das sich auch auf die verwendeten Begründungen erstreckt. Dieses Recht, das sich vermutlich auf die Erstellung automatischer Verwaltungsakte im Bereich der öffentlichen Verwaltung bezieht, soll sich auch auf den privatwirtschaftlichen Bereich beziehen. Im Falle eines Vertrages per Bildschirmtext oder anderer EDV-Verfahren müßte der Betroffene die Gründe für jede Ablehnung eines Vertragsangebots mitgeteilt bekommen.

2. Anwendungsbereich

Vom Anwendungsbereich her schützt die Richtlinie alle Informationen über eine bestimmte oder bestimmbare natürliche Person; die Daten juristischer Personen sind – wie im deutschen Recht auch – nicht geschützt (Art. 1 Abs. 1 und Art. 2 lit. a). Sachlich gilt die Richtlinie für die Verarbeitung personenbezogener Daten, d. h. für deren Erhebung[19], Speicherung, Aufbewahrung, Verknüpfung, Veränderung, Benutzung, Weitergabe, Sperrung und Löschung. Die Phase der Datenerhebung ist von der Richtlinie nicht umfaßt (Art. 2 lit b n.F.); die ursprünglich vorgesehene Regelung der Anonymisierung ist – zum Bedauern der Kreditwirtschaft[20] – ersatzlos gestrichen worden.

Weiterhin fallen Akten – entgegen den Vorschlägen des Europaparlaments – nicht unter die Richtlinie; nur die automatisierte Datenverarbeitung sowie die nichtautomatisierte Datenverarbeitung in Dateien ist von der Richtlinie umfaßt (Art. 3 Abs. 1)[21]. Allerdings ist der Begriff der „Datei" in Art. 2 lit. c) so weit definiert, daß auch Akten unter den Dateibegriff fallen können[22]; zu Recht hat daher der Zentrale Kreditausschuß eine ausdrückliche Klarstellung im Richtlinientext gefordert[23].

Die Regelungen sind auf Dateien privater wie öffentlicher Stellen anwendbar. Auch die Kirchen und caritative Einrichtungen sind – anders noch als im ersten Entwurf (Art. 3 Abs. 2 lit. b a.F.) von der Richtlinie umfaßt. Nur die rein private und persönliche Verarbeitung wird von der Anwendung ausgenommen (Art. 3 Abs. 2, 2. Spiegelstrich).

3. Kollisionsrechtliche Fragen[24]

Als schwierig gestaltete sich die Regelung des räumlichen Anwendungsbereiches. Nach Art. 4 Abs. 1 lit. a des ersten Entwurfs sollte die Richtlinie für alle „in" einem EG-Mitgliedsstaat „befindlichen" Dateien gelten. Diese Regelung machte Probleme: Dateien sind nicht „befindlich"; sie sind als solche immateriell, ohne räumliche Fixiertheit. Körperlich sind die Datenträger, auf denen sich die Datei befindet. Insofern ist die Lokalisierung des Datenträgers entscheidend. – Gleichzeitig wäre nach dieser Regelung die Richtlinie auch dann anwendbar, wenn z. B. Daten amerikanischer Staatsangehöriger durch einen amerikanischen Konzern auf deutschem Boden in einer Datei geführt werden – ein m. E. wenig sinnvolles Ergebnis.

Im zweiten Entwurf wurde die Anknüpfung an den Standort der Datei daher fallengelassen. Statt dessen wird nunmehr Bezug auf den Ort genommen, an dem der Verantwortliche der Verarbeitung ansässig ist (Art. 4 Abs. 1 lit. a n.F.). Dabei bezeichnet der Begriff des „Verantwortlichen" die Einrichtung, die

- personenbezogene Daten verarbeitet oder (etwa im Wege der Auftragsdatenverarbeitung) verarbeiten läßt *und*

---

[16] Vgl. PUBLAW.2, Final Report (Europe) A report to the Commission of the European Communities on an evaluation of the implementation of the Commission's Guidelines for improving the synergy between the public and the private sectors in the information market, Luxemburg 1993 (unveröff.). Einen Überblick über den Diskussionsstand findet sich bei *Burkert*, Journal of Law and Information Science 3 (1992), 47 ff.

[17] Vgl. zur Problematik der EG-Kompetenzen auf dem Gebiet des Datenschutzes auch *Ellger*, Der Datenschutz im grenzüberschreitenden Datenverkehr, 1990, S. 434 ff.; *Karpenstein*, Gedächtnisschrift für Christoph Sasse II, 1981, 889, 900 f.; *Spannowsky*, REDP 3 (1991), 31, 39 ff.

[18] Vgl. bereits die Stellungnahme der GDD zum ersten Entwurf, vorgelegt auf der 16. DAFTA, S. 5: „Die Datenverarbeitung in der öffentlichen Verwaltung erfolgt unter völlig anderen Prämissen als in der Privatwirtschaft, da die Daten der Bürger für öffentliche Zwecke zumeist zwangsweise erhoben und verarbeitet werden."

