DATENSCHUTZGRUPPE NACH ARTIKEL 29

5019/02/DE

WP 46

VIERTER JAHRESBERICHT

ÜBER DEN STAND DES SCHUTZES NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN UND DES SCHUTZES DER PRIVATSPHÄRE IN DER GEMEINSCHAFT UND IN DRITTLÄNDERN

BERICHTSJAHR 1999

Angenommen am 17. Mai 2001

A: 1999 in dem jeweiligen Land angenommene legislative Maßnahmen im Bereich der ersten Säule der EU, die sich auf den Schutz der Privatsphäre und den Datenschutz ausgewirkt haben (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG).

B: 1999 in dem jeweiligen Land durchgeführte Änderungen beim Datenschutzes und beim Schutz der Privatsphäre im Bereich der zweiten und dritten Säule der EU.

C: Rechtsprechung (nationale Gerichte)

D: Spezifische Themen

E: Websites

Die durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1] eingesetzte

GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN hat,

unter Berücksichtigung der Artikel 29 und Artikel 30 Absatz 6 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf die Artikel 12, 13 und 15,

den vorliegenden Bericht angenommen:

1. EINFÜHRUNG

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten[2] legt ihren vierten Jahresbericht für das Jahr 1999 vor. Der Bericht richtet sich an die Kommission, das Europäische Parlament und den Rat ebenso wie an die breite Öffentlichkeit. Die Gruppe ist das unabhängige Beratungsgremium der EU zum Thema Datenschutz und Privatsphäre[3]. Ihr Jahresbericht soll einen Überblick über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und in Drittländern[4] geben.

---

1 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, Amtsblatt L 281 vom 23.11.1995, S. 31, verfügbar unter:

http://europa.eu.int/comm/*internal_market*/de/dataprot/index.htm

2 Eingesetzt durch Artikel 29 der Richtlinie 95/46/EG. Die Aufgaben der Gruppe sind in Artikel 30 und in Artikel 14 Absatz 3 der Richtlinie 97/66/EG festgelegt.

3 Siehe Artikel 29 Absatz 1 zweiter Satz der Richtlinie 95/46/EG.

4 Siehe Artikel 30 Absatz 6 der Richtlinie 95/46/EG.

Die sogenannte allgemeine Datenschutzrichtlinie, d. h. die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (nachstehend „die Richtlinie"), wurde am 24. Oktober 1995 angenommen; für ihre Durchführung galt eine Frist von längstens drei Jahren ab dem Annahmedatum (d. h. bis zum 24. Oktober 1998)[5]. Die spezifische Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, die am 15. Dezember 1997 vom Europäischen Parlament und dem Rat angenommen wurde, übernahm das Umsetzungsdatum der allgemeinen Richtlinie.

Der erste Bericht erläuterte die Zusammensetzung und die Aufgaben der Gruppe und enthielt die wichtigsten Fakten, die 1996 im Bereich des Datenschutzes zu beobachten waren[6]. Der zweite Bericht bezog sich auf das Jahr 1997 und richtete sich im wesentlichen nach der Gliederung des ersten Berichts, um die Analyse von Entwicklungen zu erleichtern. Der dritte Jahresbericht setzte diese Tradition fort. Er beschäftigte sich zunächst mit den wichtigsten Entwicklungen in der Europäischen Union, und zwar sowohl in den Mitgliedstaaten als auch auf der Gemeinschaftsebene. Anschließend befasste er sich mit der Arbeit des Europarats. Des weiteren ging der Bericht auf die wichtigsten Entwicklungen in Drittländern und weitere Entwicklungen auf internationaler Ebene ein.

Der vorliegende vierte Bericht erhielt eine neue, leserfreundlichere Gliederung und stellt die Aktivitäten der Gruppe im Jahr 1999 stärker in den Vordergrund. Diese Aktivitäten sind nunmehr in einem eigenen Kapitel (2.3) zusammengefasst. Der Jahresbericht der Datenschutzgruppe nach Artikel 29 ist weniger als Zusammenfassung denn vielmehr als Ergänzung der Jahresberichte der Datenschutzbehörden der einzelnen Länder gedacht. Darüber hinaus wurde der gestiegenen Bedeutung von Privatsphäre und Datenschutz und dem wachsenden Interesse der Bevölkerung in der Europäischen Union an den Entwicklungen auf diesen Gebieten in der Gemeinschaft Rechnung getragen und die wichtigsten Fragestellungen im Zusammenhang mit der EU verstärkt in den Mittelpunkt gestellt.

Auf der Ebene der Gemeinschaft ging es im Jahr 1999 hauptsächlich um die Übermittlung personenbezogener Daten in Drittländer, insbesondere die Vereinigten Staaten von Amerika, die Schweiz und Ungarn, sowie um Fragen im Kontext von Internet und Telekommunikation.

Die Datenschutzgruppe nach Artikel 29 trat 1999 achtmal zusammen; damit hat sich die Zahl der Sitzungen gegenüber den ersten drei Jahren verdoppelt (1996, 1997 und

5 Dieses Datum ist nicht identisch mit dem Tag des Inkrafttretens: Da in der Richtlinie kein Zeitpunkt für ihr Inkrafttreten festgelegt ist, trat sie am zwanzigsten Tag nach ihrer Veröffentlichung in Kraft (siehe Artikel 254 Absatz 1 des EG-Vertrags).

6 WP 3 (5023/97): Erster Jahresbericht, angenommen am 25. Juni 1997, verfügbar unter: siehe Fußnote 1.

1998 trat die Gruppe jährlich viermal zusammen). Die Gruppe befasste sich mit 72 Tagesordnungspunkten und erörterte im Zuge der Vorbereitung ihrer Stellungnahmen, Empfehlungen und Arbeitsunterlagen rund 280 Dokumente in den verschiedenen Amtssprachen.

Vorsitzender der Gruppe ist 1999 Peter J. HUSTINX, Präsident der niederländischen Datenschutzbehörde (*Registratiekamer*). Herr HUSTINX wurde auf der 9. Sitzung am 10./11. März 1998 für zwei Jahre wieder gewählt. Auf derselben Sitzung wurde Prof. Stefano RODOTA, Präsident der italienischen Datenschutzbehörde (*Garante per la protezione dei dati personali),* als Nachfolger von Louise CADOUX (*Commission Nationale de l'Informatique et des Libertés, CNIL)* zum Stellvertretenden Vorsitzenden der Gruppe gewählt.

Die Stellungnahmen und Empfehlungen der Gruppe wurden an die Kommission und den Ausschuss nach Artikel 31 und im Einzelfall unter anderem an die Präsidenten des Rates und des Europäischen Parlaments weitergeleitet.

Sekretariat der Gruppe

Europäische Kommission
Generaldirektion Binnenmarkt
Referat „Datenschutz"

Die von der Gruppe angenommenen Dokumente stehen in allen Amtssprachen auf dem Europa-Server, Website der Europäischen Kommission, Website des Referats „Datenschutz", zur Verfügung:

http://www.europa.eu.int/comm/internal_market/de/dataprot/wpdocs/index.htm

2. ENTWICKLUNGEN IN DER EUROPÄISCHEN UNION AUF DEM GEBIET DES DATENSCHUTZES UND DES SCHUTZES DER PRIVATSPHÄRE

2.1. Richtlinie 95/46/EG

2.1.1. Umsetzung in nationales Recht

Die Datenschutzbehörden der Mitgliedstaaten wurden ersucht, über den Stand der Umsetzung der Datenschutzrichtlinien sowie über sonstige Entwicklungen auf dem Gebiet des Datenschutzes in den einzelnen Ländern zu berichten. Über den Stand der Umsetzung informieren die nachstehenden Kapitel 2.1 und 2.2. Die übrigen Entwicklungen sind in Kapitel 2.4 erläutert.

Österreich

Das Datenschutzgesetz 2000, BGBl. I Nr. 165/1999 zur Umsetzung der Datenschutzrichtlinie wurde 1999 erlassen und trat am 1. Januar 2000 in Kraft. Da Österreich ein Bundesstaat ist, kann aufgrund der Aufteilung der Verantwortlichkeiten zwischen Bund und Ländern die Richtlinie 95/46/EG auf Bundesebene nur auf denjenigen Gebieten umgesetzt werden, auf denen der Bund Gesetzgebungsvollmacht hat. Dem Bund als Gesetzgeber ist es nicht möglich, den gesamten Anwendungsbereich der Richtlinie 95/46/EG umzusetzen. Soweit Daten für Zwecke verarbeitet werden, die in den Zuständigkeitsbereich der Länder fallen, ist es Aufgabe der Länder, die Datenschutzbestimmungen der Richtlinien umzusetzen. Die ersten Datenschutzgesetze auf Länderebene wurden 2000 verabschiedet (derzeit bestehen auf Ebene der Länder sechs Datenschutzgesetze).

Belgien

Das Gesetz vom 11. Dezember 1998 zur Umsetzung der Richtlinie 95/46/EG wurde am 3. Februar 1999 im Amtsblatt (Moniteur Belge) veröffentlicht. Das Gesetz tritt im sechsten Monat nach Veröffentlichung des Durchführungserlasses im Amtsblatt in Kraft, d. h. am 1. September 2001 (der Durchführungserlass wurde am 13. März 2001 veröffentlicht).

Dänemark

1999 erfolgte keine Umsetzung.

Finnland

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr wurde mit dem Gesetz über personenbezogene Daten (523/1999) umgesetzt, das in Finnland am 1. Juni 1999 in Kraft trat.

Frankreich

1999 erfolgte keine Umsetzung.

Ende Juni 2000 unterrichtete die französische Regierung die Datenschutzbehörde (*Commission Nationale de l'informatique et des Libertés, CNIL*) über den vorläufigen Gesetzentwurf zur Umsetzung der Richtlinie 95/46/EG. Mitte September übermittelte die CNIL der Regierung ihre Stellungnahme hierzu. Nun muss noch die Stellungnahme des Staatsrates abgewartet werden, dann kann die Regierung den Gesetzentwurf verabschieden und dem Parlament zur Abstimmung vorlegen. Der Gesetzentwurf dürfte das System zur Unterrichtung der Aufsichtsbehörde noch vor der Verarbeitung von Daten vereinfachen und gleichzeitig die Befugnisse der Behörde für Folgemaßnahmen erweitern.

Deutschland

Die Frist für die Umsetzung der Richtlinie 95/46/EG wurde von der deutschen Regierung nicht eingehalten, vielmehr verfolgt die Regierung jetzt einen Zweistufenplan:

In einem ersten Schritt soll die Richtlinie 95/46/EG umgesetzt werden, wobei im gleichen Zuge noch weitere Datenschutzmaßnahmen aufgegriffen werden, wie z. B. Bestimmungen zu Videoüberwachung, Chipkarten, Anonymisierung,

Pseudonymisierung sowie Datenschutzaudits. Mit dem Abschluss der Vorarbeiten wird für Mitte 2001 gerechnet.

In einem zweiten Schritt ist eine generelle Überarbeitung des deutschen Datenschutzgesetzes geplant. Der Gesamtplan hierfür soll 2002 vorliegen.

Italien

1999 wurden verschiedene ordnungspolitische Instrumente zur Aufstellung genauer Vorschriften erlassen, welche die bereits vorhandenen Vorschriften für die mit dem Datenschutzgesetz Nr. 675 vom 31.12.96 erfolgte Umsetzung der Richtlinie 95/46/EG ergänzen. Sie beziehen sich unter anderem auf Verarbeitungsvorgänge, die ursprünglich vom Geltungsbereich der einschlägigen Bestimmungen ausgenommen waren, um die Einhaltungsfrist für bestimmte für die Verarbeitung Verantwortliche zu verlängern. Es wurden neue Gesetze, insbesondere hinsichtlich der in Artikel 8 der Richtlinie 95/46/EG genannten Verarbeitungsvorgänge, erlassen; diese betreffen vor allem öffentliche Stellen, die im allgemeinen Datenschutzgesetz (Nr. 675/1996) ermächtigt wurden, ihre Verarbeitungsvorgänge vorläufig fortzusetzen, und diejenigen Wirtschaftszweige, in denen gemäß Artikel 17 der Richtlinie ein Mindestsicherheitsstandard zur Vermeidung von Datenschutzverletzungen ausgearbeitet werden sollte.

Im Dekret Nr. 135 vom 11.05.99 wurden die allgemeinen Grundsätze festgelegt, die von öffentlichen Stellen bei der Verarbeitung sensibler Daten (einschließlich medizinischer Daten) oder Informationen über juristische Maßnahmen einzuhalten sind. Es wurde festgelegt, in welchen Fällen die Verarbeitung als einem wichtigen öffentlichen Interesse dienend betrachtet werden kann und daher zur Erfüllung dieses Zwecks automatisch erlaubt ist. Weiterhin wurden die im Datenschutzgesetz (Nr. 675/1996) verankerten allgemeinen Grundsätze durch die Maßgabe gestärkt, dass öffentliche Stellen ausschließlich Daten verarbeiten dürfen, die für die Erreichung amtlicher Zwecke erforderlich sind, sofern diese Zwecke nach Einzelfallprüfung durch die Verarbeitung anonymer Daten nicht realisierbar sind. Für die Verarbeitung von Daten über den Gesundheitszustand und das Sexualleben müssen spezifische Verpflichtungen eingehalten werden, darunter der Einsatz von Verschlüsselungstechniken oder Identifikationscodes, mit denen Betroffene nur im Bedarfsfall identifiziert werden können, und spezielle Vereinbarungen für die Aufbewahrung dieser Daten.

In das Dekret Nr. 281 vom 30.07.99 wurden spezifische Bestimmungen für die Verarbeitung personenbezogener Daten für historische, wissenschaftliche und

statistische Zwecke aufgenommen. Dieses Dekret berücksichtigt die in den Empfehlungen Nr. R(83) 10 und R(97) 18 des Europarates verankerten Grundsätze, dabei wurde die Rolle von Verhaltensregeln und ethischen Grundsätzen besonders betont. Die für die Ausarbeitung entsprechender Verhaltensregeln zuständige Gruppe war 1999 und 2000 im Auftrag von Garante tätig. Ein Entwurf der Verhaltensregeln für die Verarbeitung personenbezogener Daten für historische Zwecke kann auf der Website von Garante in italienischer und englischer Sprache eingesehen werden.

Das am selben Tag (30.07.99) ergangene Dekret Nr. 282 regelt die Verarbeitung medizinischer Daten durch öffentliche Gesundheitseinrichtungen (neben den Bestimmungen in Dekret Nr. 135/1999), Gesundheitsorganisationen oder Fachkräfte, die ihre Aufgaben auf der Grundlage einer Vereinbarung mit dem bzw. einer formalen Anerkennung durch das staatliche Gesundheitswesen erfüllen.

Die Beiträge der einschlägigen Interessengruppen über ihre Verbände zur Erarbeitung von Regeln für eine wirksame Selbstkontrolle in den einzelnen Wirtschaftszweigen unter der Schirmherrschaft und nach den Leitlinien von Garante erwiesen sich als ein nützliches Instrument zur Verwirklichung des Schutzes personenbezogener Daten durch flankierende gesetzgeberische Maßnahmen – eine Vorgehensweise, die mit Artikel 27 der Richtlinie 95/46/EG voll und ganz im Einklang steht.

Für die notwendigen Sicherheitsmaßnahmen wurden in Dekret Nr. 318 vom 28.07.99 Vorschriften zur Festlegung des Mindestsicherheitsstandards für die Verarbeitung personenbezogener Daten ausgearbeitet. Es sind verschiedene Maßnahmen je nach Zweck der Verarbeitung und abhängig vom Einsatz elektronischer oder automatischer Datenverarbeitungssysteme vorgesehen (bei der Verarbeitung von Daten ausschließlich für persönliche Zwecke sind die Auflagen weniger streng). Die Einhaltung dieser Maßnahmen ist bindend, und ihre Verletzung ist gemäß Artikel 36 des Datenschutzgesetzes (Nr. 675/1996) unter Strafe gestellt.

Irland

Die Richtlinie wurde 1999 nicht in irisches Recht umgesetzt. Die Umsetzung ist für Anfang 2001 geplant.

Luxemburg

Luxemburg hat die Richtlinie 1999 nicht umgesetzt. Der entsprechende Gesetzentwurf wird dem luxemburgischen Parlament im Oktober 2000 zur Abstimmung 2001 vorgelegt.

Portugal

Die Richtlinie 95/46/EG wurde 1998 mit dem Datenschutzgesetz (67/98) vom 26. Oktober 1998 in nationales Recht umgesetzt.

Schweden

Die EG-Richtlinie 95/46 wurde 1998 mit der Annahme des Gesetzes über personenbezogene Daten (1998:204) in schwedisches Recht umgesetzt. 1999 beschloss das Parlament, Abschnitt 33 (Übermittlung in Drittländer) in Anlehnung an die Richtlinie zu ändern. Nach dem neuen Wortlaut von Abschnitt 33 können personenbezogene Daten in ein Drittland übermittelt werden, wenn das betreffende Land einen angemessenen Schutz personenbezogener Daten gewährleistet. In einem neu aufgenommenen zweiten Absatz werden die Umstände aufgeführt, die bei der Bewertung der Angemessenheit des Schutzniveaus zu berücksichtigen sind. Der ursprüngliche Wortlaut von Abschnitt 33 sah ein absolutes Verbot der Datenübermittlung in Drittländer außer in bestimmten, in Abschnitt 34 festgelegten Situationen vor.

Spanien

Mit dem Organgesetz (Ley Orgánica) Nr. 15/1999 vom 13. Dezember 1999 zum Schutz personenbezogener Daten wurde das bestehende Datenschutzgesetz (Organgesetz 5/1992) abgeändert, um den Inhalt voll mit der Richtlinie in

Einklang zu bringen und anschließend deren Umsetzung abzuschließen. (Organgesetz insofern, als alle Gesetze, die die von der spanischen Verfassung gewährten Grundrechte regeln, als „organicas“ bezeichnet werden, die vom Parlament mit absoluter Mehrheit angenommen werden müssen.)

Niederlande

Die Richtlinie 95/46/EG wurde 1999 nicht in nationales Recht umgesetzt. Das 1999 im Parlament erörterte Datenschutzgesetz (Wet Bescherming Persoonsgegevens – WBP) vom 6. Juli 2000 tritt 2001 in Kraft.

Vereinigtes Königreich

Das Vereinigte Königreich befasste sich 1999 vorrangig mit der Festlegung der erforderlichen ordnungspolitischen und technischen Maßnahmen zur Umsetzung des Datenschutzgesetzes von 1998.

2.1.2. Verletzungsverfahren

Die Europäische Kommission entschied im Juli 1999, Frankreich, Luxemburg, den Niederlanden, Deutschland, dem Vereinigten Königreich, Irland, Dänemark, Spanien und Österreich eine mit Gründen versehene Stellungnahme wegen der Nichteinhaltung der Pflicht gemäß Artikel 32 Absatz zur Notifizierung aller zur Umsetzung der Richtlinie 95/46/EG erforderlichen Maßnahmen zu übermitteln. Die mit Gründen versehenen Stellungnahmen stellen die zweite Stufe des formalen Verletzungsverfahrens gemäß Artikel 226 des EG-Vertrags dar. Da die Kommission binnen zwei Monaten nach Eingang der Stellungnahme von Frankreich, Luxemburg, Deutschland, Irland und den Niederlanden keine zufriedenstellende Antwort erhielt, entschied die Kommission, die betreffenden Länder wegen der nicht erfolgten Notifizierung aller zur Umsetzung der Richtlinie 95/46/EG erforderlichen Maßnahmen beim Europäischen Gerichtshof zu verklagen. Dieser Schritt stellt die dritte Stufe des formalen Vertragsverletzungsverfahrens gemäß Artikel 226 des EG-Vertrags dar.

2.2. Richtlinie 97/66/EG

2.2.1. Umsetzung in nationales Recht

Die Datenschutzbehörden der Mitgliedstaaten wurden ersucht, Informationen über den Stand der Umsetzung der Datenschutzrichtlinien sowie über weitere Entwicklungen auf dem Gebiet des Datenschutzes in den einzelnen Ländern zu übermitteln. Den Stand der Umsetzung schildert das vorliegende Kapitel. Die weiteren Entwicklungen werden in Kapitel 2.4 vorgestellt.

Österreich

Österreich setzte die Richtlinie 97/66/EG mit dem Telekommunikationsgesetz, BGBl. I Nr. 100/1997, um.

Belgien

Die Bestimmungen der Richtlinie 97/66/EG wurden durch Änderungen bestehender Rechtsvorschriften in belgisches Recht integriert.

Die Artikel 78 und 79 des Verbraucherschutzgesetzes vom 14.07.91 wurden abgeändert und enthalten jetzt auch Bestimmungen für unerbetene Anrufe zu Direktmarketingzwecken. Die neuen Bestimmungen traten am 01.10.99 (Moniteur Belge: 23.06.99) in Kraft. Artikel 9 des königlichen Dekrets für den Telekommunikationsbereich vom 22.06.98 wurde am 08.07.99 um die Bestimmungen der Richtlinie über die Identifikation des Teilnehmerendgerätes ergänzt. Die Änderungen traten am 01.09.99 (Moniteur Belge: 01.09.99) in Kraft. Ein königliches Dekret für Telefonverzeichnisse wurde am 14.09.99 angenommen und trat am 18.09.99 (Moniteur Belge: 18.09.99) in Kraft. Dieses Dekret legt die Bedingungen für die Veröffentlichung personenbezogener Daten in Telefonverzeichnissen fest.

Artikel 105 Buchstabe i des Gesetzes vom 21. März 1991 über staatliche Wirtschaftsunternehmen wurde zwecks Umsetzung der Bestimmung von Richtlinie 97/66/EG bezüglich der Handhabung und Speicherung von Verkehrsdaten durch Betreiber und Anbieter von Telekommunikationsdiensten völlig neu gefasst. Die Abänderung trat am 21. Dezember 1999 (Moniteur Belge: 21.12.99) in Kraft.

Dänemark

Im Jahr 1999 erfolgte keine Umsetzung.

Finnland

Die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation wurde mit dem Inkrafttreten des Gesetzes zum Schutz der Privatsphäre und zur Datensicherheit im Bereich der Telekommunikation am 1. Juli 1999 rechtswirksam.

Frankreich

Die französische Regierung unterrichtete die CNIL im Dezember 1999 über den vorläufigen Gesetzentwurf zur Umsetzung der Richtlinie 97/66/EG und legte im Juni 2000 Informationen über ihre Verordnungsentwürfe vor. Im Januar bzw. im Juni 2000 übermittelte die CNIL ihre Stellungnahmen zu den beiden Texten.

Deutschland

Die Richtlinie 97/66/EG wurde, wie im 3. Jahresbericht (S. 10) dargestellt, in nationales Recht umgesetzt.

Italien

Die Richtlinie 97/66/EG wurde durch das Dekret Nr. 171 vom 13.05.1998 in nationales Recht umgesetzt (siehe Erläuterung im 3. Jahresbericht).

Irland

Im Jahr 1999 erfolgte keine Umsetzung. Die Umsetzung der Richtlinie in irisches Recht ist für Anfang 2001 vorgesehen.

Luxemburg

Bislang wurde noch keine Vorlage für die Umsetzung der Richtlinie ausgearbeitet. Die Umsetzung der Richtlinie kann erst Anfang 2002 erfolgen.

Portugal

Die Richtlinie 97/66/EG wurde ebenfalls 1998 mit dem Gesetz 69/98 vom 28. Oktober 1998 in portugiesisches Recht umgesetzt.

Spanien

Die Umsetzung erfolgte bereits 1998 mit dem Allgemeinen Telekommunikationsgesetz 11/1998 und mit dem königlichen Dekret 1736/1998, mit dem die Verordnung zur Weiterentwicklung von Titel III des vorgenannten Gesetzes angenommen wurde.

Schweden

Die Richtlinie 97/66/EG wurde 1999 durch Änderungen des Telekommunikationsgesetzes (1993:597) und der Telekommunikationsverordnung (1997:399) umgesetzt.

Artikel 12 über unerbetene kommerzielle Kommunikationen wurde im März 2000 durch eine entsprechende Änderung des Gesetzes über Marketingpraktiken (1995:450) umgesetzt.

Niederlande

Die Richtlinie 97/66/EG wurde durch das Telekommunikationsgesetz (Telecommunicatiewet, 'Wet van 19 oktober 1998, houdende de regels inzake de telecommunicatie') in niederländisches Recht umgesetzt.

Vereinigtes Königreich

Die Telekommunikationsverordnung von 1998 (Datenschutz und Schutz der Privatsphäre) (Direktmarketing) trat am 1. März 1999 in Kraft. Mit dieser Verordnung wird Artikel 12 der EU-Telekommunikationsrichtlinie 97/66/EG über unerbetene Kommunikationen umgesetzt.

2.2.2. Verletzungsverfahren

„Acht Mitgliedstaaten (Deutschland, Spanien, Italien, Niederlande, Österreich, Portugal, Finnland und Schweden) haben Maßnahmen zur Umsetzung der Richtlinie zum Schutz von personenbezogenen Daten (97/66/EG) notifiziert. Die gegen die Niederlande, Österreich, Portugal, Finnland und Schweden eingeleiteten

Verfahren wurden daher 1999 eingestellt, Belgien, Dänemark[7] und Irland hingegen wurden mit Gründen versehene Stellungnahmen übermittelt. Im Dezember 1999 beschloss die Kommission darüber hinaus, ein gerichtliches Vorgehen gegen Griechenland, Frankreich, Luxemburg und das Vereinigte Königreich wegen der Nichteinhaltung der Pflicht zur Notifizierung aller zur Umsetzung der Richtlinie eingeleiteten Maßnahmen."

2.3. Von der Datenschutzgruppe nach Artikel 29 erörterte Themen

Nachstehend die wichtigsten Themen, zu denen die Gruppe im Verlaufe des Jahres 1999 Stellung nahm; sie betreffen die Bereiche Übermittlung von Daten in Drittländer, Internet und Telekommunikation, das P3P-Seminar, Information im öffentlichen Sektor, die Verhaltensregeln sowie die EU-Grundrechtecharta.

2.3.1. Übermittlung von Daten in Drittländer

Die Richtlinie enthält Vorschriften, die die Gewähr dafür bieten sollen, dass personenbezogene Daten nur in solche Länder außerhalb der Europäischen Union übermittelt werden, die ein angemessenes Schutzniveau hinsichtlich der Verarbeitung personenbezogener Daten oder im Falle bestimmter Ausnahmen (Artikel 25 und 26 der Richtlinie 95/46/EG) gewährleisten. Ohne entsprechende Vorschriften würde das durch die Richtlinie erreichte hohe Datenschutzniveau rasch untergraben, bedenkt man nur die Leichtigkeit, mit der Daten in internationalen Netzen verschoben werden können.

Die Richtlinie sieht vor, dass bestimmte Übermittlungen bei Bedarf blockiert werden können, dies allerdings nur als letztes Mittel; daneben gibt es verschiedene Mittel und Wege um zu gewährleisten, dass ein angemessener Datenschutz gewährleistet bleibt, ohne deshalb internationale Datenströme und die damit zusammenhängenden kommerziellen Transaktionen zu unterbrechen.

Die Kommission kann gemeinsam mit dem Ausschuss nach Artikel 31 der Richtlinie 95/46/EG, der mit Vertretern der Mitgliedstaaten besetzt ist, befinden, dass ein Drittland ein angemessenes Schutzniveau gewährleistet. Sie muss hierzu

7 Da Dänemark zwischenzeitlich eine Notifizierung übermittelt hatte, wurde das Verfahren 2000 eingestellt.

die Gruppe nach Artikel 29 konsultieren, die ihrerseits eine Stellungnahme über das Schutzniveau in dem betreffenden Drittland abgibt.

Am 24. Juli 1998 nahm die Gruppe ein Arbeitspapier zur Übermittlung von personenbezogenen Daten in Drittländer[8] an, in dem die Anforderungen der Richtlinie 95/46/EG erläutert und die konkreten Faktoren genannt werden, die bei der Beurteilung des Schutzniveaus berücksichtigt werden sollten.

Wenn kein angemessenes Schutzniveau gewährleistet ist, können durch vertragliche Vereinbarungen ausreichende Garantien hinsichtlich des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen geschaffen werden, die die Übermittlung von Daten in solche Länder ermöglichen[9].

Das Hauptaugenmerk der Gruppe lag 1999 auf der Frage der Datenübermittlung in Drittländer, vor allem in die Vereinigten Staaten von Amerika, die Schweiz und Ungarn.

2.3.1.1. Vereinigte Staaten von Amerika: Grundsätze des „sicheren Hafens“

Hintergrund für die Ausarbeitung der Grundsätze des “sicheren Hafens” ist die Tatsache, dass die Vereinigten Staaten in Fragen des Schutzes der Privatsphäre eine andere Auffassung vertreten als die Europäische Gemeinschaft. Die Vereinigten Staaten verfolgen einen sektoralen Ansatz, der auf einer Mischung aus Rechtsvorschriften, Regulierungsmaßnahmen und Selbstkontrolle beruht und nach Auffassung der Gruppe nicht in allen Fällen einen angemessenen Schutz für die Übermittlung personenbezogener Daten aus der Europäischen Union gewährleistet. Am 4. November 1998 gab das US-Handelsministerium eine Reihe von Grundsätzen zum Schutz der Privatsphäre heraus, mit denen ein dauerhafter Rahmen für die Übermittlung von personenbezogenen Daten zwischen den USA und der EU geschaffen werden sollte.

Auf diese Initiative folgte im Laufe des Jahres 1999 eine ganze Reihe intensiver Gespräche auf bilateraler Ebene zwischen der amerikanischen Regierung und der Europäischen Kommission, so trafen in den Monaten März, Mai und November 1999 der Generaldirektor der Direktion Binnenmarkt, Herr Mogg, und der Staatssekretär im US-Handelsministerium, Herr Aaron, zusammen.

---

8 Verfügbar auf der in Fußnote 1 angegebenen Website.

9 Siehe Artikel 26 Absätze 2 und 4 der Richtlinie 95/46/EG.

Die Kommission informierte die Gruppe eingehend über den Verlauf der Gespräche und ersuchte sie zu verschiedenen Punkten um Rat im Hinblick auf die Verbesserung und eindeutigere Formulierung der Grundsätze des „sicheren Hafens“, und stellte auch verschiedentlich Fragen, die vom DoC aufgeworfen worden waren; daneben wurde die Gruppe auch um ihren Beitrag zu einem Text über die Gewährleistung des in der Richtlinie 95/46/EG geforderten „angemessenen Schutzniveaus“ gebeten. Das Ergebnis dieser Aktivitäten sind vier veröffentlichte Stellungnahmen und eine veröffentlichte Arbeitsunterlage.

Januar 1999

Am 26. Januar 1999 verabschiedete die Gruppe ihre erste Stellungnahme **(Stellungnahme 1/99**[10]**)** zum *„Stand des Datenschutzes in den Vereinigten Staaten und zu den derzeitigen Verhandlungen zwischen der Europäischen Kommission und der amerikanischen Regierung“*, in der sie die Diskussionsteilnehmer und die im Ausschuss nach Artikel 31 der Richtlinie 95/46/EG organisierten Vertreter der Mitgliedstaaten dringend zur Berücksichtigung der folgenden Schwachstellen im Textentwurf der USA auf:

- Das „Zugangsrecht des Einzelnen“, soll im US-Text auf ein „angemessenes“ Maß beschränkt werden, was nicht den OECD-Leitlinien entspricht, in denen nicht das Recht an sich beschränkt, sondern lediglich eine angemessene Anwendung postuliert wird.
- Der OECD-Grundsatz der Zweckbindung fehlt völlig.
- Daten, auf die sich ein „eigentumsähnliches Recht“ bezieht und „manuell verarbeitete Daten“ sind von den US-Grundsätzen gänzlich ausgenommen.
- Die Begriffe „Risikomanagement“ (*risk management*) und „Informationssicherheit“ (*information security*) sind zu vage und zu schlecht eingrenzbar.

April-Mai

10 WP 15 (5092/98): Stellungnahme 1/99 zum Stand des Datenschutzes in den Vereinigten Staaten und zu den derzeitigen Verhandlungen zwischen der Europäischen Kommission und der amerikanischen Regierung, angenommen am 26. Januar 1999.

Nachdem das US-Handelsministerium am 19. April eine überarbeitete Fassung der Grundsätze des „sicheren Hafens“ freigegeben hatte, gab die Gruppe am 3. Mai ihre zweite Stellungnahme **(Stellungnahme 2/99**[11]**)** zur *„Angemessenheit der ‚Internationalen Grundsätze des sicheren Hafens‘“* ab.

Sie räumt darin Fortschritte in vielen Bereichen ein, wie der Definition von personenbezogenen Daten (die sich jetzt auf eine „identifizierte oder identifizierbare Person“ bezieht) und der weiteren Übermittlung der Daten (Unterscheidung zwischen Übermittlungen an Organisationen, die sich an die Grundsätze halten, und Übermittlungen an Dritte, die nicht in das Konzept des „sicheren Hafens“ einbezogen sind). Bedenken äußert die Gruppe hinsichtlich der in den Rechtsvorschriften der Mitgliedstaaten vorgesehenen Ausnahmen, da dies die Tür für die Auslegung der nationalen Durchführungsmaßnahmen durch Organisationen öffnen könnte, die sich an ein Selbstregulierungssystem eines Drittlands halten. Im Hinblick auf manuell verarbeitete Daten sollte nach Auffassung der Gruppe eine Gleichbehandlung von automatisch und manuell verarbeiteten Daten, die in Dateien gespeichert sind, gewährleistet sein. Abschließend ging die Gruppe ausführlich auf die Grundsätze „Mitteilung und Wahlmöglichkeit“, „Weitere Übermittlung“, „Zugriff“ und „Durchsetzung“ ein.

Juni

Die Zahl der „häufig gestellten Fragen (Frequently Asked Questions, FAQ)“ wuchs in den Monaten April bis Juni 1999 von sechs auf 15. Daraufhin nahm die Gruppe am 7. Juni ihre dritte Stellungnahme **(Stellungnahme 4/99**[12]**)** speziell zu den *FAQs* an, in der sie die Ansicht vertrat, dass

- die FAQs maßgebenden Charakter haben sollten, vorausgesetzt, sie stimmen mit den Grundsätzen des „sicheren Hafens“ überein und werden zusammen mit diesen berücksichtigt;

11 WP 19 (5047/9): Stellungnahme 2/99 zur Angemessenheit der „Internationalen Grundsätze des sicheren Hafens“, ausgegeben vom US-Handelsministerum am 19. April 1999. Angenommen am 3. Mai 1999.

12 WP 21 (5066/99): Stellungnahme 4/99 zu den häufig gestellten Fragen (Frequently Asked Questions), vorgelegt vom US-Handelsministerium im Zusammenhang mit den vorgeschlagenen „Grundsätzen des sicheren Hafens“. Angenommen am 7. Juni 1999 (in EN).

- die endgültige Liste der FAQs erschöpfend sein sollte und die FAQs nicht unilateral geändert werden sollten;

- die FAQs im Lichte der Erfahrungen betrachtet werden sollten, die bei der Anwendung des Konzepts des „sicheren Hafens“ gemacht werden, und gegebenenfalls angepasst und/oder ergänzt werden sollten.

Darüber hinaus ging die Stellungnahme ausführlich auf die FAQs ein: 1 (Sensible Daten), 2 (Ausnahmen für Journalisten), 3 (Nachhaftung), 4 (Headhunting), 5 (Die Aufgabe der Datenschutzbehörden), 6 (Selbst-Zertifizierung), 11 (Unabhängige Prüfung von Beschwerden) und 13 (Wahlmöglichkeit (opt-out)).

Juli 1999

Am 7. Juli, wurde von der Gruppe eine **Arbeitsunterlage**[13] zum *„Gegenwärtigen Stand der Diskussion zwischen der Europäischen Kommission und der Regierung der Vereinigten Staaten über die ‚Internationalen Grundsätze des Sicheren Hafens‘“* angenommen. Hierbei handelt es sich um eine Mitteilung an den nach Artikel 31 der Richtlinie eingesetzten Ausschuss (Vertreter der EU-Mitgliedstaaten).

Die Gruppe lenkte die Aufmerksamkeit des Ausschusses auf folgende Punkte:

- Es sollte sichergestellt werden, dass Artikel 25 der Richtlinie 95/46/EG eine solide Rechtsgrundlage darstellt.

- Der Geltungsbereich des Konzepts des „sicheren Hafens“ sollte in mehreren Punkten konkretisiert werden.

- Die Bedingungen der Umsetzung und Durchführung der Grundsätze des „sicheren Hafens“ sollten festgelegt werden.

- Der Inhalt der Grundsätze 1 (Mitteilung), 2 (Wahlmöglichkeit) und 6 (Zugriff) sollte genauer ausgearbeitet werden.

---

13 WP 23 (5075/99): Arbeitsdokument zum gegenwärtigen Stand der Gespräche zwischen der Europäischen Kommission und der Regierung der Vereinigten Staaten über die „Internationalen Grundsätze des sicheren Hafens“, die am 1. Juni 1999 vom US-Handelsministerium vorgelegt wurden. Angenommen am 7. Juli 1999.

Dezember 1999

In ihrer vierten, am 3. Dezember 1999 angenommenen Stellungnahme **(Stellungnahme 7/99**[14]**)** zum *„Datenschutzniveau, das die Grundsätze des sicheren Hafens in ihrer veröffentlichten Form, die dazu gehörigen häufig gestellten Fragen (FAQ) und andere, vom US-Handelsministerium veröffentlichte Dokumente gewährleisten"* bekräftigte die Gruppe ihre generellen Bedenken gegenüber dem Konzept des „sicheren Hafens" und forderte die Kommission auf, bei der amerikanischen Seite auf wesentliche Verbesserungen zu dringen und dabei Folgendes zu fordern:

- Der Geltungsbereich der Grundsätze des „sicheren Hafens" ist zu präzisieren; vor allem muss dem Missverständnis vorgebeugt werden, US-Unternehmen könnten die Grundsätze des „sicheren Hafens" auch dort anwenden, wo die Richtlinie selbst anzuwenden ist.

- Es sind Regelungen vorzusehen, die die zweifelsfreie Erkennung von Teilnehmern des „sicheren Hafens" ermöglichen und verhindern, dass Unternehmen weiterhin die Vorteile des sicheren Hafens genießen, obwohl sie ihren Status als „sicherer Hafen", aus welchen Gründen auch immer verloren haben.

- Es ist eindeutig festzulegen, dass alle Teilnehmer des „sicheren Hafens" einer staatlichen Stelle mit ausreichenden Durchsetzungsbefugnissen unterstehen müssen.

- Es muss zur Regel werden, dass Beschwerdestellen des Privatsektors ungelöste Beschwerdestellen an diese staatliche Stelle verweisen.

- Die zulässigen Ausnahmen sind präziser und enger zu fassen, damit sie wirklich Ausnahmen sind, d. h. nur zugestanden werden, wo und soweit das notwendig ist und nicht als Einladung zur Umgehung der Grundsätze verstanden werden können. Das gilt vor allem für die Regelung des Zugangsrechts.

- Der Grundsatz der Wahlmöglichkeit ist zu stärken, denn er ist das Kernstück des amerikanischen Konzepts.

---

14 WP 27 (5146/99): Stellungnahme 7/99 zum Datenschutzniveau, das die Grundsätze des sicheren Hafens in ihrer veröffentlichten Form, die dazu gehörigen häufig gestellten Fragen (FAQ) und andere vom US-Handelsministerium am 15./16. November 1999 veröffentlichte Dokumente gewährleisten. Angenommen am 3. Dezember 1999.

Außerdem forderte die Gruppe die Kommission auf, Artikel 2 des Entscheidungsentwurfs vom 24. November 1999 zu ändern und die Arbeit an Mustervertragsbestimmungen im Hinblick auf eine Feststellung oder Feststellungen nach Artikel 26 Absatz 4 der Richtlinie 95/46/EG (Garantien für Übermittlungen in Gebiete, die kein angemessenes Schutzniveau gewährleisten) zu beschleunigen.

2.3.1.2. Schweiz

Die Gruppe wurde darüber unterrichtet, dass die Europäische Kommission einen Entscheidungsentwurf auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erstellt habe, in dem festgestellt werde, dass die Schweiz aufgrund ihrer internen Gesetzgebung ein angemessenes Schutzniveau im Sinne von Artikel 25 Absatz 2 der besagten Richtlinie gewährleiste. Um der Europäischen Kommission mit Unterstützung des nach Artikel 31 der Richtlinie 95/46/EG eingesetzten Ausschusses eine Stellungnahme zu unterbreiten, führte die Gruppe eine Analyse der in der Schweiz anwendbaren Datenschutzvorschriften[15] durch.

In Anbetracht der Verteilung der Kompetenzen zwischen der Eidgenossenschaft und den Kantonen, gilt das eidgenössische Gesetz (Datenschutzgesetz vom 19. Juni 1992 in der geänderten und ergänzten Fassung des Schweizer Bundesrates vom 14. Juni 1993) für die in der Gesamtheit des Schweizer Privatsektors durchgeführte Verarbeitung von personenbezogenen Daten sowie für die von den Bundesbehörden durchgeführte Verarbeitung. Die kantonalen Bestimmungen betreffen ihrerseits die Verarbeitung von personenbezogenen Daten im öffentlichen Sektor auf kantonaler oder kommunaler Ebene. Unter die Zuständigkeit der Kantone fällt zum Beispiel die Verarbeitung, die in den Bereichen Polizei, Schule, Gesundheitswesen und insbesondere öffentliche Krankenhäuser durchgeführt wird. Um ganz genau zu sein, muss hervorgehoben werden, dass die Kantone ebenfalls dazu veranlasst werden, bestimmte Verarbeitungsvorgänge von personenbezogenen Daten in Ausübung des eidgenössischen Rechts durchzuführen, z. B. für die Erhebung von Steuern des Bundes.

Sowohl die Rechtsvorschriften des Bundes als auch diejenigen der Kantone sind so konzipiert, dass sie übereinstimmen mit:

---

15 Um über bestimmte Punkte genauere Informationen zu erhalten, wandte sich der Vorsitzende der Gruppe am 15. März 1999 in einem Schreiben an den Eidgenössischen Datenschutzbeauftragten, der dieses Schreiben am 24. März 1999 beantwortete. Darüber hinaus bestehen informelle Kontakte zwischen dem Sekretariat der Gruppe und dem Eidgenössischen Datenschutzbeauftragten.

1.- dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108). Dieses Übereinkommen wurde von der Schweiz am 2. Oktober 1997 ratifiziert und legt internationale Verpflichtungen sowohl für die Eidgenossenschaft als auch für die Kantone fest, ohne direkt anwendbar zu sein.

2.- der eidgenössichen Verfassung (geändert durch Volksabstimmung am 18. April 1999), wie durch die Rechtsprechung des Bundesgerichts ausgelegt. Hierbei muss unterstrichen werden, dass der neue Verfassungstext jeder natürlichen Person das Recht auf Achtung ihrer Privatsphäre verleiht und insbesondere das Recht auf Schutz vor der missbräuchlichen Verwendung ihrer persönlichen Daten (Artikel 13 über den Schutz der Privatsphäre).

In ihrer Schlussfolgerung empfahl die Gruppe der Kommission und dem Ausschuss nach Artikel 31 der Richtlinie 95/46/EG festzustellen, dass die Schweiz ein angemessenes Schutzniveau im Sinne von Artikel 25 Absatz 6 der Richtlinie gewährleistet.

2.3.1.3. Ungarn

Um der Europäischen Kommission mit Unterstützung des nach Artikel 31 der Richtlinie 95/46/EG eingesetzten Ausschusses eine Stellungnahme zu unterbreiten, führte die Gruppe eine Analyse der in Ungarn anwendbaren Datenschutzvorschriften[16] durch.

Die Rechtslage im Hinblick auf den Schutz personenbezogener Daten wird geregelt durch das Gesetz LXIII vom 17. November 1992, das am 1. Mai 1993 in Kraft trat und später geändert wurde[17]. Der Geltungsbereich dieses Gesetzes geht

16 Um über gestimmte Punkte genauere Informationen zu erhalten, wandte sich der Vorsitzende der Gruppe an den ungarischen Datenschutzbeauftragten (Schreiben vom 22. März und 19. April 1999 und Antwortschreiben vom 25. März bzw. 23. April 1999).

17 Vgl. zuletzt das Gesetz LXXII vom 22. Juni 1999, durch das der Begriff des „Auftragsverarbeiters“ in die ungarische Gesetzgebung eingeführt wird.

über den reinen Schutz von personenbezogenen Daten hinaus; es regelt ebenfalls den Zugang der Öffentlichkeit zu Verwaltungsdokumenten. Der Datenschutzbeauftragte, dessen Kompetenzen ebenfalls durch das Gesetz festgelegt sind und der am 30. Juni 1995 vom Parlament ernannt wurde, ist verantwortlich für die Kontrolle der Anwendung dieser beiden Regelungen.

Im Hinblick auf den Schutz personenbezogener Daten ist es ferner angezeigt, Folgendes festzuhalten:

- die internationalen Verpflichtungen Ungarns aufgrund der am 8. Oktober 1997 erfolgten Ratifizierung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108),

- den von der Verfassung garantierten Schutz der Privatsphäre, insbesondere was die Verarbeitung personenbezogener Daten betrifft[18],

- das Vorhandensein sektoraler Gesetze, die in so unterschiedlichen Bereichen wie Geheimdienste, Statistiken, Geschäftsanbahnungen, wissenschaftliche Forschung und seit kurzem im Bereich der Gesundheit Datenschutzbestimmungen enthalten.

Nach Ansicht der Gruppe gewährleistet das ungarische Gesetz über den Datenschutz ein angemessenes Schutzniveau. Die Gruppe empfahl daher der Kommission und dem Ausschuss nach Artikel 31 der Richtlinie 95/46/EG festzustellen, dass Ungern ein angemessenes Schutzniveau gemäß Artikel 25 Absatz 6 dieser Richtlinie gewährleistet.

2.3.1.4. Die Gruppe nahm Vorgespräche zum Schutzniveau in Hongkong, Norwegen und Island auf.

18 Die englische Übersetzung von Artikel 59 der Verfassung, die durch die ungarischen Behörden erstellt wurde, lautet wie folgt: „(1) In the Republic of Hungary everyone is entitled to the protection of his or her reputation and to privacy of the home, of personal effects, particulars, papers, records and data, and to the privacy of personal affairs and secrets. (2) For the acceptance of the law on the protection of the security of personal data and records, the votes of two thirds of the MPs present are necessary.“

2.3.2. Arbeitsunterlagen[19] zu den Modell-Vertragsbestimmungen von ICC und CBI

Die Internationale Handelskammer (International Chamber of Commerce, ICC) hat Bestimmungen ausgearbeitet, die einen grenzüberschreitenden Datenverkehr und zugleich einen wirksamen Schutz personenbezogener Daten weltweit im Sinne von Artikel 26 Absätze 2 und 4 der Richtlinie 95/46/EG gewährleisten sollen.

Die ursprüngliche Fassung dieser Bestimmungen wurde der Generaldirektion „Binnenmarkt" der Europäischen Kommission im September 1998 vorgelegt und sollte als Entscheidung der Kommission gemäß der Richtlinie 95/46/EG angenommen werden. Eine überarbeitete Fassung der Bestimmungen wurde der Generaldirektion „Binnenmarkt" am 18. Dezember 1998 vorgelegt.

Die Gruppe analysierte die Bestimmungen der Internationalen Handelskammer und machte weitere Anregungen und Anmerkungen. Sie schlug unter anderem vor, die Bestimmungen sollten auch auf „Controller-Controller"-Situationen anwendbar sein. Dies bedeutet, dass die Bestimmungen Garantien für den Fall beinhalten sollten, dass personenbezogene Daten aus der EU an andere für die Verarbeitung Verantwortliche im Ausland veräußert werden. In diesem Fall besteht für natürliche Personen kein Schutz. Bislang bezieht sich die Fassung der Internationalen Handelskammer ausschließlich auf „Controller-Processor"-Situationen, die in gewissem Umfang durch Artikel 17 Absatz 3 der Richtlinie 95/46/EG abgedeckt sind. Die Gruppe ersuchte die Internationale Handelskammer, ihren Text im Lichte der Kommentare zu überarbeiten.

Auch der britische Industrieverband CBI erarbeitete einen Entwurf für vertragliche Bestimmungen zur Regelung der Übermittlung personenbezogener Daten aus der Europäischen Union in Drittländer. Das Papier des CBI (Fassung vom 15. Dezember 1998) umfasst eine Reihe von Modell-Vertragsbestimmungen mit Erklärungen; es wurde dem Generaldirektor der Generaldirektion "Binnenmarkt" der Europäischen Kommission am 23. Dezember 1998 vorgelegt.

19 Diese Arbeitsunterlagen wurden nicht veröffentlicht, sondern direkt an die ICC bzw. den CBI übermittelt, um in einem möglichst frühen Stadium auf deren interne Diskussionen Einfluss zu nehmen.

In ihrer Arbeitsunterlage empfahl die Gruppe der Europäischen Kommission, dem Ersuchen des CBI nachzukommen und diese Punkte weiter zu erörtern und dabei die aufgezeigten Mängel zu berücksichtigen.

2.3.3. Internet und Telekommunikation

Die Datenschutzgruppe nahm verschiedene Empfehlungen an, die sich mit den wichtigsten Aspekten von Internet und Telekommunikation auseinander setzen:

2.3.3.1. Arbeitsunterlage zur Verarbeitung personenbezogener Daten im Internet

Die Europäische Konferenz der Datenschutzbeauftragten vom 23. und 24. April 1998 in Dublin äußerte den Wunsch, die Gruppe solle systematischer an das Thema herangehen, die anstehenden Fragen definieren und Lösungen erarbeiten, um sicherzustellen, dass die Rechte der Benutzer zum Schutz ihrer Privatsphäre bei der weiteren Entwicklung des Internet und der damit zusammenhängenden Dienstleistungen angemessen berücksichtigt werden, denn dadurch könnte das Vertrauen sowohl in die kommerziellen als auch in die privaten Anwendungen erheblich gesteigert werden. Die Datenschutzbeauftragten erinnerten daran, dass die EU-Datenschutzbestimmungen mit den entsprechenden Modalitäten, unabhängig von den verwendeten technischen Mitteln, uneingeschränkt für die Verarbeitung personenbezogener Daten im Internet gelten.