[19] Vgl. zum Fehlen der Erhebung im ersten Entwurf *Ellger*, RDV 1991, 124.

[20] Vgl. die Stellungnahme des Zentralen Kreditausschusses vom Dezember 1992, S. 11.

[21] Für den öffentlichen Bereich bedeutet dies allerdings einen Rückschritt, da nach dem neuen BDSG Akten und Dateien vom Gesetz umfaßt sind.

[22] Datei soll demnach „jede strukturierte Sammlung personenbezogener Daten" bezeichnen; Inhalt und Ausmaß der erforderlichen Strukturierung wird – anders als im BDSG – nicht definiert.

[23] Vgl. Stellungnahme des Zentralen Kreditauschusses vom Dezember 1992, S. 5.

[24] Vgl. hierzu auch *Koch*, RDV 1991, 105 ff.

- über Zweck und Ziel der Datenverarbeitung, verwendete Daten und Verfahren sowie über die Übermittlungsadressaten entscheidet (Art. 2 lit. d).

Diese Definition macht es sehr schwer, den Verantwortlichen zu bestimmen. Schon nach geltendem BDSG ist es schwierig, Auftragsdatenverarbeitung von Funktionsübertragungen (etwa im Bereich des Outsourcing) abzugrenzen. Nach der neuen Richtlinie wäre zusätzlich zweifelhaft, ob derjenige als „verantwortlich" anzusehen ist, der nur über Zweck und Ziel der Datenverarbeitung entscheidet und alles andere in der Kompetenz der verarbeitenden Stelle beläßt.

Diese Schwierigkeiten werden durch Art. 4 Abs. 1 lit. b verstärkt. Hiernach soll die Richtlinie auch dann zur Anwendung kommen, wenn der Verantwortliche außerhalb der EG[27] ansässig ist, sofern er für seine Datenverarbeitung automatisierte oder nichtautomatisierte „Mittel" im Hoheitsgebiet eines Mitgliedsstaates verwendet. Auch hier taucht wieder der unklare Begriff der „Mittel" auf; die Begründung verweist erläuternd auf Terminals und Fragebögen. Im übrigen trifft den Verantwortlichen in diesem Fall die Pflicht zur Benennung eines im EG-Gebiet ansässigen Vertreters (Art. 4 Abs. 2).

4. Zulässigkeit der Verarbeitung personenbezogener Daten

In Anlehnung an das deutsche Recht enthält die Richtlinie Regelungen zur Zulässigkeit der Datenverarbeitung.

a) Verbot mit Erlaubnisvorbehalt

Parallel zum BDSG enthält der Richtlinienentwurf ein Verbot der Verarbeitung aller personenbezogenen Daten in oder aus Dateien, das nur ausnahmsweise in besonders gelagerten Fällen aufgehoben ist. Nach Art. 7 n.F. (= Art. 8 a.F.) ist die Verarbeitung personenbezogener Daten nur zulässig, wenn

- der Betroffene eingewilligt hat (lit. a) oder
- die Verarbeitung zur Erfüllung eines Vertragsverhältnisses bzw. zur Durchführung eines vertragsähnlichen Vertrauensverhältnisses erforderlich ist (lit. b) oder
- der Dateiverantwortliche ein berechtigtes, das Interesse des Betroffenen am Unterbleiben der Datenverarbeitung übersteigendes Interesse mit der Verarbeitung verfolgt (lit. f)[28].

Gestrichen ist gegenüber dem alten Entwurf und dem BDSG (§ 28 Abs. 1 Satz 1 Nr. 3) die Berufung darauf, daß die Daten aus jedermann zugänglichen Quellen stammen und ihre Verarbeitung ausschließlich Korrespondenzzwecken dient[29]. Keine Erwähnung findet auch die nach bisherigem deutschen Recht erleichterte Übermittlung nicht-sensibler Daten in Listenform (§§ 28 Abs. 2 Satz 1 lit. b; 29 Abs. 2 Nr. 1 lit. b BDSG)[30].

Die Einwilligung muß nach Art. 2 lit. g ausdrücklich erteilt werden; eine konkludente Einwilligung reicht – anders im BDSG (vgl. § 4 Abs. 2) – nicht aus. Die EG-Kommission will den Betroffenen gegen seinen Willen schützen. Selbst wenn die Umstände eine Einwilligung eindeutig nahelegen, muß der Betroffene noch einmal ausdrücklich sein Einverständnis erklären.