Die Gruppe teilt[20] die Ansicht der Konferenz der EU-Datenschutzbeauftragten. Das Internet ist kein rechtsfreier Raum. Bei der Verarbeitung personenbezogener Daten im Internet sind die gleichen Datenschutz-Grundsätze zu berücksichtigen wie bei Offline-Computeranwendungen[21]. Dies schränkt die Verwendung des

20 WP 16 (5013/99): Arbeitsunterlage: Die Verarbeitung personenbezogener Daten im Internet. Angenommen am 23.2.1999.

21 Siehe auch Ministererklärung der Bonner Konferenz über globale Netze, Juni 1997, verfügbar unter: http://www2.echo.lu/bonn/conference.html

Internet keineswegs ein, sondern ist im Gegenteil eine Grundvoraussetzung, um das Vertrauen der Benutzer in das Funktionieren des Internet und die dort angebotenen Dienstleistungen zu gewinnen. Somit ist der Datenschutz im Internet eine unerlässliche Grundvoraussetzung für das Betreiben des elektronischen Geschäftsverkehrs.

Die allgemeine Datenschutzrichtlinie 95/46/EG gilt für jegliche Verarbeitung personenbezogener Daten innerhalb ihres Anwendungsbereichs, unabhängig von den hierbei eingesetzten technischen Mitteln. Daher ist die Verarbeitung personenbezogener Daten im Internet nach Maßgabe dieser Richtlinie zu behandeln.

Die speziellere Richtlinie 97/66/EG über den Schutz der Privatsphäre und der personenbezogenen Daten im Bereich der Telekommunikation ergänzt die allgemeine Richtlinie 95/46/EG, indem sie rechtliche und technische Bestimmungen spezifiziert[22]. Das Internet ist ein Computernetz, das allen offen steht. Somit gehört es zum Bereich der öffentlichen Telekommunikation. Dies wiederum bedeutet, dass die Bestimmungen der Richtlinie 97/66/EG für die Verarbeitung personenbezogener Daten bei der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste in öffentlichen Telekommunikationsnetzen in der Gemeinschaft[23] Anwendung findet.

2.3.3.2. Empfehlung über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet

Hintergrund für die Aufstellung dieser Empfehlung[24] war, dass gegenwärtig im Internet alle Arten von Verarbeitungsvorgängen über Hardware und Software ablaufen, von denen die Betroffenen keine Kenntnis haben und die für sie also

22 Richtlinie 95/46/EG gilt für alle Fragen, die nicht spezifisch in Richtlinie 97/66/EG behandelt werden, wie z. B. die Pflichten des für die Datenverarbeitung Verantwortlichen, die Rechte des Betroffenen oder nicht öffentlich zugängliche Telekommunikationsdienste (siehe Punkt 11 der Einleitung der Richtlinie 97/66/EG).

23 Siehe Artikel 3 Absatz 1 der Richtlinie 97/66/EG.

24 WP 17 (5093/98): Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware. Angenommen am 23. Februar 1999

„unsichtbar“ sind. Beispielsweise kann ein Server mittels so genannter „Cookies” bestimmte Daten auf der Festplatte des Internet-Benutzers speichern und abrufen, ohne dass der Benutzer dies bemerkt. Ebenso können mittels handelsüblicher Internet-Software (dazu gehören insbesondere Browser, FTP[25], E-Mail, News- und Chat-Programme) verschiedene Arten von personenbezogenen Daten über die Benutzer gesammelt, verknüpft und verbreitet und somit ohne deren Wissen Benutzerprofile erstellt werden. Mit diesen Techniken lassen sich so genannte „Clicktrails“ über Internet-Benutzer anlegen. Clicktrails beinhalten Informationen über das Verhalten einer Person, deren Identität, Suchweg oder Auswahlverhalten beim Besuch einer Website. Sie enthalten Links, die der Benutzer aufgerufen hat und die auf dem Webserver protokolliert sind.

Die Gruppe stellte fest, dass die verschiedenen Praktiken der Verarbeitung personenbezogener Daten im Internet mit der EU-Datenschutzrichtlinie und insbesondere mit der Forderung, dass die Betroffenen über die fraglichen Verarbeitungsvorgänge informiert und damit darauf aufmerksam gemacht werden, nicht im Einklang stehen. Die Gruppe empfahl den Anbietern von Internet-Software daher eine Anpassung ihrer Programme gemäß den in dieser Richtlinie spezifizierten Datenschutzgrundsätzen. Insbesondere sollten die Hard- und Softwareprodukte so konfiguriert werden, dass sie nicht standardmäßig das Sammeln, Speichern oder Senden von client-persistenten Informationen ermöglichen. Auf diese Weise könnten die Benutzer selbst über ihre Daten bestimmen.

2.3.3.3. Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs

Im Kontext der Erörterungen im Rat der Europäischen Union über die Überwachung des Fernmeldeverkehrs und der Entschließungen des Europäischen Parlaments zum Abhörsystem Echelon erachtete die Gruppe es für notwendig, ihre Fachkenntnis in die öffentliche Diskussion einzubringen.

Die Gruppe erinnert daran, dass jede Überwachung des Fernmeldeverkehrs, d. h. jede Kenntnisnahme von Inhalt und/oder Daten im Zusammenhang mit privaten Telekommunikationsverbindungen zwischen zwei oder mehreren Teilnehmern durch einen Dritten, insbesondere der mit der Telekommunikationsnutzung verbundenen Verkehrsdaten, eine Verletzung des Rechts von Einzelpersonen auf Privatsphäre und eine Verletzung des Brief- und Fernmeldegeheimnisses darstellt. Nach Artikel 8 Absatz 2 der

25 FTP = File Transfer Protocol

Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950[26] und seiner Auslegung durch den Europäischen Gerichtshof für Menschenrechte ist eine Überwachung nur zulässig, wenn sie drei Anforderungen genügt: eine Rechtsgrundlage ist vorhanden, die Maßnahme ist in einer demokratischen Gesellschaft erforderlich und trägt zu einem der in der Konvention genannten Ziele bei[27].

Die Rechtsgrundlage muss klare und ausführliche Bestimmungen über Grenzen und Modalitäten dieses Eingriffs umfassen, was insbesondere angesichts der kontinuierlichen Weiterentwicklung der technischen Hilfsmittel erforderlich ist. Die Rechtsvorschrift muss der Öffentlichkeit zugänglich sein, damit die Bürger die Folgen ihres Verhaltens absehen können. Eine groß angelegte oder allgemeine Überwachung des Fernmeldeverkehrs muss darin untersagt sein.

Das in den Rechtssystemen der Mitgliedstaaten verankerte Recht auf Schutz der Privatsphäre ist auf Ebene der Europäischen Union in der Richtlinie 95/46/EG festgeschrieben. Die Grundsätze der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950 und des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 werden in dieser Richtlinie präzisiert. Die Richtlinie 97/66/EG[28] konkretisiert die Bestimmungen der oben genannten Richtlinie, indem sie die Mitgliedstaaten verpflichtet, die Vertraulichkeit der über öffentliche Telekommunikationsnetze oder öffentlich zugängliche Telekommunikationsdienste übermittelten Nachrichten sicherzustellen.

Mit dieser Empfehlung weist die Gruppe darauf hin, wie die Grundsätze des Schutzes des Grundrechte und –freiheiten natürlicher Personen, insbesondere ihre Privatsphäre *und das Brief- und Fernmeldegeheimnis*, auf die auf europäischer Ebene zur Überwachung des Fernmeldeverkehrs beschlossenen Maßnahmen anzuwenden sind. Der Anwendungsbereich der Empfehlung zielt auf Überwachungen im weiteren Sinne ab, d. h. die Überwachung des Inhalts des Fernmeldeverkehrs, aber auch der mit dem Fernmeldeverkehr

---

26 Es ist darauf hinzuweisen, dass die vom Europarat für den Bereich der Fernmeldeüberwachung anerkannten Grundgarantien unabhängig von der auf Gemeinschaftsebene getroffenen Unterscheidung zwischen gemeinschaftlicher oder einzelstaatlicher Zuständigkeit für die Staaten Verpflichtungen mit sich bringen.

27 Auch nach dem Übereinkommen Nr. 108 des Europarates ist eine Einmischung nur zulässig, wenn eine demokratische Gesellschaft sie zum Schutz der in Artikel 9 Absatz 2 des Übereinkommens genannten nationalen Interessen benötigt und sie ausschließlich auf dieses Ziel beschränkt bleibt (doch ist darauf hinzuweisen, dass die im Übereinkommen Nr. 108 und die in der Konvention zum Schutz der Menschenrechte und Grundfreiheiten genannten nationalen Interessen nicht genau übereinstimmen).

28 Richtlinie vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. L 24 vom 30. Januar 1998, S. 1.

zusammenhängenden Daten, insbesondere durch vorbereitende Maßnahmen wie „Monitoring“ und „Datamining“ der Verkehrsdaten, die beabsichtigt sein könnten, um über die Zweckmäßigkeit einer Überwachung zu entscheiden.

Die Gruppe weist nachdrücklich darauf hin, dass die Pflichten, die die Richtlinie 95/46/EG (Artikel 17 Absätze 1 und 2) und 97/66/EG (Artikel 4, 5 und 6) Netzbetreibern und Diensteanbietern wie auch den Mitgliedstaaten in Bezug auf Datensicherheit und –vertraulichkeit auferlegen, die Regel und nicht die Ausnahme sind. Netzbetreiber und Diensteanbieter müssen die notwendigen Maßnahmen ergreifen, um die Überwachung des Fernmeldeverkehrs für Stellen, die gesetzlich nicht dazu berechtigt sind, je nach Stand der Technik zu erschweren oder unmöglich zu machen.

Abschließend stellt die Gruppe eine Checkliste zur Wahrung der Grundrechte und Grundfreiheiten bei der Überwachung durch staatliche Behörden auf.

2.3.3.4. Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke

Die Bekämpfung der Computerkriminalität ist ein Thema, dem international immer größere Aufmerksamkeit zuteil wird. Die G8-Länder[29] haben einen 10-Punkte-Aktionsplan verabschiedet, der 1999 mit Unterstützung einer Fachgruppe für Hightech-Kriminalität umgesetzt wurde, der Vertreter der Strafverfolgungsbehörden der G8-Staaten angehörten. Eine der wichtigsten und brisantesten Fragen ist die Aufbewahrung von Verkehrsdaten (Daten über bereits abgeschlossene und gerade geschaltete Verbindungen) durch Internet-Dienstanbieter (Internet Service Provider) für Strafverfolgungszwecke und die Offenlegung dieser Daten gegenüber den Strafverfolgungsbehörden. Die G8-Arbeitsgruppe zur Hightech-Kriminalität beabsichtigt, Empfehlungen zur Aufbewahrung und Offenlegung von Verkehrsdaten abzugeben. Parallel hierzu erarbeitet der Europarat einen Entwurf für ein Übereinkommen über Cyberkriminalität.

Die Datenschutzgruppe ist sich der Tatsache bewusst, dass Verkehrsdaten bei der Ermittlung in Internet-Strafsachen eine wichtige Rolle spielen können, möchte die Regierungen der Mitgliedstaaten jedoch an die Grundsätze erinnern, wonach die Grundrechte und -freiheiten natürlicher Personen zu schützen sind, wobei in diesem Zusammenhang insbesondere die Achtung der Privatsphäre und das Brief-, Post- und Fernmeldegeheimnis zu berücksichtigen sind.

Die Gruppe ist sich ferner der Belastung bewusst, die sich für Telekommunikationsbetreiber und –dienstanbieter ergeben.

---

29 Die G8-Länder sind: Deutschland, Frankreich, Italien, Japan, Kanada, das Vereinigtes Königreich, die Vereinigten Staaten von Amerika und Russland.

Wie die Gruppe bereits in ihrer Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs vom 3. Mai 1999[30] dargelegt hat, wird die Kenntnisnahme Dritter von Verkehrsdaten über die Nutzung von Telekommunikationsdiensten generell als Überwachung des Fernmeldeverkehrs betrachtet und stellt daher eine Verletzung des Rechtes des Einzelnen auf Achtung der Privatsphäre und der Vertraulichkeit der Kommunikation Artikel 5 der Richtlinie 97/66/EG dar. Darüber hinaus ist eine solche Offenlegung von Verkehrsdaten nicht mit Artikel 6 dieser Richtlinie vereinbar. Die Gruppe ist daher der Auffassung, dass, will man eine unannehmbare Bedrohung der Privatsphäre vermeiden und gleichzeitig den Erfordernissen einer effizienten Strafverfolgung Rechnung tragen, das wirksamste Vorgehen darin besteht, grundsätzlich nicht zuzulassen, dass Verkehrsdaten allein für Strafverfolgungszwecke aufbewahrt werden.

2.3.4. P3P-Seminar

Die Europäische Kommission veranstaltete gemeinsam mit dem World Wide Web Consortium (W3C), das sich mit der Entwicklung der „Platform for Privacy Preferences (P3P)“ und der Datenschutzgruppe nach Artikel 29 ein Seminar zu diesem Thema. P3P geht davon aus, dass der Schutz der Privatsphäre und der Datenschutz zwischen dem Internet-Nutzer, dessen Daten erfasst werden, und der Website, die die Daten erfasst, zu vereinbaren ist. Die Philosophie stützt sich auf die Überlegung, dass der Nutzer in die Erfassung seiner personenbezogenen Daten durch eines Site einwilligt, sofern die erklärten, die Privatsphäre berührenden Praktiken des Sites wie die Zwecke, für die Daten erfasst werden, und die Frage, ob die Daten für weitere Zwecke verwendet oder an Dritte weitergeleitet werden oder nicht, den Anforderungen des Nutzers genügen. Das World Wide Web Consortium hat sich bemüht, ein einheitliches Vokabular zu entwickeln, mit dem die Präferenzen der Nutzer und die Praktiken der Sites artikuliert werden. Das P3P-Seminar war die Folgeveranstaltung zur Stellungnahme 1/98 der Gruppe. Ziel des Seminars war zu erörtern, wie das „Protocol for Privacy Preferences“ (P3P) den rechtlichen Anforderungen der Datenschutzrichtlinie zwecks Durchführung in der EU Rechnung tragen kann.

30 Verfügbar unter: siehe Fußnote 1.

2.3.5. Informationen des öffentlichen Sektors

Die Europäische Kommission legte ein Grünbuch mit dem Titel „Informationen des öffentlichen Sektors: Eine Schlüsselressource für Europa“ zur öffentlichen Anhörung vor[31]. Vorrangiges Ziel des Grünbuchs ist es, die Diskussion darüber anzuregen, wie Informationen des öffentlichen Sektors für die Bürger und die Wirtschaft besser zugänglich gemacht werden können und ob eine Harmonisierung der Vorschriften der einzelnen Länder auf diesem Gebiet notwendig erscheint. Ein zentraler Aspekt des Grünbuchs ist die Verfügbarkeit von Informationen des öffentlichen Sektors. Das Grünbuch ignoriert dabei den Schutz von personenbezogenen Daten nicht, wenngleich dieser Schutz offenkundig keinen primären Schwerpunkt des Papiers darstellt.

Die Gruppe leistete mit ihrer Stellungnahme 3/99 einen Beitrag zu dieser Anhörung[32].

Diese Stellungnahme zielt darauf ab, Überlegungen über den Umfang des Schutzes personenbezogener Daten anzustellen; dies ist notwendig, um den Zugriff auf Daten des öffentlichen Sektors, die sich auf natürliche Personen beziehen, zu erleichtern. Es wird jedoch nicht der Anspruch erhoben, sämtliche Fragen zu beantworten, die durch die Versöhnung des Ziels eines einfacheren Zugriffs auf Daten des öffentlichen Sektors auf der Grundlage des erklärten Willens des Staates, eine stärkere Transparenz gegenüber dem Staatsbürger walten zu lassen, mit dem Schutz personenbezogener Daten laut Definition in der Richtlinie 95/46/EG aufgeworfen werden. Sie bezweckt, auf der Grundlage der Richtlinie 95/46/EG sowie anhand konkreter Erfahrungen, die im Bereich der bekanntesten Register, die öffentlich zugänglich gemachte personenbezogene Daten umfassen, gemacht wurden, eine erste Reihe von Ansatzpunkten zu liefern, die bei der Entscheidungsfindung zu berücksichtigen sind.

---

31 KOM (1998)585, verfügbar unter: http://europa.eu.int/servlet/portail/Renderservlet?model=xml

32 WP 20 (5026/99/FR + 5055/99 alle anderen Sprachen): Stellungnahme 3/99 betreffend die Informationen des öffentlichen Sektors und Schutz personenbezogener Daten, Beitrag zu der mit dem Grünbuch der Europäischen Kommission unter dem Titel „Informationen des öffentlichen Sektors – eine Schlüsselressource für Europa“ begonnenen Anhörung, KOM (1998) 585. Angenommen am 3. Mai 1999.

Nach dem Grundsatz der Zweckbindung (Artikel 6 der Richtlinie 95/46/EG) dient die Sammlung personenbezogener Daten bestimmten, ausdrücklich festgelegten legitimen Zwecken; ihre Weiterverarbeitung hat zweckbestimmungskonform zu erfolgen. Diesem Prinzip ist also bei der Umsetzung des Zugriffs auf personenbezogene Daten des öffentlichen Sektors ein hoher Stellenwert einzuräumen.

Dabei muss von Fall zu Fall entschieden werden, inwieweit ein Gesetz die Veröffentlichung bzw. den Zugriff der Öffentlichkeit auf personenbezogene Daten erforderlich macht bzw. gestattet. Hier stellt sich die Frage, ob der Zugriff völlig frei und unbegrenzt erfolgen kann, ob die Daten unabhängig von der ursprünglichen Zweckbestimmung für alle möglichen Zwecke genutzt werden können oder ob die gesetzliche Regelung lediglich einen teilweisen Zugriff und/oder eine Nutzung im Einklang mit dem ursprünglich verfolgten Ziel, weswegen die Daten öffentlich zugänglich gemacht wurden, vorsieht. Es gibt daher nicht nur eine einzige Kategorie von personenbezogenen Daten, die der Öffentlichkeit zugänglich gemacht und aus der Sicht des Datenschutzes einheitlich verarbeitet werden sollten, sondern es gilt vielmehr, anhand einer Stufenanalyse zwischen dem Recht des Einzelnen, auf den sich diese Daten beziehen, und dem Recht der Öffentlichkeit auf Zugriff zu Informationen abzuwägen. Auch der Zugriff der Öffentlichkeit auf Daten kann bestimmten Bedingungen unterworfen sein (wie Rechtfertigung durch ein legitimes Interesse); selbst die Nutzung der Daten z. B. zu kommerziellen Zwecken oder durch Medien kann beschränkt werden. Diese Fragen werden durch zahlreiche Beispiele veranschaulicht.

2.3.6. Verhaltensregeln

Artikel 27 der Richtlinie 95/46/EG sieht vor, dass die Kommission und die Mitgliedstaaten die Ausarbeitung von Verhaltensregeln fördern, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen, die die Mitgliedstaaten zur Umsetzung der Richtlinie erlassen. Die Entwürfe für gemeinschaftliche Verhaltensregeln können der Datenschutzgruppe nach Artikel 29 unterbreitet werden. Die Gruppe nimmt insbesondere dazu Stellung, ob die ihr unterbreiteten Entwürfe mit den zur Umsetzung der Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Die Kommission kann dafür Sorge tragen, dass die Verhaltensregeln, zu denen die Gruppe eine positive Stellungnahme abgegeben hat, in geeigneter Weise veröffentlicht werden. Die Gruppe hat eine

Arbeitsunterlage[33] erarbeitet, mit der das Verfahren sowie einige spezifische Regeln für die gemeinschaftlichen Verfahrensregeln geklärt werden. Der Vorsitzende, das Sekretariat (von der Kommission gestellt) und die Mitglieder haben bis zur Annahme einer endgültigen Fassung der Stellungnahme spezifische Aufgaben wahrzunehmen. Bislang wurden noch keine Verhaltensregeln angenommen. Die Gruppe und die Organisationen, die Entwürfe eingereicht haben, haben die Diskussion über die endgültige Form der Verfahrensregeln noch nicht abgeschlossen.

FEDMA

Die FEDMA (Federation of European Direct Marketing) in ihrer Eigenschaft als Vertreterin des Direktmarketingsektors auf europäischer Ebene hat einen Entwurf für gemeinschaftliche Verfahrensregeln für die Verwendung personenbezogener Daten im Direktmarketing vorgelegt[34]. Ihre nationalen Mitglieder sind die Verbände für den Direktabsatz (Direct Marketing Associations, DMA) von zwölf Mitgliedstaaten der Europäischen Union (alle außer Luxemburg, Dänemark und Griechenland) sowie der Schweiz, Ungarns, Polens, der Tschechischen Republik und der Slowakischen Republik, die Nutzer, Diensteanbieter und Medien/Betreiber im Bereich des Direktmarketing vertreten. Der FEDMA gehören auch rund 500 Firmen als Direktmitglieder an. Direkt oder indirekt über die Handelsverbände vertritt die FEDMA insgesamt rund 10 000 Direktmarketingorganisationen.

Die Datenschutzgruppe hat eine Untergruppe gebildet, die sich mit den FEDMA-Verfahrensregeln befasst und die am 3. Dezember 1998 der Datenschutzgruppe ihren ersten Bericht vorlegte. Darin kommentierte sie die erste Entwurfsfassung der von der FEDMA am 18. August 1998 vorgestellten Verfahrensregeln für Europa. In ihrem Bericht gelangt die Untergruppe zu der Schlussfolgerung, dass der Entwurf in vielen Punkten nicht mit der Richtlinie im Einklang steht und keinen ausreichenden Mehrwert bietet. Darüber hinaus wurde ein Treffen mit der FEDMA vorgeschlagen, bei dem die strittigen Punkte erörtert werden sollten. Die Kommentare gingen (ohne Veröffentlichung) der FEDMA zu. Am 12. Juli 1999 legte die FEDMA der Untergruppe eine überarbeitete Fassung vor. Nach einer neuerlichen Analyse gelangte die Untergruppe zu dem Schluss, das zwar deutliche Verbesserungen vorgenommen worden seien, der Entwurf jedoch immer noch nicht

33 WP 13 (5004/98): Künftige Arbeit im Hinblick auf Verhaltensregeln: Arbeitsunterlage über das Verfahren für die Prüfung der Verhaltensregeln der Gemeinschaft durch die Arbeitsgruppe. Angenommen am 10. September 1998 (in 11 Sprachen).

34 In diesem Entwurf bleiben Fragen des Online-Direktmarketing und des elektronischen Geschäftsverkehrs, die von der FEDMA gesondert bearbeitet werden, ausgeklammert. Die FEDMA-Untergruppe ist der Ansicht, dass auch die Verfahrensregeln für den elektronischen Geschäftsverkehr der Gruppe vorgelegt werden sollten.

völlig mit der Richtlinie im Einklang stehe und auch weiteren Mehrwert beinhalten könnte (z. B. insbesondere mit Blick auf für den Direktmarketingsektor typische Verarbeitungsvorgänge sowie die grenzübergreifende Bearbeitung von Einzelbeschwerden).

IATA

Im Jahr 1997 hat die IATA (International Air Transport Association) der Datenschutzgruppe das Dokument „Recommended Practice 1774 - Protection of privacy and transborder data flows of personal data used in international air transport of passengers and cargo“ (Empfohlene Verfahren für den Schutz der Privatsphäre und für die grenzüberschreitende Übermittlung von Passagier- und Frachtgutdaten im internationalen Luftverkehr) (RP 1174) vorgelegt. Diese Leitlinien werden von der IATA bereits seit Jahren ihren Mitgliedern empfohlen. Nach dem Inkrafttreten der Richtlinie 95/46/EG überarbeitete die IATA ihr Papier RP 1174 mit dem Ziel der Einhaltung der Richtlinie und eines möglichen Beitrags zur freien Übermittlung von personenbezogenen Daten zwischen ihren internationalen Mitgliedern.

2.3.7. EU-Charta der Grundrechte

Die Gruppe gab gegenüber dem Konvent, der mit der Ausarbeitung der Europäischen Charta der Grundrechte betraut ist, die dringende Empfehlung ab, zusätzlich zum Recht auf die Achtung der Privatsphäre auch das Grundrecht auf Datenschutz in die Charta aufzunehmen[35].

2.4. Wichtige Entwicklungen in den Mitgliedstaaten

35 WP 26 (5143/99): Empfehlung 4/99 über die Aufnahme des Grundrechts auf Datenschutz in den Europäischen Grundrechtskatalog. Angenommen am 7. September 1999.

Wie auch in den vergangenen Jahren wurden die Datenschutzbehörden der verschiedenen Mitgliedstaaten ersucht, ihre Beiträge zu den Entwicklungen im Bereich des Datenschutzes in ihren Ländern im Jahr 1999 zu übermitteln. Diese Beiträge sind nachfolgend zusammengefasst. Am Ende der Beiträge sind jeweils die Adressen der entsprechenden Websites aufgeführt, auf denen die vollständigen Texte der Jahresberichte der Datenschutzbehörden abrufbar sind. Anhang 3 enthält die vollständige Liste dieser Adressen.

Der einzige Unterschied gegenüber dem Vorjahr besteht darin, dass die Datenschutzbehörden gebeten wurden, einen Fragebogen auszufüllen, statt eine Zusammenfassung der wichtigsten Entwicklungen in ihrem Land zu erstellen. In diesem Fragebogen geht es um fünf spezifische Themen:

A: 1999 in dem jeweiligen Land angenommene legislative Maßnahmen im Bereich der ersten Säule der EU, die sich auf den Schutz der Privatsphäre und den Datenschutz ausgewirkt haben (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG).

B: 1999 in dem jeweiligen Land durchgeführte Änderungen beim Datenschutz und beim Schutz der Privatsphäre im Bereich der zweiten und dritten Säule der EU.

C: Rechtsprechung (nationale Gerichte): Beschreibung der wichtigsten Rechtsfälle im Jahr 1999 in dem jeweiligen Land, die den Datenschutz und den Schutz der Privatsphäre berühren, insbesondere Verfahren mit einer grenzüberschreitenden Dimension.

D: Spezifische Themen - z. B. Aktivitäten von Datenschutzbehörden: Beschreibung der Themen im Bereich des Datenschutzes, die 1999 in dem jeweiligen Land Probleme aufgeworfen haben, oder sonstiger Themen, die im Bereich des Datenschutzes und des Schutzes der Privatsphäre in Jahr 1999 von Bedeutung waren und die entweder im eigenen Land oder auf EU-Ebene behandelt werden müssen (z. B. durch Maßnahmen der nationalen Behörde).

E: Die jeweiligen Adressen der Websites, auf denen die Jahresberichte abrufbar sind.

ÖSTERREICH

A. In Österreich angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Zusammen mit dem Datenschutzgesetz (DSG) von 2000 nahm das Parlament das Bundesstatistikgesetz von 2000, BGBl. I Nr. 163/1999, das Bundesarchivgesetz, BGBl. I Nr. 162/1999, und die Änderung des Versicherungsvertragsgesetzes, BGBl. I Nr. 150/1999 an.

Ziel des Bundesstatistikgesetzes ist es, eine Rechtsgrundlage für die Beschaffung von Daten für statistische Erhebungen aus öffentlichen Registern und von Verwaltungsbehörden zu schaffen, um zum einen die Belastung der Auskunftspersonen zu verringern und zum anderen der Statistik Austria die rationellere Erstellung von Statistiken zu ermöglichen. Darüber hinaus stellt das Gesetz Qualitätskriterien und -grundsätze auf, die bei der Erstellung von Statistiken und volkswirtschaftlichen Gesamtrechnungen eingehalten werden müssen, sowie die dazu gehörigen Kontrollmechanismen, um objektive amtliche Statistiken zu gewährleisten, die den internationalen Standards entsprechen und wissenschaftlichen Ansprüchen genügen.

Das Bundesgesetz über die Sicherung, Aufbewahrung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz) trat ebenfalls am 1. Januar 2000 in Kraft. Mit diesem Gesetz soll eine rechtsverbindliche Definition für Archivmaterial geschaffen werden, die auch den heute verfügbaren technischen Möglichkeiten zur Erstellung schriftlicher Aufzeichnungen Rechnung trägt und darüber hinaus eindeutige rechtliche Bestimmungen für den Schutz und die Speicherung/Lagerung von historisch wertvollen Dokumenten und/oder die Schaffung von Rechtsgrundlagen für den Zugang zu dem Archiv festlegt. Zuständig hierfür ist der Bund.

Die Datenschutzrichtlinie gab unter anderem den unmittelbaren Anlass für die Änderung des Versicherungsvertragsgesetzes, da bisher nicht eindeutig geregelt war, in welchem Umfang private Versicherer auf Gesundheitsdaten zugreifen dürfen. Aus diesem Grund wurde in Abschnitt 11a des Versicherungsvertragsgesetzes eine Rechtsgrundlage für die Nutzung von Gesundheitsdaten durch Versicherer eingeführt. Die Bestimmung regelt, wann und für welche Zwecke Versicherer Gesundheitsdaten verwenden dürfen und an wen diese übermittelt werden dürfen. Darüber hinaus wurden Bestimmungen zum Schutz der Rechte der Betroffenen aufgenommen.

Im BGBl. I Nr. 190/1999 wurde das Signaturgesetz (SIG) in Österreich eingeführt, das durch Umsetzung der Richtlinie 1999/93/EG den rechtlichen Rahmen für die Erzeugung und Verwendung von elektronischen Signaturen und für die Erbringung von Signatur- und Zertifizierungsdienstleistungen schafft.

B. In Österreich durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Die Sicherheitspolizeigesetznovelle von 1999, BGBl. I Nr. 146/1999, enthält unter anderem Bestimmungen für die folgenden Bereiche: Als Ausgleich für die Abschaffung der Grenzkontrollen beim Beitritt Österreichs zum Schengen-Durchführungsübereinkommen sind Maßnahmen zur Kontrolle von Personen und Gütern im internationalen Verkehr (sogenannte „Schleierfahndung“, nicht auf konkrete Verdachtsmomente begründete Kontrollen) vorgesehen. Außerdem wurden Bestimmungen für polizeiliche Unterlagen eingeführt, die die Verwendung von durch DNA-Analysen gewonnenen genetischen Informationen betreffen. Da verschiedene internationale Verordnungen (EURATOM-Verordnung Nr. 3, Entscheidung der Europäischen Kommission vom 30. November 1994, Beschluss des Rates vom 27. April 1998, Europol-Übereinkommen) die Durchführung von eingehenden Sicherheitsüberprüfungen vorschreiben, wurde die Zahl der Fälle, in denen Sicherheitsüberprüfungen zulässig sind, erhöht, darüber hinaus ist es jetzt unter bestimmten Umständen möglich, zur Sicherheitsüberprüfung nachrichtendienstliche Ermittlungen durchzuführen. Im Innenministerium wurde ein Beratungsgremium für Menschenrechtsfragen eingesetzt, das den Innenminister in Menschenrechtsfragen berät.

BELGIEN

A. In Belgien angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Keine.

B. In Belgien durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

1999 wurden zur Stärkung der Verbrechensbekämpfung mehrere legislative Maßnahmen eingeleitet, die einerseits auf Cyberkriminalität und andererseits auf Straftaten im Zusammenhang mit Kinderpornografie und Menschenhandel ausgerichtet sind.

Im Laufe des Jahres 1999 wurden Gesetzentwürfe ausgearbeitet und der Kommission für den Schutz der Privatsphäre zur Stellungnahme vorgelegt. In einem dieser Entwürfe ging es um die Zusammenarbeit von Telekommunikationsfirmen bei der Überwachung des Fernmeldeverkehrs. Die Kommission begründete ihre negative Stellungnahme zu diesem Entwurf vorrangig damit, dass der Anwendungsbereich des Entwurfs und die Umstände, unter denen die Justizbehörden entsprechende Daten anfordern und einsehen können, zu weit gefasst seien. In bezug auf einen weiteren Gesetzentwurf zur Cyberkriminalität äußerte die Kommission Bedenken, insbesondere im Hinblick auf die Pflicht der Telekommunikationsbetreiber zur Aufbewahrung von Verkehrsdaten und die Risiken, die mit der Einführung eines allgemeinen Systems zur Überwachung des Fernmeldeverkehrs[36] verbunden sind.

Die Kommission gab auch eine Stellungnahme zur Verarbeitung personenbezogener Daten im Rahmen von „VICLAS" (Violent Crime Linkage Analysis System) ab. Dieses System stützt sich auf die Analyse von Daten über Opfer und Täter von Schwerverbrechen und eventueller Serienverbrechen (z. B. Mord, sexuelle Gewalt), um mögliche Verbindungen zwischen solchen Verbrechen herzustellen. Das System wird in mehreren Ländern innerhalb und außerhalb der EU eingesetzt. Zwar steht der Nutzen dieses Systems außer Zweifel, doch brachte die Kommission einige Kritikpunkte im Hinblick auf seine Übereinstimmung mit den belgischen Rechtsvorschriften zum Schutz der Privatsphäre an. Insbesondere unterstrich sie die dringende Notwendigkeit eines rechtlichen Rahmens für die Verarbeitung der in VICLAS gespeicherten sensiblen und medizinischen Daten durch Justizbehörden. Außerdem verwies sie auf eine Reihe von Informationen über Opfer, die nur im Bedarfsfall systematisch gespeichert werden sollten. In Bezug auf DNA-Informationen sprach sich die Kommission gegen eine Vermehrung von DNA-Datenbanken aus und vertritt die Meinung, dass in VICLAS keine eigene DNA-Datenbank angelegt, sondern das bisherige Verfahren für die Abfrage und Nutzung solcher Daten eingehalten werden sollte. Abschließend empfahl die Kommission eine Aufbewahrung der Daten je nach Qualität über einen befristeten Zeitraum und nicht - wie ursprünglich vorgesehen - für generell 30 Jahre.

36 Der endgültige Wortlaut dieser Gesetze wurde im Jahr 2000 ausgearbeitet und angenommen (für Straftaten im Internet).

C. Wichtige Rechtsprechung

Keine wichtige Rechtsprechung im Bereich des Schutzes der Privatsphäre und des Datenschutzes.

D. Spezifische Themen

Wie in Absatz B oben dargelegt, wurde von amtlicher Seite zur Erarbeitung von Maßnahmen zur Verbrechensbekämpfung Stellung genommen (Überwachung des Fernmeldeverkehrs, Sammlung von Daten über Verbrechen usw.).

Angesichts der steigenden Anzahl von Anfragen bei der Kommission bezüglich der Bedingungen für den Einsatz von Videoüberwachungssystemen hat die Kommission auf eigene Initiative eine Stellungnahme zu diesem Thema veröffentlicht, die eine frühere Stellungnahme von 1995 zum gleichen Thema ablöst. In dieser Stellungnahme wird die Anwendung der neuen Rechtsvorschriften zum Schutz der Privatsphäre auf die Verarbeitung von Bilddaten und insbesondere auf den Einsatz von Überwachungskameras interpretiert und geklärt.

Es fanden regelmäßige Treffen mit Mitgliedern der belgischen Kommission statt, die eine Studie über die Juden während des Zweiten Weltkriegs geraubten Besitztümer leitete. Die Kommission für den Schutz der Privatsphäre hat die Bedingungen für die Zusammenarbeit mit den Banken und Versicherungsgesellschaften und für die Übermittlung von denen Daten an die für die Studie zuständige Kommission festgelegt.

Außerdem untersuchte die Kommission die Frage der Anwendung der Rechtsvorschriften zum Schutz der Privatsphäre auf Verstorbene und gelangte zu dem Ergebnis, dass gegenwärtig keine angemessenen Vorschriften existieren, die den Schutz personenbezogener Daten eines Verstorbenen gewährleisten und die z. B. den Erben des Verstorbenen ein Zugangsrecht zu gewissen Daten einräumen (z. B. falls eine Überprüfung der medizinischen Unterlagen des Verstorbenen notwendig ist, wenn ein Kunstfehler als Todesursache vermutet wird). Die Kommission sprach sich für die Einleitung entsprechender legislativer Maßnahmen aus, um in solchen Situationen Abhilfe zu schaffen.

Weiterhin nahm die Kommission auf eigene Initiative Stellung zu den neuen Nutzungsmöglichkeiten von Telefonverzeichnissen und insbesondere zur Online-

Veröffentlichung von Telefonverzeichnissen, die eine Umkehrsuche, z. B. anhand der Telefonnummer, gestatten. Die Kommission betonte, dass eine solche Veröffentlichung nur unter ganz bestimmten Voraussetzungen erfolgen dürfe und unter anderem der vorherigen Unterrichtung und Zustimmung der Betroffenen bedürfe.

E. Website

http://www.privacy.fgov.be

DÄNEMARK

A. In Dänemark angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

In Dänemark werden jedes Jahr verschiedene Gesetze und Verordnungen mit Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz verschiedet. Eine vollständige Auflistung all dieser Rechtsvorschriften ist an dieser Stelle nicht möglich. Insbesondere im Bereich der Telekommunikation wurden 1999 mehrere neue Verordnungen angenommen.

B. In Dänemark durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Keine.

C. Wichtige Rechtsprechung

Alle Rechtsfälle im Zusammenhang mit den beiden Einwohnermeldegesetzen wurden 1999 von der dänischen Datenschutzbehörde verwaltungsrechtlich entschieden.

D. Spezifische Themen

1999 befasste sich die dänische Datenschutzbehörde mit zwei Fällen, in denen es um die Frage der Überwachung der Internet-Nutzung von Arbeitnehmern und Studenten anhand eines Protokolls ging. Die dänische Datenschutzbehörde kam in beiden Fällen zu dem Ergebnis, dass die Protokollierung der Internet-Nutzung von Studenten und Arbeitnehmern in den Geltungsbereich des Gesetzes über behördliche Register fällt. Die dänische Datenschutzbehörde vertrat die Auffassung, dass die Datenaufzeichnung rechtmäßig ist, wenn ihr ein begründeter Zweck zugrundeliegt und die Arbeitnehmer und Studenten von der Datenaufzeichnung zuvor in Kenntnis gesetzt wurden.

Die dänische Datenschutzbehörde sprach auch Sicherheitsbelange im Zusammenhang mit dem Umstand an, dass viele behördliche Register – darunter auch Register mit sensiblen Daten – vom Privatunternehmen „Computer Science Corporation" (CSC) unterhalten werden. Nach Auffassung der dänischen Datenschutzbehörde gibt es diesbezüglich keine Sicherheitsprobleme, solange die Einhaltung der einschlägigen Rechtsvorschriften durch CSC gewährleistet ist. Dabei sei die Tatsache, dass CSC ein Privatunternehmen ist, nicht von Bedeutung.

1999 hat die dänische Datenschutzbehörde gegenüber dem Justizministerium Stellung zu den Plänen bezogen, ein DNA-Verzeichnis mit Personen anzulegen, denen Schwerverbrechen zur Last gelegt werden oder die wegen bestimmter Schwerverbrechen bereits angeklagt oder verurteilt wurden. Die dänische Datenschutzbehörde befand, dass die Eintragung nicht verurteilter Personen in das Verzeichnis nicht im Widerspruch zum Gesetz über behördliche Register steht. Dennoch empfahl die dänische Datenschutzbehörde, das Verzeichnis per Gesetz autorisieren zu lassen.

E. Website

www.datatilsynet.dk (nur in dänischer Sprache)

FINNLAND

A. In Finnland angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Mit Blick auf die Umsetzung der Grundsätze der Richtlinie wurden die Prüfungen in verschiedenen Bereichen der Rechtsvorschriften fortgesetzt. Beispielsweise wurden 1999 die Bestimmungen des Gesetzes über die Unterrichtung der Bevölkerung untersucht, das dem nationalen System für die Unterrichtung der Bevölkerung zugrundeliegt. Das Gesetz über elektronische Ausweise trat im Dezember 1999 in Kraft. Ende 1999 verabschiedete das Parlament das Gesetz über elektronische Dienste in der Verwaltung, das am 1. Januar 2000 in Kraft trat. Das am 1. Dezember 1999 in Kraft getretene Gesetz über eine offene Verwaltung regelt die Offenlegung personenbezogener Daten aus Verwaltungsdateien, die Vorschriften für die Geheimhaltung von Unterlagen und personenbezogenen Daten sowie bewährte Verfahren im Informationsmanagement.

B. In Finnland durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Den Bestimmungen der EU-Datenschutzrichtlinie wird auch im Hinblick auf Themen im Bereich der zweiten und dritten Säule Rechnung getragen. 1999 wurde unter anderem eine Prüfung der Rechtsvorschriften für Dateien mit personenbezogenen Daten veranlasst, die von polizeilichen Stellen geführt werden.

C. Wichtige Rechtsprechung

Nach finnischem Recht ist die Staatsanwaltschaft zur Anhörung des Beauftragten für den Datenschutz verpflichtet, bevor sie wegen Verletzung des Gesetzes über personenbezogene Daten Klage erhebt. Die Gerichte sind verpflichtet, bei der gerichtlichen Verhandlung eines solchen Falls dem Datenschutzbeauftragten Gelegenheit zur Anhörung zu geben. In 15 Fällen gab der Datenschutzbeauftragte eine Stellungnahme ab. In diesen Fällen ging es unter anderem um die gesetzwidrige Aufbewahrung von Dateien, die Verwertung von Dateien mit personenbezogenen Daten für andere als die ursprünglich vorgesehenen Zwecke, illegales Eindringen in Computersysteme sowie um Fragen der Offenlegung und Geheimhaltung von Daten.

D. Spezifische Themen

Das Amt des Datenschutzbeauftragten befasste sich hauptsächlich mit Fragen des Datenschutzes im Gesundheitswesen und in der Arbeitswelt. Eine deutliche Zunahme von Anfragen, ob eine Verletzung des Schutzes der Privatsphäre vorliegt, war vor allem in den Bereichen elektronische Dienste und Kundenkontakte, elektronischer Handel im Internet, Internet-Nutzung und allgemeine Fragen im Zusammenhang mit der elektronischen Datenübermittlung, Telekommunikation und dem Einsatz neuer Technologien zu verzeichnen. Das Problem besteht generell in der Einführung von Informationstechnik und neuen Technologien, ohne dass zuvor die Rechtsgrundlage untersucht und die Verarbeitung personenbezogener Daten angemessen geplant wurde.

Das Hauptziel des Amtes des Datenschutzbeauftragten bestand in der Verhütung von Datenschutzverletzungen. Aus diesem Grund veröffentlichte das Amt Leitlinien und Informationsbroschüren zu dem neuen Gesetz über personenbezogene Daten (insgesamt 15 Broschüren) und führte rund 140 Aufklärungsseminare durch. Das Amt bezog zu insgesamt 55 Regierungsvorlagen hinsichtlich der Verarbeitung personenbezogener Daten Stellung oder wurde im Parlament dazu angehört.

Das Amt setzte sich für die Ausarbeitung von Verhaltensregeln ein, die den Besonderheiten der einzelnen Wirtschaftszweige gemäß Artikel 27 der EU-Datenschutzrichtlinie Rechnung tragen. In den einzelnen Wirtschaftszweigen wurden Maßnahmen zur Ausarbeitung entsprechender Verhaltensregeln eingeleitet. Die Verhaltensregeln für Schadens- und Lebensversicherungsgesellschaften und den Sport wurden bereits 1999 ausgearbeitet. Vor allem private Krankenversicherungsgesellschaften stellten Leitlinien für die Verarbeitung personenbezogener Daten auf. Eine Reihe von zentralen Verwaltungsbehörden arbeiteten Leitlinien aus, die als Verhaltensregeln für den jeweiligen Verwaltungsbereich eingestuft werden können.

Aufgrund des Inkrafttretens der EU-Datenschutzrichtlinie gab es weniger Fälle in bezug auf die Offenlegung von Daten gegenüber Empfängern im Ausland als in den Jahren zuvor. Die Weitergabe von Daten in Länder außerhalb der EU erfolgte hauptsächlich zum Zwecke des Direktmarketing. In einem Fall setzte der Datenschutzbeauftragte die Europäische Kommission von der genehmigten Übermittlung in Kenntnis.

E. Website

www.tietosuoja.fi

FRANKREICH

A. In Frankreich angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Datenschutzfragen nehmen in den Nachrichten immer mehr Raum ein – von epidemiologischen Untersuchungen zu HIV über die Einrichtung von Datenbanken, in denen der „genetische Fingerabdruck" von Sexualstraftätern erfasst wird, bis hin zum aktiven Vorgehen der CNIL, durch das gewährleistet werden soll, dass Websites im Internet die Rechtsvorschriften einhalten.

Zwei neue Rechtsvorschriften lösten 1999 in Frankreich intensive Diskussionen in der Öffentlichkeit aus, bei denen es um zwei soziale Themen von erheblichem Belang für den Datenschutz ging.

Die erste Streitfrage betraf den Aufbau einer landesweiten Datenbank mit „genetischen Fingerabdrücken" gemäß dem Gesetz vom 17. Juni 1998 zur Prävention und strafrechtlichen Verfolgung von Sittlichkeitsdelikten und zum Schutz der Jugend. Die Datenbank enthält ausschließlich die genetischen Fingerabdrücke von verurteilten Sexualstraftätern, die Daten von Verdächtigen werden nicht gespeichert. Neben weiteren Sicherheitsmaßnahmen wurden, nachdem die CNIL ihre Stellungnahme abgegeben hatte, vorrangig Durchführungsmaßnahmen eingeleitet, die dafür sorgen, dass für Identifizierungszwecke nur nicht-codierende DNA-Segmente verwendet werden, d. h. Abschnitte, die keine Rückschlüsse auf organische, physiologische oder morphologische Merkmale der Betroffenen zulassen.

Das zweite Diskussionsthema bezog sich auf die Aufstellung von Registern, in denen Personen erfasst werden, die einen so genannten *„pacte civil de solidarité"* (PACS, zivilrechtlicher Solidaritätsvertrag) geschlossen haben, der unverheiratet zusammenlebenden, auch gleichgeschlechtlichen Paaren gewisse Rechte einräumt (z. B. Abgabe einer gemeinsamen Steuererklärung, Sozialversicherungsansprüche, Recht auf Wohnung, insbesondere beim Tod des Partners usw.). Letztlich sollen diese Register dazu dienen, dass Personen, die einen PACS-Vertrag abschließen wollen, nachprüfen können, ob ihr Partner nicht bereits mit einer anderen Person einen derartigen Vertrag unterzeichnet hat. Nach Stellungnahme der CNIL kam man überein, dass diese Register legal von solchen öffentlichen oder privaten

Einrichtungen konsultiert werden dürfen, die für die Umsetzung der durch die neuen Rechtsvorschriften gewährten Rechte zuständig sind (Finanzämter, Sozialversicherung, Kreditinstitute). Da die in diesen Registern erfassten Daten zweifellos auch moralische Fragen betreffen und die Daten daher als sensibel einzustufen sind, dürfen sie weiteren Personenkreisen wie Vermietern oder Familienangehörigen nicht zugänglich gemacht werden. Darüber hinaus äußerte die CNIL den Wunsch – dem auch Rechnung getragen wurde –, dass aus den Registern keine Listen von Partnern nach deren sexueller Orientierung erstellt werden können dürfen. Und zu guter Letzt wird dank der CNIL keine „PACS-Bescheinigung“ ausgestellt, so dass etwa Arbeitgeber oder Vermieter nicht in Versuchung geraten, Bewerber zur Vorlage dieser Bescheinigung zu drängen und auf diese Weise an vertrauliche Informationen zu gelangen.

Außerdem verabschiedete das Parlament gesetzgeberische Maßnahmen, die es den Steuerbehörden erlauben, Sozialversicherungsnummern heranzuziehen Besteuerungsgrundlagen festzulegen und zu prüfen sowie Steuern einzuziehen (Artikel 107 des Finanzgesetzes für 1999). Der Staatsrat wurde um seine Entscheidung zu dieser Bestimmung ersucht und nahm sie an, da das Ziel eingeschränkt sei und garantiere, dass das Gesetz über „Informatik und Freiheit“ soweit es betroffen sei, volle Anwendung finde. Die Durchführungsmaßnahmen, die der vorherigen Überprüfung durch die CNIL bedürfen, legen fest, dass die Sozialversicherungsnummer nicht zur Identifikation sämtlicher von den Steuerbehörden geführten Unterlagen verwendet werden darf. Zudem kann bei gravierenden Verletzungen der informationellen Selbstbestimmung die Vernichtung der Akten, die diese Nummer enthalten, angeordnet werden.

B. In Frankreich durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Keine.

C. Wichtige Rechtsprechung

Die CNIL verwies zwei Fälle an die Justiz. Der erste betraf die Weitergabe einer Liste der Mitglieder einer regionalen religiösen Jugendgemeinschaft an eine Organisation der extremen Rechten, die Nazi-Memorabilia verkauft. Der zweite Fall betraf die Anmerkung „entspricht nicht dem geforderten Profil, homosexuell“ in den Bewerbungsunterlagen bei einem großen Unternehmen.

Die Gerichte haben über beide Fälle noch nicht entschieden.

D. Spezifische Themen

Neben den beiden vorgenannten, in der Öffentlichkeit diskutierten Themen, zu denen die CNIL Stellung nahm, sind im Jahr 1999 vor allem die folgenden Tendenzen zu verzeichnen:

- Eine Zunahme der Anträge auf Einsicht in sicherheitsrelevante Akten (vor allem seitens der Polizei) um mehr als 67 %, dies entspricht 671 Anträgen, die 1100 Überprüfungen und direkte Einsichtnahmen der fraglichen Akten zur Folge hatten.

- Eine allgemeine Zunahme der Zahl der Beschwerden (um 31 %) und der neuen Verarbeitungsdeklarationen (250 pro Tag).

- Ganz erhebliche Aktivitäten in den Bereichen Einzelhandel und Telekommunikation im Zusammenhang mit den in diesen Wirtschaftszweigen tätigen Akteuren.

Die CNIL stand als treibende Kraft hinter der Annahme der von wichtigen Einzelhandelsunternehmen aufgestellten 4. Verhaltensregeln für den Einzelhandel. Diese sehen insbesondere die Aufnahme von zwei zusätzliche Kontrollkästchen in Online-Bestellformulare vor. Durch Markieren des ersten Kästchens kann die betreffende Person die Zusendung von Werbematerial durch das fragliche Einzelhandelsunternehmen verweigern, während das zweite Kästchen die Möglichkeit bietet, die entgeltliche Weitergabe von Daten an Dritte zu untersagen.