Neu ist auch, daß die Einwilligung nur wirksam sein soll, sofern der Betroffene u. a. über die Empfänger der personenbezogenen Daten informiert worden ist (Art. 2 lit. g). Es dürfte keinem Unternehmen gelingen, wirklich über alle künftigen Empfänger vorab Informationen zu erteilen. Tritt eine nicht vorgesehene Übermittlungskonstellation auf, muß der Kunde nochmals um Einwilligung gebeten werden, was zu erheblichen Verzögerungen im Wirtschaftsverkehr führen kann.

b) Sondervorschriften für sensitive Daten

Für deutsche Verhältnisse neu[31] sind die Sondervorschriften für sensitive Daten (Art. 8 n.F. = Art. 17 Abs. 1 a.F.). In Anlehnung an das französische Datenschutzgesetz und die Europaratskonvention soll jede automatisierte Verarbeitung von Daten über

- rassische und ethnische Herkunft,
- politische Meinung,
- religiöse oder philosophische Überzeugungen,
- Gewerkschaftszugehörigkeit sowie
- Gesundheit und Sexualleben

verboten sein. Hiermit wird die alte Sphärentheorie, die in Deutschland aufgrund des Volkszählungsurteils gerade erst abgelehnt worden ist, europaweit etabliert. Allerdings soll ausnahmsweise eine Verarbeitung solch sensibler Daten mit Einwilligung des Betroffenen zulässig sein (Art. 8 Abs. 2 lit. a.F.). Ferner läßt Art. 8 Abs. 2 lit. c eine Verarbeitung der obengenannten Daten zu, wenn die Verarbeitung unter solchen Bedingungen erfolgt, „daß sie die Privatsphäre und die Grundfreiheiten offenkundig nicht beeinträchtigt". Diese Klausel ist viel zu vage und abstrakt; insbesondere sollte die Verarbeitung von Daten nicht erst bei „offensichtlicher" Verletzung von „Grundfreiheiten" unzulässig sein.

Gleichzeitig verbot Art. 17 Abs. 3 des ersten Entwurfs jegliche Speicherung von Daten über strafrechtliche Verurteilungen außerhalb des öffentlichen Bereichs. Diese Vorschrift war viel zu restriktiv; in vielen Fällen sind private Organisationen auf Daten über Vorstrafen angewiesen (Kredite; Personaleinstellungen etc.). Der neue Entwurf behält das Verbot bei (Art. 8 Abs. 4 n.F.), beläßt aber den Mitgliedstaaten die Möglichkeit, Ausnahmen zuzulassen.

5. Der betriebliche Datenschutzbeauftragte

Viel zu spät[32] wurde von deutschen Institutionen ein weiteres Charakteristikum des Richtlinienentwurfs bemerkt:

Der betriebliche Datenschutzbeauftragte, eine deutsche Sondereinrichtung, ist in dem Entwurf nicht mehr erwähnt. Von Selbstregulierung und Verpflich-

---

[27] Der Entwurf spricht fälschlicherweise vom „Hoheitsgebiet der Gemeinschaft".

[28] Dieses typisch deutsche Element der Richtlinie ruft aus der Sicht anderer EG-Staaten große Verständnisprobleme hervor; insbesondere die Redeweise von „legitimate interests" stößt bei britischen Juristen auf Verwunderung. Siehe hierzu *Skupper*, EuZW 1993, 145, 147.

[29] Vgl. *Rüpke*, EuZW 1993, 149, 153.

[30] Vgl. hierzu auch *Rüpke*, EuZW 1993, 149, 154.

[31] Siehe zur bisherigen Rechtslage auch *Simitis*, Festschr. für Pderazzini, 1990, S. 469 ff.

[32] Vgl. zur Kritik am Verhalten der Fachverbände CR 1993, 62, 192 und 327.

zur Einrichtung eigener betrieblicher Kontrollinstitutionen ist nicht mehr die Rede[33].

a) Stellung der Aufsichtsbehörden

Statt dessen werden die Befugnisse der Aufsichtsbehörden gegenüber dem bisherigen deutschen Stand deutlich verstärkt. Nach Art. 30 Abs. 1 n.F. ist in jedem Mitgliedstaat mindestens eine unabhängige staatliche Behörde einzurichten, die für die Kontrolle[34] des Datenschutzes zuständig ist; dabei besteht die Möglichkeit, zwischen Landesbehörden, Landes- und Bundesdatenschutzbeauftragten zu differenzieren.

Die staatlichen Kontrollinstanzen haben Untersuchungsbefugnisse, insbesondere

- das Recht auf Zugriff zu Daten und
- das Recht zur Einholung erforderlichen Informationen. Im Vergleich zum BDSG, das lediglich Anordnungen zur Datensicherheit zuließ (§ 38 Abs. 5 Satz 1), stehen der Aufsichtsbehörde nunmehr weitreichende Eingriffsbefugnisse zu (Art. 30 Abs. 2), etwa
- Sperrung oder Löschung von Daten,
- Verbot der Verarbeitung,
- Vernichtung eines Datenträgers oder
- Befugnis zur Verwarnung des Verantwortlichen (etwa im Rahmen eines Bußgeldverfahrens).

Im übrigen haben sie die Befugnis, die Justizbehörden bei Feststellung von Datenschutzverstößen einzuschalten. Hier bleibt allerdings unklar, ob die Aufsichtsbehörden damit Strafverfolgungsmaßnahmen unabhängig davon einleiten können, ob es sich um ein Antragsdelikt handelt (vgl. § 43 Abs. 4 BDSG).

b) Konsequenzen für den betrieblichen Datenschutzbeauftragten

Im Ergebnis ist damit das deutsche Selbstregulierungskonzept ad absurdum geführt: Statt betrieblichen Datenschutzbeauftragten werden in Zukunft staatliche Behörden die Datenschutzkontrolle über die betriebliche Datenverarbeitung übernehmen[35]. Entgegen der Ansicht von *Walz*[36] brauchen die Unternehmen auch im Rahmen ihrer nach Art. 17 n.F. bestehenden Datensicherheitspflichten nicht einen eigenen Datenschutz- (oder besser Datensicherheits-) Beauftragten zu bestellen. Sie können dies tun, brauchen dies aber nicht.