Die CNIL führte ihre seit Jahren betriebene aktive Aufklärungspolitik und Überprüfung von Websites fort. Eine Liste der Websites, die sich zur Einhaltung des Gesetzes verpflichten, wurde auf der CNIL-Website veröffentlicht.

Die CNIL führte auch eine Studie zum „Spamming“ (Zusendung unerwünschter E-Mail-Sendungen) durch, die der Öffentlichkeit am 14. Oktober 1999 zugänglich gemacht wurde (www.cnil.fr). Nach Auffassung der CNIL verstößt das Sammeln von E-Mail aus öffentlich zugänglichen Bereichen des Internet und deren Verwertung für jede Art der Kundenwerbung gegen das Gesetz, wenn die Betroffenen nicht eindeutig darüber aufgeklärt wurden, dass dies geschieht und ihnen nicht Gelegenheit gegeben wurde, bei der Erfassung der Daten online diese Art der Verwendung zu untersagen.

Mit Blick auf den Fernmeldeverkehr sprach die CNIL eine Empfehlung bezüglich der neuen Mobilfunkdienste aus, die Anrufe zum Spartarif ermöglichen, wenn der Teilnehmer der Wiedergabe von Werbung während des Gesprächs zustimmt. Die Empfehlung wurde veröffentlicht und allen Mobilfunkbetreibern zugestellt. Im Einzelnen wird gefordert, dass der fragliche Dienst dem Teilnehmer die Möglichkeit bieten muss, Anrufe zu tätigen, ohne dass Werbung abgespielt wird. Wenn die Werbung für den Angerufenen zu hören ist, muss dieser vorher hierüber informiert werden und die Möglichkeit haben, den Anruf zurückzuweisen.

Auch ein Bericht über Daten über den Standort von Mobiltelefonen wurde erstellt. Die CNIL ist der Ansicht, dass Standortdaten mit Blick auf die freie Wahl des Aufenthaltsorts als hochgradig sensibel einzustufen sind. Sie sollten keinesfalls länger als für die Rechnungsstellung notwendig gespeichert bleiben. Dieser Zeitraum sollte im übrigen für alle Netzbetreiber einheitlich festgelegt werden. Hinsichtlich der Verwendung von Standortdaten für die Kommunikation mit Dritten, unabhängig davon, ob es sich bei diesen um Personen oder um „lokale“ Mehrwertdienste handelt, forderte die CNIL, dass die Standortdaten keinesfalls standardmäßig übermittelt werden dürften, sondern nur in Notfällen. Dem Anrufer müsse von Fall zu Fall eine eindeutige und einfache Möglichkeit geboten werden, die Übertragung dieser Daten zuzulassen oder zu verweigern.

E. Website

www.cnil.fr **- dort „publications“ und danach „rapports annuels“ anklicken.**

DEUTSCHLAND

A. In Deutschland angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Mit einem Gesetz zum Schutz gegen ansteckende Krankheiten wird u. a. die Verarbeitung personenbezogener Daten im Bereich der Bekämpfung von Krankheiten geregelt.

Es wurde ein Gesetz über die Verkehrsstatistik in Verbindung mit dem Gesetz über die Binnenschifffahrt verabschiedet. Es enthält Bestimmungen für den Datenschutz im Bereich der Verkehrsstatistik und der Binnenschifffahrt.

B. In Deutschland durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Gesetz zur Änderung des DNA-Identitätsfeststellungsgesetzes vom 2. Juni 1999 (Bundesgesetzblatt I, Seite 1242).

Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs vom 28. Dezember 1999 (Bundesgesetzblatt I, Seite 2491).

Verlängerung der Gültigkeit von Paragraph 12 des Gesetzes über Fernmeldeanlagen (FAG) bis zum 31. Dezember 2001 (Bundesgesetzblatt I, Seite 2492).

C. Wichtige Rechtsprechung

1. Urteil des Bundesverfassungsgerichts vom 14. Juli 1999 über das Verbrechensbekämpfungsgesetz/Artikel 10 GG/Telekommunikationsüberwachung durch den Bundesnachrichtendienst (BVerfGE 100, 313).

2. Beschluss des Bundesverfassungsgerichts vom 27. Oktober 1999 über das Einsichtsrecht der Verwaltungsgerichte in geheimhaltungsbedürftige Unterlagen (BVerfGE 101, 106).

D. Spezifische Themen

- Aufbau einer landesweiten Gebäude-Bilddatenbank

- Datenschutz bei Fusionen und Unternehmensspaltungen

- Transparenz im Schufa-Scoring-Verfahren

- Datenschutz bei der Umstellung von Inhaberaktien auf Namensaktien

- Konflikt zwischen dem Datenschutz und der Unabhängigkeit der Medien

- Verbunddatei zur DNA-Analyse: Speicherung von Informationen nur auf Grundlage eines Gerichtsbeschlusses oder mit Einwilligung der Betroffenen

- Geldwäsche-Datei: Uneinigkeit über den Umfang der Daten, die über verdächtige Personen gespeichert werden

- Videoüberwachung durch die Polizei

E. Website

www.bfd.bund.de **oder** www.datenschutz.bund.de

(mit Links zu den Websites der Bundesländer)

GRIECHENLAND

Im Jahr 2000 traf die griechische Datenschutzbehörde die folgenden Beschlüsse von großer Tragweite:

Bedingungen für rechtmäßige Verarbeitung personenbezogener Daten für die Zwecke des Direktmarketing/der Werbung sowie zur Überprüfung der Kreditwürdigkeit

1) In bezug auf den Handel mit personenbezogenen Daten für die Zwecke des Direktmarketing und/oder der Verkaufsförderung ist die Verarbeitung entsprechender Daten mit Einschränkungen als gesetzmäßig zu betrachten. Die

Erfassung von personenbezogenen Daten darf entweder nach Zustimmung der Betroffenen oder anhand von für die Öffentlichkeit bestimmten Verzeichnissen wie z. B. Telefonverzeichnisse und Messekataloge erfolgen, sofern die Betroffenen der Aufnahme ihrer Daten in diese Verzeichnisse zugestimmt oder ihre Daten für ähnliche Zwecke veröffentlicht haben. Die Erfassung personenbezogener Daten ist auch dann als gesetzmäßig zu betrachten, wenn diese Daten aus öffentlich zugänglichen Quellen erfasst werden, allerdings nur, wenn die Bedingungen für den gesetzmäßigen Zugang zu diesen Daten eingehalten werden. Daten, die zu den vorgenannten Zwecken erfasst werden, können den vollständigen Namen sowie Anschrift und Beruf umfassen. Der Erfasser ist verpflichtet, das Sonderregister der Datenschutzbehörde zu konsultieren, in das auf Antrag Personen aufgenommen werden, die die Zustimmung für die Verwendung ihrer Daten für Direktmarketing- und Verkaufsförderungsaktivitäten verweigern und deren Daten somit nicht erfasst werden dürfen.

Mit seinem ersten Schreiben an einen Betroffenen muss der Versender den Empfänger über seine Informationsquelle unterrichten und die Zustimmung des Betroffenen zur Verwendung der Daten einholen. In ihrer Entscheidung verweist die Datenschutzbehörde auch auf das Verbraucherschutzgesetz, das die Übermittlung von Werbebotschaften mittels Telefon, Fax, elektronischer Post und sonstiger elektronischer Medien ohne ausdrückliche Zustimmung des Verbrauchers untersagt.

Hinsichtlich der Verarbeitung personenbezogener Daten zur Überprüfung der Kreditwürdigkeit wird die Datenschutzbehörde Bedingungen festlegen, die die Verarbeitung von Daten ohne Zustimmung der Betroffenen einschränkt. Im Einzelnen soll die Erfassung der folgenden Daten erlaubt sein: Konkursanträge, Entscheidungen über Konkursanträge, Wechsel, Versteigerungen von beweglichem Vermögen und Immobilien, Veränderungen bei Firmen, Aktiengesellschaften, Kapitalgesellschaften und Joint Ventures, Hypotheken und hypothekarische Sicherung, Pfändungen und Schecks gemäß Präsidialdekret Nr. 1923, ungedeckte Schecks, protestierte Wechsel und protestierte Orderpapiere.

Für die vorgenannten Kategorien sollen bestimmte zeitliche Begrenzungen für die Speicherung der Daten sowie Einschränkungen hinsichtlich der Aufzeichnung nachfolgender Änderungen in bezug auf diese Daten, z. B. unmittelbare Aufzeichnung der Begleichung eines fälligen Schecks, festgelegt werden.

Nach der Erfassung der Daten müssen die verantwortlichen Unternehmen die Betroffenen über die Erfassung unterrichten. Falls die Betroffenen gegen die Erfassung Einspruch erheben und die Löschung der Daten fordern, sind die Unternehmen verpflichtet, die Daten zu löschen und die Betroffenen über die möglichen Folgen dieser Löschung und möglichen Konsequenzen in bezug auf den

Austausch von Informationen aufklären. Die vorgenannten Daten dürfen nur an Unternehmen übermittelt werden, die die Daten entsprechend den Bestimmungen für die gesetzmäßige Verwendung nutzen. Es wird darauf hingewiesen, dass die Empfängerunternehmen nur berechtigt sind, Negativauskünfte zu sammeln. Positive Auskünfte über die finanzielle Situation von Betroffenen wie z. B. Immobilienbesitz dürfen nur mit Zustimmung der Betroffenen gesammelt werden. Damit wird die Erstellung von Gesamtprofilen über die finanzielle Situation von Betroffenen ohne deren Kenntnis verhindert.

Mit dieser Entscheidung will die Datenschutzbehörde die Bedingungen für die Verarbeitung von Daten über die Kreditwürdigkeit von Personen festlegen und dabei gleichzeitig den Schutz der Bürger im Hinblick auf die Verarbeitung personenbezogener Daten und das Recht griechischer Unternehmen auf den gesetzmäßigen Zugang zu für die Sicherheit von Datenaustauschvorgängen notwendigen Informationen gewährleisten.

Nichtaufnahme von Religionszugehörigkeit und sonstigen personenbezogenen Daten in Personalausweise

Die wichtigste und am heftigsten umstrittene Entscheidung der griechischen Datenschutzbehörde betraf die Nichtaufnahme einer Reihe von personenbezogenen Daten in den griechischen Personalausweis. Die Entscheidung, die sich unter anderem auf Angaben zur Religionszugehörigkeit bezieht, wird wie folgt begründet:

1. Die Personalausweise sind öffentliche Dokumente, die personenbezogene Daten enthalten. Diese Daten sind in den Archivierungssystemen der zuständigen Behörden verzeichnet und unterliegen der Verarbeitung zu dem Zweck, die Identität der jeweiligen Person zu verifizieren.

2. Gemäß Artikel 4 Absatz 1 Buchstabe b des griechischen Datenschutzgesetzes 2472/1997 müssen personenbezogene Daten, damit sie gesetzmäßig verarbeitet werden dürfen, „relevant und angemessen sein und dürfen den für den jeweiligen Fall im Zusammenhang mit den genannten Zwecken erforderlichen Umfang nicht überschreiten“. Die Grundsätze der Zweckbindung sowie der Notwendigkeit und der Angemessenheit der Daten im Hinblick auf den Zweck der Verarbeitung sind somit als Grundvoraussetzung für das gesetzmäßige Betreiben jedweden Archivierungssystems definiert. Eine Verarbeitung von personenbezogenen Daten über den angestrebten Zweck hinaus oder eine für das Erreichen dieses Zwecks weder angemessene noch notwendige Verarbeitung ist somit ungesetzmäßig.

3. Im vorliegenden Fall gehen im Hinblick darauf, dass der Zweck der Verarbeitung die Verifizierung der Identität des Betroffenen ist, die folgenden, in Dekret 127/1969 betreffend von der Polizeibehörde ausgestellte Personalausweise vorgesehenen Daten aus folgenden Gründen über den eigentlichen Zweck der Verarbeitung hinaus:

   a. Fingerabdruck des Betroffenen. Für die Verifizierung der Identität des Betroffenen ist ein Fingerabdruck nicht notwendig, da diese Verifizierung grundsätzlich anhand der Fotografie vorgenommen werden kann. Hinzu kommt, dass nach allgemeiner Auffassung ein Fingerabdruck („Erfassung“) mit dem Verdacht oder der Bestätigung einer strafrechtlich relevanten Handlung verbunden ist („Kriminalisierung“). Wird nun der gesamten griechischen Bevölkerung ein solches Attribut – oder auch nur die damit potenziell verbundene Implikation - zugewiesen, so übersteigt dies das notwendige Maß und verletzt die von der Verfassung unter Schutz gestellte Menschenwürde.

   b. Vollständiger Name der Ehefrau/des Ehemanns: Seit 1983 nimmt die Frau mit der Heirat nicht mehr automatisch den Namen des Ehemanns an. Außerdem dient diese Angabe nicht dem Zweck, zu dem der Personalausweis ausgestellt wird.

   c. Beruf: Diese Angabe ist nicht Bestandteil der physischen Identität einer Person, sie kann sich ändern und entspricht nach Ausstellung des Ausweises möglicherweise nicht mehr der Realität. Darüber hinaus ist diese Angabe ein gesellschaftliches Unterscheidungsmerkmal, das nicht zwangsläufig der Verarbeitung unterliegen sollte.

   d. Staatsangehörigkeit/Nationalität: Entsprechend der geltenden Rechtsvorschriften dürfen nur griechische Staatsbürger einen griechischen Personalausweis besitzen.

   e. Wohnanschrift: Diese Angabe ist weder notwendig noch geeignet (da Änderungen möglich sind), um die Identität einer Person nachzuweisen.

   f. Religionszugehörigkeit: Diese Angabe betrifft die Privatsphäre des Einzelnen und ist daher weder angemessen noch notwendig, um die Identität einer Person nachzuweisen.

4. Die Verarbeitung der vorgenannten Daten verstößt auch dann gegen das Gesetz, wenn der Betroffene hierzu seine ausdrückliche Zustimmung gemäß Gesetz 2472/1997, Artikel 5 Absatz 1 und Artikel 7 Absatz 2 Buchstabe a erteilt, da die Zustimmung eines Betroffenen jedwede Form der Verarbeitung ausschließt, die gegen das Gesetz oder die Grundsätze der Zweckbindung und der Notwendigkeit verstößt. Inhalt und Ausübung des Rechts auf informationelle Selbstbestimmung, das unter anderem durch die Zustimmung des Betroffenen zur Verarbeitung personenbezogener Daten einschließt, sind nicht im Einzelnen festgelegt. Sie werden im Kontext des und in engem Zusammenhang mit dem Zweck des Archivierungssystems oder der Verarbeitung in dem Sinne festgelegt, dass dieses Recht nicht zur Registrierung von Daten führen darf, die für den Zweck jedweden Archivierungssystems/jedweder Verarbeitung irrelevant sind.

Der Staatsrat befasst sich mit einer Beschwerde gegen die vorgenannte Entscheidung. Mit einer Entscheidung ist Ende Februar 2001 zu rechnen.

Entscheidung über die Identifizierung anhand von Fingerabdrücken

Die Datenschutzbehörde ist zuständig für die Untersuchung der Rechtmäßigkeit der Verarbeitung dieser Art von personenbezogenen Daten, da diese Verarbeitung, die die Erfassung, den Vergleich und die Archivierung von biometrischen Merkmalen umfasst, im Sinne des Gesetzes 2472/97 eine automatische Verarbeitung dahingehend darstellt, dass sie die Erkennung von Personen erlaubt.

Die Behörde macht die für die Verarbeitung Verantwortlichen darauf aufmerksam, dass in dem Fall, dass mit den vorgenannten Mitteln Daten erhoben werden, diese Erfassung und Verarbeitung die Grenzen des Angemessenheitsgrundsatzes gemäß Artikel 4 Absatz 1b des Gesetzes 2472/97 überschreitet, da der verfolgte Zweck, d. h. die Überwachung der Anwesenheit von Arbeitnehmern, durch gemäßigtere Mittel erreicht werden kann. Die Identifizierung von Betroffenen anhand von Fingerabdrücken dient üblicherweise der erkennungsdienstlichen Behandlung durch die Polizei. Die Erfassung von Fingerabdrücken in einem Archivierungssystem zum Zweck der Überwachung der Anwesenheit am Arbeitsplatz kann daher, ganz abgesehen von der verständlichen Reaktion der Betroffenen, nicht als vorrangig gegenüber dem Recht auf Schutz der Privatsphäre angesehen werden, so dass kein Grund für eine Ausnahme von dem allgemein gültigen Grundsatz besteht, dass derartige Informationen nur von Behörden gesammelt und gespeichert werden dürfen, die Kraft Gesetz hierzu bevollmächtigt sind. Die Zulassung einer derartigen Ausnahme wäre nur in Sonderfällen denkbar, etwa zum Zweck der Überwachung des Zugangs zu Bereichen, in denen vertrauliche Akten aufbewahrt werden oder bei Einrichtungen mit Zugangsbeschränkung.

Die Datenschutzbehörde erachtet daher dieses spezifische Mittel zur Erfassung und Verarbeitung von personenbezogenen Daten für ungesetzmäßig.

Abschließend ist festzuhalten, dass - da die Erfassung von Daten als wegen Überschreitung der Zweckbindung ungesetzmäßig erachtet wird - die mögliche Zustimmung von Betroffenen die Verarbeitung nicht legitimiert.

Gemäß Artikel 21 Absatz 1 des Gesetzes 2472/97 ist daher die Datenschutzbehörde der Auffassung, dass die für die Verarbeitung Verantwortlichen dazu verpflichtet werden müssen, innerhalb eines Monats nach Zustellung dieses Beschlusses die Verarbeitung abzubrechen (soweit sie bereits begonnen wurde) und alle relevanten Daten (die Fingerabdruck-Dateien) zu vernichten. Die für die Verarbeitung Verantwortlichen sind verpflichtet, gemäßigtere und wirksamere Mittel zur Überwachung einzusetzen, wobei vom Gesetz zugelassene und vorgesehene administrative Mittel zur Überwachung zu bevorzugen sind.

IRLAND

A. In Irland angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Keine.

B. In Irland durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Keine.

C. Wichtige Rechtsprechung

Keine in diesem Bereich.

D. Spezifische Themen

Keine, mit Ausnahme der Frage der Nutzung von Verzeichnissen, die eine Umkehrsuche gestatten, im Bereich der Telekommunikation, die später auf der Sitzung der Datenschutzgruppe erörtert wurde und die zur Formulierung der Stellungnahmen 7/2000 führte.

E. Website

www.dataprivacy.ie

ITALIEN

A. In Italien angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Relevante Gesetzestexte:

- Dekret Nr. 250 des Präsidenten der Republik Italien vom 22.06.99, das den Einsatz von Systemen für die Überwachung des Zustroms von Fahrzeugen in die Innenstädte und die Bildaufzeichnung im Straßenverkehr regelt (Straßenverkehrskontrolle, Bestrafung von Straßenverkehrsdelikten). Der Einsatz dieser Systeme wird auch im Hinblick auf die Vorkehrungen für die Sammlung und Aufbewahrung solcher Daten geregelt.

- Dekret Nr. 437 von 22.10.99, in dem die Voraussetzungen und Regelungen für die Ausstellung elektronischer Ausweise und elektronischer Ausweisdokumente festgelegt sind.

- Dekret vom 08.02.99, einschließlich der technischen Vorschriften für die Erstellung, Übermittlung, Vervielfältigung usw. von elektronischen Dokumenten.

- Gesetz Nr. 422 vom 19.10.99 zur Ratifikation des Übereinkommens über die Zustellung von gerichtlichen und außergerichtlichen Dokumenten in

zivilrechtlichen und kommerziellen Angelegenheiten in den Mitgliedstaaten der Europäischen Union.

- Dekret vom 18.02.99 zur Genehmigung des nationalen Statistikplans, in dem die Statistiker den von der Verarbeitung Betroffenen und ihren personenbezogenen Daten mehr Aufmerksamkeit widmen.

- Dekret Nr. 261 vom 22.07.99 zur Umsetzung der Richtlinie 97/67/EG über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstequalität, wobei die Geheimhaltung der Korrespondenz und der Schutz personenbezogener Daten als Grundvoraussetzungen genannt werden.

- Dekret Nr. 14 des Präsidenten der Republik Italien vom 16.03.99 einschließlich der Durchführungsverordnungen für die Richtlinien 95/18/EG und 95/19/EG über die Erteilung von Genehmigungen an Eisenbahnunternehmen und über die Zuteilung von Fahrwegkapazität der Eisenbahn und die Berechnung von Wegeentgelten. Gemäß Artikel 7 dieses Dekrets sind die verantwortlichen Stellen zur Einhaltung der im Gesetz Nr. 675/1996 verankerten Datenschutzbestimmungen verpflichtet.

- Leitlinien des Ministerpräsidenten für die computergestützte Verwaltung des Datenflusses zwischen öffentlichen Verwaltungsbehörden.

B. In Italien durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Keine.

C. Wichtige Rechtsprechung

Der Schwerpunkt der Rechtsprechung lag 1999 auf der Bewertung des Geltungsbereichs der Bestimmungen für den Zugriff auf Verwaltungsaufzeichnungen (Gesetz Nr. 241 vom 07.08.90) auf der Grundlage der Bestimmungen des Datenschutzgesetzes. Im Laufe des Jahres 1999 haben die Gerichte mehrere Entscheidungen erlassen, wobei insbesondere auf zwei Entscheidungen der 6. Kammer des Staatsrats hingewiesen wird (Nr. 59 vom 26.01.99 und Nr. 65 vom 27.01.99).

Die Verfahren für das Einlegen einer Beschwerde bei Garante – gemäß Artikel 29 des Datenschutzgesetzes – traten 1999 in Kraft. Sie stellen eine Alternative zu gerichtlichen Schritten dar und bringen den Betroffenen rasche Entscheidungen. Diese

Art von Beschwerde kann nur bei einem teilweisen oder völligen Verzicht auf die Wahrnehmung der Rechte eingelegt werden, die den Betroffenen gemäß Artikel 13 des Datenschutzgesetzes zustehen (Recht auf Einsichtnahme, Berichtigung, Erteilung von Auskünften, Löschung usw.). 1999 wurden bei Garante 150 Beschwerden eingelegt; nur in drei Fällen wurde die Entscheidung der Behörde vor einem ordentlichen Gericht angefochten.

In allen drei Berufungsfällen trat Garante zur Verteidigung seiner Entscheidung vor Gericht auf. In diesem Zusammenhang sei auf einen Fall verwiesen, in dem es um die Möglichkeit zur Anwendung des Datenschutzgesetzes ging – und damit um die Möglichkeit eines Betroffenen, Widerspruch einzulegen –, selbst bei Verarbeitungsvorgängen, die nicht mit dem Vorhandensein einer Datenbank im Zusammenhang stehen. In dem konkreten Fall ging es um die Ausübung einer journalistischen Tätigkeit und um die Rolle der Verhaltensregeln für Journalisten, die in Zusammenarbeit mit den einschlägigen Fachverbänden ausgearbeitet wurden und die im Datenschutzgesetz verankerten Grundsätze ergänzen.

D. Spezifische Themen

Zur umfassenden Regelung von Fragen des Datenschutzes in Italien und zur Gewährleistung der vollständigen Umsetzung der in den Richtlinien 95/46/EG und 97/66/EG verankerten Grundsätze in italienisches Recht sind legislative Maßnahmen in Bereichen wie Direktmarketing, Sozialversicherung, Arbeitswelt und Datenfluss in elektronischen Netzen erforderlich. Großes Gewicht soll auch der Definition von Mechanismen und Schutzmaßnahmen beigemessen werden, die insbesondere auf Verarbeitungsvorgänge für justizielle Zwecke und Strafverfolgungszwecke anwendbar sind und die gegenwärtig nur zum Teil vom Datenschutzgesetz geregelt werden. Aus allgemeiner Sicht werden die obengenannten Verarbeitungsvorgänge von keiner der beiden Richtlinien abgedeckt, da sie nicht in den Geltungsbereich des Gemeinschaftsrechts fallen.

Das Parlament beabsichtigte jedoch, diese Verarbeitungsvorgänge nicht von den einschlägigen Datenschutzbestimmungen auszunehmen, die nachfolgend durch Ad-hoc-Maßnahmen festgelegt werden sollten.

1999 standen die nachstehend aufgeführten Themen im Vordergrund. Damit wurde beabsichtigt, eine effektive Umsetzung der Datenschutzbestimmungen zu gewährleisten sowie Mechanismen für den effektiven Austausch von Meinungen und Informationen mit Garante bei Entscheidungsprozessen des Parlaments oder der Verwaltungsbehörden - auch in den Bereichen Computerwissenschaft und technologische Entwicklung - zu schaffen:

- Notwendigkeit der Schaffung wirksamer Konsultationsmechanismen in bezug auf Garante gemäß Artikel 28 Absatz 2 der Richtlinie 95/46/EG

- Bewertung und Regelung der Videoüberwachung

- Verarbeitung von genetischen Daten

- Vereinfachte Erteilung von Auskünften gegenüber Betroffenen im Bankwesen

- Regeln für die Zustimmung zu Verarbeitungsvorgängen im medizinischen Bereich

- Einsichtnahme in personenbezogene Daten wie sie beispielsweise in Mitarbeiterbeurteilungen, medizinischen Gutachten usw. enthalten sind

- Einzelgebührennachweise

- Folgearbeiten auf Gemeinschaftsebene zu den Erörterungen der Richtlinien für digitale Signaturen und den elektronischen Geschäftsverkehr

- Vorschriften für die Verarbeitung von Daten im Rahmen von Maßnahmen der so genannten dritten Säule

E. Website

www.garanteprivacy.it

PORTUGAL

B. In Portugal durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Ratifikation des CIS-Übereinkommens durch das Dekret des Präsidenten der Republik 129/99 und durch die Entschließung des Parlaments Nr. 32/99, beide vom 21. April 1999.

C. Wichtige Rechtsprechung

Verfahren 41025, 1. Kammer des Obersten Verwaltungsgerichts – Urteil vom 15. April 1999

Verfahren 41022, 1. Kammer des Obersten Verwaltungsgerichts – Urteil vom 15. April 1999

Urteile in Berufungsverfahren, die von Datenverarbeitern gegen Entscheidungen der portugiesischen Datenschutzbehörde angestrengt worden waren. Beide Urteile unterstützten die Auffassung der Datenschutzbehörde.

4. Website

http://www.cnpd.pt

Eine Zusammenfassung in englischer Sprache kann dort ebenfalls abgerufen werden.

SPANIEN

A. In Spanien angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Im königlichen Dekret Nr. 994/1999 vom 11. Juni 1999 wurde die Verordnung über die Sicherheitsmaßnahmen für automatische Archivierungssysteme, die personenbezogene Daten enthalten, genehmigt.

B. In Spanien durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

1999 stellte die **französische Datenschutzkommission (CNIL)** fünf Kooperationsanträge bei der Datenschutzbehörde nach Artikel 114.2 des Schengener Übereinkommens. In diesen Anträgen ging es um den Zugriff auf die Dateien des

Schengen-Informationssystems (SIS) und um die Löschung der Namen von Personen, denen laut SIS die Einreise in den Schengenraum zu verwehren ist und deren Daten von den spanischen Behörden eingegeben wurden.

Es wurden daher Maßnahmen eingeleitet um festzustellen, ob die Erfassung der Daten dieser Personen im Rahmen der geltenden Rechtsvorschriften rechtmäßig war. In allen Fällen wurde festgestellt, dass die Betroffenen nach einem Ausweisungsverfahren gemäß dem Einwanderungsgesetz und nach Erteilung eines Einreiseverbots aus dem Staatsgebiet abgeschoben worden waren. In allen untersuchten Fällen wurde die CNIL von den Maßnahmen und den Gründen für die Erfassung dieser Personen im SIS in Kenntnis gesetzt.

Im Hinblick auf öffentlich zugängliche Dateien betreffend Maßnahmen im Bereich der dritten Säule wurden 1999 46 Dateien zu Gerichtsverfahren und 45 Dateien zu den Maßnahmen der Sicherheitskräfte erfasst.

Die Mehrzahl der neun Aufsichts- und Kontrollmaßnahmen der Behörde mit Blick auf die staatlichen Sicherheitskräfte 1999 hatte vorbeugenden Charakter.

Erwähnenswert ist das noch aus der Zeit vor 1999 stammende **Organgesetz** (Ley Orgánica) **4/1997**, das den Einsatz von Videokameras durch die Sicherheitskräfte in der Öffentlichkeit regelt.

C. Wichtige Rechtsprechung

1. Rechtsprechung des Verfassungsgerichts in bezug auf Artikel 18.4 der spanischen Verfassung:

1999 erließ das Verfassungsgericht drei Urteile, die direkt den Schutz personenbezogener Daten berühren: Nr. 30/1999 vom 8. März, Nr. 44/1999 und Nr. 45/1999 vom 23. März. In diesen Urteilen bekräftigte das Verfassungsgericht die gerichtliche Anordnung von 1998, insbesondere auf der Grundlage des Urteils Nr. 11/1998 vom 13. Januar, in Anerkennung der „informationellen Selbstbestimmung", wie sie in der deutschen Rechtsprechung bezeichnet wird.

Die drei Urteile beziehen sich auf einen einzigen Vorgang, bei dem ein Arbeitgeber aufgrund der ihm vorliegenden Daten über die Gewerkschaftszugehörigkeit seiner Arbeitnehmer Gelder im Zusammenhang mit der Wahrnehmung des Streikrechts von Arbeitnehmern einbehalten hatte.

Die Beschwerdeführer, Mitglieder einer bestimmten Gewerkschaft, waren in einer Firma tätig, in welcher der Betriebsrat mit Unterstützung der Gewerkschaften einen Streik ausgerufen hatte.

Obwohl die betroffenen Mitarbeiter nicht an dem Streik teilnahmen, behielt die Firma Gelder von allen Mitarbeitern ein, die als Mitglieder einer bestimmten Gewerkschaft – einer der Gewerkschaften, die den Streik unterstützen - registriert waren. Dieses Vorgehen war möglich, weil die Firma Daten über die Gewerkschaftszugehörigkeit anhand eines spezifischen elektronischen Schlüssels zur Kennzeichnung der Gewerkschaftszugehörigkeit abrufen konnte.

Obwohl die Firma die Gelder auf Antrag erstattete, wandten sich die Arbeitnehmer an das Verfassungsgericht und machten geltend, dass ihr Recht auf Freiheit in Gewerkschaftsangelegenheiten gemäß Artikel 28 der spanischen Verfassung nach Maßgabe von Artikel 18 Absatz 4 verletzt worden sei, der - zur Wahrung der Ehre und des Rechts auf den Schutz der Privatsphäre und der Familie - rechtliche Grenzen für den Einsatz von Informationstechnik vorsieht.

Die Beschwerde wurde mit der Begründung zugelassen, dass Daten über die Gewerkschaftszugehörigkeit, eine nach Artikel 16 der Verfassung geschützte Entscheidung aus ideologischen Gründen, nach spanischem Recht einem besonderen Schutz unterstellt seien, jedoch für andere Zwecke als solchen, die den Grund für ihre Erfassung darstellten, verwendet wurden und dass weiterhin der entsprechende elektronische Schlüssel nicht vorschriftsgemäß verwendet worden sei, da bei der Erfassung personenbezogener Daten im Computer Sorge dafür getragen werden müsse, deren missbräuchliche Verwendung zu verhindern.

Im Urteil wurde entschieden, dass sowohl das Recht auf Freiheit in Gewerkschaftsangelegenheiten als auch das Recht auf Schutz der Privatsphäre verletzt worden war.

2. Die wichtigsten Urteile der Verwaltungsgerichte 1999 im Rahmen ihrer Aufsichtsfunktion für die Tätigkeit der Datenschutzbehörde:

1999 haben die Gerichte der höheren Instanzen 29 Urteile über Verwaltungsbeschwerden erlassen, die gegen Entscheidungen der Datenschutzbehörde eingereicht wurden. Dies ist ein deutlicher Anstieg gegenüber 13 Urteilen im Jahr davor.

Von den 29 in diesem Jahr verkündeten Urteilen ging es in 27 Fällen um Strafverfahren und in zwei Verfahren um den Schutz von Rechten. Diese Urteile sind jedoch nicht weiter erwähnenswert, da sie keine wesentlichen neuen Erkenntnisse beinhalten.

D. Spezifische Themen

Die Anträge auf Aufnahme in das **Allgemeine Datenschutzregister** sind 1999 gegenüber 1998 um 50 % gestiegen. Die Zahl der bearbeiteten Anträge auf Erteilung einer Genehmigung für grenzüberschreitende Datenübermittlungen stieg gegenüber dem Vorjahr um 25 %. Es gab keine Rückschläge bei der Verwaltung der Dateierfassungen.

Am 31. Dezember 1999 waren insgesamt 1 081 Dateien im Register für grenzüberschreitende Datenübermittlungen verzeichnet, davon waren 1 028 Einträge in privatem Besitz und 53 in öffentlichem Besitz.

Von den 39 im Jahr 1999 eingereichten Genehmigungsanträgen für die grenzüberschreitende Übermittlung personenbezogener Daten wurden 36 bewilligt, bei zwei Anträgen wurde das Verfahren von dem für die Verarbeitung Verantwortlichen eingestellt oder zurückgestellt, und über einen weiteren Antrag war am 31. Dezember 1999 noch nicht entschieden worden.

Die **Aufsichts- und Kontrolltätigkeiten** lassen sich zwei allgemeinen Kategorien zuordnen. In der einen Kategorie geht es um Beschwerden über die Verletzung der Grundsätze des damals geltenden Datenschutzgesetzes LORTAD, und in der anderen Kategorie um die Entwicklung von proaktiven sektorspezifischen Kontrollplänen zur Überprüfung der Einhaltung der Vorschriften für den Schutz personenbezogener Daten im öffentlichen und im privaten Sektor.

Bei den als Reaktion auf entsprechende Klagen eingeleiteten Maßnahmen ging es um das Recht auf Einsichtnahme in medizinische Krankenblätter und Fragen wie z. B. die

Registrierung der vom Krankenhauspersonal in öffentlichen Krankenhäusern verwendeten Dateien bei deren Übermittlung an private Verwaltungsstellen.

Im Rahmen der entsprechenden Pläne für den öffentlichen Sektor wurden Kontrollen in Einrichtungen wie der staatlichen Steuerverwaltungsbehörde und der Generaldirektion für Verkehr, beim nationalen AIDS-Register und in zwei öffentlichen Krankenhäusern durchgeführt. Im Nachgang zu diesen Kontrollen gab der Direktor der Datenschutzbehörde eine Reihe von Empfehlungen heraus. Im privaten Sektor konzentrierten sich verschiedene Kontrollen auf die wichtigsten Festnetzbetreiber: Telefónica de España, S.A., Retevisión S.A., Lince Telecomunicaciones S.A. (UNI 2) und Euskaltel S.A.

Die folgenden drei Fälle sind klassische Beispiele für die Aufsichtstätigkeit der Datenschutzbehörde.

Gegenstand des ersten Falls war das von den spanischen Gesundheitsbehörden durchgeführte Projekt TAIR, das unter anderem auf eine Flexibilisierung bei der Fakturierung und Bearbeitung von Arzneimittelrezepten zielte. Zu diesem Zweck druckt der behandelnde Arzt während der Beratung ein Etikett mit den Identifikationsdaten des Patienten in Textform und einem Balkencode zum leichteren Einlesen der Daten aus und klebt dieses Etikett auf das Rezept. Gemäß einer Vereinbarung zwischen den Gesundheitsbehörden (die einen Teil der Arzneimittelkosten tragen) und den Apothekerkammern (die den Gesundheitsbehörden den von diesen getragenen Kostenanteil in Rechnung stellen) werden alle auf dem Rezept enthaltenen Daten im Computer erfasst und ergeben zusammen eine Datei mit personenbezogenen Daten, die zur nachfolgenden Verarbeitung nach Maßgabe der Rechtsvorschriften für das Gesundheitswesen an die Gesundheitsbehörden übermittelt wird. Nach sorgfältiger Untersuchung des gesamten Ablaufs kam die Datenschutzbehörde zu dem Ergebnis, dass das spanische Recht durch diese Art der Verarbeitung nicht verletzt wird, und zwar sowohl aufgrund der rechtlichen Garantien als auch aufgrund der vorgeschalteten Sicherheitsmaßnahmen. Angesichts der spezifischen Implikationen für den Schutz der Privatsphäre wird die Behörde in Zusammenarbeit mit den Gesundheitsbehörden den Fortgang des Projekts jedoch weiterhin beobachten, um zu gewährleisten, dass die Datenschutzbestimmungen jederzeit eingehalten und angemessene Garantien gewährt werden.

Gegenstand einer weiteren Untersuchung war eine von der spanischen Tochtergesellschaft einer nordamerikanischen Firma geführte Datei in Spanien. Die Untersuchung wurde eingeleitet, weil die Datei Informationen über Vornamen, Nachnamen, Postanschrift, elektronische Adressen und den beruflichen Hintergrund von rund 130 000 Personen, überwiegend mit Wohnsitz in Spanien, enthielt. Diese Daten stammten angeblich aus einer Datenbank der nordamerikanischen

Muttergesellschaft, in der sich Personen aus aller Welt, die sich Informationen über die Produkte der Firma zuschicken lassen möchten, freiwillig über die Websites der Firma registrieren lassen können.

Zur Untersuchung der Frage, ob diese Art der Verarbeitung mit den spanischen Datenschutzbestimmungen vereinbar ist, mussten die Umstände im Hinblick auf die Informationsgrundsätze und die bei der ursprünglichen Erfassung der Daten auf den Websites in den USA erteilte Zustimmung berücksichtigt werden.

Die Datenschutzbehörde entschied, dass angesichts des Nichtvorhandenseins angemessener Informationen für die Zwecke der spanischen Datenschutzbestimmungen im Hinblick auf die Datenübermittlung an die spanische Tochtergesellschaft und im Hinblick auf die nachfolgende Verarbeitung dieser Daten durch die Tochtergesellschaft die von den Betroffenen erteilte Zustimmung mangels grundlegender Informationen für die rechtmäßige Verarbeitung der Daten durch die Tochtergesellschaft nicht ausreichend sei und verhängte folglich Sanktionen gegen die spanische Firma.

Im dritten Fall wurden sogenannte „Scoring-“ oder Bewertungsverfahren untersucht. Eine Telekommunikationsgesellschaft leitet einen Bericht über ihre eigenen oder potenzielle Kunden an eine andere Stelle weiter, die sich auf Informationen über Liquidität und Bonität spezialisiert hat. Dieser Bericht wird danach mit einer neuen Einstufung zurückgegeben, die Informationen über die Kreditwürdigkeit jedes Kunden enthält und auf deren Grundlage die Telekommunikationsgesellschaft über eine Annahme oder Ablehnung von Dienstanträgen entscheidet. Dies kann die Übermittlung und Verarbeitung personenbezogener Daten ohne Einwilligung der Betroffenen im Sinne der spanischen Rechtsvorschriften für den Schutz personenbezogener Daten einschließen, und aus diesem Grund wurden gegen mehrere Betreiber Sanktionsmaßnahmen verhängt.

Auf der **Frühjahrstagung der Aufsichtsbehörden** im April 1999 in Helsinki legten die Delegationen der spanischen und niederländischen Aufsichtsbehörden die Ergebnisse eines gemeinsamen Projekts zur Entwicklung einer gemeinschaftlichen - oder harmonisierten – Methodik und Verfahrensweise für Kontrollen oder Prüfstrategien für den Schutz der Privatsphäre vor. Zwei Kontrollteams beider Behörden hatten ein Seminar im April 1999 in Madrid zu einem Gedanken- und Erfahrungsaustausch genutzt. Die beiden Delegationen erarbeiteten die allgemeinen Leitlinien und forderten weitere Delegationen zur Teilnahme an diesem Projekt auf.

Die erste auf diesen auf dem Seminar in Madrid vereinbarten gemeinschaftlichen Methoden basierende Aufsichts- und Kontrollaktivität wurde bereits geplant und

durchgeführt. Die Wahl fiel auf Internet-Diensteanbieter, da diese Firmen weltweit ein und dieselben Dienste anbieten. Beide Delegationen einigten sich auf die zukünftige Weiterverwendung dieses Modells, da es die erwarteten Ergebnisse lieferte. Zwischenzeitlich wurden zwei weitere Prüfungen bei zwei weiteren Internet-Diensteanbietern durchgeführt.

Die aktuellste Fassung des 1997 von der Datenschutzbehörde erstellten Katalogs mit den **Empfehlungen für Internet-Nutzer** wurde im Mai 1999 veröffentlicht. Dieser Katalog informiert Internet-Nutzer über den sicheren Zugriff auf das Internet.

Weiterhin ist zu betonen, dass Spanien in der Europäischen Union eine Vorreiterrolle bei der Ausarbeitung und Erfassung eines Datenschutzkodex für das Internet gespielt hat, der auch vom spanischen Verband für den elektronischen Geschäftsverkehr gefördert wird.

Ein weiteres erwähnenswertes Ereignis ist die Fertigstellung des Entwurfs für **Empfehlungen der Datenschutzbehörde für DV-Verantwortliche in Firmen, die Auskunft über Liquidität und Bonität geben**. Die Empfehlungen zielen darauf ab, die Verarbeitungsvorgänge in derartigen Firmen enger mit den Bestimmungen des Datenschutzgesetzes LORTAD in Übereinstimmung zu bringen.

Die Empfehlungen lassen sich drei Gruppen zuordnen. Die ersten beiden Gruppen beziehen sich auf zwei allgemeine Arten von Dateien, mit denen Auskunft über Liquidität und Bonität gegeben wird. In der ersten Gruppe von Empfehlungen geht es um Dateien, die Informationen über die Verletzung monetärer Verpflichtungen enthalten, die von Gläubigern oder von Parteien, die im Auftrag und im Interesse dieser Gläubiger handeln, gemeldet wurden. In der zweiten Gruppe geht es um Dateien, in denen Daten aus öffentlich zugänglichen Quellen verarbeitet werden. Die dritte Gruppe von Empfehlungen betrifft die Durchführung von Maßnahmen gemäß der Verordnung über Sicherheitsmaßnahmen.

Laut Gesetz hat die Datenschutzbehörde gegenüber den Bürgern eine Informationspflicht, sie befasst sich daher mit **Anfragen und Beschwerden** und klärt die Bürger über ihre Rechte im Hinblick auf die automatische Verarbeitung personenbezogener Daten auf. 1999 startete die Behörde Informationskampagnen in den Medien, veröffentlichte Broschüren, Handbücher und CD-ROMs sowie Informationen auf ihrer eigenen Website, auf der im Laufe des Jahres 506 362 Besucher registriert wurden, d. h. 43 % mehr als 1998.

Die Behörde bietet persönliche Beratung in ihren Büros, telefonische Beratung und Beratung auf dem Postweg oder per E-Mail an. Die 15 000 bearbeiteten Anfragen im Jahr 1999 stellen eine Zunahme um 20 % gegenüber den schriftlichen Anfragen des Jahres 1998 dar, was überwiegend auf den auf der Website eingerichteten Mail-Link zurückzuführen ist.

In den Anfragen ging es überwiegend um Bereiche, die für die Bürger von besonderem Interesse sind: das Recht, Auskunft von der Behörde zu erhalten, Aufzeichnungen über Liquidität und Bonität, Dateien für Werbezwecke und die Wahrnehmung der Rechte auf Einsichtnahme, Berichtigung und Löschung gegenüber den für die Verarbeitung Verantwortlichen.

In den folgenden Bereichen wurden die meisten Anfragen verzeichnet: Geltungsbereich des Datenschutzgesetzes, dessen Sicherheitsbestimmungen, Telekommunikation, medizinische Daten, Wahlerhebungsdaten, statistische Daten, Datenübermittlungen, Berufsfachschulen, Versicherungswesen und Arbeitsbeziehungen. Dieser letztgenannte Bereich tritt aufgrund von Themen wie z. B. die Einsichtnahme des Arbeitgebers in die elektronische Post von Mitarbeitern, Einscannen der Fotos von Mitarbeitern und deren Einbindung auf den Websites der Firmen zunehmend in den Vordergrund.

Zu den Aufgaben der Datenschutzbehörde gemäß Artikel 37 Buchstabe h des Organgesetzes Nr. 15/1999 für den Schutz personenbezogener Daten zählt die Abgabe konsultativer Stellungnahmen zu allgemeinen Vorschriften, die gemäß diesem Gesetz ausgearbeitet werden sollen.

Im Laufe des Jahres wurde die Datenschutzbehörde zu insgesamt 35 Vorschriften konsultiert, das sind 59 % mehr als 1998. Dazu gehörten insbesondere:

- der Vorentwurf für ein Gesetz über Maßnahmen zur Kontrolle chemischer Substanzen, die zur Herstellung chemischer Waffen gemäß dem am 13. Januar 1993 in Paris unterzeichneten Übereinkommen über das Verbot der Entwicklung, Herstellung, Lagerung und des Einsatzes chemischer Waffen und über die Vernichtung solcher Waffen abgeleitet werden können
- der Gesetzentwurf für die Erneuerung der Verordnung zur Regelung der Aktivitäten des Risikobewertungszentrums der Banco de España (*Central de Riesgos del Banco de España*, CIRBE)
- der Vorentwurf für ein Gesetz zur Einrichtung der katalanischen Datenschutzbehörde

- der Vorentwurf für ein Gesetz über elektronische Signaturen, der nachfolgend mit dem königlichen Dekret Nr. 14/1999 vom 17. September 1999 für elektronische Signaturen angenommen wurde

- der Vorentwurf für ein Gesetz über flankierende Steuer-, Verwaltungs- und Sozialmaßnahmen zum Haushaltsgesetz 2000

Besonders zu erwähnen sind die kontinuierlichen Bemühungen der Behörde im Laufe des Jahres 1999 um Aufklärung und Erteilung von Auskünften und um die Veröffentlichung der Grundsätze, Kriterien, Pflichten und weiterer Themen im Zusammenhang mit der Sicherheitsverordnung vor ihrem Inkrafttreten.

E. Website

Auszüge aus dem Jahresbericht der Behörde sind unter der folgenden Adresse abrufbar: https://www.agenciaprotecciondatos.org/

Es ist geplant, den aktuellen Jahresbericht der spanischen Behörde auf dieser Website verfügbar zu machen.

SCHWEDEN

A. In Schweden angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Keine.

B. In Schweden durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

1999 wurden in Schweden mehrere neue Gesetze über die Verarbeitung personenbezogener Daten angenommen, so z. B. das Gesetz (1999:90) über die Verarbeitung personenbezogener Daten durch Steuerbehörden im Zuge strafrechtlicher Ermittlungen und das Gesetz (1999:163) betreffend Aufzeichnungen über Geldwäscherei.

Das 1998 angenommene Polizeidatengesetz wurde 1999 durch die Polizeidatenverordnung (1999:81) ergänzt.

Die oben erwähnten Gesetze enthalten spezifische Bestimmungen hinsichtlich der Verarbeitung personenbezogener Daten in diesen Bereichen. Das allgemein anwendbare Gesetz über personenbezogene Daten findet insoweit Anwendung, wie die Verarbeitung personenbezogener Daten nicht explizit in diesen oder anderen Bestimmungen geregelt ist.

C. Wichtige Rechtsprechung

Im April verurteilte das Amtsgericht Stockholm einen Geschäftsmann wegen Verletzung des bisherigen Datenschutzgesetzes. Der Geschäftsmann hatte auf seiner Website abschätzige Meinungen und Beurteilungen über zahlreiche Personen veröffentlicht. Er hatte für sich in Anspruch genommen, dass das Recht auf freie Meinungsäußerung die Veröffentlichung derartiger Informationen im Internet erlaube. Gegen das Urteil des Amtsgerichts wurde beim Schwedischen Berufungsgericht in Stockholm Berufung eingelegt, das die Auffassung vertrat, dass die Veröffentlichung vielmehr eine Verletzung des neuen Gesetzes über personenbezogene Daten darstelle. Das Berufungsgericht stimmte dem Einwand des Geschäftsmanns nicht zu, dass er diese Informationen *ausschließlich* für journalistische Zwecke veröffentlicht habe und dass das Gesetz über personenbezogene Daten somit nicht anwendbar sei. Gegen das Urteil des Berufungsgerichts wurde beim Obersten Gerichtshof Berufung eingelegt. Das Verfahren ist dort noch anhängig.

D. Spezifische Themen

1999 untersuchte die Datenschutzbehörde eine Website, auf der Krankenhausmitarbeiter namentlich genannt wurden, die von einem Disziplinarausschuss gerügt worden waren. Die Datenschutzbehörde stellte jedoch fest, dass die Informationen auf der Website von der Redaktion einer Zeitschrift veröffentlicht worden waren und die Veröffentlichung somit unter das Grundrecht auf

freie Meinungsäußerung fiel. Das Gesetz über personenbezogene Daten war auf diesen Fall folglich nicht anwendbar.

In einem anderen Fall mit Bezug zum Internet hatte eine schwedische Kommunalbehörde auf ihrer Website eine Liste mit den Namen aller Einwohner der Gemeinde veröffentlicht, ohne zuvor die Zustimmung der Einwohner einzuholen. Die Kommunalbehörde führte an, dass die Liste als ein künstlerischer Ausdruck zu sehen sei und gemäß einer Bestimmung des Gesetzes über personenbezogene Daten nicht der Zustimmungspflicht der Einwohner unterliege. Die Datenschutzbehörde war jedoch der Ansicht, dass trotz der schwierigen Definition des Begriffs „künstlerischer Ausdruck“ der Gesetzgeber nicht im Sinn gehabt haben könne, die Verarbeitung von Daten - wie in der vorliegenden Veröffentlichung geschehen - von den Bestimmungen auszunehmen. Die Kommunalbehörde löschte daraufhin die Informationen von der Website, und der Fall wurde zu den Akten gelegt.