Die Richtlinie hindert demnach die Unternehmen nicht daran, freiwillig Datenschutzbeauftragte einzurichten. Sie sind dazu jedoch nicht verpflichtet; insbesondere wird die Stellung eines solchen Beauftragten nicht mehr dergestalt weisungsfrei und unabhängig sein können/müssen wie nach dem BDSG (vgl. § 36 Abs. 3). Auch das Aufgabenfeld eines solchen Beauftragten dürfte nicht mehr das gleiche sein: Statt umfassender Datenschutzkontrolle werden Erfüllung der Meldepflichten (s.u.), Datensicherheitsvorkehrungen und Schulung der Mitarbeiter im Vordergrund stehen[37]. Die Richtlinie hindert im übrigen zwar den deutschen Gesetzgeber daran, für Unternehmen mit Sitz in Deutschland an der Pflicht zu Bestellung der Datenschutzbeauftragten festzuhalten; nur für ausländische Unternehmen käme eine solche (bußgeldbewehrte) Pflicht nach der Umsetzung der Richtlinie nicht mehr in Betracht. Eine solche Inländerdiskriminierung wäre allerdings kaum wünschenswert.

6. Meldepflichten

Art. 18 Abs. 2 und 3 n.F. sieht – in Anlehnung an das französische Recht und den britischen Data Protection Act[38] – bei automatisierter Verarbeitung personenbezogener Daten weitreichende Meldepflichten vor. Dies ist dem deutschen Recht fremd, das bislang eine Pflicht zur Registrierung von Dateien nur bei geschäftsmäßiger Speicherung zum Zwecke der Übermittlung oder im Bereich der Auftragsdatenverarbeitung vorsieht (§ 32 BDSG). Die Einführung einer umfassenden Meldepflicht erstaunt darüber hinaus insofern, als der britische Data Protection Registrar die Registrierung erst im Juni 1991 als überflüssig kritisiert hat[39]; er hat selbst eine Einschränkung der Meldepflichten auf sensible Daten gefordert[40].

a) Umfang der Meldungen

Mit der Umsetzung der Richtlinie werden alle Unternehmen verpflichtet sein, der Kontrollbehörde folgende Angaben mitzuteilen:

- Name und Anschrift des Verantwortlichen und seines Vertreters
- Zweckbestimmung der Verarbeitung
- Kategorien der betroffenen Personen
- Beschreibung der verarbeiteten Daten
- mögliche Datenempfänger
- geplante Transfers in Drittländer
- Beschreibung der Datensicherungsmaßnahmen
- alle Änderungen obiger Daten.

Von diesen Meldepflichten können bestimmte, ‚harmlose' Verarbeitungskategorien ausgenommen werden (Art. 19 n.F.), wie etwa das Erstellen von Dokumenten, die Erfüllung gesetzlicher Pflichten oder die Abfrage öffentlich zugänglicher Datenbanken. Allerdings ist eine solche Befreiung nur im Einzelfall durch die Kontrollbehörde oder nach Anhörung der Kontrollbehörde möglich. Unter diese Exemtionsregeln sollen etwa 80% aller Verarbeitungsvorgänge fallen[41].

Die Gesellschaft für Datenschutz und Datensicherung (GDD) hat in einer Studie errechnet, daß aufgrund dieser Meldepflichten „mit monatlich ca.

---

[33] Anders allerdings die Auslegung von *Körner-Dammann*, RDV 1993, 14, 20: „Der betriebliche Datenschutzbeauftragte wird folglich durch die Richtlinie nicht tangiert."

[34] Die GDD vermutet an dieser Stelle zu Recht eine irreführende Übersetzung, vgl. die Ausführungen von *Bernd Hentschel*, GDD-Mitteilungen 1992, Heft 5/6, S. 6. Art. 30 verweist in der englischen Fassung darauf, daß die Behörde die Aufgabe habe, „to supervise the protection of personal data". Diese wird in der deutschen Fassung mit „Gewährleistung des Schutzes personenbezogener Daten" übersetzt.

[35] So auch *Geis*, CR 1993, 31 ff., *Schneider*, CR 1993, 38.

[36] DuD 1993, 134 f.

[37] *Kopp*, RDV 1993, 1, 8 geht allerdings davon aus, daß die Aufsichtsbehörde eine Befreiung von der Meldepflicht mit der Pflicht zur Bestellung eines Datenschutzbeauftragten verbinden lasse. Davon steht allerdings nichts in der Richtlinie; im übrigen ist damit auch noch nicht gesagt, welche Stellung und welcher Aufgabenbereich einem solchen Datenschutzbeauftragten zukommen soll.

[38] Vgl. dazu *Skipper*, EuZW 1993, 145, 146. Einen Überblick über den englischen Data Protection Act 1984 gibt *Walden*, Data protection, in: Reed (Hrsg.), Computer law, 2. Aufl., London 1993, 273 ff.

[39] Seventh Report of the Data Protection Registrar, London, June 1991, S. 14. Die Berichte finden sich vollständig dokumentiert in *Chalton/Gaskill* (Hrsg.), Encyclopedia of Data Protection, Loseblattausgabe, Stand: März 1993, Pt. 4.

[40] Draft EC General Directive on Data protection syn 287, Views of Data Protection Registrar, veröffentlicht in: *Chalton/Gaskill* (Hrsg.), a.a.O., Rdn. 4-574.

[41] Vgl. *Kopp*, RDV 1993, 1, 7.

5 000 Meldungen für neu angelegte Dateien in der zentralen EDV und in PCs und mit ca. 175 000 Meldungen für im Aufbau veränderte Dateien aus einem Kreis von 120 bis 140 Unternehmen zu rechnen" sein wird[42]. Zu Recht wird in der Studie auf die enorme Belastung der Unternehmen durch ein solch bürokratisches Meldeverfahren hingewiesen.

Selbst wenn man eine obligatorische Meldepflicht für sinnvoll hielte, ist der Katalog der zu meldenden Daten als unannehmbar anzusehen, da er die Grenzen des Möglichen sprengt. Statt auf generelle Verarbeitungsarten abzustellen, werden Einzelinformationen über konkrete Datensätze der Meldepflicht unterworfen. Jede Änderung etwa der Datensicherungsmaßnahmen oder des Verantwortlichen ist künftig zu melden; dadurch wird das Unternehmen dazu gezwungen, permanent umfangreiches Material an die Meldebehörden weiterzuleiten.

b) Prüfung eingegangener Meldungen

Nach der Meldung überprüfen die Kontrollbehörden, ob eine Datenverarbeitung geplant ist, die hinsichtlich der Rechte und Freiheiten von Personen besondere Risiken aufweisen (Art. 18 Abs. 4). Ist dies der Fall, gibt die Behörde nach spätestens 15 Tagen das Ergebnis ihrer Prüfung bekannt. Unklar bleibt allerdings, was die Behörde in den 15 Tagen eigentlich prüfen soll, insbesondere ist nach dem Wortlaut des Entwurfs unklar, ob jede risikoreiche Verarbeitung bereits per se verboten sein soll[43].

Diese Unsicherheit ist um so bedauerlicher, als die unklaren Begriffe in Art. 19 n.F. wiederverwendet werden. Nach dieser Vorschrift sollen die Mitgliedstaaten ihren Kontrollbehörden erlauben können, im Einzelfall auf die Einhaltung der Meldepflicht ganz oder teilweise zu verzichten, sofern „Verarbeitungen (sic!) ... die Rechte oder Freiheiten der betroffenen Personen nicht beeinträchtigen".

Im übrigen läßt der Entwurf den Mitgliedstaaten die Möglichkeit, „gewisse" risikoreiche Handlungen einer „vorherigen Genehmigung" (eine contradictio in adiecto) durch die Kontrollbehörde zu unterwerfen (Art. 18 Abs. 5).

Die gemeldeten Daten werden im übrigen in einem Register gespeichert (Art. 21 n.F.). Dieses Register kann von jedermann eingesehen werden. Angesichts der sehr weitreichenden Meldepflicht erscheint dieses Einsichtsrecht als zu weitreichend; es ist daher zu hoffen, daß Deutschland von der Möglichkeit Gebrauch macht, nach Art. 14 Abs. 1, 21 n.F. das Einsichtsrecht zum Schutz des Unternehmens und des Betroffenen einzuschränken.

7. Grenzüberschreitender Datentransfer

Eine besondere Bedeutung spielen die Regelungen zum grenzüberschreitenden Datenaustausch, die daher im folgenden ausführlicher dargestellt werden sollen[44].

a) Datentransfer innerhalb der EG

Nach Art. 1 Abs. 2 n.F. dürfen die Mitgliedstaaten den freien Verkehr personenbezogener Daten untereinander nicht aus Gründen des Datenschutzes beschränken. Man entnimmt aus dieser Regelung, daß der Datenschutzstandard innerhalb der EG mit Umsetzung der Richtlinie einheitlich sein wird und soll. Innerhalb dieses europäischen Datenraums sei dann jede nationale Beschränkung des Datenverkehrs unzulässig sein. Beschränkungen dürfen nur noch auf die EG-Richtlinie, nicht aber auf nationale Sonderregeln gestützt sein[45]. Ob dieses Ideal wirklich erreicht wird, ist aber nach der Neukonzeption des Richtlinientextes äußerst fraglich. Der zweite Entwurf der Richtlinie enthält zahlreiche nationale Vorbehalte (Art. 5 Abs. 2; 8 Abs. 3 und Abs. 4 und 5; 10 Abs. 1; 12 Abs. 3; 14 Abs. 1 und 3 u. a.); insoweit werden die Mitgliedstaaten weiterhin eigene Wege gehen können.

b) Datentransfer in Drittstaaten

Anders als der EG-Binnentransfer gestaltet sich die Regelung zum Export von Daten in Drittstaaten, d. h. in Staaten, die nicht der EG angehören, schwieriger.

aa) Erster Entwurf

Der erste Entwurf der Richtlinie enthielt noch rigorose Beschränkungen des Datenaustausches mit Drittstaaten.