Die Verarbeitung personenbezogener Daten im Internet war 1999 in Schweden Gegenstand einer lebhaften Diskussion. Ende 1998 beauftragte die schwedische Regierung die Datenschutzbehörde, die Notwendigkeit von Ergänzungsbestimmungen zu untersuchen, um bestimmte Datenübermittlungen in Drittländer, die insbesondere im Zusammenhang mit der Verarbeitung personenbezogener Daten in internationalen Kommunikationsnetzen wie dem Internet als unschädlich angesehen werden können, vom Verbot gemäß Abschnitt 33 des Gesetzes über personenbezogene Daten auszunehmen. Die Datenschutzbehörde schlug der Regierung eine rasche Änderung der Verordnung über personenbezogene Daten (1998:1191) vor, dieser Vorschlag wurde im wesentlichen positiv aufgenommen. Es lagen jedoch triftige Gründe für die Änderung des Gesetzes über personenbezogene Daten vor. Die Regierung schlug dann eine Änderung von Abschnitt 33 des Gesetzes über personenbezogene Daten vor. Der Vorschlag wurde vom schwedischen Parlament angenommen, und die Änderung (wie unter Punkt 1.A. oben beschrieben) trat am 1. Januar 2000 in Kraft.

E. Website

Der Jahresbericht der Datenschutzbehörde für das Jahr 1999 ist in englischer Sprache auf der folgenden Website abrufbar: www.datainspektionen.se/in_english/

NIEDERLANDE

A. In den Niederlanden angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Keine.

B. In den Niederlanden durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Keine.

C. Wichtige Rechtsprechung

Keine.

D. Spezifische Themen

1999 beschäftigte sich die Registratiekamer vorrangig mit drei Themen:

1. Die Stellung der Verbraucher in bezug auf die Datenautobahn.

Das Zeitalter des Internet und der Mobilkommunikation eröffnet dem Verbraucher viele neue Chancen und Möglichkeiten. Aufgrund des Internet bieten sich dem Verbraucher weitaus mehr Möglichkeiten beim Einkauf von Waren und Dienstleistungen usw., doch das Internet birgt auch gewisse Gefahren, da ein Verbraucher einem Anbieter im Internet nur schwer Vertrauen entgegenbringen kann. Bei einer Bestellung über eine Website kann der Verbraucher nie sicher sein, ob er die gewünschten Produkte bestellt hat und ob sein Geld bei der richtigen Person ankommt. Die Registratiekamer kommt zu dem Schluss, dass fast alles, was der ‚digitale Verbraucher' unternimmt, aufgezeichnet wird, ohne dass der Verbraucher dies bemerkt. Daher müsse der Verbraucher aufgeklärt und geschützt werden. Aus diesem Grund befasste sich die Registratiekamer intensiv mit dem Schutz der Privatsphäre von Verbrauchern und leitete eine Untersuchung über die Verwertung personenbezogener Daten durch Internet-Diensteanbieter ein. Die Ergebnisse dieser Untersuchung wurden im Juni 2000 veröffentlicht.

2. Vorbereitungen für das Inkrafttreten des Datenschutzgesetzes (Wet Bescherming Persoonsgegevens)

Im Februar 1998 wurde der Zweiten Kammer des niederländischen Parlaments der Entwurf für das Datenschutzgesetz (Wet Bescherming Persoonsgegevens, WBP) vorgelegt. Seitdem wird über diesen Gesetzentwurf heftig debattiert. Mit diesem Gesetz wird die Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten umgesetzt. Der Ständige Rechtsausschuss des Parlaments ließ sich von der Registratiekamer hinsichtlich der Auswirkungen dieses Gesetzes beraten. Die Zweite Kammer nahm das Datenschutzgesetz im November 1999 einstimmig an. 2001 wird das Datenschutzgesetz in Kraft treten.

3. Erhebliche Zunahme des „Screening“ von Personen und Firmen im Jahr 1999

Beim „Screening“ wird z. B. ein Bewerber oder ein Geschäftspartner auf seine Verlässlichkeit oder Vertrauenswürdigkeit überprüft. Dies erfordert die Einsichtnahme in verschiedene Quellen. Dabei wird häufig nicht nur die Wirksamkeit einer solchen Bewertung überbetont, sondern das Screening ist auch mit einem erheblichen Eindringen in die Privatsphäre einer Person verbunden. Ein Screening sollte nur dann erfolgen, wenn es keine weniger drastische Alternative gibt. Ein Screening sollte anhand klarer, vorgegebener Kriterien und auf der Grundlage rechtmäßig beschaffter Informationen erfolgen. Um sich ein möglichst umfassendes Bild von den bestehenden Instrumenten zur Integritätsprüfung zu verschaffen, veranstaltete die Registratiekamer 1999 eine Rundtischkonferenz zum Thema „Screening” in den Niederlanden.

Wichtige Veröffentlichungen

Alle Veröffentlichungen sind ungekürzt in niederländischer Sprache auf der Website der Registratiekamer abrufbar. In den meisten Fällen ist auch eine englische Zusammenfassung jeder Veröffentlichung online verfügbar.

- ‘Informatieverstrekking door de fiscus – ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving’ (Erteilung von Auskünften durch Steuerbehörden – Befreiung von der Verpflichtung zur Wahrung des Steuergeheimnisses im Zusammenhang mit den

Datenschutzgesetzen). Dieser Bericht wurde dem Staatssekretär für Finanzen sowie der Zweiten Kammer des Parlaments vorgelegt. In diesem Bericht erklärt die Registratiekamer, weshalb die gesetzlichen Vorschriften für die Bereitstellung personenbezogener Daten durch die Steuerbehörden nicht mehr zeitgemäß sind. Das Steuergesetz müsse daher überarbeitet werden.

- 'Werken met gegevens' (Über den Umgang mit Daten). Diese Veröffentlichung befasst sich mit den Zentren für Arbeit und Einkommen (Centres for Work and Income, CWI). Öffentliche und private Einrichtungen für Arbeit und Einkommen arbeiten immer häufiger zusammen. Aus diesem Grund bieten Exekutivorgane, Sozialeinrichtungen und Arbeitsvermittlungsstellen ihre Dienste vermehrt in derartigen Zentren an. Die Registratiekamer erstellte eine Liste und Analyse der Möglichkeiten und Grenzen der CWI und erarbeitete eine Reihe von Regeln für diese Art der praktischen Zusammenarbeit.

- 'Koning Klant' (König Kunde). In diesem Bericht legt die Registratiekamer dar, wie die Leitlinien und Vorschriften des WBP auf die Verarbeitung von Verbraucherdaten anzuwenden sind und wie die wirtschaftlichen Interessen der Unternehmen und die Interessen der Verbraucher bei der Verarbeitung personenbezogener Daten gegeneinander abgewogen werden sollten.

- ‚Intelligent Software Agents and Privacy' (Bericht über intelligente Software-Agenten und den Schutz der Privatsphäre - in Zusammenarbeit mit der kanadischen Datenschutzbehörde in Ontario) und 'At face value: on biometrical identification and privacy' (Auf einen Blick: Biometrische Identifikation und der Schutz der Privatsphäre). Diese beiden Berichte befassen sich mit neuen technischen Entwicklungen, die sich auf den Schutz der Privatsphäre der Bürger auswirken können.

- Eine weitere Veröffentlichung befasste sich mit einer Untersuchung der Zusammensetzung und Nutzung der Einwohnerverzeichnisse in drei Gemeinden. Dieser Bericht zeigt, dass die in diesen Einwohnerverzeichnissen gespeicherten Daten über die Bürger unzureichend geschützt sind. Es ist davon auszugehen, dass dies auch in anderen Gemeinden der Fall ist.

E. Websites

Website der niederländischen Datenschutzbehörde: http://www.registratiekamer.nl

Neben der ungekürzten niederländischen Fassung des Jahresberichts ist auch eine englische Zusammenfassung online abrufbar.

VEREINIGTES KÖNIGREICH

A. Im Vereinigten Königreich angenommene legislative Maßnahmen im Bereich der ersten Säule der EU (mit Ausnahme der Richtlinien 95/46/EG und 97/66/EG)

Es wurden keine weiteren legislativen Maßnahmen angenommen.

B. Im Vereinigten Königreich durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

1999 gab es im Bereich des Datenschutzes und des Schutzes der Privatsphäre keine wesentlichen Änderungen im Rahmen der zweiten und dritten Säule.

C. Wichtige Rechtsprechung

Das Versorgungsunternehmen Midlands Electricity plc legte beim Datenschutzgericht am 7. Mai 1999 Rechtsmittel gegen einen Vollstreckungsbescheid ein, den der Datenschutzbeauftragte am 1. Dezember 1998 gemäß Abschnitt 10 des Datenschutzgesetzes von 1984 erlassen hatte. Der Vollstreckungsbescheid wurde wegen der Nutzung personenbezogener Daten, die das Unternehmen im Rahmen seiner Versorgungstätigkeit gesammelt hatte, für Direktmarketingzwecke erlassen. Bei der Direktvermarktung ging es um Waren und Dienstleistungen Dritter, die nicht im Zusammenhang mit der Stromversorgung oder einer sonstigen Versorgungstätigkeit standen und die den Kunden über eine Zeitschriftenbeilage mit ihren Abrechnungsdaten angeboten wurden. Das Datenschutzgericht bestätigte den Vollstreckungsbescheid, der am 1. Januar 2001 in Kraft trat und Midlands Electricity plc dazu verpflichtete, für die künftige Zustellung der Zeitschrift die Einwilligung der Kunden einzuholen.

D. Spezifische Themen

Oberste Priorität im Jahr 1999 hatte die Umsetzung der EU-Datenschutzrichtlinie 95/46/EG und der übrigen Bestimmungen der Telekommunikationsrichtlinie 97/66/EG.

E. Website

www.dataprotection.gov.uk

2.5. Aktivitäten der Gemeinschaft

2.5.1. Vorschlag für eine Verordnung über den Datenschutz durch die Organe und Einrichtungen der Gemeinschaft

Die Organe und Einrichtungen der Gemeinschaft – und insbesondere die Kommission – verarbeiten im Rahmen ihrer Tätigkeit ständig personenbezogene Daten. Die Kommission tauscht im Rahmen der gemeinsamen Agrarpolitik, für die Verwaltung der Zollverfahren, der Strukturfonds und im Rahmen anderer Gemeinschaftspolitiken personenbezogene Daten mit den Mitgliedstaaten aus. Damit dieser Datenaustausch durch die Mitgliedstaaten nicht aus Datenschutzgründen in Frage gestellt wird, hat die Kommission 1990 erklärt, dass sie die in dem damals vorgelegten Richtlinienentwurf enthaltenen Grundsätze ebenfalls einhalten werde.

Zum Zeitpunkt der Annahme der Richtlinie 95/46/EG, die das Ziel hat, einen gemeinschaftlichen Rahmen für die Harmonisierung der Bestimmungen der Mitgliedstaaten aufzustellen, haben sich die Kommission und der Rat in einer öffentlichen Erklärung verpflichtet, die Richtlinie einzuhalten, und die übrigen Organe und Einrichtungen der Gemeinschaft aufgefordert, diesem Beispiel zu folgen.

In der Regierungskonferenz für die Überprüfung der Verträge wurde die Frage der Anwendung der Datenschutzbestimmungen auf die Organe der Gemeinschaft aufgeworfen. Der nach Abschluss der Verhandlungen in Amsterdam unterzeichnete Vertrag bringt in den Vertrag zur Gründung der Europäischen Gemeinschaft eine diesbezügliche spezifische Bestimmung ein.

Der neue Artikel 286 sieht daher vor, dass ab 1. Januar 1999 die Vorschriften der Gemeinschaft über den Datenschutz, wie sie zum großen Teil in den Richtlinien 95/46/EG und 97/66/EG festgelegt sind, auf die Organe und Einrichtungen der Gemeinschaft Anwendung finden. Darüber hinaus legt der Artikel fest, dass die Anwendung dieser Vorschriften von einer unabhängigen Kontrollinstanz überwacht werden muss.

Die Kommission legte hierauf am 14. Juli 1999 ihren Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr vor. Bereits zu Beginn des Legislativverfahrens kündigten das Europäische Parlament und der Rat an, dass sie das Ziel der Kommission teilten, zu einer raschen Einigung zu gelangen, die es möglich machen würde, die Verordnung bereits nach der ersten Lesung anzunehmen – eine neue Vorgehensweise, die mit dem Amsterdamer Vertrag in das Mitentscheidungsverfahren aufgenommen wurde.

2.5.2. Richtlinie über elektronische Signaturen

Im Nachgang zu der Mitteilung der Kommission über „Sicherheit und Vertrauen in elektronische Kommunikation – Ein europäischer Rahmen für digitale Signaturen und Verschlüsselung“ vom Oktober 1997 legte die Europäische Kommission im Mai 1998 einen Entwurf für eine Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vor. Die Richtlinie wurde am 13. Dezember 1999[37] angenommen. Ziel ist die EU-weite Anerkennung von elektronischen Signaturen. Elektronische Signaturen ermöglichen beim Empfang von Daten über elektronische Netze, z. B. über das Internet, die Feststellung der Herkunft der Daten und die Überprüfung des unveränderten Inhalts der Daten. Die Richtlinie will keine ins Detail gehende

37 Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.01.2000, S. 12.

http://www.europa.eu.int/comm/ internal_market/en/media/index.htm

Regulierung aufstellen, sondern legt lediglich die Anforderungen für Zertifikate für elektronische Signaturen und Zertifizierungsdienste fest, um ein Mindest-Sicherheitsniveau zu gewährleisten und die freie Verwendung im Binnenmarkt zu ermöglichen.

Die wichtigsten Elemente:

- Rechtswirkung: Die Richtlinie legt fest, dass einer elektronischen Signatur die rechtliche Wirksamkeit und die Zuverlässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden darf, weil sie in elektronischer Form vorliegt.
- freier Verkehr von Waren und Dienstleistungen in bezug auf elektronische Signaturen
- Haftung der Diensteanbieter
- ein technologieneutraler Rahmen
- Datenschutz

Da elektronische Signaturen auch als Mittel zur Identifizierung und Authentifizierung dienen können, müssen Diensteanbieter die Identität ihrer Kunden überprüfen und haften für die im Zertifikat enthaltenen Angaben. Daher wurde es für notwendig erachtet, die allgemeinen Grundsätze für die Sammlung personenbezogener Daten und die Zweckbindung (Artikel 8 der Richtlinie) weiter zu entwickeln. Da für die meisten Transaktionen im Geschäftsverkehr per Gesetz keine Identifizierung des Kunden vorgeschrieben ist, muss die Möglichkeit bestehen, in dem Zertifikat Pseudonyme zu verwenden. Soweit keine Anforderungen hinsichtlich der rechtlichen Identifizierung bestehen, hat der Nutzer die Möglichkeit, in den Zertifikaten seinen Namen oder aber Pseudonyme anzugeben. Dies ist eine unverzichtbare Voraussetzung für die Vereinbarkeit der Forderung nach Authentifizierung mit den Anforderungen des Datenschutzes und des Schutzes der Privatsphäre im elektronischen Geschäftsverkehr.

2.5.3. Richtlinie über den elektronischen Geschäftsverkehr

Wie in der Mitteilung der Kommission über den elektronischen Geschäftsverkehr vom Mai 1997 angekündigt, unterbreitete die Europäische Kommission im November 1998 einen Entwurf für eine Richtlinie, mit der ein einheitlicher

rechtlicher Rahmen für den elektronischen Geschäftsverkehr für den gesamten Binnenmarkt festgelegt werden sollte. Im Dezember 1999 wurde der Entwurf vom Rat angenommen[38].

Die Richtlinie enthält keine konkreten Vorschriften für den Datenschutz und den Schutz der Privatsphäre im elektronischen Geschäftsverkehr. Die Datenschutzgruppe forderte die Kommission bei ihren Sitzungen im März und im Mai 1999 auf der Grundlage des Kommissionsentwurfs auf, die Zusammenhänge zwischen dieser Richtlinie und den Datenschutzrichtlinien klarzustellen. Unter den Punkten 14, 15 und 30 der Begründung wird erklärt, dass der bestehende Rahmen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in vollem Umfang auf die Verarbeitung personenbezogener Daten im Kontext des elektronischen Geschäftsverkehrs anwendbar sei. Darüber hinaus wird festgestellt, dass bei der Umsetzung der Richtlinie über den elektronischen Geschäftsverkehr die Grundsätze des Schutzes personenbezogener Daten uneingeschränkt zu beachten sind. Auch der Wortlaut des Artikels, in welchem bestimmte Umstände aus dem Anwendungsbereich ausgenommen werden, wurde klargestellt.

Wirtschaftsteilnehmer, die beabsichtigen, personenbezogene Daten zu verarbeiten, müssen daher auch die Verpflichtungen einhalten, die sich aus den Richtlinien 95/46/EG und 97/66/EG ergeben. Natürliche Personen haben dieselben Rechte wie bei der Offline-Verarbeitung. Dies ist von besonderer Bedeutung im Hinblick auf die Information der Verbraucher über die beabsichtigte Verarbeitung, die Bestimmung und Eingrenzung des Zwecks, eine rechtliche Grundlage für die Verarbeitung sowie im Einzelfall die Vorschriften betreffend kommerzielle Kommunikationen, unabhängig davon, ob hierfür eine vorherige Zustimmung erforderlich ist oder nicht.

2.5.4. Transparenzrichtlinie 98/34/EG

Diese Richtlinie erweitert den Anwendungsbereich der Richtlinie 83/189 (die sich auf nationale Rechtsvorschriften mit Auswirkung auf den freien Warenverkehr bezieht) auf technische Vorschriften für Dienste der Informationsgesellschaft. Die Richtlinie sieht vor, dass die Kommission vor deren endgültiger Annahme über alle Entwürfe für nationale Vorschriften, die sich direkt auf diese Dienste

38 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. L 178 vom 17. Juli 2000, S. 1. Verfügbar unter: siehe Fußnote 40)

auswirken, unterrichtet werden muss und diese gemeinsam mit den übrigen Mitgliedstaaten überprüft, um zu gewährleisten, dass sie mit dem Grundsatz des freien Dienstleistungsverkehrs und dem Grundsatz der Kontrolle durch das Ursprungsland im Einklang stehen (d. h. die einheitliche Gültigkeit von ordnungspolitischen Maßnahmen („one-stop regulatory shop"), wonach für eine Dienstleistung, die in einem Mitgliedstaat angeboten wird, sofern sie den Rechtsvorschriften dieses Mitgliedstaats entspricht, unabhängig von den Rechtsvorschriften der übrigen Mitgliedstaaten, Rechtssicherheit bezüglich des freien Verkehrs in der gesamten Europäischen Union besteht). Gemäß der Rechtsprechung des Europäischen Gerichtshofs (Urteil vom 30.4.96 in der Rechtssache C-194/94), wäre, sofern es ein Mitgliedstaat verabsäumt, eine derartige nationale Vorschrift zu notifizieren, diese Vorschrift für die Wirtschaftsteilnehmer nicht bindend.

Ein solches System eines strukturierten Dialogs zwischen den Administrationen der Mitgliedstaaten und der Kommission, das sich auf die Grundregeln des Binnenmarktes stützt, bietet den Vorteil, dass etwaige Probleme, die sich aus der Entwicklung von Online-Diensten ergeben können, bereits im Vorfeld erkannt und umgehend Lösungen erarbeitet werden können.

1999 wurden technische Vorschriften mit Auswirkung auf die Erbringung entsprechender Dienste sowie auf den freien Fluss personenbezogener Daten wie z. B. Überwachung des Fernmeldeverkehrs, Zugang zu Verkehrsdatensystemen, elektronische Signaturen, notifiziert[39].

2.5.5. Überarbeitung der Rechtsvorschriften im Bereich der Telekommunikation 1999

Die Kommission sah sich vor der Aufgabe, die Umsetzung und die Notwendigkeit einer Anpassung der Rechtsvorschriften für die technologische Entwicklung im Bereich der Telekommunikation zu überprüfen. Dabei legte die Kommission den Schwerpunkt auf die Konvergenz der Kommunikationsmedien. Sie schlug die Schaffung eines vereinfachten, eindeutigen und technologieneutralen rechtlichen Rahmens vor. Sämtliche notwendigen Bestimmungen sollten in einer

39 http://europa.eu.int/comm/enterprise/tris/

Rahmenrichtlinie zusammengefasst werden, die durch eine Reihe spezifischer Richtlinien, u. a. zum Datenschutz, zu ergänzen wären. In diesem Zusammenhang schlug die Kommission eine Änderung der Richtlinie 97/66/EG über den Schutz der Privatsphäre im Bereich der Telekommunikation vor. Mit der Mitteilung der Kommission wurde eine öffentliche Anhörung eingeleitet.

2.5.6. Normung

Nach Vorbereitungsgesprächen mit den europäischen Normungsorganisationen, der Wirtschaft, Datenschutzbehörden, Geheimhaltungsexperten und den Mitgliedstaaten sowie Diskussionen im Rahmen verschiedener internationaler Konferenzen erteilte die Europäische Kommission den Normungsorganisationen der Europäischen Union 1999 ein entsprechendes Mandat. Mit diesem Mandat soll die Durchführung der Richtlinie 95/46/EG sowohl innerhalb der Union als auch auf internationaler Ebene unterstützt werden.

Der erste Schritt beinhaltet die Analyse und Bewertung der potenziellen Rolle, die die europäischen Normungsorganisationen bei der Unterstützung der Richtlinie 95/46/EG einnehmen könnten. So könnten insbesondere europaweite Konsensplattformen zu einer reibungslosen Umsetzung der Richtlinie in den Mitgliedstaaten und zur Verbesserung des Schutzniveaus für natürliche Personen bei der Verarbeitung personenbezogener Daten in Drittländern beitragen. Entsprechende Aktivitäten könnten sowohl substanzielle Gesichtspunkte (Grundsätze und rechtliche Durchsetzung des Datenschutzes sowie Wiedergutmachung) als auch verfahrenstechnische Aspekte (offenes Verfahren, Schaffung von „Win-Win“-Situationen, Stärkung des Wettbewerbs) umfassen. Darüber hinaus wären die Ausarbeitung von Verfahrensregeln und die Förderung der Entwicklung von Technologien für einen besseren Schutz der Privatsphäre denkbar, wobei gleichzeitig der Notwendigkeit zur Schaffung eines einheitlichen Systems mit einem angemessenen Maß an Interoperabilität Rechnung getragen werden sollte. Mit Blick auf internationale Initiativen muss eine Koordination des europäischen Standpunkts erfolgen, um Reibungspunkte mit den in der Richtlinie festgelegten rechtlichen Anforderungen zu vermeiden.

2.5.7. Technologien für einen besseren Schutz der Privatsphäre

Die Europäische Kommission unterstützt das Konzept der Technologien für einen besseren Schutz der Privatsphäre (Privacy Enhancing Technologies, PET) u. a.

durch die Veranstaltung des Workshops zum Thema Datenschutz und Technologie am 20. Oktober 1999, bei dem auch Redner von Datenschutzbehörden vertreten waren. Auch bei der Vorbereitung des Arbeitsprogramms für Technologien für die Informationsgesellschaft 2000 wurde vorgeschlagen, eine spezielle PET-Aktionslinie einzuführen und als Begleitmaßnahmen für Projekte mit Auswirkung auf den Schutz der Privatsphäre horizontale Maßnahmen einzusetzen.

2.5.8. Europol

Der Rat der Europäischen Union nahm am 12. März 1999 Leitlinien für die Übermittlung personenbezogener Daten durch Europol in Drittländer und an dritte Institutionen an.

3. EUROPARAT

Der Europarat setzte seine ständigen Arbeiten zu Fragen des Datenschutzes fort.

Der Beratende Ausschuss (T-PD) schloss seine Arbeiten zu einer Änderung des Übereinkommens SEV Nr. 108 ab, das den Europäischen Gemeinschaften den Beitritt zu dem Übereinkommen erlaubt. Diese Änderung wurde vom Ministerkomitee am 15. Juni 1999 angenommen und zur Annahme durch alle Beteiligten freigegeben. Darüber hinaus setzte der Ausschuss seine Arbeiten am Entwurf eines Zusatzprotokolls zum Übereinkommen SEV Nr. 108 im Hinblick auf die Tätigkeit von Aufsichtsbehörden und auf den grenzüberschreitenden Datenverkehr fort.

Die Projektgruppe Datenschutz (CJ-PD) nahm am 15. Oktober 1999 den Entwurf für eine Empfehlung für den Schutz von personenbezogenen Daten, die zu Versicherungszwecken gesammelt und verarbeitet werden, an und will den Entwurf für die Begründung im Jahr 2000 abschließen. Die Empfehlung Nr. R (99) 5 zum Schutz der Privatsphäre im Internet wurde vom Ministerkomitee am 23. Februar 1999 angenommen. Die Projektgruppe legte ihre Stellungnahmen zur Empfehlung 1402 (1999) der Parlamentarischen Versammlung zur Kontrolle der Sicherheitsdienste und zum Entwurf des Übereinkommens über Cyberkriminalität vor und bereitete den Entwurf einer Stellungnahme zum zweiten Zusatzprotokoll zum Europäischen Übereinkommen über Rechtshilfe in Strafsachen vor.

Die Gemeinschaft, vertreten durch die Kommission, interveniert sowohl in der CJ-PD als auch im Beratenden Ausschuss, wenn die erörterten Themen in den Bereich der externen Zuständigkeiten fallen, die sich aus den Richtlinien 95/46/EG und 97/66/EG

ergeben. Dies war bei den obengenannten Texten der Fall. Diese Zusammenarbeit mit dem Europarat soll die vollständige Übereinstimmung mit den Richtlinien der Gemeinschaft gewährleisten.