Nach Art. 24 Abs. 1 a.F. sollten personenbezogene Daten nach Drittstaaten nur bei Vorliegen eines „angemessenen Schutzniveaus" übermittelt werden. Ausnahmsweise sollte ein Datentransfer auch in Staaten zulässig sein, die kein angemessenes Schutzniveau einhalten (Art. 25 a.F.). Hierzu war jedoch erforderlich, daß der Dateiverantwortliche glaubhaft macht, daß ein angemessenes Schutzniveau sichergestellt ist, die EG-Kommission und alle Mitgliedstaaten vorher unterrichtet worden sind und binnen zehn Tagen keinen Widerspruch erheben. Diese Regelung war viel zu bürokratisch; sie hätte dazu geführt, daß in vielen Fällen notwendige Daten nicht ins Ausland transferiert werden können[46].

bb) Der geänderte Vorschlag

Die Regelungen zum grenzüberschreitenden Datenverkehr wurden in Europaparlament und EG-Kommission grundlegend überarbeitet.

(1) Angemessenes Schutzniveau

Der geänderte Entwurf behält zunächst teilweise die Terminologie des ersten Vorschlags bei. Ein Datentransfer in einen Drittstaat ist nur zulässig, sofern

---

[42] GDD, Mitteilungen 1992, Heft 5/6, S. 10.

[43] Vgl. auch *Wind/Siegert*, CR 1993, 53.

[44] Vgl. zu den bisher ergangenen Gerichts- und Verwaltungsentscheidungen bei grenzüberschreitendem Datentransfer *Vassilaki*, An empirical survey of cases concerning the transborder flow of personal data, in: The Computer Law and Security Report Int., Heft 9, S. 33 ff.

[45] Vgl. zu Auswirkungen auf vertragliche Vereinbarungen zum Datenschutz *Ehmann*, CR 1991, 234 ff.

[46] Vgl. zur Kritik am alten Entwurf *Hoeren*, Electronic Data Interchange the perspectives of private international law and data protection, in: Law, Computers & Artificial Intelligence 1 (1992), S. 325 ff.

Drittstaat ein angemessenes Schutzniveau gewährleisten kann (Art. 26 n.F.). Wann ein solches Schutzniveau vorliegt, bleibt aber auch im neuen Entwurf unklar[47]. Offen ist z. B., ob das EG-Recht oder das nationale Datenschutzrecht als Maßstab dienen soll. Beides ist nach dem zweiten Entwurf nicht identisch, da dieser Entwurf weitreichende nationale Vorbehalte enthält (s. o.). Es wird in Zukunft also kein einheitliches EG-Datenschutzrecht geben, was die Frage des „angemessenen Datenschutzniveaus" verschärft. Im übrigen kann das Recht des ausländischen Staates nicht nur an der Meßlatte seiner Gesetze gemessen werden; vielmehr ist die Umsetzung dieser gesetzlichen Regelungen in der Praxis erforderlich. Neben dem geschriebenen Recht sind Rechtsprechung und die Tätigkeit der Aufsichtsorgane zu beachten; dabei sind auch zeitliche Veränderungen zu berücksichtigen. All dies läßt eine Prüfung der Angemessenheit fast aussichtslos erscheinen.

Schließlich ist nicht klar, wer die Angemessenheit feststellt. Daß die EG-Kommission autoritativ Feststellungen zum Datenschutzrecht in allen Staaten der Welt trifft, klingt utopisch. Wenn aber nicht die EG-Kommission die Angemessenheit prüft, bleibt die Entscheidung dem einzelnen Mitgliedsstaat oder gar dem privaten DV-Anwender überlassen. Angesichts der damit verbundenen unterschiedlichen Prüfungsergebnisse bleibt die Idee einer Vereinheitlichung des internationalen Datentransfers auf der Strecke.

(2) Ausnahmen

Der neue Entwurf erlaubt in mehreren Fällen einen Transfer von Daten auch in ein Land ohne hinreichendes Datenschutzniveau (Art. 26 Abs. 1 n.F.):

(a) Vorvertragliche Einwilligung

Ein solcher Datentransfer soll zulässig sein, wenn der Betroffene im Rahmen vorvertraglicher Beziehungen seine Einwilligung gegeben hat. Eine Ausnahme soll dann gelten, wenn ein Mitgliedsstaat bei besonders sensiblen Daten[48] eine Einwilligung des Betroffenen nicht zuläßt.

Auffällig ist die paternalistische Tendenz der Richtlinie. Eine Einwilligung des Betroffenen in den Datentransfer soll – anders als nach § 4 Abs. 1 BDSG – nur im Zusammenhang vorvertraglicher Beziehungen zulässig sein. In allen anderen Fällen soll eine Einwilligung nicht möglich sein. Dies ist unhaltbar. Das Datenschutzrecht dient dem Schutz des Betroffenen hinsichtlich der Verarbeitung seiner Daten. Wenn der Betroffene nun auf diesen Schutz nach entsprechender Aufklärung ausdrücklich verzichtet, darf ihm eine Regelung nicht diesen Schutz gegen seinen Willen aufzwingen wollen. Es muß daher für den Betroffenen generell möglich sein, in jedweden Datenexport einzuwilligen[49].

(b) Aufklärung des Betroffenen

Im übrigen soll der Datenexport in ein Land ohne angemessenes Datenschutzniveau auch dann zulässig sein, wenn ein solcher Transfer für die Erfüllung eines Vertrages zwischen dem Betroffenen und der übermittelnden Stelle erforderlich ist und der Betroffene über die datenschutzrechtlichen Lücken informiert worden ist. Gerade die Pflicht zur Unterrichtung des Betroffenen wird die Unternehmen schwer treffen. Denn selbst wenn der Auslandsbezug eines Vertrages für alle Beteiligten offensichtlich ist, muß der Betroffene über den datenschutzrechtlichen Stand im Drittland informiert werden. Dies erscheint überbürokratisch[50].

Zu Recht verweist die bereits erwähnte Stellungnahme des Arbeitskreises Datenschutz der Spitzenorganisationen der Wirtschaft auf die Folgen, etwa für die Bankwirtschaft:

> „Dieser Unterrichtungspflicht würde ein Kreditinstitut bei der Entgegennahme eines internationalen Zahlungsauftrages nicht mit hinreichender Verläßlichkeit nachkommen können. Zum einen gehen den Kreditinstituten internationale Zahlungsaufträge vielfach postalisch zu, so daß eine unmittelbare Unterrichtung des Kunden nicht erfolgen kann. Der Zahlungsauftrag müßte bis zur erfolgten Information des Kunden unausgeführt bleiben; dies würde dem Interesse des Kunden an einer unverzüglichen Auftragsausführung widersprechen.
>
> Zum anderen ist dem auftragnehmenden Kreditinstitut nicht in jedem Fall bekannt, über welche Drittstaaten ein internationaler Zahlungsauftrag geleitet wird. Dies wird oftmals von der Entscheidung nachgeschalteter Clearing-Stellen abhängen"[51].

Es fragt sich, wie die Bankwirtschaft künftig der Verpflichtung nachkommen soll, Zahlungsaufträge unverzüglich auszuführen. Erteilt der Kunde einen Zahlungsauftrag schriftlich (was in der Praxis häufig vorkommt), dürfte die Bank diesen Auftrag zunächst nicht ausführen, solange sie ihren Informationspflichten nicht nachgekommen ist. Selbst wenn der Kunde vorab auf eine Information verzichtet oder die datenschutzrechtliche Situation im jeweiligen ausländischen Staat kennt, muß die Bank vor Ausführung des Zahlungsauftrages informieren. Darin liegt eine Absurdität, die nur durch Aufhebung der Informationspflicht behoben werden kann.

(3) Ausnahmeregelung (Art. 27)

Daten dürfen nach Art. 27 n.F. auch dann ausnahmsweise in einen Drittstaat ohne angemessenes Datenschutzniveau transferiert werden,

- wenn der Verantwortliche ausreichende Nachweise dafür erbringen kann, daß die tatsächliche Wahrnehmung der Rechte des Betroffenen gewährleistet ist und
- der Mitgliedstaat nach Unterrichtung der Kommission und der anderen Mitgliedstaaten das Vorhaben genehmigt hat.

Den Nachweis der Sicherung der Rechte kann der Verantwortliche durch die Vorlage von „geeigneten vertraglichen Bestimmungen" bringen. Was darunter zu verstehen ist, bleibt unklar. Zwar sind in jüngster Zeit Musterverträge für den internationalen Daten-

---

[47] Vgl. auch zur Kritik aus amerikanischer Sicht *Epperson*, Contracts for Transnational Information services, Securing Equivalency of Data Protection, in: Harvard International Law Journal 22 (1991), 157, 162 ff.

[48] Siehe hierzu die obigen Ausführungen zu Art. 8 a n.F.

[49] So auch *Ellger*, CR 1993, 2, 8.

[50] So auch *Ellger*, CR 1993, 8.

[51] Stellungnahme vom 16.11.1992, S. 22.

transfer entwickelt worden[52]. Diese Verträge sind jedoch als Vereinbarungen zugunsten des betroffenen Dritten zu konzipieren, was z. B. nach englischem Recht aufgrund des dortigen Grundsatzes der „privity of contract" nicht möglich ist. Im übrigen wirft der Vertrag zugunsten Dritter eine Reihe ungelöster Rechtsfragen auf, wie etwa das Problem, ob eine Vertragspartei auch ohne Zustimmung des betroffenen Dritten den Vertrag auflösen könnte[53].