4. WICHTIGE ENTWICKLUNGEN IN DRITTLÄNDERN

4.1. Europäischer Wirtschaftsraum

Der Gemischte Parlamentarische Ausschuss EWR nahm zwei Beschlüsse zur Umsetzung der Richtlinien 95/46/EG und 97/66/EG im EWR-Abkommen[40] an. Die Beschlüsse verpflichten die EFTA/EWR-Länder zur Umsetzung der Richtlinien und erweitern den freien Verkehr personenbezogener Daten gemäß Artikel 1 der Richtlinie 95/46/EG auf den gesamten Europäischen Wirtschaftsraum. Die Beschlüsse schreiben ferner ein spezifisches Verfahren für die Umsetzung der Beschlüsse der Kommission zur Angemessenheit des Schutzniveaus in Drittländern vor.

Die Beschlüsse des Gemischten Parlamentarischen Ausschusses traten jedoch nicht sofort in Kraft, da Norwegen, Island und Liechtenstein auf die Notwendigkeit nationaler Verfahren gemäß Artikel 103 des EWR-Abkommens hingewiesen hatten. Die Beschlüsse des Gemischten Parlamentarischen Ausschusses können erst in Kraft treten und die Richtlinien im gesamten EWR erst Gültigkeit erlangen, wenn alle drei Länder den Abschluss ihrer nationalen Verfahren notifiziert haben.

4.1.1. Island

A. In Island angenommene legislative Maßnahmen im Bereich der ersten Säule der EU

40 Beschluss Nr. 83/1999 vom 25. Juni 1999 über die Änderung des Protokolls 37 und des Anhangs XI (Telekommunikationsdienste) des EWR-Abkommens und Beschluss Nr. 84/1999 vom 25. Juni 1999 über die Änderung des Anhangs XI (Telekommunikationsdienste) des EWR-Abkommens.

In Island wurden 1999 keine weiteren legislativen Maßnahmen eingeleitet, die spezifische Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz hatten.

B. In Island durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Island gehört nicht der Europäischen Union an, eine Angleichung von Maßnahmen im Bereich der zweiten Säule der EU ist daher nach dem EWR-Abkommen nicht relevant. Weiterhin gleicht Island nur solche Maßnahmen im Bereich der dritten Säule der EU an, die als Bestandteil des EWR-Abkommens anerkannt wurden. 1999 gab es in Island keine Änderungen im Datenschutz und im Schutz der Privatsphäre im Bereich der dritten Säule der EU.

C. Wichtige Rechtsprechung (nationale Gerichte)

1999 berührten in Island nur sehr wenige Rechtsfälle Themen, die mit dem Schutz der Privatsphäre und dem Datenschutz im Zusammenhang standen, und keinem dieser Fälle kann eine grenzübergreifende Dimension zuerkannt werden. In einem der Fälle, die den Schutz der Privatsphäre berührten, verkündete der Oberste Gerichtshof von Island am 25. Februar 1999 seine Entscheidung (Rechtssache Nr. 252/1998). In der Entscheidung wurde bekräftigt, dass die Veröffentlichung von Informationen über Privatangelegenheiten eines Patienten in Buchform eine strafbare Handlung gemäß Abschnitt 230 des Strafgesetzbuches darstellt.

D. Spezifische Themen

Keine.

E. Website

www.personuvernd.is

4.1.2. Norwegen

A. In Norwegen angenommene legislative Maßnahmen im Bereich der ersten Säule der EU

Die Richtlinie 95/46/EG wurde noch nicht in eine nationale Rechtsvorschrift umgesetzt. Das Ministerium erarbeitet derzeit einen Gesetzentwurf zur Vorlage im Parlament.

Die Richtlinie 97/66/EG ist zum Teil im Telekommunikationsgesetz von 1995 umgesetzt, allerdings nicht die Bestimmungen bezüglich Datenschutz und Schutz der Privatsphäre. Die Datenschutzbehörde erarbeitet derzeit eine Vorschrift für den Bereich der Telekommunikation. Ziel dieser Maßnahme ist es, die Bestimmungen der Richtlinie bezüglich Datenschutz und Schutz der Privatsphäre umzusetzen.

Sonstige Rechtsvorschriften zum Datenschutz im Bereich der ersten Säule der EU, die 1999 erlassen wurden

Das Gesetz über das Schengen-Informationssystem (SIS) wurde 1999 im Parlament angenommen. Das Gesetz regelt die Verarbeitung personenbezogener Daten im SIS.

Darüber hinaus wurden vom Parlament keine weiteren Rechtsvorschriften mit wesentlichen Auswirkungen auf den Datenschutz und den Schutz der Privatsphäre verabschiedet.

B. In Norwegen durchgeführte Änderungen im Bereich der zweiten und dritten Säule der EU

Sonstige Datenschutz-Rechtsvorschriften 1999 im Bereich der zweiten und dritten Säule der EU

Das oben erwähnte Schengen-Informationssystem ist auch in der dritten Säule der EU enthalten. Das Gesetz über das Schengen-Informationssystem enthält auch Vorschriften zu Fragen des Datenschutzes im Bereich der dritten Säule.

Weitere Rechtsvorschriften mit wesentlichen Auswirkungen auf den Datenschutz und den Schutz der Privatsphäre wurden vom Parlament nicht verabschiedet.

C. Wichtige Rechtsprechung (nationale Gerichte)

1999 wurden Fälle zu Fragen des Datenschutzes vorwiegend von der Datenschutzbehörde entschieden, als Berufungsinstanz fungiert hierbei das Justizministerium. Die 1999 behandelten Fälle betrafen zumeist die Frage, ob für die Verarbeitung personenbezogener Daten die Zustimmung der Betroffenen benötigt wird und wenn ja, in welcher Form diese Zustimmung erteilt werden soll. Die wichtigsten Fälle:

- Staatliche Straßenverwaltungsbehörde – Die Datenschutzbehörde untersagte die Übermittlung von Daten über das Rauchverhalten von Mitarbeitern durch den Gesundheitsdienst der Behörde an eine Klinik zu Forschungszwecken ohne vorherige aktive Zustimmung der Betroffenen. Der Fall wurde an das Justizministerium als Berufungsinstanz verwiesen, das die Übermittlung unter Vermutung der Zustimmung gestattete.

- American Express – Die Datenschutzbehörde entschied, dass für die Übermittlung von Transaktionsdaten von American Express an deren Kooperationspartner die aktive Zustimmung des Betroffenen erforderlich ist. Das Justizministerium bestätigte diese Entscheidung.

- Telenor Media AS – Die Datenschutzbehörde entschied, dass für die Veröffentlichung von Verzeichnisdaten im Internet die aktive Zustimmung der Betroffenen erforderlich ist. Das Justizministerium bestätigte diese Entscheidung.

Die Entscheidungen wurden unter Anwendung des norwegischen Datenschutzgesetzes von 1978 getroffen.

D. Spezifische Themen

Ein bedeutender Fall, der 1999 vor dem Obersten Gerichtshof verhandelt wurde, betraf den Zugang der Polizeibehörde zu IP-Nummerndaten über die Kunden des Telekommunikationsunternehmens Telenor.

Dabei ging es um die Frage, ob die Polizeibehörde für die Einsichtnahme dieser Daten eine Beschlagnahmeverfügung braucht. Der Oberste Gerichtshof entschied, dass in diesem speziellen Fall keine Beschlagnahmeverfügung benötigt wird.

Die Entscheidung wurde unter Anwendung des Telekommunikationsgesetzes von 1995 getroffen.

E. Website

Die Website hat folgende Adresse: www.datatilsynet.no. Sie enthält u. a. grundlegende Informationen in englischer Sprache sowie die englische Übersetzung der geltenden Datenschutz-Rechtsvorschriften.

4.2. Beitrittsländer

Die intensivierte Heranführungsstrategie zielt bei allen Beitrittsländern darauf ab, die Integration des gemeinschaftlichen Besitzstandes zu ermöglichen. In diesem Sinne liegt der Schwerpunkt zum einen auf der Annahme von Rechtsvorschriften und zum anderen auf der Schaffung der Verwaltungsstrukturen - beispielsweise unabhängige Kontrollbehörden -, die für die wirksame Umsetzung des gemeinschaftlichen Besitzstandes erforderlich sind.

Die meisten Beitrittsländer haben bereits gesetzgeberische Vorhaben auf den Weg gebracht, um ihre Datenschutzgesetze entweder durch Annahme neuer Datenschutzgesetze oder durch Änderungen der bestehenden Gesetzestexte mit den Richtlinien der Gemeinschaft in Übereinstimmung zu bringen. Slowenien nahm am 8. Juli 1999 das Gesetz über den Schutz personenbezogener Daten an. In der Slowakei wurde am 6. Oktober 1999 die Kontrollstelle für den Schutz personenbezogener Daten eingerichtet. Am 21. April 1999 unterzeichnete Polen das Übereinkommen SEV Nr. 108 des Europarates zum des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

4.3. Vereinigte Staaten von Amerika

„Sicherer Hafen“ (ausführliche Angaben hierzu siehe Abschnitt 2.3.1.1)

4.4. Andere Drittländer

4.4.1. Australien

Die Kommission hält die Datenschutzgruppe über die Entwicklungen in Australien ständig auf dem Laufenden. In den ersten Monaten des Jahres 1999 leisteten die Kommissionsdienststellen mit ihren Stellungnahmen einen Beitrag zu den Grundsätzen über die faire Behandlung personenbezogener Daten (National Principles for the Fair Handling of Personal Information, NPFHPI), die vom australischen Beauftragten für den Schutz der Privatsphäre herausgegeben wurden. Die Datenschutzgruppe erhielt eine Kopie der Stellungnahmen.

Auf der 15. Sitzung der Datenschutzgruppe am 30. März 1999 setzte die Kommission die Gruppe von einem Treffen mit dem stellvertretenden Generalstaatsanwalt, Norman Reaburn, am 3. März 1999 in Kenntnis, dessen Dienststelle einen Entwurf für Rechtsvorschriften für den privaten Sektor ausarbeitet.

Im August veröffentlichte die australische Regierung ein Informationspapier zu den Gesetzentwurf, der die Initiativen zur Selbstkontrolle für den privaten Sektor ergänzen soll, und forderte die Öffentlichkeit zur Stellungnahme auf. Die Kommissionsdienststellen leisteten hierzu einen informellen Beitrag, eine Kopie ihrer Stellungnahmen übermittelten sie der Datenschutzgruppe.

Am 16. Dezember 1999 kündigte die australische Bundesregierung gesetzgeberische Vorhaben zur Stärkung und Unterstützung der Selbstregulierung an. Die Gesetzentwürfe beruhen auf den nationalen Grundsätzen über die faire Behandlung personenbezogener Daten (NPFHPI) des australischen Beauftragten für den Schutz der Privatsphäre. Diese Grundsätze beinhalten sowohl spezifische Kodexvereinbarungen als auch Standardvorschriften für Fälle, die nicht von den Kodizes abgedeckt werden. Dadurch würde ein einheitlicher Mindeststandard in ganz Australien gewährleistet. Die Kodizes müssten vom australischen Beauftragten für den Schutz der Privatsphäre genehmigt werden.

4.4.2. Kanada

Kanada verabschiedet derzeit das Gesetz über den Schutz personenbezogener Daten und elektronischer Dokumente (Personal Information Protection and Electronic Documents Act). Der Gesetzentwurf sichert den Bürgern das Recht auf den Schutz personenbezogener Daten zu, die im Rahmen kommerzieller Tätigkeiten gesammelt, verwendet oder offengelegt werden, und legt die Grundsätze für die Verarbeitung solcher Daten fest. Außerdem sieht es vor, dass Beschwerden vom Beauftragten für den Schutz der Privatsphäre entgegengenommen und bearbeitet und im Bedarfsfall an das Bundesgericht weitergeleitet werden. Am 16. Februar 1999 leiteten die Kommissionsdienststellen ihre Stellungnahme an Industry Canada mit Kopie an die Datenschutzgruppe weiter.

4.4.3. Japan

Die Kommissionsdienststellen nehmen seit 1998 an einem hochrangigen Dialog mit Vertretern des japanischen Handels- und Industrieministeriums über die Leitlinien für den Schutz von in Computersystemen verarbeiteten personenbezogenen Daten in der Privatwirtschaft teil. Im März, Juli und September 1999 fanden Treffen statt. Die Datenschutzgruppe wurde vom Fortgang der Gespräche in Kenntnis gesetzt.

4.4.4. Ungarn

Siehe Abschnitt 2.3.1.2.

4.4.5. Schweiz

Siehe Abschnitt 2.3.1.3.

5. SONSTIGE ENTWICKLUNGEN AUF INTERNATIONALER EBENE

5.1. Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

Konferenz über den elektronischen Geschäftsverkehr

Die OECD veranstaltete am 12./13. Oktober in Paris ein Forum zum elektronischen Geschäftsverkehr (E-Commerce). Hauptziel dieser Konferenz war die Bewertung der Fortschritte bei den drei Aktionsplänen, die auf der Ministerkonferenz in Ottawa (Oktober 1998) vereinbart worden waren; daher wurden auf dem Treffen drei Ziele verfolgt: a) Förderung und Stärkung des in Ottawa eingeleiteten breit angelegten Dialogs zwischen den Interessengruppen der digitalen Wirtschaft; b) Bestandsaufnahme der Fortschritte bei der Erfüllung der Verpflichtungen zur Umsetzung der Maßnahmen, die in den in Ottawa entwickelten Aktionsplänen beschrieben werden (in Anlehnung an die vier Kernthemen, die das Gerüst der Ministerkonferenz von Ottawa bildeten: „Vertrauensbildung", „Ausbau der Infrastruktur", „Festlegung des regulatorischen Rahmens" und „Maximierung der positive Effekte"), c) Bewertung der Prioritäten und Meinungsaustausch darüber, welche Maßnahmen im Zuge des expandierenden globalen elektronischen Marktes noch zu treffen sind. Es wurde unterstrichen, dass die Achtung der Privatsphäre die wichtigste Voraussetzung für die Stärkung des Vertrauens der Verbraucher und folglich für die Entwicklung des elektronischen Geschäftsverkehrs ist. Der Bericht des Forums ist unter folgender Adresse abrufbar:

http://www.oecd.org//dsti/sti/it/ec/act/Paris_ec/pdf/forum_report.pdf

Vertragliche Vereinbarungen für die internationale Übermittlung personenbezogener Daten

Nach einer ersten Studie von Herrn Dix (Datenschutzbeauftragter des Landes Brandenburg, Deutschland) beauftragte die OECD eine Expertin (Elisabeth Longworth aus Neuseeland) mit der Erstellung eines Berichts über die Anwendung vertraglicher Lösungen für den grenzüberschreitenden Datenverkehr; dieser Bericht wurde auf der Dezembersitzung der Arbeitsgruppe für Informationssicherheit und Privatsphäre (WPISP) erstmals erörtert. Die endgültige Fassung des Berichts wurde im Mai 2000 angenommen.

„Privacy Wizard"

Zur stärkeren Sensibilisierung der Internet-Nutzer für Datenschutzpraktiken auf den von ihnen besuchten Websites hat die OECD in Zusammenarbeit mit der Wirtschaft sowie Experten für den Schutz der Privatsphäre und Verbrauchergruppen beschlossen, auf der Grundlage der Leitlinien der OECD zum Schutz der Privatsphäre einen HTML-*Wizard* (Privacy Policy Statement Generator) zu entwickeln. Der *Wizard* erfüllt klar definierte Anforderungen und ermöglicht Webmastern die Entwicklung von Maßnahmen zum Schutz vertraulicher Daten und die Generierung einer Geheimhaltungsmitteilung, die die Besucher einer Website über die Geheimhaltungspolitik der betreffenden Organisation informiert. Dieser *Wizard*, der 2000 endgültig angenommen wurde, beinhaltet kein Kennzeichnungsverfahren, sondern stellt lediglich ein

Aufklärungsinstrument dar, das über die Datenschutzpraktiken der betreffenden Organisationen informiert.

5.2. Welthandelsorganisation (WTO)

Das Arbeitsprogramm der WTO zum elektronischen Geschäftsverkehr berücksichtigt auch den Datenschutz.

5.3. Weltorganisation für geistiges Eigentum (WIPO)

Im Zusammenhang mit der Entwicklung des Internet-Bereichsnamensystems (Internet Domain Name System) nahmen die Dienststellen der Kommission gegenüber ICANN (Internet Corporation for Assigned Numbers and Names – Zentralstelle für die Vergabe von Internet-Namen und -Adressen) Stellung zu dem neuen Registrierungsprozess für die Zuteilung von Internet-Bereichsnamen und insbesondere zu dem von ICANN erarbeiteten Mustervertrag zwischen Vergabestellen und Antragstellern, die einen Bereichsnamen der zweiten Ebene beantragen. Darüber hinaus gaben Dienststellen der Kommission auch Stellungnahmen gegenüber der WIPO zu deren Vorschlägen zum Schutz von Marken und zur Zuteilung von Bereichsnamen ab.

Dienststellen der Kommission begannen auch mit der Ausarbeitung des Entwurfs für eine Mitteilung zu dem gesamten Themenkomplex unter Einbeziehung des Datenschutzes sowie eines Vorschlags für einen Internet-Bereichsnamen oberster Stufe (Top-Level Domain) für die EU[41].

6. ANHÄNGE

I Mitglieder der Datenschutzgruppe nach Artikel 29

41 KOM(2000) 202 endg.; angenommen am 11. April 2000.

II Liste der von der Datenschutzgruppe nach Artikel 29 bis 1999 angenommenen Dokumente

III Websites der nationalen Datenschutzbehörden

Geschehen zu Brüssel am 17. Mai 2001

Für die Datenschutzgruppe

Der Vorsitzende

Stefano RODOTA

ANHANG I

6.1. Mitglieder der Datenschutzgruppe nach Artikel 29

ÖSTERREICH	**BELGIEN**
Waltraut KOTSCHY Vertreterin Bundeskanzleramt Österreichische Datenschutzkommission Ballhausplatz, 1 A - 1014 WIEN Tel.43/1/531 15 26 79	Paul THOMAS Vertreter Ministère de la Justice Commission de la protection de la vie privée Boulevard de Waterloo, 115 B - 1000 BRUXELLES Tel.32/2/542 72 00
DÄNEMARK	**FINNLAND**
Henrik WAABEN Vertreter Registertilsynet Christians Brygge, 28 – 4 DK - 1559 KOEBENHAVN V Tel.45/33/14 38 44	Reijo AARNIO Vertreter Ministry of Justice Office of the Data Protection Ombudsman P.O. Box 315 FIN - 00181 HELSINKI Tel.358/9/18251
FRANKREICH	**DEUTSCHLAND**
Michel GENTOT Com. Nat. de l'Informat. et des Libertés Rue Saint Guillaume, 21 F - 75340 PARIS CEDEX 7 Tel.33/1/53 73 22 22	Dr. Joachim JACOB Vertreter Der Bundesbeauftragte für den Datenschutz Friedrich-Ebert-Str. 1 D – 53173 BONN (Bad Godesberg) Tel.49/228/819 95 0

GRIECHENLAND	**IRLAND**
Constantin DAFERMOS Vertreter Ministry of Justice 8 Omirou Street 10654 Athens, Greece Tel.301/33 52 600-10	Joe MEADE Vertreter Data Protection Commissioner Irish Life Centre, Block 4 Talbot Street, 40 IRL - DUBLIN 1 Tel.353/1/874 85 44
ITALIEN	**LUXEMBURG**
Prof. Stefano RODOTA Vorsitzender Garante per la protezione dei dati personali Piazza di Monte Citorio, 121 I - 00186 ROMA Tel.39/06/69 67 77 03	René FABER Vertreter Commission à la Protection des Données Nominatives Ministère de la Justice Boulevard Royal , 15 L - 2934 LUXEMBOURG Tel.352/487 180
NIEDERLANDE	**PORTUGAL**
Peter HUSTINX Vertreter Registratiekamer Prins Clauslaan 20 Postbus 93374 NL - 2509 AJ's GRAVENHAGE Tel.31/70/381 13 00	João SIMOES DE ALMEIDA Vertreter CNPD Rua de S. Bento, 148 P – 1 200-821 Lisboa Codex Tel.351/21/392 84 00

SPANIEN	**SCHWEDEN**
Juan Manuel FERNÁNDEZ LÓPEZ Vertreter Agencia de Protección de Datos C/ Sagasta, 22 E - 28004 MADRID Tel.34/91/399 62 20	Ulf WIDEBÄCK Vertreter Datainspecktionen Fleminggatan, 14 9th Floor Box 8114 S - 104 20 STOCKHOLM Tel.46/8/657 61 00
VEREINIGTES KÖNIGREICH	
Elizabeth FRANCE Vertreterin Executive Department The Office of the Information Commissioner Water Lane Wycliffe House UK - WILMSLOW – CHESHIRE SK9 5AF Tel.44/1625/54 57 00 (Zentrale)	
ISLAND	**NORWEGEN**
Sigrún JÓHANNESDÓTTIR Beobachterin Ministry of Justice Data Protection Commission Arnarhvoll IS - 150 REYKJAVIK Tel.354/560 90 10	Georg APENES Beobachter Datatilsynet The Data Inspectorate P.B. 8177 Dep N – 0034 OSLO Tel.47/22/39 69 00

ANHANG II

6.2. Liste der von der Datenschutzgruppe nach Artikel 29 bis 1999 angenommenen Dokumente

WP 15 (5092/98): Stellungnahme 1/99 zum Stand des Datenschutzes in den Vereinigten Staaten und zu den derzeitigen Verhandlungen zwischen der Europäischen Kommission und der amerikanischen Regierung. Angenommen am 26. Januar 1999

WP 16 (5013/99): Arbeitsunterlage: Die Verarbeitung personenbezogener Daten im Internet. Angenommen am 23. Februar 1999

WP 17 (5093/98): Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware. Angenommen am 23. Februar 1999

WP 18 (5005/99): Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs. Angenommen am 3. Mai 1999

WP 19 (5047/99): Stellungnahme 2/99 zur Angemessenheit der „Internationalen Grundsätze des sicheren Hafens", ausgegeben vom Wirtschaftsministerium der USA am 19. April 1999. Angenommen am 3. Mai 1999

WP 20 (5055/99): Stellungnahme 3/99 betreffend die Informationen des öffentlichen Sektors und Schutz personenbezogener Daten. Beitrag zu der mit dem Grünbuch der Europäischen Kommission unter dem Titel „Informationen des öffentlichen Sektors – eine Schlüsselressource für Europa" begonnenen Anhörung, KOM (1998) 585. Angenommen 3. Mai 1999

WP 21 (5066/99): Stellungnahme 4/99 zu den häufig gestellten Fragen (Frequently asked Questions), vorgelegt vom US-Handelsministerium im Zusammenhang mit den vorgeschlagenen „Grundsätzen des sicheren Hafens". Angenommen am 7. Juni 1999

WP 22 (5054/99): Stellungnahme 5/99 zum Schutzniveau personenbezogener Daten in der Schweiz. Angenommen am 7. Juni 1999

WP 23 (5075/99): Arbeitsunterlage zum gegenwärtigen Stand der Diskussion zwischen der Europäischen Kommission und der Regierung der Vereinigten Staaten über die „Internationalen Grundsätze des sicheren Hafens". Angenommen am 7. Juli 1999

WP 24 (5070/99) : Stellungnahme 6/99 zum Schutzniveau personenbezogener Daten in Unganr. Angenommen am 7. September 1999

WP 25 (5085/99): Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke. Angenommen am 7. September 1999

WP 26 (5143/99): Empfehlung 4/99 über die Aufnahme des Grundrechts auf Datenschutz in den Europäischen Grundrechtskatalog. Angenommen am 7. September 1999

WP 27 (5146/99): Stellungnahme 7/99 zum Datenschutzniveau, das die Grundsätze des sicheren Hafens in ihrer veröffentlichten Form, die dazu gehörigen häufig gestellten Fragen (FAQ) und andere vom US-Handelsministerium am 15./16. November 1999 veröffentlichte Dokumente gewährleisten. Angenommen am 3. Dezember 1999

ANHANG III

6.3. Websites der nationalen Datenschutzbehörden

BELGIEN

http://www.privacy.fgov.be/inhoud.html

DÄNEMARK

Keine eigene Website. E-Mail-Adresse: dt@datatilsynet.dk

DEUTSCHLAND

http://www.bfd.bund.de/aktuelles/index.html

FINNLAND

http://www.tietosuoja.fi/

FRANKREICH

http://www.cnil.fr/images/home/home_r08_c02bis.gif

GRIECHENLAND

http://www.dpa.gr/

IRLAND

http://www.dataprivacy.ie/

ITALIEN

http://astra.garanteprivacy.it/garante/HomePageNs

LUXEMBURG

Keine eigene Website.

NIEDERLANDE

http://www.registratiekamer.nl/

ÖSTERREICH

http://www.bka.gv.at/datenschutz/dvrnr.htm#wem

PORTUGAL

http://www.cnpd.pt/bin/principal.htm

SCHWEDEN

http://www.datainspektionen.se/start/start.shtml

SPANIEN

https://www.agenciaprotecciondatos.org/

VEREINIGTES KÖNIGREICH

http://www.dataprotection.gov.uk/

BEOBACHTER

ISLAND

http://www.personuvernd.is/tolvunefnd.nsf/pages/index.html

NORWEGEN

http://www.datatilsynet.no/inngang/inngmain.html