IV. Konsequenzen für das deutsche Recht

Aus deutscher Sicht wird sich durch die EG-Richtlinie das Datenschutzszenario entscheidend ändern. Für die Privatwirtschaft bestehen die wichtigsten Änderungen in

- der Abschaffung der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten
- den weitreichenden Meldepflichten
- den neuen Beschränkungen für grenzüberschreitenden Datenverkehrs.

Gerade diese Änderungen führen dazu, daß die deutsche Wirtschaft den Plänen der EG-Kommission zum Datenschutz von Anfang an skeptisch gegenüberstand. Die GDD hat im Herbst letzten Jahres eine Umfrage unter deutschen Unternehmen zur geplanten EG-Datenschutzrichtlinie durchgeführt. Hiernach versprachen sich 45% der befragten 110 Unternehmen keine Auswirkungen der Richtlinie auf den Abbau von Wettbewerbsverzerrungen; 32,4% beurteilten die Auswirkung sogar negativ. Kritisiert wurde vor allem der erhöhte Aufwand für Verwaltung (53,4%), und Personal (46,2%)[54].

Diese Befürchtungen sind – wie oben gezeigt – realistisch. Man kann nur hoffen, daß die EG-Richtlinie in der Form, wie sie derzeit geplant ist, nicht in Kraft tritt. Eine Arbeitsgruppe des Ministerrats hat noch einmal am 14. und 15. April sowie am 3./4. Juni 1993 über den Entwurf beraten, um bis zum Ende des Jahres einen gemeinsamen Standpunkt von Parlament und Kommission präsentieren zu können. Anfang 1994 soll die Richtlinie dann in Kraft treten und bis zum 1. Juli 1994 umgesetzt werden; dabei ist eine Übergangsfrist für „Altdateien" bis zum 1. Juni 1997 vorgesehen[55].

Die Diskussion in Deutschland zu diesem Thema ist allerdings noch zu schwach. Immer wieder wird auf den weiterbestehenden hohen Schutzstandard in Deutschland hingewiesen, demgegenüber die EG-Richtlinie nur Mindestregeln und keine besonderen Änderungen vorgebe[56]. In den Unternehmen wird das Thema „Datenschutz" darüber hinaus als marginales Spezialgebiet der betrieblichen Datenschutzbeauftragten oder der Rechtsabteilung angesehen[57]. Es wird hierbei übersehen, daß datenschutzrechtliche Bestimmungen massiv in das Informationsmanagement eines Unternehmens eingreifen: Datenschutz *kann* ein solches Informationsmanagement unmöglich machen; er *kann* aber auch ein solches Management fördern. Alles hängt davon ab, wie Datenschutz konzipiert ist. In dieser Hinsicht kommt es jetzt darauf an, daß die deutsche Wirtschaft die Weichenstellung in Brüssel nicht einfach gleichgültig hinnimmt, sondern sie entscheidend in ihrem Sinne beeinflußt[58].

---

[52] Vgl. den Modellvertrag des Europarats in CR 1993, 64, die Klauseln dieses Vertrages sind kommentiert bei *Pitrat*, Histoire des clauses ou comment l'esprit vient un Comt, Vortragsmanuskript des ICC-Symposiums „Model Contract clauses and their Use in Transborder Data Flows" (Brüssel, 6. Mai 1993). Siehe ferner die Hinweise im 8 Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten 1989, S. 130 f. und im 10. Tätigkeitsbericht (1991), S. 162.

[53] Vgl. hierzu *Napier*, Contractual Solutions to the problem of Equivalent Data Protection in Transborder Data flows, Luxembourg 1990 (unveröff.). Kritisch im übrigen auch *Ehmann*, CR 1991, 234, *Körner-Dammann*, RDV 1993, 14, 18, *Simitis*, RDV 1990, 3, 12.

[54] GDD (Hrsg.), Auswertung der Erhebung über die möglichen Auswirkungen der geplanten EG-Datenschutzrichtlinie auf die Wirtschaft – Durchgeführt im Herbst 1992 und vorgelegt zur 16. DAFTA am 12. bis 13. November 1992 in Köln, S. 10. Vgl. allerdings zur methodischen Kritik an dieser Studie CR 1993, 254 f.

[55] Die Interpretation dieser Regelung ist allerdings unklar. Zu Recht verweist der Zentrale Kreditausschuß darauf, daß nur eine Interpretation akzeptabel ist, wonach der Altbestand der bis zum 1. Juli 1994 erstellten Dateien von den neuen Regelungen nicht berührt sind; vgl. die Stellungnahme des Zentralen Kreditausschusses vom Dezember 1992, S. 6.

[56] Vgl. etwa *Körner-Dammann*, RDV 1993, 14, 19 f.

[57] So auch das Ergebnis der oben erwähnten GDD-Umfrage, S. 10.

[58] Vgl. zur Stellung der Aufsichtsbehörden gegenüber den EG-Plänen CR 1993, 252 ff.